McAfee™
Together is power.

Revision A

Endpoint Intelligence Agent

(3.2.0 Product Guide)

COPYRIGHT

TRADEMARK ATTRIBUTIONS

LICENSE INFORMATION

License Agreement

Contents

Preface

Contents

About this guide

This information describes the guide's target audience, the typographical conventions and icons used in this guide, and how the guide is organized.

Audience

McAfee documentation is carefully researched and written for the target audience.

The information in this guide is intended primarily for:

Conventions

This guide uses these typographical conventions and icons.

Italic	Title of a book, chapter, or topic; a new term; emphasis
Bold	Text that is emphasized
`Monospace`	Commands and other text that the user types; a code sample; a displayed message
Narrow Bold	Words from the product interface like options, menus, buttons, and dialog boxes
Hypertext blue	A link to a topic or to an external website
ℹ	**Note:** Extra information to emphasize a point, remind the reader of something, or provide an alternative method
💡	**Tip:** Best practice information
❗	**Caution:** Important advice to protect your computer system, software installation, network, business, or data
⚠	**Warning:** Critical advice to prevent bodily harm when using a hardware product

Find product documentation

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

Task

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

1 Introduction

Most enterprises today face a challenge in understanding executables running on the endpoints in their networks. With malware increasing at a rampant pace, it has become imperative for networks to understand executables sending traffic on the network. Enterprises want a means to keep a check on their endpoints, get user and executable information, and be able to determine that their endpoints and network are safe and secure.

As an administrator, you want to look out for executables that can exploit your endpoints. In addition, you want to establish good and bad executables in the network and track any change in network behavior. When a network issue happens, one of the analyzing factors can be to check the endpoints and track executables that initiated network connections.

Contents

Endpoint Intelligence Agent

McAfee® Endpoint Intelligence Agent (McAfee EIA) is an endpoint solution that resides on an endpoint to provide per-connection information like user identity and hash values about executables that initiate network connection to supported network devices. This information is sent to network devices and used for policies, auditing, decision-making, and classifying executables.

Endpoint Intelligence Agent is managed by McAfee® ePolicy Orchestrator® (McAfee ePO) and can be deployed to multiple endpoints.

McAfee EIA supports these network devices:

- McAfee® Firewall Enterprise (Firewall Enterprise)
- McAfee® Network Threat Behavior Analysis Appliance

McAfee EIA works with enterprise point-product Windows installations on all endpoints. Consumer point-product installations are not supported.

Features

McAfee EIA has these salient features:

- **Multiple gateways** — Supports multiple gateways and can send metadata to multiple device types simultaneously.
- **Malware detection** — Capable to perform dynamic analysis and classify executables and non-executables like doc and pdfs as **Low Risk** or **Malware**.

- **User group mapping** — Fetches user details and groups mapped to a user and provides details to network devices.
- **Access protection** — Integrates with McAfee Management Service (MMS) to host the EIA services and restart EIA services if it stops. EIA also integrates with Arbitrary Access Protection (AAC) that protects directories, services, and registry entries. AAC also protects against various attacks and instances of being debugged by other processes.
- **Application back tracking** — McAfee EIA includes service and script back tracking. Service back tracking identifies services behind generic processes and script back tracking identifies the script that initiates traffic.

Benefits

These are the advantages of McAfee EIA:

- **Network visibility** — Provides visibility into the executables that initiated network traffic in an enterprise network
- **User information** — Gives user information like user name, user type, domain details, and list of groups mapped to a user
- **Executable details** — Provides characteristics of an executable such as the version, the endpoints where it was executed, the number of connections made, the applications invoked, and the events associated with it
- **Data file details** — Provides details of detection like MD5 of the process, full path of the process, malware detection name, summary of artifacts, and attribute details like document MD5 and filename
- **Executable file reputation** — Provides reputation for each executable using its own malware indicators and heuristics
- **Baseline profile** — Enables detection of unknown executables in the network that the administrator can classify as whitelisted or blacklisted, thereby creating an intelligent baseline for the network

Terminologies

These terms that are used throughout this guide.

Network device

McAfee EIA can communicate with multiple network devices simultaneously like McAfee Firewall Enterprise and McAfee Network Threat Behavior Analysis (NTBA).

Metadata

McAfee EIA sends connection information, called metadata, for every outgoing connection. When McAfee EIA is installed on an endpoint, it monitors IPv4 traffic based on TCP and UDP protocols. When a connection attempt is made, McAfee EIA sends metadata information for that connection to Firewall Enterprise or to the NTBA appliance over an encrypted channel. The network devices process metadata and make it available at policy decision points before the connection request packet is received.

Many network environments contain computers or servers that have multiple users logged on at the same time. The user information in the metadata allows the supported network devices to determine what users are associated with what connections, even if those connections are coming from the same IP address.

Metadata includes executable information like user and connection details, heuristics, and reputation for an executable, which can be used by network devices. Firewall Enterprise uses metadata for auditing, policies, and advanced malware detection, and NTBA appliance uses metadata for enhanced malware detection.

The metadata consists of the following information:

- Mandatory information:
  - MD5 hash value
  - The executable file name on the disk (full path) and hash of an executable that generated the connection
  - SID, user name, user type (system users, local users, and domain users) and domain
  - 5-tuple information such as source IP address, destination IP address, source port, destination port, and protocol
- Optional information is executable file reputation that includes:
  - Confidence level
  - Malware name
  - Associated executable path
  - Associated executable MD5
  - Service name and path
  - Script name and MD5
  - Heuristic bitmap
  - Evidence string
  - File name (same as in **File Properties** or file name on the system)
  - File version
  - Signer name
  - SHA1 of the signer
  - Product name

The optional information is sent in metadata only when reputation is available.

User group data

User information like user name and groups mapped to a user are sent over a DTLS channel to network devices.

Confidence level

McAfee EIA uses a heuristic-based approach and computes a risk level, called confidence level, for each executable initiating traffic in the network.

The confidence levels associated with an executable are specified in numeric values. Each of these values corresponds to the following confidence levels:

- 0 - Unknown
- 2-4 - Low Risk
- 5-6 - Malware

Executable file reputation

When network traffic is generated, the reputation of an executable file is critical for the network device to configure response actions to prevent malicious files on the network.

McAfee EIA analyzes different characteristics of executable files to determine an endpoint application's trust. McAfee EIA uses in-built heuristics and malware indicators to compute reputation for an executable.

The executable file reputation is sent as part of the metadata that allows network devices to calculate the overall confidence level for an executable file connection. This enables devices to configure response actions when malicious and unknown executables are detected on the network.

Computing executable file reputation using McAfee EIA enables you to:

- Monitor executable files sending traffic from endpoints.
- Detect new and unknown executable files in the network.
- Determine confidence level for new and unknown executable files.
- Create whitelists and blacklists for executable files for your networks.

Endpoint Baseline Generator

The Endpoint Baseline Generator tool is used to create a standard for endpoints. The tool scans a system, calculates the reputation for all the executable files (excluding dll files) on the system, and generates the baseline profile (an .xml file) with the reputation details of each executable.

The baseline profile is uploaded from a clean system to NTBA and Firewall Enterprise, which use the baseline profile to evaluate the confidence level of the executables on the network. This helps to secure network connections made by similar endpoints, enabling McAfee EIA to report any deviations from that standard.

ⓘ Endpoint Baseline Generator can scan external hard drives with fixed media such as a hard disk or a USB drive.

Baseline profile

The Endpoint Baseline Generator generates a baseline profile that classifies executable files based on confidence levels. This profile acts as a reputation source for network devices to define a whitelist or blacklist database and monitor endpoint executable files.

The baseline profile .xml file provides information like MD5 hash value, confidence level, and heuristic bitmap. This information provides reputation to the network device to define a classification list consisting of the whitelisted, blacklisted, or unclassified (new or unknown executables) entries and monitor endpoint executables. The confidence levels can't be modified and are imported as part of the baseline profile.

You can edit the list of MD5 hashes generated, through import and export operations supported on Firewall Enterprise and NTBA. For more information, see *McAfee NTBA Administration Guide* and *McAfee Firewall Enterprise Product Guide.*

Log Collector tool

Log Collector is an internal to McAfee EIA tool that collect logs in the McAfee EIA installation folder. An administrator can execute LogCollector.exe on an endpoint to get diagnostic information such as logs and registry values. These details can be used to debug McAfee EIA issues.

VSCore

McAfee EIA uses VSCore service to intercept and hold a connection until the metadata related to that connection is sent to the supported network device. McAfee EIA 2.6.2 uses VSCore 15.6.0.

How McAfee EIA works

These are the high-level steps of how McAfee EIA sends executable information to the network devices.

Establish a DTLS connection

If the DTLS channel doesn't exist when the first SYN packet comes to McAfee EIA, then in:

- **Static mode** — Based on the preconfigured gateway details, a DTLS channel is created for that gateway. Metadata for the packet is sent to the network device before the SYN packet.
- **Dynamic mode** — When the gateway details are not preconfigured, the first SYN packet is sent to the network device. The network device sends a custom ICMP message to McAfee EIA. From the ICMP message, McAfee EIA gets the gateway details and establishes a DTLS connection with the network device. When a SYN is re-sent, the metadata is sent to the network device before forwarding the SYN packet.

Perform a two-way handshake

Endpoint Intelligence Agent uses heartbeat messages to detect the status of the DTLS connection. To save bandwidth, the heartbeat is sent as part of metadata, but not as a separate message. If Endpoint Intelligence Agent does not receive a response, even after sending three heartbeat messages, it declares the peer as dead.

Push configuration to endpoints

McAfee® Endpoint Intelligence Manager (McAfee EIM) configures certificates and policies for authentication of an endpoint. The Endpoint Intelligence Manager pushes certificates to endpoints to establish DTLS connection.

Send metadata to supported network devices

Endpoint Intelligence Agent leverages the McAfee Global Threat Intelligence (McAfee GTI) capability to provide file reputation information. Endpoint Intelligence Agent uses NTBA as a McAfee GTI proxy. It forwards the McAfee GTI queries to the network device and the network device talks to the McAfee GTI server and caches the response. It also forwards the response to McAfee EIA.

ⓘ McAfee EIA provides metadata for TCP and UDP connections over IPv4.

McAfee EIA sends metadata for an established connection to supported network devices over an encrypted channel. McAfee EIA receives notification whenever an executable initiates traffic. It uses MD5 of an executable to look up and check if the reputation is already available in the cache. If available, it sends the reputation information along with network and user information in the metadata. If the reputation is not available, it computes reputation and updates the cache, and sends a separate reputation message to the network devices.

McAfee EIA uses dynamic analysis capabilities for detection of malicious files and their malware status. It provides details of detection like MD5 of the process, full path of the process, malware detection name, summary of artifacts, and attribute details like document MD5 and filename. The artifacts are sent over a TLS connection to the network devices.

EIA also sends user group mapping information like user and list of groups mapped to users over the DTLS channel. This information is sent every 6 hours. Information about universal groups and global groups is sent, but details of local groups and domain local group details are not sent.

[NTBA only] In parallel, McAfee EIA uses the public key of the executable signer to look up the cache to compute trust information. If available, the trust details and certificate expiry time are sent to NTBA.

The network devices receive the executable file reputation and malware details as part of the metadata. This enables the network devices to classify executables as **Low Risk** or **Malware** and configure response actions such as raising alerts or blocking the files, when malicious and unknown executables are detected on the network. This can facilitate clean traffic on the network and prevent malware intrusions.

Communicating with network devices

Endpoint Intelligence Agent can communicate with two supported network devices, Firewall Enterprise and NTBA. At any given time, McAfee EIA can send metadata to multiple network devices of the same type, provided they are handling traffic to different destination subnets.

Metadata corresponding to a specific connection is sent only to one network device of a particular type. For example, if two firewalls are configured, EIA can send metadata only to one firewall. If there are multiple devices of different types, then metadata corresponding to a specific connection is sent to all the devices. For example, if a firewall and NTBA are configured, metadata is sent to both the devices.

For backward compatibility, network devices configured with EIA 2.3.x or 2.4.2 are also supported.

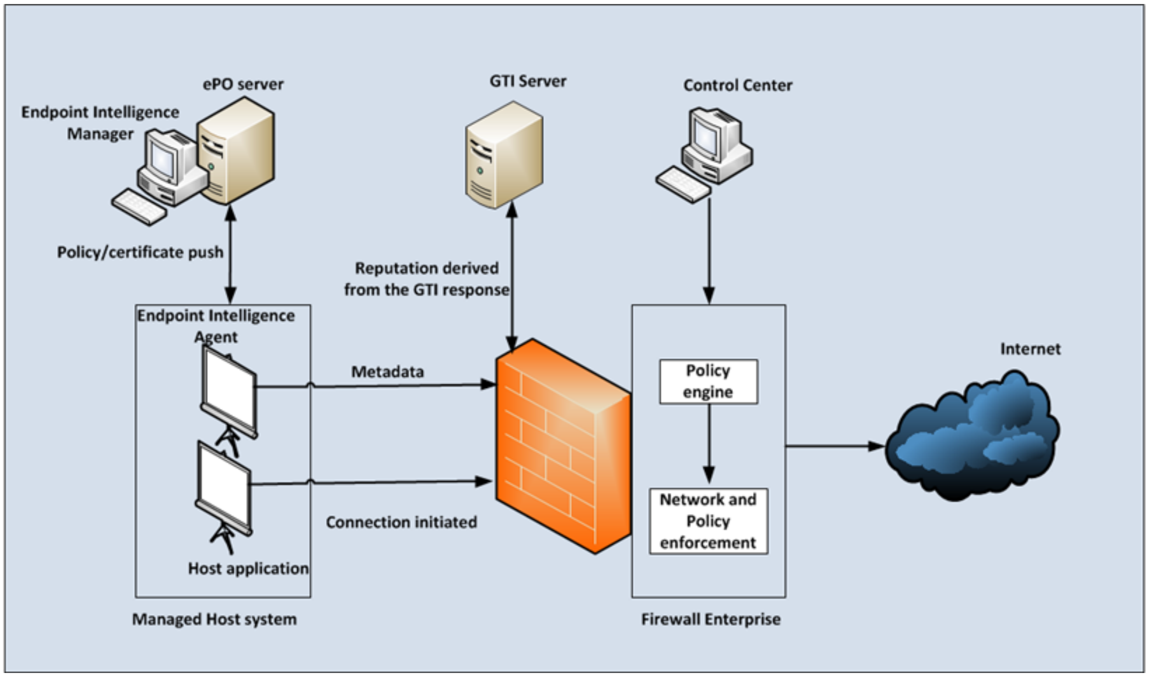


Figure 1-1 Integrating Endpoint Intelligence Agent with Firewall Enterprise

1 ePolicy Orchestrator installs and configures the Endpoint Intelligence Agent settings on managed endpoints.

2 Firewall Enterprise is configured for Endpoint Intelligence Agent using the Admin Console. If your firewall is managed by Control Center, the firewall is configured on the Control Center Management Server.

3 Endpoint Intelligence Agent sends metadata to Firewall Enterprise. User information and other metadata is used for auditing and advanced malware detection.

For more information to configure and view the reputation data, see the *McAfee Firewall Enterprise Product Guide*.

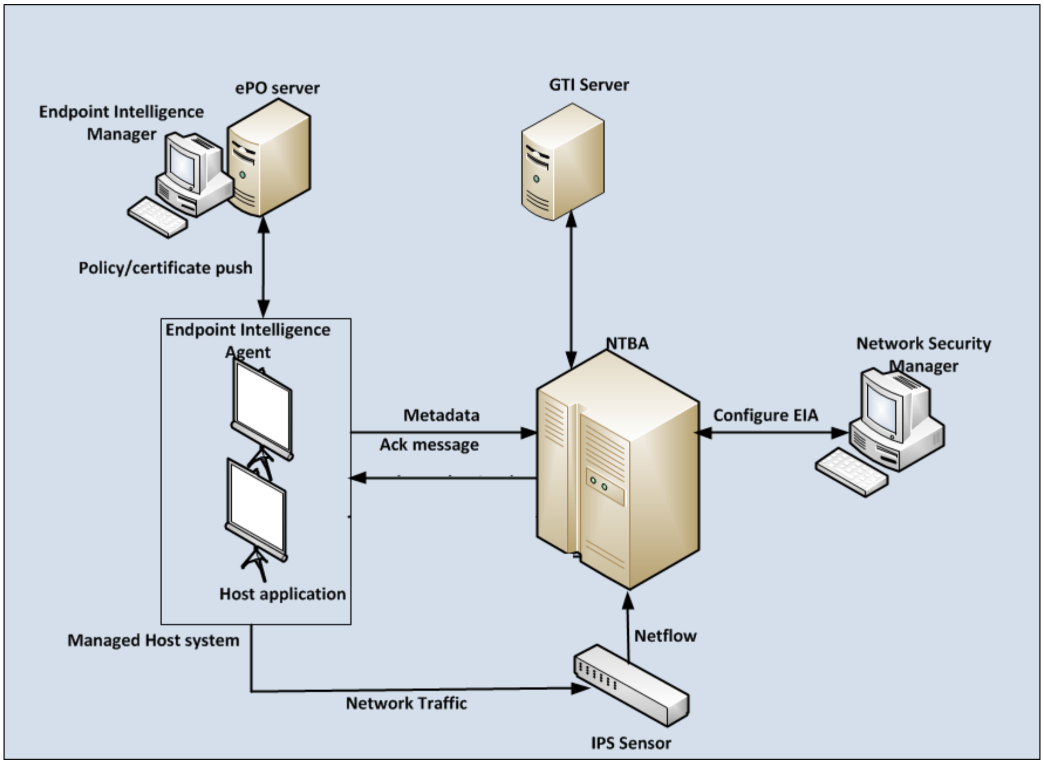


Figure 1-2 Integrating Endpoint Intelligence Agent with NTBA

1. ePolicy Orchestrator installs and configures the Endpoint Intelligence Agent settings on managed endpoints.
2. McAfee Network Security Manager (Manager) is used to configure McAfee EIA to establish trusted connections between the NTBA appliance and the managed endpoints.
3. The NTBA appliance uses the configuration provided by the Manager and the ePolicy Orchestrator server to connect and authenticate with McAfee EIA endpoints.
4. Endpoint Intelligence Agent sends metadata to the NTBA appliance. The NTBA uses the metadata for effective malware detection on the network.

When the McAfee GTIcapability is enabled on the NTBA appliance, McAfee EIA sends a McAfee GTI request that consists MD5. NTBA communicates with McAfee GTI server and sends a response to McAfee EIA consisting of MD5 and the corresponding McAfee GTI value. Based on this response (McAfee GTI value) the confidence score in the reputation cache is refreshed.

For more information on configuring and managing McAfee EIA with NTBA, see the *McAfee NTBA Administration Guide*.

Determining your discovery method

Endpoints running Endpoint Intelligence Agents have two ways to determine the gateway to send connection metadata to: *static* and *dynamic*.

- **Static** — If the connection has a destination IP address for Firewall Enterprise or source IP address for NTBA that matches a route entry, McAfee EIA sends metadata to the specified gateway IP address for that route.
- **Dynamic** — McAfee EIA receives ICMP Destination Unreachable (DU) packets from Firewall Enterprise. McAfee EIA parses these packets and updates the routing table with the new destination addresses for which metadata has to be sent.

> For fast recovery, network devices send an ICMP reset packet to EIA, and EIA establishes a DTLS connection immediately.

Systems running Endpoint Intelligence Agent can have a combination of static and dynamic configurations. When a connection attempt is made, Endpoint Intelligence Agent checks its route configuration using static or dynamic mode.

> Firewall Enterprise and NTBA both use static and dynamic modes.

Integrating with other McAfee products

McAfee EIA supports these network devices and seamlessly integrates with other McAfee products.

Table 1-1 McAfee EIA 3.2.0 compatibility with other McAfee products

Product	Version
McAfee® ePolicy Orchestrator® (McAfee® ePO™)	5.9.0 and later
McAfee® Agent	4.8.0 Patch 2 and later
McAfee® Firewall Enterprise	8.3.1 with latest P-patch, 8.3.2 and later
McAfee® Firewall Enterprise Control Center	5.3.1 and later
McAfee® Network Threat Behavior Analysis	9.1.3.12 and later
McAfee® Network Security Manager	9.1.7.75 and later
McAfee® Product Improvement Program (PIP)	1.2 and later
McAfee® ePO Minimum Escalations Reporting (ePO-MER)	2.5.5 and later
McAfee® Minimum Escalations Reporting (MER)	3.0 and later
McAfee® ePO Virtual Technician (ePO-MVT)	1.1.2 and later
McAfee® Virtual Technician (MVT)	7.6 and later
McAfee® Endpoint Suites Installer	3.x and later

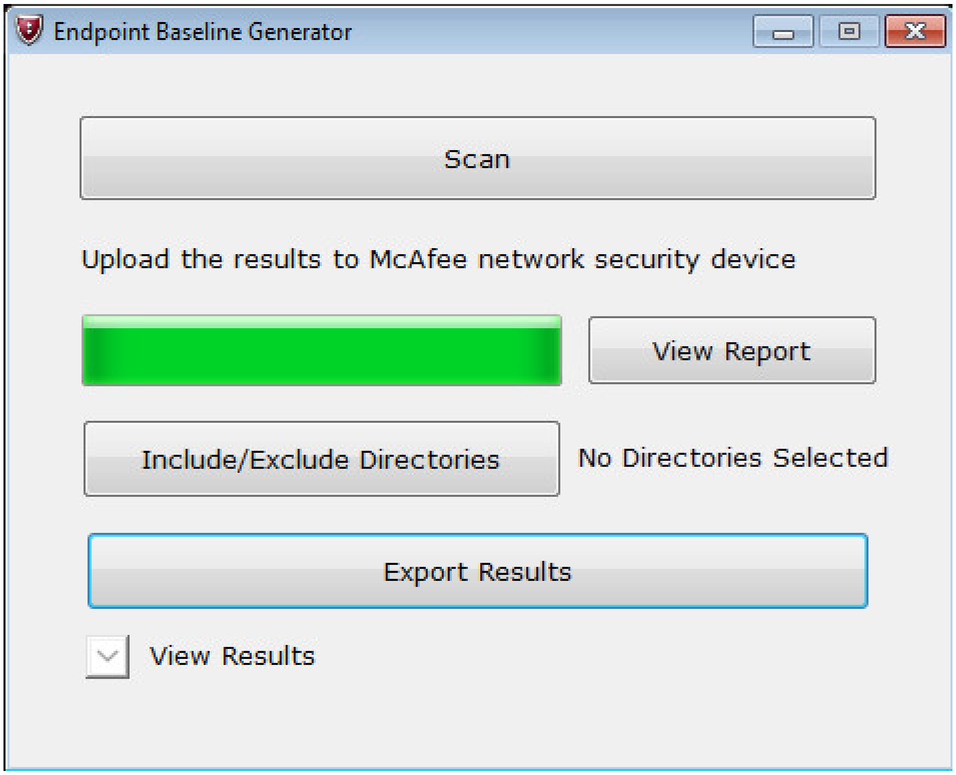
Scan endpoints in your network

Create a baseline profile for each executable in your network and use their confidence levels to whitelist or blacklist executables.

Task

1 Go to the **Endpoint Baseline Generator** tool. To scan specific directories, click **Include/Exclude Directories** and select the directories to be scanned.

2 Click **Scan**.



Upload the results to McAfee network security device

No Directories Selected

Figure 1-3 Completed scan

You can cancel the scan in the middle and still generate a valid XML file to be imported by the network device.

3 When the scan is complete, click **View Report**.

The XML report is displayed. The following is a sample of the MD5 associated with an application.

```
</SysInfo>
<MD5 value ='317cd1ce327b6520bf4ee007bcd39e61' name="bfsvc.exe" version='6.1.7601.17514'>
    <ProductName>Microsoft® Windows® Operating System</ProductName>
    <ConfidenceLevel>2</ConfidenceLevel>
    <StaticBitmap>a0aaeaaba20200000000000000000000</StaticBitmap>
    <SHA1>0fda55930034f945dc6bdfa3e6ddc0e37208bcfe</SHA1>
</MD5
```

The confidence levels can't be modified and are imported as part of the baseline profile.

4 To export and save the results in an XML format, click **Export**.

5 To view the details of the scan, click **View Results**.

2 Setting up Endpoint Intelligence Agent with ePolicy Orchestrator

Install the Endpoint Intelligence Management Extension, check in the Endpoint Intelligence Agent package, and deploy McAfee EIA to managed endpoints.

Before installing these components, make sure you have installed the McAfee Agent extension, uploaded the McAfee Agent package, and deployed McAfee Agent on managed endpoints.

Contents

System requirements

Make sure your ePolicy Orchestrator and managed systems meet these requirements.

The following are the product requirements for Endpoint Intelligence Agent 3.2.0 on McAfee ePO.

Product	Supported version
ePolicy Orchestrator server	5.9.0 and later
McAfee Agent	4.8.0 Patch 2 and later
Endpoint Intelligence Management extension	3.2.0

Firewall Enterprise ePO extension 5.3.0 or earlier versions cannot co-exist with Endpoint Intelligence Manager ePO extension.

- Endpoint Intelligence Agent runs on the following Microsoft operating systems:
  - Windows 7
  - Windows 8.1
  - Windows 10 R2 (64-bit)
  - Windows Server 2008
  - Windows Server 2008 R2 (64-bit)
  - Windows Server 2012 (64-bit)
  - Windows Server 2012 R2 (64-bit)

McAfee recommends running Endpoint Intelligence Agent on systems with at least 2 GB of RAM.

Download Endpoint Intelligence Management extension and McAfee EIA package

Download the Endpoint Intelligence Management extension and the McAfee EIA package to the ePolicy Orchestrator server.

> **Before you begin**
>
> You must have a valid grant number to download these files from the McAfee downloads site.

Task

1. In a web browser, go to www.mcafee.com/us/downloads.
2. Enter your grant number, then go to the appropriate product and version.
3. Download the eia_epo_deploy_<version>.zip file.
4. Download the eim_epo_extension_<version>.zip file.
5. [Optional] Download the eim_epo_extension_help_<version>.zip file.

Install the Endpoint Intelligence Management extension

Install the Endpoint Intelligence Management extension from your download location to your ePolicy Orchestrator server.

Task

1. In the ePolicy Orchestrator console, click on the menu icon (≡) and select **Software** | **Extensions**.
2. In the **Extensions** page, click **Install Extension**.
3. Browse to the **eim_epo_extension_<version>.zip** file.
4. Click **Open** to select the file, then click **OK** to proceed with the selection.
5. Click **OK** to install the extension.

> To complete the installation process, you don't need to restart the system. If you uninstall McAfee EIA and install any version, you must restart your system for the installed McAfee EIA version to function properly.

Upload the Endpoint Intelligence Agent package

Upload the Endpoint Intelligence Agent package to the ePolicy Orchestrator server. This package contains the files necessary to install Endpoint Intelligence Agent on managed systems.

Task

1. In the ePolicy Orchestrator console, click on the menu icon (≡) and select **Software** | **Master Repository**.
2. Click **Check In Package**. The **Check In Package** wizard appears.
3. In the **Package type** list, select **Product or Update (.ZIP)**, then browse and select the **ePO_Deploy.zip** file.

> Extract the eia_epo_deploy_<version>.zip file to get the ePO_Deploy.zip file.

4. Click **Next**.
5. Click **Save**.

The package is added to the Master Repository.

Deploy the Endpoint Intelligence Agent

You can deploy Endpoint Intelligence Agents to the managed endpoints.

Task

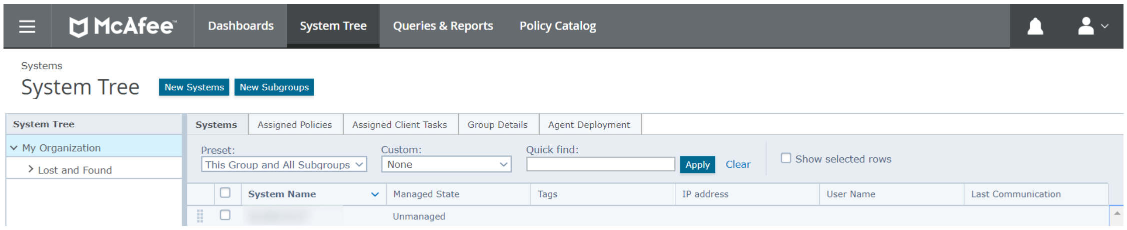
1. In the ePolicy Orchestrator console, click on the menu icon (≡) and select **Client task** | **Client Task Catalog**. The **Client Task Catalog** page opens.
2. Click **New Task**. The **New Task** window appears.
3. In the **Task Types** list, select **Product Deployment**.
4. Click **OK**. The **Client Task Catalog: New Task - McAfee Agent: Product Deployment** window appears.
5. In the **Task Name** field, enter a name for the task.
6. From the **Products and components** menu, select **Endpoint Intelligence Agent <version>**.
7. Click **Save**.
8. Run the task.
   a. Click the **System Tree** icon. The **Systems** tab appears.
   b. Select the systems to deploy Endpoint Intelligence Agent.
   c. Select **Actions** | **Agent** | **Run Client Task Now**. The **Run Client Task Now** page appears.
   d. In the **Task Type** column, select **Product Deployment**, and in the **Task Name** column, select the task you created.
   e. Click **Run Task Now**.

Enable Real-Protect RaptorClient Service

You can enable Endpoint Intelligence Agent service on the managed endpoints.

Task

1 On the ePolicy Orchestrator console, click the **System Tree** tab. The **Systems Tree** page opens.



Preset: This Group and All Subgroups

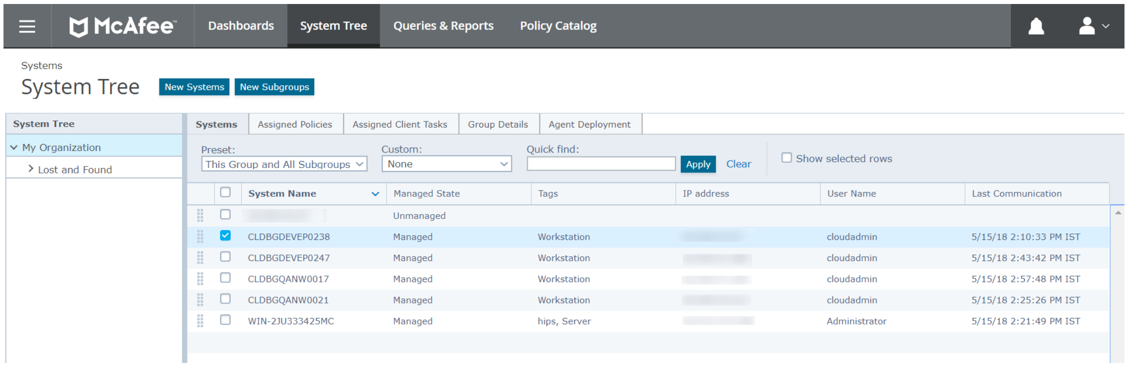
Custom: None

Quick find:

□ Show selected rows

	System Name	Managed State	Tags	IP address	User Name	Last Communication
□	[redacted]	Unmanaged				

2 Select the client machine from the **System Name** column on which you want to install the Endpoint Intelligence Agent.



Preset: This Group and All Subgroups

Custom: None

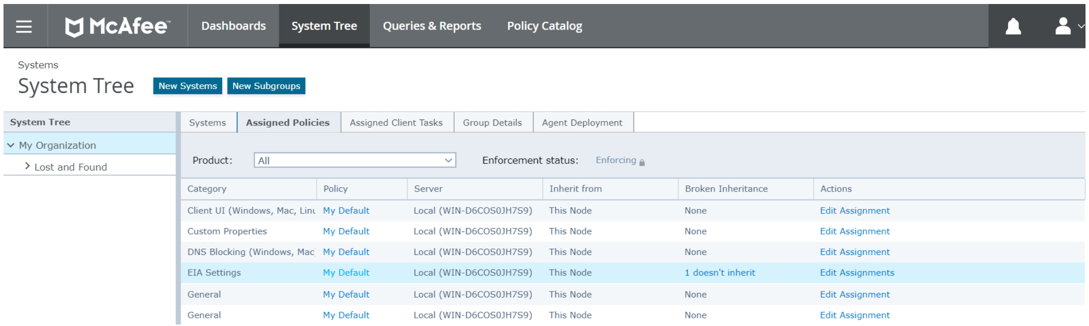
Quick find:

□ Show selected rows

	System Name	Managed State	Tags	IP address	User Name	Last Communication
□	[redacted]	Unmanaged				
☑	CLDBGDEVEP0238	Managed	Workstation	[redacted]	cloudadmin	5/15/18 2:10:33 PM IST
□	CLDBGDEVEP0247	Managed	Workstation	[redacted]	cloudadmin	5/15/18 2:43:42 PM IST
□	CLDBGQANW0017	Managed	Workstation	[redacted]	cloudadmin	5/15/18 2:57:48 PM IST
□	CLDBGQANW0021	Managed	Workstation	[redacted]	cloudadmin	5/15/18 2:25:26 PM IST
□	WIN-2JU333425MC	Managed	hips, Server	[redacted]	Administrator	5/15/18 2:21:49 PM IST

3 Click the **Assigned Policies** tab. Select the **EIA Settings**policy.

The policy information appears.

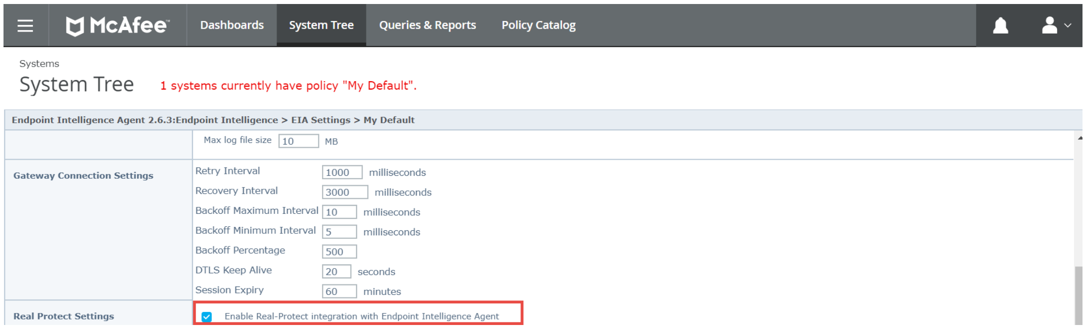


Product: All

Enforcement status: Enforcing

Category	Policy	Server	Inherit from	Broken Inheritance	Actions
Client UI (Windows, Mac, Linu	My Default	Local (WIN-D6COS0JH7S9)	This Node	None	Edit Assignment
Custom Properties	My Default	Local (WIN-D6COS0JH7S9)	This Node	None	Edit Assignment
DNS Blocking (Windows, Mac	My Default	Local (WIN-D6COS0JH7S9)	This Node	None	Edit Assignment
EIA Settings	My Default	Local (WIN-D6COS0JH7S9)	This Node	1 doesn't inherit	Edit Assignments
General	My Default	Local (WIN-D6COS0JH7S9)	This Node	None	Edit Assignment
General	My Default	Local (WIN-D6COS0JH7S9)	This Node	None	Edit Assignment

4 Select the **Enable Real-Protect integration with Endpoint Intelligence Agent** checkbox.



Systems

System Tree 1 systems currently have policy "My Default".

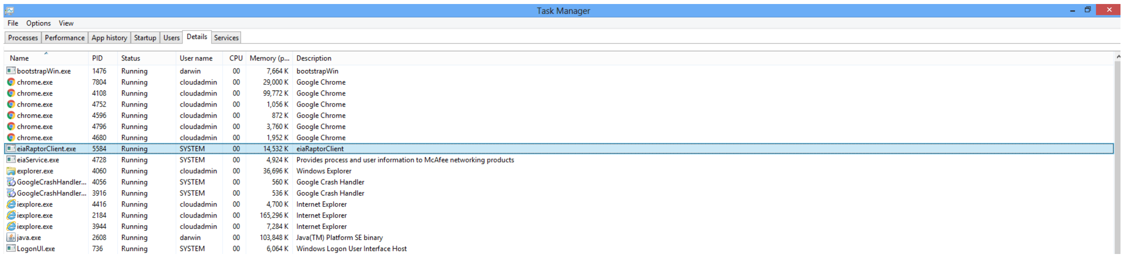
Endpoint Intelligence Agent 2.6.3:Endpoint Intelligence > EIA Settings > My Default

	Max log file size	10	MB
Gateway Connection Settings	Retry Interval	1000	milliseconds
	Recovery Interval	3000	milliseconds
	Backoff Maximum Interval	10	milliseconds
	Backoff Minimum Interval	5	milliseconds
	Backoff Percentage	500	
	DTLS Keep Alive	20	seconds
	Session Expiry	60	minutes
Real Protect Settings	☑ Enable Real-Protect integration with Endpoint Intelligence Agent		

5 Click **Save**.

6 The Endpoint Intelligence Agent can be installed now.

7 Post installation, the EIA RaptorClient Service status can be checked in the **Task Manager** where EIA is installed in your system.


Task Manager
File Options View
Processes Performance App history Startup Users Details Services

Name	PID	Status	User name	CPU	Memory (p...	Description
bootstrapWin.exe	1476	Running	darwin	00	7,664 K	bootstrapWin
chrome.exe	7804	Running	cloudadmin	00	29,000 K	Google Chrome
chrome.exe	4108	Running	cloudadmin	00	99,772 K	Google Chrome
chrome.exe	4752	Running	cloudadmin	00	1,056 K	Google Chrome
chrome.exe	4596	Running	cloudadmin	00	872 K	Google Chrome
chrome.exe	4796	Running	cloudadmin	00	3,760 K	Google Chrome
chrome.exe	4680	Running	cloudadmin	00	1,952 K	Google Chrome
eiaRaptorClient.exe	5584	Running	SYSTEM	00	14,532 K	eiaRaptorClient
eiaService.exe	4728	Running	SYSTEM	00	4,924 K	Provides process and user information to McAfee networking products
explorer.exe	4060	Running	cloudadmin	00	36,696 K	Windows Explorer
GoogleCrashHandler...	4056	Running	SYSTEM	00	560 K	Google Crash Handler
GoogleCrashHandler...	3916	Running	SYSTEM	00	536 K	Google Crash Handler
iexplore.exe	4416	Running	cloudadmin	00	4,700 K	Internet Explorer
iexplore.exe	2184	Running	cloudadmin	00	165,296 K	Internet Explorer
iexplore.exe	3944	Running	cloudadmin	00	7,284 K	Internet Explorer
java.exe	2608	Running	darwin	00	103,848 K	Java(TM) Platform SE binary
LogonUI.exe	736	Running	SYSTEM	00	6,064 K	Windows Logon User Interface Host

Upgrade the Endpoint Intelligence Agent

You can upgrade from Endpoint Intelligence Agent 2.3.x, 2.4.x, 2.5.x or 2.6.x to Endpoint Intelligence Agent 3.2.0. Before upgrading, ensure that you are running ePolicy Orchestrator version 5.9.0 or later.

Task

1 Go to www.mcafee.com/us/downloads and download the latest McAfee EIA package .zip file.

2 Upload the package into the ePolicy Orchestrator repository.

3 Deploy the agent on the endpoints.

Endpoint Intelligence Agent and VSCore files upgrade to the latest version. All upgrade attempts generate logs in the installation directory.

> You don't need to restart the system to complete the upgrade process.

> After successful upgrade, you need to push the policies to the endpoints through ePO.

Upgrade the Endpoint Intelligence Management extension

You can upgrade from Endpoint Intelligence Management extension from 2.3.x, 2.4.x, 2.5, 2.6.x to 3.2.0. Before upgrading, ensure that you are running ePolicy Orchestrator version 5.9.0 or later.

Task

1. Go to www.mcafee.com/us/downloads and download the latest Endpoint Intelligence Management extension .zip file.
2. Install the extension on the ePolicy Orchestrator server.
   - a In the ePolicy Orchestrator console, click on the menu icon (≡) and select **Software** | **Extensions**.
   - b In the **Extensions** page, click **Install Extension**.
   - c Browse to the Endpoint Intelligence Management .zip file.
   - d Click **Open** to select the file, then click **OK** to proceed with the selection.
   - e Click **OK** to install the extension.

> After successful upgrade, you need to push the policies to the endpoints through ePO.

Endpoint Intelligence Agent in McAfee Endpoint Suites

McAfee EIA is available as part of the McAfee Endpoint Suites Installer 3.1 and later.

With inclusion of McAfee EIA in McAfee Endpoint Suites, you can easily install McAfee EIM and then deploy McAfee EIA to your endpoints, eliminating the need to individually install McAfee EIA.

The installer for McAfee Endpoint Suites provides an easy deployment and a centrally managed solution for the installation of ePolicy Orchestrator, SQL Server Express, and many McAfee products.

McAfee EIA is included in these product suites:

- Complete Endpoint Protection Enterprise Suite (CEE)
- Complete Endpoint Protection Business Suite (CEB)
- Endpoint Protection Advanced Suite (EPA)
- Endpoint Protection Suite (EPS)

For more details, see the *McAfee Endpoint Suites Installation Guide*.

> McAfee Endpoint Suites Installer 3.1 includes McAfee EIA2.4. McAfee EIA 3.0 will be part of the next release of Endpoint Suites. However, you can download McAfee EIA 3.0 from the Software Manager.

Contents

Install a product suite

You can install McAfee EIA by installing one of the product suites from the McAfee Endpoint Suites.

Before you begin

- Install a supported operating system:
  - Microsoft Windows 2008 Server R2 or later
  - Microsoft Windows Server 2012 or later
- Install Microsoft .NET Framework 3.5 Service Pack 1

> You cannot install the software packages from a network share or a mapped drive.

The product suites are Complete Endpoint Protection Enterprise Suite (CEE), Complete Endpoint Protection Business Suite (CEB), Endpoint Protection Advanced Suite (EPA), and Endpoint Protection Suite (EPS). Each suite contains McAfee ePO and a set of McAfee products.

Task

1. In a web browser, go to www.mcafee.com/us/downloads .
2. Enter your grant number and download and extract the installer archive for your product suite. A folder structure os created.
3. Navigate to and double-click EASI.exe to launch the installer.
4. On the Welcome screen, enter your user credentials.

   > We recommended that you do not change the username, *Admin*.

5. Select the language, accept the terms in the license agreement, then click **Next**.
6. Verify the system requirements, select a drive for installation, and click **Next**.
7. Configure the database settings and click **Install**.
8. Verify that the Message column shows this message for all the components: *The operation completed successfully*. Click **Finish**.

The ePolicy Orchestrator server is set up with McAfee products, which are ready to be deployed to the endpoints. For more details, see the *McAfee Endpoint Suites Installation Guide*.

Once the product suite is installed, use ePolicy Orchestrator to deploy McAfee EIA agents to your endpoints.

Verify your installation

Once you have installed the McAfee Endpoint Suites, verify that all components of your product suite are installed correctly.

Before you begin

Install the appropriate product suite namely CEE, CEB, EPA, or EPS.

Verify these components:

To do this...	Perform these steps...
Log on to the McAfee ePO server	After the installation, **Log On to ePolicy Orchestrator** screen appears. Log on to the server with the credentials you provided at the beginning of the installation.
Verify the product suites	In the McAfee ePO console, click on the menu icon(≡) and select **Systems** | **Master Repository** to view the product suites. If the installation was successful, you see the products from your software package displayed under the **Master Repository**. For example, Endpoint Intelligence Agent.
Verify the extensions	In the McAfee ePO console, click on the menu icon (≡) and select **Systems** | **Extensions** to view extensions. If the installation was successful, you see the extensions for all the installed products from your suite checked in to your McAfee ePO server. For example, Endpoint Intelligence Management. The *postInstall* folder includes extensions and packages of additional McAfee products for a suite.

During installation, if you selected **Enable automatic discovery of systems**, all the systems are added to the System Tree in unmanaged mode. In the McAfee ePO console, click on the menu icon (≡) and select **Systems** | **System Tree** to verify this.

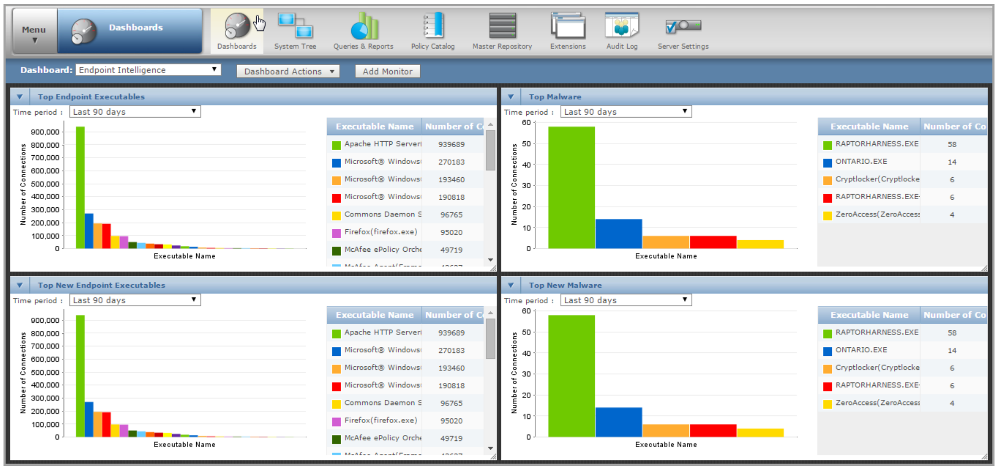
You can now deploy agents, for example, McAfee EIA to these systems to manage them.

3 Using the Endpoint Intelligence dashboard

The **Endpoint Intelligence** dashboard feature demonstrates the value of McAfee EIA even without network devices like NTBA or Firewall Enterprise.

The dashboard provides visibility to McAfee ePO about executables running on the endpoints through monitors on the McAfee ePO console. McAfee ePO can easily collect information related to executables that are initiating network connections, their reputation, updates from multiple endpoint agents, and then consolidate and display them for administrators to view and analyze further. McAfee EIA periodically sends details like the list of executables, reputation of each executable, and the number of connections initiated by each executable to the McAfee ePO dashboard.

Once the Endpoint Intelligence Management extension is installed, you can view the **Endpoint Intelligence** dashboard from the McAfee ePO console under **Dashboards** | **McAfee Dashboards.** | **Endpoint Intelligence**



Dashboard: Endpoint Intelligence

Top Endpoint Executables

Time period : Last 90 days

Executable Name	Number of C
🟩 Apache HTTP Server	939689
🟦 Microsoft® Windows	270183
🟧 Microsoft® Windows	193460
🟥 Microsoft® Windows	190818
🟨 Commons Daemon S	96765
🟪 Firefox(firefox.exe)	95020
🟩 McAfee ePolicy Orche	49719

Top Malware

Time period : Last 90 days

Executable Name	Number of Co
🟩 RAPTORHARNESS.EXE	58
🟦 ONTARIO.EXE	14
🟧 Cryptlocker(Cryptlocke	6
🟥 RAPTORHARNESS.EXE-	6
🟨 ZeroAccess(ZeroAccess	4

Top New Endpoint Executables

Time period : Last 90 days

Executable Name	Number of C
🟩 Apache HTTP Server	939689
🟦 Microsoft® Windows	270183
🟧 Microsoft® Windows	193460
🟥 Microsoft® Windows	190818
🟨 Commons Daemon S	96765
🟪 Firefox(firefox.exe)	95020
🟩 McAfee ePolicy Orche	49719

Top New Malware

Time period : Last 90 days

Executable Name	Number of Co
🟩 RAPTORHARNESS.EXE	58
🟦 ONTARIO.EXE	14
🟧 Cryptlocker(Cryptlocke	6
🟥 RAPTORHARNESS.EXE-	6
🟨 ZeroAccess(ZeroAccess	4

Figure 3-1 Endpoint Intelligence dashboard

Contents

View the Endpoint Intelligence dashboard

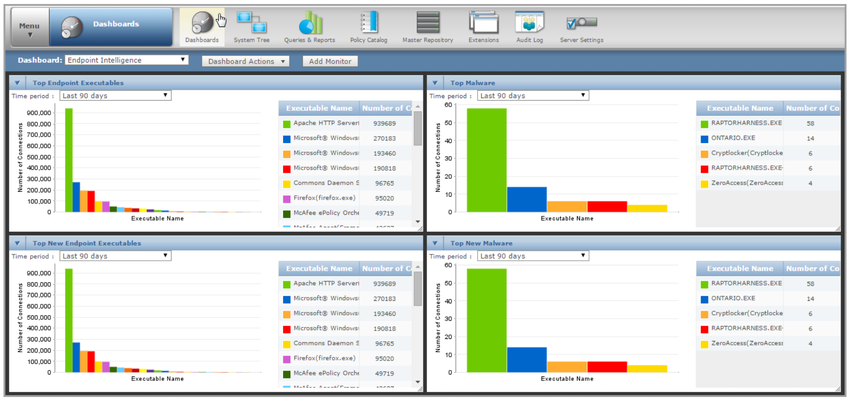
Once the Endpoint Intelligence Management extension is installed, you can view the **Endpoint Intelligence** dashboard from the McAfee ePO console.

Before you begin

Install Endpoint Intelligence Management extension. The dashboard is supported only on Endpoint Intelligence Management extension version 2.3.0 and later.

Task

1. In the ePolicy Orchestrator console, click on the menu icon (≡) and select **Reporting** | **Dashboards** .
2. From the Dashboards drop-down list, select **McAfee Dashboards** | **Endpoint Intelligence**.



Dashboard: Endpoint Intelligence

Top Endpoint Executables

Time period : Last 90 days

Executable Name	Number of C
🟩 Apache HTTP Server	939689
🟦 Microsoft® Windows	270183
🟧 Microsoft® Windows	193460
🟥 Microsoft® Windows	190818
🟨 Commons Daemon S	96765
🟪 Firefox(firefox.exe)	95020
🟩 McAfee ePolicy Orche	49719

Top Malware

Time period : Last 90 days

Executable Name	Number of Co
🟩 RAPTORHARNESS.EXE	58
🟦 ONTARIO.EXE	14
🟧 Cryptlocker(Cryptlocke	6
🟥 RAPTORHARNESS.EXE	6
🟨 ZeroAccess(ZeroAccess	4

Top New Endpoint Executables

Time period : Last 90 days

Executable Name	Number of C
🟩 Apache HTTP Server	939689
🟦 Microsoft® Windows	270183
🟧 Microsoft® Windows	193460
🟥 Microsoft® Windows	190818
🟨 Commons Daemon S	96765
🟪 Firefox(firefox.exe)	95020
🟩 McAfee ePolicy Orche	49719

Top New Malware

Time period : Last 90 days

Executable Name	Number of Co
🟩 RAPTORHARNESS.EXE	58
🟦 ONTARIO.EXE	14
🟧 Cryptlocker(Cryptlocke	6
🟥 RAPTORHARNESS.EXE	6
🟨 ZeroAccess(ZeroAccess	4

The **Top Endpoint Executables**, **Top Malware**, **Top New Endpoint Executables**, and **Top New Malware** monitors are displayed. You can hover over a bar to view executable details. Click on an executable to view more details.

> The dashboard data updates take place by default every six hours. You can configure it from **Menu** | **Policy** | **Policy Catalog** | **Endpoint Intelligence <version>** | **<Policy name>** | **Edit** page. Go to **Other Settings** options and modify the **Dashboard Update Interval** value.

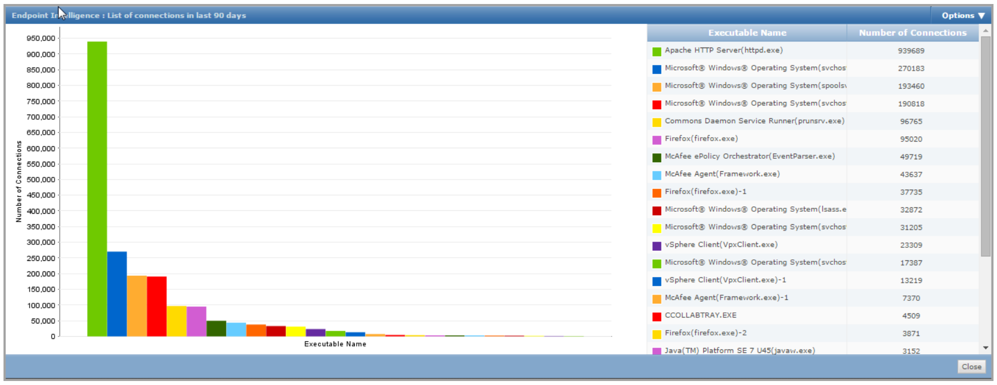
Understanding the monitors

The **Endpoint Intelligence** dashboard displays **Top Endpoint Executables**, **Top Malware**, **Top New Endpoint Executables**, and **Top New Malware** monitors.

Each monitor has these options:

- Graphical view — You can view bar graphs for executables in your network. To view more details, click an executable bar in the graph.
- Executable details — Each monitor displays the executable name, for example, Chrome.exe and the number of connections made in the network using an executable. The connections might be from a single or various endpoints.

- **Time period** — Each monitor enables you to view details for the last hour, 24 hours, 30 days, and 90 days. When selected, the details that are displayed are only for a specific monitor.
- Display options — You can click **Full Screen** to display the monitor in an expanded view. Click **Refresh** to view the latest data.



Executable Name	Number of Connections
🟩 Apache HTTP Server(httpd.exe)	939689
🟦 Microsoft® Windows® Operating System(svchos	270183
🟧 Microsoft® Windows® Operating System(spoolsv	193460
🟥 Microsoft® Windows® Operating System(svchos	190818
🟨 Commons Daemon Service Runner(prunsrv.exe)	96765
🟪 Firefox(firefox.exe)	95020
🟩 McAfee ePolicy Orchestrator(EventParser.exe)	49719
🟦 McAfee Agent(Framework.exe)	43637
🟧 Firefox(firefox.exe)-1	37735
🟥 Microsoft® Windows® Operating System(lsass.e	32872
🟨 Microsoft® Windows® Operating System(svchos	31205
🟪 vSphere Client(VpxClient.exe)	23309
🟩 Microsoft® Windows® Operating System(svchos	17387
🟦 vSphere Client(VpxClient.exe)-1	13219
🟧 McAfee Agent(Framework.exe)-1	7370
🟥 CCOLLABTRAY.EXE	4509
🟨 Firefox(firefox.exe)-2	3871
🟪 Java(TM) Platform SE 7 U45(javaw.exe)	3152

Figure 3-2 Full Screen snapshot

Dashboard monitors

McAfee EIA periodically sends details to the ePO dashboard like the list of executables, reputation of each executable, and the number of connections initiated by each executable. These values are used for the **Endpoint Intelligence** dashboard.

- **Top Endpoint Executables**— These executables are known to McAfee EIA and their reputation is available.
- **Top Malware**— These executables are a subset of **Top Endpoint Executables** and are classified as **Malware** based on reputation calculated by EIA.

> You can also import executables(excluding dlls) generated by Endpoint Baseline Generator and by default, these executables are classified as **Low Risk**.

- **Top New Endpoint Executables**— These executables are first time connections and newly known to McAfee EIA in the selected time period. If an executable is unknown, its reputation is calculated by EIA and then displayed on this monitor.
- **Top New Malware**— These executables are a subset of **Top New Endpoint Executables**. New executables are classified as**Malware** based on reputation calculated by EIA.

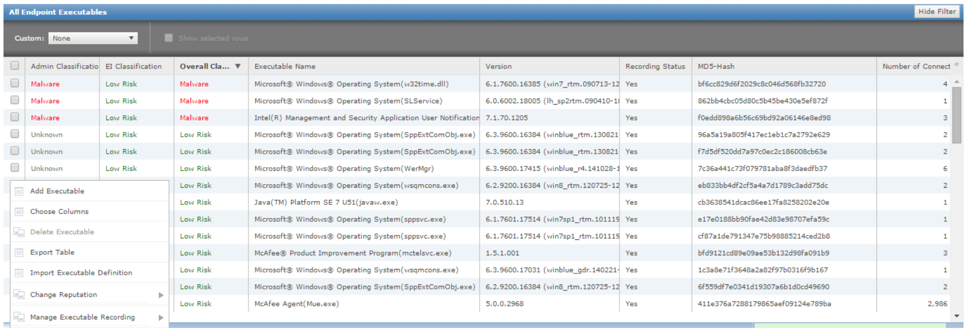
> An administrator can modify an executable's classification to **Malware** or **Low Risk**.

View all endpoint executables

The **All Endpoint Executables** page provides a snapshot of all the executables running on your internal endpoints that have made network calls. It also provides details like classification, executable name and version, recording status, hash value, and the number of connections made in the network.

By default, the order is sorted by overall classification level. Executables with classification **Malware** are displayed first.

You can click **Actions** | **Choose Columns** to select the order and details to be displayed on this page.



Admin Classificatio	EI Classification	Overall Cla... ▼	Executable Name	Version	Recording Status	MD5-Hash	Number of Connect
Malware	Low Risk	Malware	Microsoft® Windows® Operating System(w32time.dll)	6.1.7600.16385 (win7_rtm.090713-12	Yes	bf6cc829d6f2029c8c046d568fb32720	4
Malware	Low Risk	Malware	Microsoft® Windows® Operating System(SLService)	6.0.6002.18005 (lh_sp2rtm.090410-1	Yes	862bb4cbc05d80c5b45be430e5ef872f	1
Malware	Low Risk	Malware	Intel(R) Management and Security Application User Notification	7.1.70.1205	Yes	f0edd898a6b56c69bd92a06146e8ed98	3
Unknown	Low Risk	Low Risk	Microsoft® Windows® Operating System(SppExtComObj.exe)	6.3.9600.16384 (winblue_rtm.130821	Yes	96a5a19a805f417ec1eb1c7a2792e629	2
Unknown	Low Risk	Low Risk	Microsoft® Windows® Operating System(SppExtComObj.exe)	6.3.9600.16384 (winblue_rtm.130821	Yes	f7d5df520dd7a97c0ec2c186008cb63e	2
Unknown	Low Risk	Low Risk	Microsoft® Windows® Operating System(WerMgr)	6.3.9600.17415 (winblue_r4.141028-1	Yes	7c36a441c73f079781aba8f3daedfb37	6
		Low Risk	Microsoft® Windows® Operating System(wsqmcons.exe)	6.2.9200.16384 (win8_rtm.120725-12	Yes	eb833bb4df2cf5a4a7d1789c3add75dc	2
		Low Risk	Java(TM) Platform SE 7 U51(javaw.exe)	7.0.510.13	Yes	cb3638541dcac86ee17fa8258202e20e	1
		Low Risk	Microsoft® Windows® Operating System(sppsvc.exe)	6.1.7601.17514 (win7sp1_rtm.101119	Yes	e17e0188bb90fae42d83e98707efa59c	1
		Low Risk	Microsoft® Windows® Operating System(sppsvc.exe)	6.1.7601.17514 (win7sp1_rtm.101119	Yes	cf87a1de791347e75b98885214ced2b8	1
		Low Risk	McAfee® Product Improvement Program(mctelsvc.exe)	1.5.1.001	Yes	bfd9121cd89e09ae53b132d98fa091b9	3
		Low Risk	Microsoft® Windows® Operating System(wsqmcons.exe)	6.3.9600.17031 (winblue_gdr.140221-	Yes	1c3a8e71f3648a2a82f97b0316f9b167	1
		Low Risk	Microsoft® Windows® Operating System(SppExtComObj.exe)	6.2.9200.16384 (win8_rtm.120725-12	Yes	6f559df7e0341d19307a6b1d0cd49690	2
		Low Risk	McAfee Agent(Mue.exe)	5.0.0.2968	Yes	411e376a7288179865aef09124e789ba	2,986

Figure 3-3 All Endpoint Executables page

Task

1. From the EIA dashboard, click a bar on any monitor graph. The All Endpoint Executables page is displayed.

   The executables displayed on this page are not limited for the time period specified on a monitor.

2. Click **Show/Hide Filter** and from the **Custom** drop-down, select **Add..** to filter executables based on properties like hash, recording status, version, and others. Click **Update Filter** and **Save** the filter with a name.

   The executables are displayed based on the filter.

   Select **None** to clear the applied filters.

3. Click the up/down arrow to sort the executables by **Overall Classification** levels. View details for an executable like version, recording status, hash value, and number of connections made by an executable in the network.

4. From **Actions**, you can view and use these options:

   - **Add Executables**— Add one or more executables to this page.
   - **Delete Executables**— Select one or more executable for deletion.
   - **Export Table**— Export all the executables on this page into zip, CSV, XML, HTML, or PDF formats
   - **Import Executable Definition**— Import an .xml file and add to this list of executables.
   - **Change Reputation**— As an administrator, you can modify an executable's classification to **Malware** or **Low Risk** in your network.
   - **Manage Executable Recording**— Record an executable's activities in the network.

Click a row to view specific executable and endpoint details.

Tasks

- *Manage executable recording status* on page 29
  You can record an executable's status like activities performed. By default, all executables are recorded.
- *Modify executable reputation* on page 29
  As an administrator, you can modify an executable's reputation to **Malware** or **Low Risk** and in turn decide executables safe or unsafe for your network.
- *Import executables* on page 29
  You can import executables (excluding dll files) from a baseline profile generated by Endpoint Baseline Generator. By default, all executable imported are classified as **Low Risk**.
- *Export executable details* on page 30
  You can export executable details from the All Endpoint Executables page in various formats such as CSV, PDF.

Manage executable recording status

You can record an executable's status like activities performed. By default, all executables are recorded.

Task

1. In the ePolicy Orchestrator console, click on the menu icon (≡) and select **Network** | **Endpoint Executables**. The All Endpoint Executables page is displayed.
2. Select one or more executables, right-click **Actions** and select **Manage Executable Recording**.
   - **Record Selected Executables** — Records activities performed by selected executables and displays on the dashboard monitors. The status is displayed as **Yes**.
   - **Stop Recording Selected Executables** — Stops displaying the recorded and selected executables activities. The recording status changes to **No**.

Modify executable reputation

As an administrator, you can modify an executable's reputation to **Malware** or **Low Risk** and in turn decide executables safe or unsafe for your network.

The overall classification is derived from EIA classification and Admin classification. Admin classification takes precedence over EIA classification. If EI classification is **Low Risk** and Admin classification is **Malware**, the overall classification will be **Malware**.

Perform these steps to change one or more executables reputation.

Task

1. From the EIA dashboard, click on a monitor graph or executable row. The All Endpoint Executables page is displayed.
2. Select one or more executables, right-click **Actions** and select **Change Reputation**.
   - **Low Risk** — Changes the Admin Classification value of the selected executable to **Low Risk**.
   - **Malware** — Changes the Admin Classification value of the selected executable to **Malware**.

Import executables

You can import executables (excluding dll files) from a baseline profile generated by Endpoint Baseline Generator. By default, all executable imported are classified as **Low Risk**.

Before you begin

XML file to be imported is created on a clean system.

Task

1. From the EIA dashboard, click on a monitor graph of executable bar. The All Endpoint Executables page is displayed.
2. Right-click **Actions** and select **Import Executable Definition** and browse to an XML file. Click **Import**.

The executables are added to the existing list of executable on the All Endpoint Executables page.

Export executable details

You can export executable details from the All Endpoint Executables page in various formats such as CSV, PDF.

Task

1. In the ePolicy Orchestrator console, click on the menu icon (≡) and select **Network** | **Endpoint Executables**. The All Endpoint Executables page is displayed.
2. Click on **Actions** and select **Export Table** to provide export details and click **Export**.
    - **Export information** — Provides the number of executable details that are being exported.
    - **Compress files** — Compresses exported file in .zip format.
    - **File format** — Specifies a format for the exported data. Options include CSV, HTML, XML and PDF.
    - **What to do with exported files** — Specifies what the system does with the files once they are created. Select **Open or save from a link** to open the exported file or right-click the link to save it to a desired location.

The executable details are exported in the selected format.

View executable and endpoint details

You can drill-down to the executable and endpoint details to decide whether an executable is safe or unsafe for your network.

Task

1. In the ePolicy Orchestrator console, click on the menu icon (≡) and select **Network** | **Endpoint Executables**.

   The All Endpoint Executables page is displayed.
2. Select an executable row and double-click to view executable and endpoint details.

   The Executable Details page is displayed.
3. Click the **Executable Information** tab to view details for an executable like name, classification, version, hash value, and other details.
4. Click the **Top Reported Endpoints** tab to view details like IP address and number of connections made from endpoints. By default, the endpoints are sorted by the **Number of Connections** made in the network.

Once you view executable and endpoint details like classification, executable hash, and endpoint IP address, you can analyze further if an executable running in your network is safe or unsafe, and perform response actions.

4 Configure Endpoint Intelligence Agent on McAfee ePO

You need to configure an McAfee EIA policy for network devices and other McAfee products, set up the network devices, and assign policies to the managed systems to make Endpoint Intelligence Agent ready for integration. These policies and assignments must be done from the ePolicy Orchestrator console.

Contents

Configure policy

Configure routes and gateway connection settings for network devices. You can edit or duplicate an existing policy, or create a new policy. After setting a policy, apply policies to managed systems.

Two preconfigured policies are generated for Endpoint Intelligence Agent:

- **McAfee Default** is read-only and cannot be deleted. It can be duplicated.
- **My Default** is editable.

Tasks

- *Create a policy* on page 32
  You can create a new policy if you do not want to use the preconfigured policy.
- *Approvals to create or edit policies* on page 32
- *Remove Endpoint Intelligence Agent from Managed endpoints* on page 33
  You can remove Endpoint Intelligence Agent from the managed endpoints in ePolicy Orchestrator console.
- *Configure routes and other settings* on page 34
  Edit a policy to specify routes, log settings, and malware engine settings for the managed systems.
- *Modify the data channel Time to Live* on page 37
  The data channel Time to Live controls when the connection between ePolicy Orchestrator and Endpoint Intelligence Agent times out. On networks with slower connectivity, you might need to increase the Time to Live.
- *Assign policy to managed systems* on page 38
  For Endpoint Intelligence Agent to communicate with Firewall Enterprise or NTBA, a policy must be applied to managed systems.

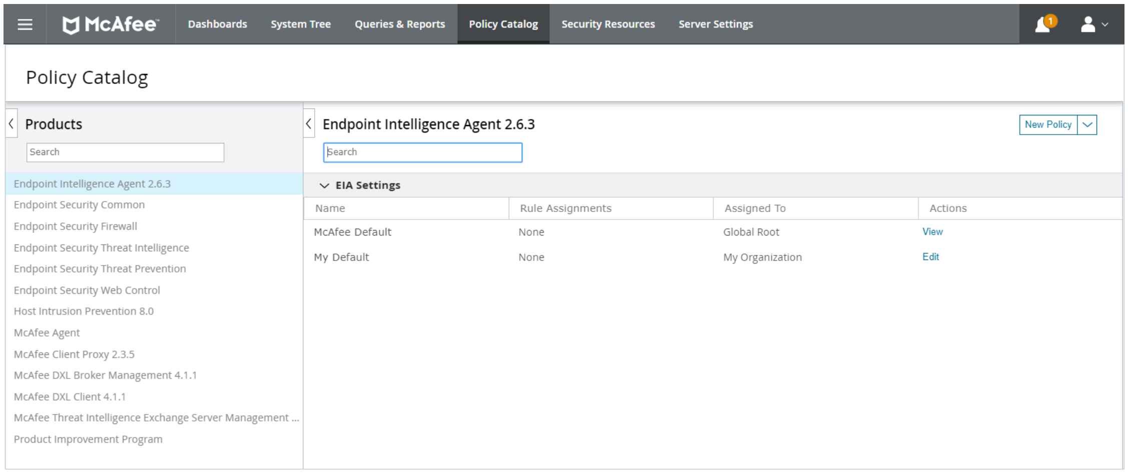
Create a policy

You can create a new policy if you do not want to use the preconfigured policy.

> If you are an administrator and want to create or edit policies without review, ensure that the **Administrator/Approver need approval for policy changes** setting is disabled.
>
> For more information, refer Approvals to create or edit policies on page 32.

Task

1 In the ePolicy Orchestrator console, click on menu icon (≡) and select **Policy** | **Policy Catalog**.



Policy Catalog

Products

- Endpoint Intelligence Agent 2.6.3
- Endpoint Security Common
- Endpoint Security Firewall
- Endpoint Security Threat Intelligence
- Endpoint Security Threat Prevention
- Endpoint Security Web Control
- Host Intrusion Prevention 8.0
- McAfee Agent
- McAfee Client Proxy 2.3.5
- McAfee DXL Broker Management 4.1.1
- McAfee DXL Client 4.1.1
- McAfee Threat Intelligence Exchange Server Management ...
- Product Improvement Program

Endpoint Intelligence Agent 2.6.3

EIA Settings

Name	Rule Assignments	Assigned To	Actions
McAfee Default	None	Global Root	View
My Default	None	My Organization	Edit

Figure 4-1 Policy Catalog page

2 From the **Product** list, select **Endpoint Intelligence Agent <version>**. The **Category** is set as **EIA Settings**

3 Click **New Policy**.

4 From the **Create a policy based on this existing policy** list, select a policy.

5 In **Policy Name**, enter a name for your policy.

6 [Optional] In **Notes**, enter a description.

7 Click **OK** to save the policy.

The new policy is displayed in the **Policy Catalog** page.

Approvals to create or edit policies

With ePO 5.10, you can choose if an admin/non-admin user requires approval from other users to create or edit policies. It also permits the user to edit pre-configured policies.

For more information, see *McAfee ePolicy Orchestrator Product Guide*.

> By default, EIA policies cannot be configured or edited by non-admin users.

Remove Endpoint Intelligence Agent from Managed endpoints

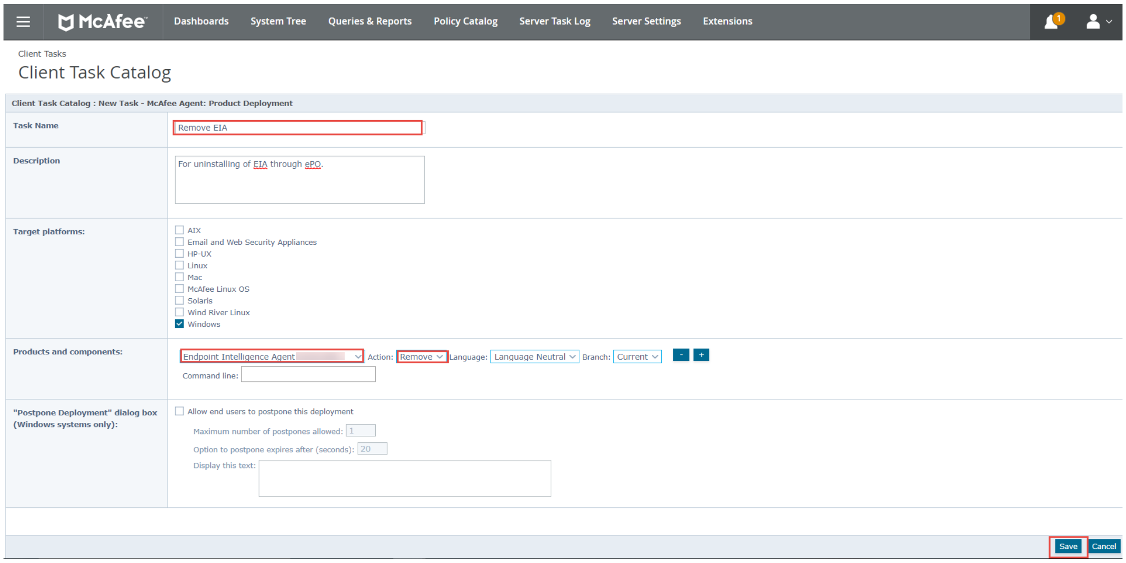
You can remove Endpoint Intelligence Agent from the managed endpoints in ePolicy Orchestrator console.

Task

1. In the ePolicy Orchestrator console, go to menu (≡), and select **Client Task** | **Client Task Catalog**. The **Client Task Catalog** page opens.
2. Click **New Task**.

   The **New Task** window opens.
3. In the **Task Types** drop-down list, select **Product Deployment**.
4. Click **OK**.

   The **Client Task Catalog: New Task - McAfee Agent: Product Deployment** window opens.
5. In the **Task Name** field, enter a name for the task to be created.
6. From **Products and components** option, select **Endpoint Intelligence Agent <version>** and in the **Action** drop-down list, select **Remove**.



Client Tasks

Client Task Catalog

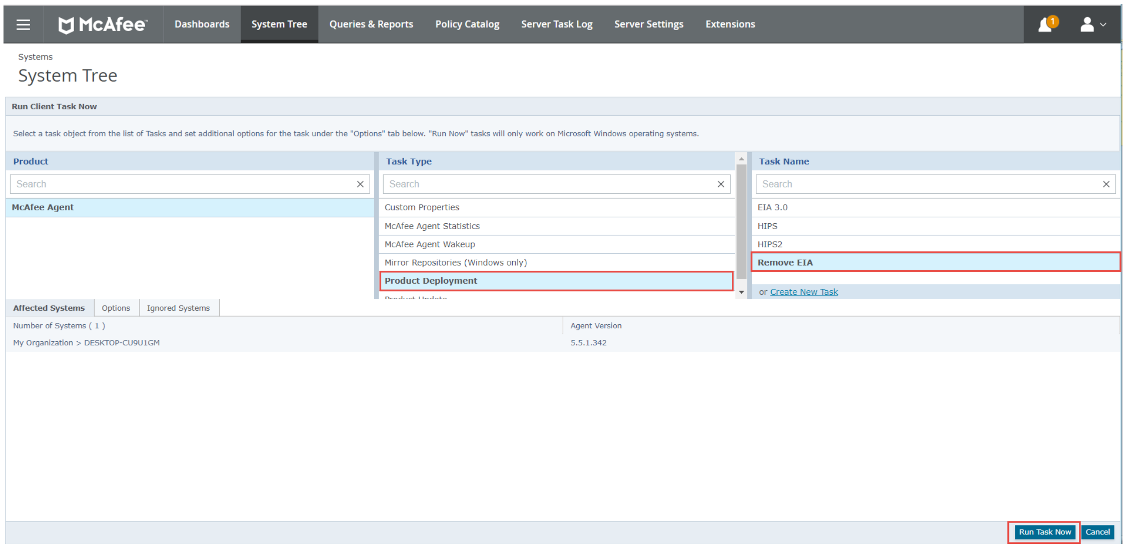
Client Task Catalog : New Task - McAfee Agent: Product Deployment

Task Name	Remove EIA
Description	For uninstalling of EIA through ePO.
Target platforms:	□ AIX □ Email and Web Security Appliances □ HP-UX □ Linux □ Mac □ McAfee Linux OS □ Solaris □ Wind River Linux ☑ Windows
Products and components:	Endpoint Intelligence Agent [redacted] Action: Remove Language: Language Neutral Branch: Current - + Command line:
"Postpone Deployment" dialog box (Windows systems only):	□ Allow end users to postpone this deployment Maximum number of postpones allowed: 1 Option to postpone expires after (seconds): 20 Display this text:

7. Click **Save**.
8. To run the task perform the following steps:
   1. Click on **System Tree** icon. The **Systems** page opens.
   2. Select the managed endpoint from which Endpoint Intelligence Agent has to be uninstalled.
   3. Go to **Actions** | **Agent** | **Run Client Task Now**.
   4. In the **Task Type** column, select **Product Deployment**.

e In the **Task Name** column, select the task you created.

f Click **Run Task Now**.



Systems

System Tree

Run Client Task Now

Select a task object from the list of Tasks and set additional options for the task under the "Options" tab below. "Run Now" tasks will only work on Microsoft Windows operating systems.

Product	Task Type	Task Name
Search	Search	Search
McAfee Agent	Custom Properties	EIA 3.0
	McAfee Agent Statistics	HIPS
	McAfee Agent Wakeup	HIPS2
	Mirror Repositories (Windows only)	Remove EIA
	Product Deployment	
	Product Update	or Create New Task

Affected Systems | Options | Ignored Systems

Number of Systems (1)	Agent Version
My Organization > DESKTOP-CU9U1GM	5.5.1.342

Configure routes and other settings

Edit a policy to specify routes, log settings, and malware engine settings for the managed systems.

Endpoint Intelligence Agent can now send metadata to multiple device types simultaneously. Discovery mode is supported on both the network devices, Firewall Enterprise and NTBA. You can define static routes for each network device and for backward compatibility, devices and routes defined on EIA 2.3.x and 2.4.2 are also supported and can be modified.

EIA can send data to multiple devices of the same type, provided they are handling traffic to different destination subnets. For example, two firewalls cannot expect metadata for a single connection.

If you do not configure firewall information for a particular route, McAfee EIA automatically discovers the firewall for that route if the firewall is deployed in dynamic mode.

Task

1 In the ePolicy Orchestrator console, click on the menu icon (≡) and select **Policy** | **Policy Catalog**.

2 In the **Product** list, select **Endpoint Intelligence Agent <version>**.

3 In the **Name** column, click the hyperlink for a policy you want to configure.

4 From **Routes**, select **Firewall** or **NTBA** and define routes.

a Click **Add**.

To remove a route, select the entry and click **Remove Route**.

b Select **Exempt route** if you want to exempt routes for specific destinations.

Example: You have a subnet configured for route discovery, but you don't want to send metadata for a particular endpoint in that network.

c Enter the network address and subnet mask. The **Device IP** and **Port** fields are grayed out.

d Select **Exempt Route**.

e Click **Add Routes**.

f Select one or more routes and click **Delete** or **Clear All** to remove routes.

> If you upgrade from previous versions, the routes defined on 2.3.x or 2.4.2 for a network device are automatically displayed.

5 Specify the following information for various options.

Option	Definition
Supported 2.3.x or 2.4.2 device	Specifies the network device mapped to EIA 2.3.x or 2.4.2. You can also edit a device and route. The supported options are **Firewall** and **NTBA**. By default, **Firewall** is selected. The defined route is displayed in **Routes**. This option is only for backward compatibility to support network devices on EIA 2.3.x or 2.4.2.
Routes	Specifies the routes on which Endpoint Intelligence Agent sends information to network devices. EIA can send data to multiple devices of the same type, provided they are handling traffic to different destination subnets. • **Firewall** — Specifies endpoint information is sent to one or more firewalls. • **NTBA** — Specifies endpoint information is sent to one or more NTBAs. • **Add** — Specifies one or more routes using which Endpoint Intelligence Agent communicates with the device. Use the **Add Routes** page options to define the source or destination IP addresses, subnet mask, and network device address. By default, port 9008 is used for communication. • **Delete** — Removes the route. • **Clear All**— Clears all defined routes from the list.
Log Settings Specifies the default runtime parameters and settings for Endpoint Intelligence Agent. We recommend that you keep these at default values.	• **Log level** — Specifies the logging level for the Endpoint Intelligence Agent. By default, this is selected as**Info**. You can select other logging levels like **Fatal**, **Error**, **Warn**, and **Debug** based on your need. • **Rotate log files** — Specifies the number of times the log files are rotated in the system. After this limit, the log files are removed. For example, if the log number is 0, the old versions are removed. By default, this limit is set to 10. The range is 0-100. • **Max log file size** — Specifies the limit of log file size in MB. Once the log files reach this log size, they are rotated as per the **Rotate log files**. By default, this value is set to 10 MB. The range is 1-2048 MB.

Option	Definition
Gateway Connection Settings	• **Retry Interval** — [Error occurrence] Specifies the waiting time in milliseconds before retrying a connection to the gateway. By default, this is set to 1000. The limit range is 1-5000 milliseconds. • **Recovery Interval** — [Recovery from a slow device connection] Specifies the time in milliseconds prior to reducing the delay on sending packets to the network device. By default, this is set to 3000 milliseconds. Interval range is 50-60000 milliseconds. • **Backoff Maximum Interval** — Specifies the amount of time to send and process the connection information. By default, this is set to 10 milliseconds. The time range is 5 to 200 milliseconds. • **Backoff Minimum Interval** — Specifies the minimum amount of time to send and process the connection information. By default, this is set to 5 milliseconds. The time range is 5 to 100 milliseconds. • **Backoff Percentage** — [Slow device connection detected] Specifies the percentage increase in the current delay period. This increases the amount of time Endpoint Intelligence Agent gets to send connection information to device and for device to process this connection information. By default, this is set to 500. The percentage range is 200 to 999. • **DTLS Keep Alive** — Specifies the intervals in seconds at which an endpoint sends acknowledgments to the network device. By default, this is set to 20 seconds. Range is 10-60 seconds. • **Session Expiry** — Specifies the maximum amount of time in minutes for which the device session exists. After this time, the session times out. By default, this value is set to 60 minutes. The session time range is 10 to 300 minutes.
Malware Engine Settings	• **Enable Malware Engine integration with Endpoint Intelligence Agent** — Specifies if you wish to integrate the malware engine with McAfee EIA to dynamically analyze executables for classification. By default, this checkbox is selected. • **Add Executable** — Specifies the executable that you wish to monitor. The executable name must not contain the characters ", <, >, :, ?, /, \, |, *, and only blanks as the executable name. • **Remove Executable** — Removes the selected executables from the list of monitored executables.
Other Settings	• **Ignore virtual traffic** — Specifies ignoring traffic from virtual adaptors. By default, this checkbox is selected. • **Dashboard Update Interval** — Specifies the time at which the Endpoint Intelligence dashboard data is updated. By default, this is set to 6 hours. Range is 1-24 hours.

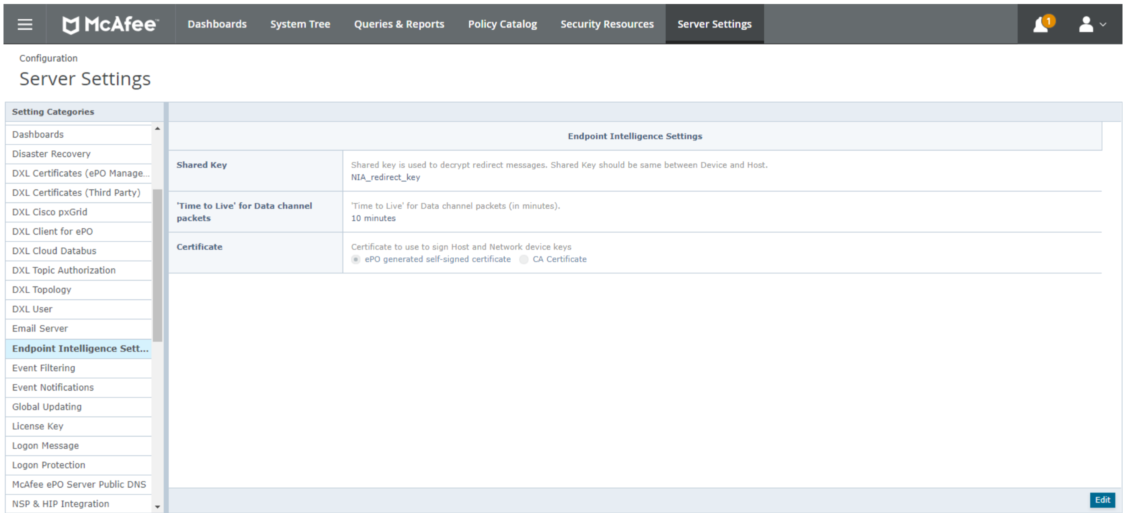
6 Click **Save** to complete the device, route, and other configuration.

Modify the data channel Time to Live

The data channel Time to Live controls when the connection between ePolicy Orchestrator and Endpoint Intelligence Agent times out. On networks with slower connectivity, you might need to increase the Time to Live.

Task

1. In the ePolicy Orchestrator console, click on the menu icon (≡) and select **Configuration** | **Server Settings**.
2. From **Setting Categories**, click **Endpoint Intelligence Settings** and then click **Edit**.

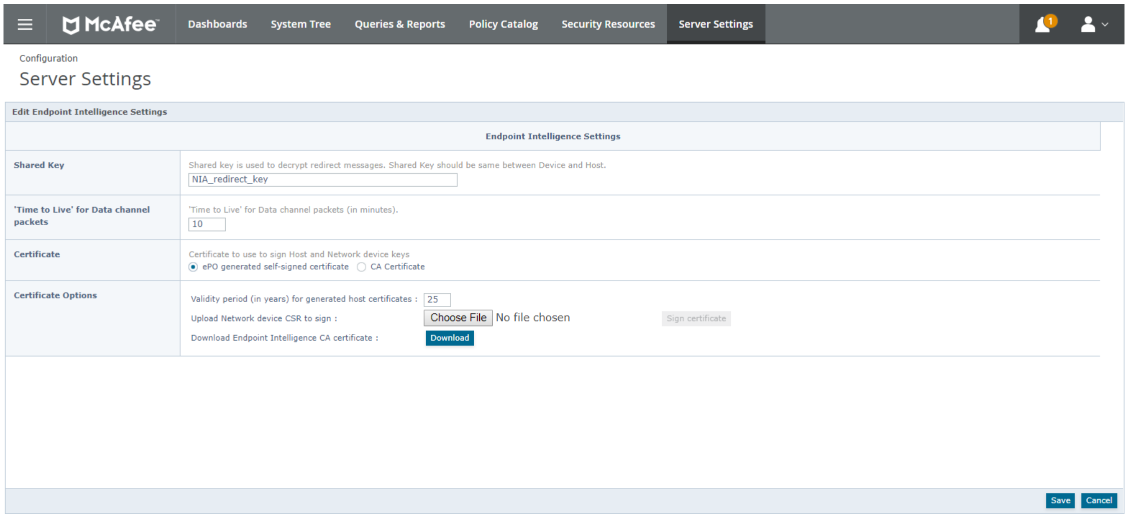


Configuration
Server Settings

Endpoint Intelligence Settings	
Shared Key	Shared key is used to decrypt redirect messages. Shared Key should be same between Device and Host. NIA_redirect_key
'Time to Live' for Data channel packets	'Time to Live' for Data channel packets (in minutes). 10 minutes
Certificate	Certificate to use to sign Host and Network device keys ● ePO generated self-signed certificate ○ CA Certificate

Figure 4-2 Endpoint Intelligence Settings page

3. In **'Time to Live' for Data channel packets (in minutes)**, enter the amount of time in minutes. Valid values are 1–1440. The default value is 10 minutes.



Configuration
Server Settings

Edit Endpoint Intelligence Settings

Endpoint Intelligence Settings	
Shared Key	Shared key is used to decrypt redirect messages. Shared Key should be same between Device and Host. NIA_redirect_key
'Time to Live' for Data channel packets	'Time to Live' for Data channel packets (in minutes). 10
Certificate	Certificate to use to sign Host and Network device keys ● ePO generated self-signed certificate ○ CA Certificate
Certificate Options	Validity period (in years) for generated host certificates : 25 Upload Network device CSR to sign : Choose File No file chosen Sign certificate Download Endpoint Intelligence CA certificate : Download

Figure 4-3 Edit Endpoint Intelligence Settings page

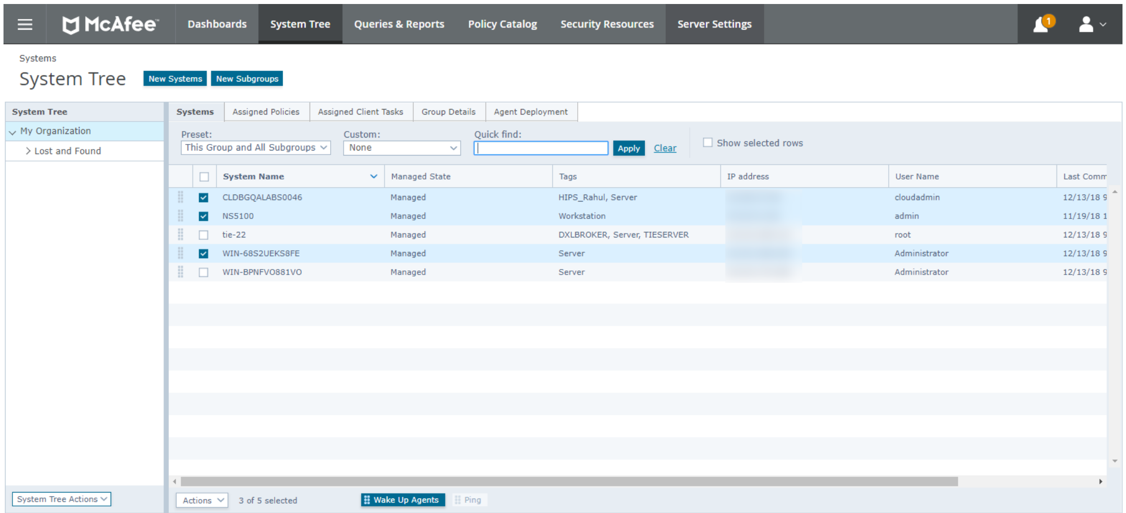
4. Click **Save**.

Assign policy to managed systems

For Endpoint Intelligence Agent to communicate with Firewall Enterprise or NTBA, a policy must be applied to managed systems.

Task

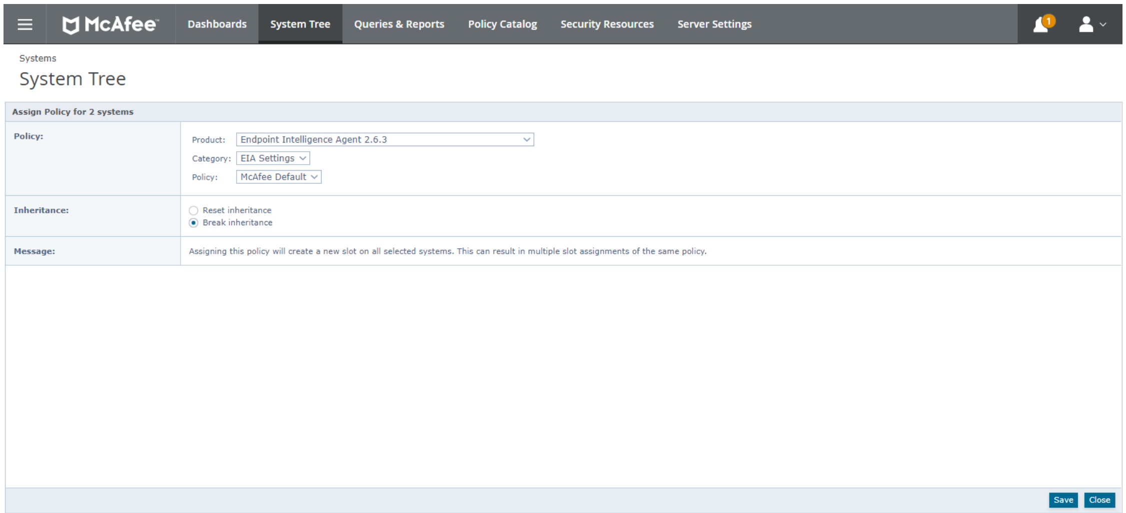
1. In the ePolicy Orchestrator console, click on the menu icon (≡) and select **Menu** | **Systems** | **System Tree**.
2. Select the systems to apply policy to.
3. Select **Actions** | **Agent** | **Set Policy & Inheritance**.



	System Name	Managed State	Tags	IP address	User Name	Last Comm
☑	CLDBGQALABS0046	Managed	HIPS_Rahul, Server	[redacted]	cloudadmin	12/13/18 9
☑	NS5100	Managed	Workstation	[redacted]	admin	11/19/18 1
□	tie-22	Managed	DXLBROKER, Server, TIESERVER	[redacted]	root	12/13/18 9
☑	WIN-68S2UEKS8FE	Managed	Server	[redacted]	Administrator	12/13/18 9
□	WIN-BPNFVO881VO	Managed	Server	[redacted]	Administrator	12/13/18 9

Figure 4-4 Systems tab

4. From the **Product** menu, select **Endpoint Intelligence Agent <version>**.



Assign Policy for 2 systems

Policy:	Product: Endpoint Intelligence Agent 2.6.3 Category: EIA Settings Policy: McAfee Default
Inheritance:	○ Reset inheritance ● Break inheritance
Message:	Assigning this policy will create a new slot on all selected systems. This can result in multiple slot assignments of the same policy.

Figure 4-5 Assign Policy page

5. From the **Policy** menu, select the policy.
6. Click **Save**.

Configure certificates for network devices

Certificate configuration is necessary for the encrypted communication between network devices and McAfee EIA.

Configuring the certificates consists of these high-level steps:

1. In the network device, generate and export the certificate for McAfee EIA.
2. Sign the certificate in the Endpoint Intelligence Management extension.

> As a non-admin user, based on the permissions set in **User Management** | **Permission Sets** | **Endpoint Intelligence**, you can download signed certificates from ePO.

3. Export the ePolicy Orchestrator certificate authority (CA) certificate.
4. Load the signed certificate and the CA certificate into the network device.

When creating certificates, they must meet these requirements:

- Public key lengths must be 4096 bits or lower.
- The host certificate used by McAfee EIA must be signed by the same certificate authority that generated the CA certificate.

For Firewall Enterprise, refer to the chapter *McAfee EIA* in the *McAfee Firewall Enterprise Product Guide* . For NTBA, refer to the chapter, *Integrating with McAfee Endpoint Intelligence Agent* in the *McAfee NTBA Administration Guide* to enable McAfee EIA integration.

Tasks

- *Configure certificates using SCEP* on page 39
  If you do not want to use the ePolicy Orchestrator CA to sign the certificate, you can use the Simple Certificate Enrollment Protocol (SCEP) instead.

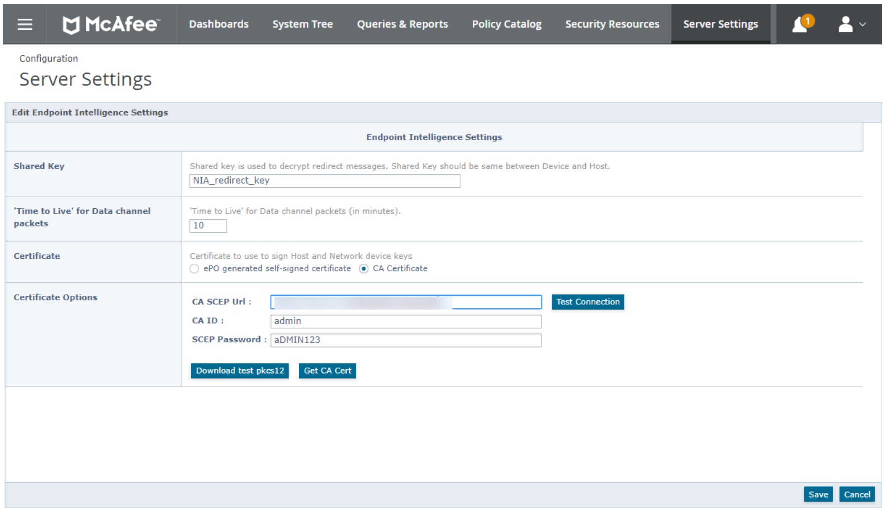
Configure certificates using SCEP

If you do not want to use the ePolicy Orchestrator CA to sign the certificate, you can use the Simple Certificate Enrollment Protocol (SCEP) instead.

Task

1. In the ePolicy Orchestrator console, click on the menu icon (≡) and select **Configuration** | **Server Settings**.
2. Select **Endpoint Intelligence Settings**, then click **Edit**.

3. Configure SCEP settings.
   a. Select **CA Certificate.**
   b. Enter the information in **CA SCEP Url**, **CA ID** and **SCEP Password**.
   c. Click **Test Connection** to verify the information. A success message appears.



Shared Key: Shared key is used to decrypt redirect messages. Shared Key should be same between Device and Host.
NIA_redirect_key

'Time to Live' for Data channel packets: 'Time to Live' for Data channel packets (in minutes).
10

Certificate: Certificate to use to sign Host and Network device keys
○ ePO generated self-signed certificate ● CA Certificate

Certificate Options:
CA SCEP Url : [redacted]
CA ID : admin
SCEP Password : aDMIN123

Figure 4-6 SCEP settings

4. [Optional] Click **Get CA Cert** to manually download the CA certificate and **Download test pkcs12** to test the certificate type.
5. On the network device, configure the CA certificate.
6. Save your changes.

5 Configuring McAfee EIA with network devices and other McAfee products

Endpoint Intelligence Agent integrates with network devices and other McAfee products. This section helps you to configure McAfee EIA on these devices and products and be ready to integrate.

Set up network devices and other McAfee products

These are the products that can integrate with McAfee EIA. You can set up these using these references.

Firewall Enterprise

You can enable McAfee EIA on the Firewall Enterprise using the Admin Console.

For more information on configuring and managing McAfee EIA on the Firewall Enterprise, see the *McAfee Firewall Enterprise Product Guide*.

NTBA

You can enable McAfee EIA integration on the NTBA Appliance using the McAfee Network Security Manager (Manager).

For more information on setup, configuring and managing McAfee EIA on the NTBA appliance, see section, *Integrating with McAfee Endpoint Intelligence Agent* in the *McAfee NTBA Administration Guide*.

ePO-PIP

You can configure PIP to collect details like system environment (software and hardware details), effectiveness of installed McAfee product features, and McAfee product errors and related Microsoft Windows events.

For more details, refer to the *McAfee Product Improvement Program Quick Start Guide*.

Minimum Escalations Reporting (WebMER)

You can enable WebMER to collect logs from endpoints and enable McAfee EIA to have more visibility and troubleshoot any issues. ePO-MER is an ePO deployable version of WebMER.

For more information on setup, refer to the *McAfee MER for ePO Walkthrough Guide*.

McAfee Virtual Technician (MVT)

McAfee Virtual Technician (MVT) is a diagnostic tool that can find and resolve many of the most common issues with McAfee products. After scanning your system, you can resolve any detected issue. The scan results are also passed to McAfee Technical Support for a open Service Request. ePO-MVT is an ePO deployable version of McAfee Virtual Technician.

For more information, refer to the *ePO -MVT Walkthrough Guide*.

Tasks

- *Set up Firewall Enterprise* on page 42
  McAfee Firewall Enterprise (Firewall Enterprise) allows you to protect your network from unauthorized users and attackers, and to protect internal users as they access the Internet.
- *Set up Product Improvement Program (PIP)* on page 43
  McAfee Product Improvement Program (formerly Telemetry) collects the data from the client systems where ePO-managed McAfee products are installed. The data collected by Product Improvement Program (PIP) is used by McAfee to improve the overall user experience, provide better- performing product features, and perform proactive data collection for faster troubleshooting of customer issues.
- *Set up ePolicy Orchestrator MER* on page 45
  The ePolicy Orchestrator deployable Minimum Escalation Requirements (ePO-MER) tool collects the McAfee product data from your system so that a problem can be analyzed and resolved by McAfee support.
- *ePO-MVT* on page 48
  ePO-MVT is an ePO deployable version of McAfee Virtual Technician.

Set up Firewall Enterprise

McAfee Firewall Enterprise (Firewall Enterprise) allows you to protect your network from unauthorized users and attackers, and to protect internal users as they access the Internet.

Firewall Enterprise combines an application-layer firewall, user-based policy, IPsec VPN capabilities, SSL decryption, and McAfee Global Threat Intelligence into one security appliance that is designed to offer centralized perimeter security.

These features provide powerful configuration options that allow you to control your users' access to almost any publicly available service on the Internet, while mitigating threats to your organization.

McAfee EIA-Firewall Enterprise integration

At a high level, follow these steps to integrate McAfee EIA with Firewall Enterprise:

1. Configure certificates manually.
   a. Generate the firewall certificate.
   b. Sign the firewall certificate and export the CA certificate.
   c. Load the certificates.
2. Configure McAfee EIA settings using the Admin Console.
   a. Configure authentication and certificate settings.
   b. Configure agent discovery.
   c. Configure the executable file reputation.
   d. Modify advanced firewall settings.
   e. Create an explicit McAfee EIA communication rule.

For more details, refer to the chapter, *McAfee EIA* in the *McAfee Firewall Enterprise Product Guide*.

Post integration, you can:

- View connected endpoints using the Admin Console.
- View related firewall audit.

Set up Network Threat Behavior Analysis

The McAfee NTBA Appliance is a feature-rich, non-intrusive solution for monitoring network traffic by analyzing flow information flowing through network in real time. The NTBA Appliance complements the NAC and IPS Sensor capabilities in a scenario in which Network Security Platform, NAC Sensors, and NTBA Appliances are installed and managed through the Network Security Manager.

The NTBA Appliance gathers flow information from across users, applications, endpoints, and network devices, and stores them in an embedded database. You can see real-time data and a moving profile of applications, endpoints, zones, and interface traffic. The NTBA Appliance provides a graphical configurable real-time view of the network traffic.

McAfee EIA-NTBA integration

After McAfee EIA is installed on the endpoints and is ready to send metadata to NTBA, enable McAfee EIA integration in McAfee® Network Security Manager at the **Global** or **Device** level.

On the **EIA Integration** page, select **EIA Integration** and configure the McAfee ePO server settings. Refer to the *NTBA Administration Guide* for more details.

Post integration, you can:

- Create whitelists and blacklists for your network.
- Configure NTBA policies for McAfee EIA alerts.
- View executables running on endpoints.
- Analyze executable behavior.

Set up Product Improvement Program (PIP)

McAfee Product Improvement Program (formerly Telemetry) collects the data from the client systems where ePO-managed McAfee products are installed. The data collected by Product Improvement Program (PIP) is used by McAfee to improve the overall user experience, provide better- performing product features, and perform proactive data collection for faster troubleshooting of customer issues.

You can install McAfee Product Improvement Program when installing the McAfee ePO 5.0 and later and McAfee Agent 4.8 and later. On the **Ready to Install the Program** dialog box, decide if you want to **Allow McAfee to collect anonymous diagnostic and usage data**, then click **Install** to begin installing the ePO software.

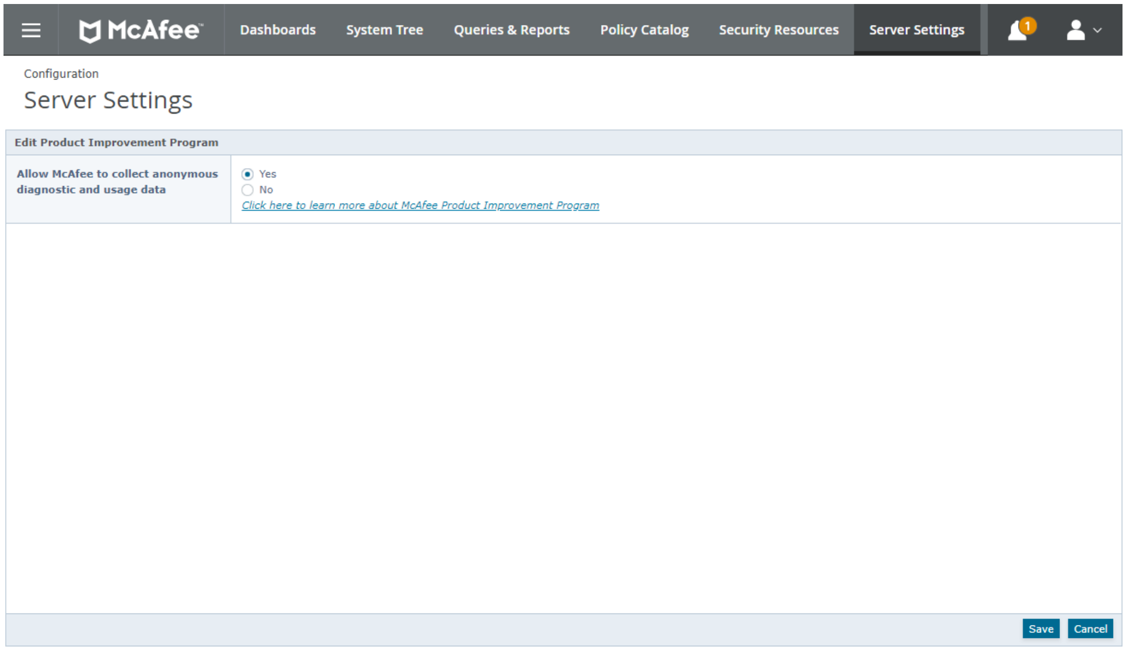
The collected data is aggregated on the McAfee ePO server and sent to the McAfee Product Improvement Program server once a day (default collection period) and stored at \TelemetryData. The collected data is filtered to remove any personally identifiable information.

McAfee EIA-PIP integration

At a high level, follow these steps to integrate McAfee EIA with PIP.

1 Install the PIP software with McAfee ePO.

2 Enable the PIP software on the McAfee ePO server.



Configuration

Server Settings

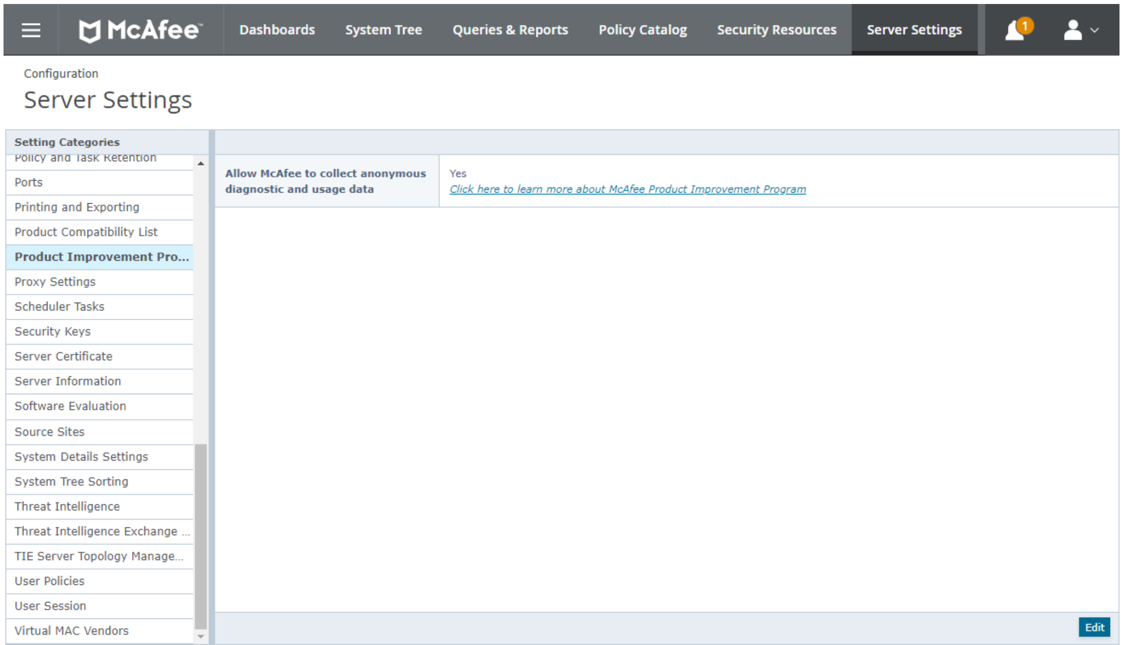
Edit Product Improvement Program

Allow McAfee to collect anonymous diagnostic and usage data: ● Yes ○ No

Click here to learn more about McAfee Product Improvement Program

Figure 5-1 Server Settings | Setting Categories option

3 Apply the PIP policy to managed endpoints.



Configuration

Server Settings

Allow McAfee to collect anonymous diagnostic and usage data: Yes

Click here to learn more about McAfee Product Improvement Program

Figure 5-2 Assign PIP policy

PIP collected data

The following is a list of the data currently collected from an endpoint.

- **Data collected from endpoints**
  - IPv6 traffic details
  - RSA public key size details (Example: 2048 bytes)
  - Certificate size details (Example: 1271 bytes)
- **Data collected from McAfee ePO Server**
  - Number of configured endpoints using McAfee EIA
  - Number of ePolicy Orchestrator clients
  - Operating system version details on endpoints where McAfee EIA is installed
  - Configured network device details
  - Other McAfee Endpoint suite products that are being used by ePolicy Orchestrator

Set up ePolicy Orchestrator MER

The ePolicy Orchestrator deployable Minimum Escalation Requirements (ePO-MER) tool collects the McAfee product data from your system so that a problem can be analyzed and resolved by McAfee support.

ePO-MER covers a large number of McAfee products running on Windows operating systems. The information collected includes event logs, file version details, files, process details, and registry details.

To help collect logs and details in real time when an issue occurs, every McAfee EIA can collect data from an endpoint on demand, or the McAfee ePO server can consolidate details from all endpoints where ePO-MER is installed.

McAfee EIA-ePO-MER integration

At a high-level, these are the steps to deploy ePO-MER on managed endpoints.

1 Go to https://support.mcafee.com/epomer and download and install the ePO-MER deployment package.

2 From the ePolicy Orchestrator console:

   a Install the Policy Management MER extension.

   b Install the MER Deployment package.

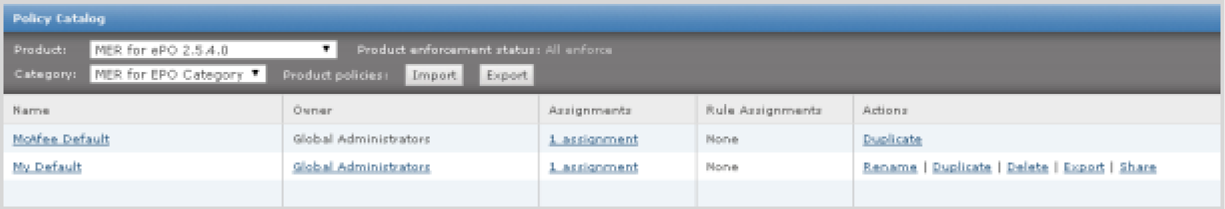
   c Deploy the MER tool on the managed endpoints.

Refer to the *McAfee MER for ePO Walkthrough Guide* for more details.

Configure a MER policy

After MER is installed on the endpoints, configure a MER policy to collect system data and scan the endpoints for collecting logs.

1 In the ePolicy Orchestrator console, click on the menu icon (≡) and select **Policy** | **Policy Catalog**.



Policy Catalog

Product: MER for ePO 2.5.4.0 ▾ Product enforcement status: All enforce

Category: MER for EPO Category ▾ Product policies: Import Export

Name	Owner	Assignments	Rule Assignments	Actions
McAfee Default	Global Administrators	1 assignment	None	Duplicate
My Default	Global Administrators	1 assignment	None	Rename | Duplicate | Delete | Export | Share

Figure 5-3 Policy Catalog page

2. In the **Product** list, select **MER for ePO <version>**. The **Category** is set as **MER for EPO Category**.

3. Click **New Policy**.

4. In the **Create a policy based on this existing policy** list, select a policy.

5. In **Policy Name**, enter a name for your policy.

6. [Optional] In **Notes**, enter a description.

7. Click **OK** to save the policy.

The new policy is displayed on the **Policy Catalog** page.

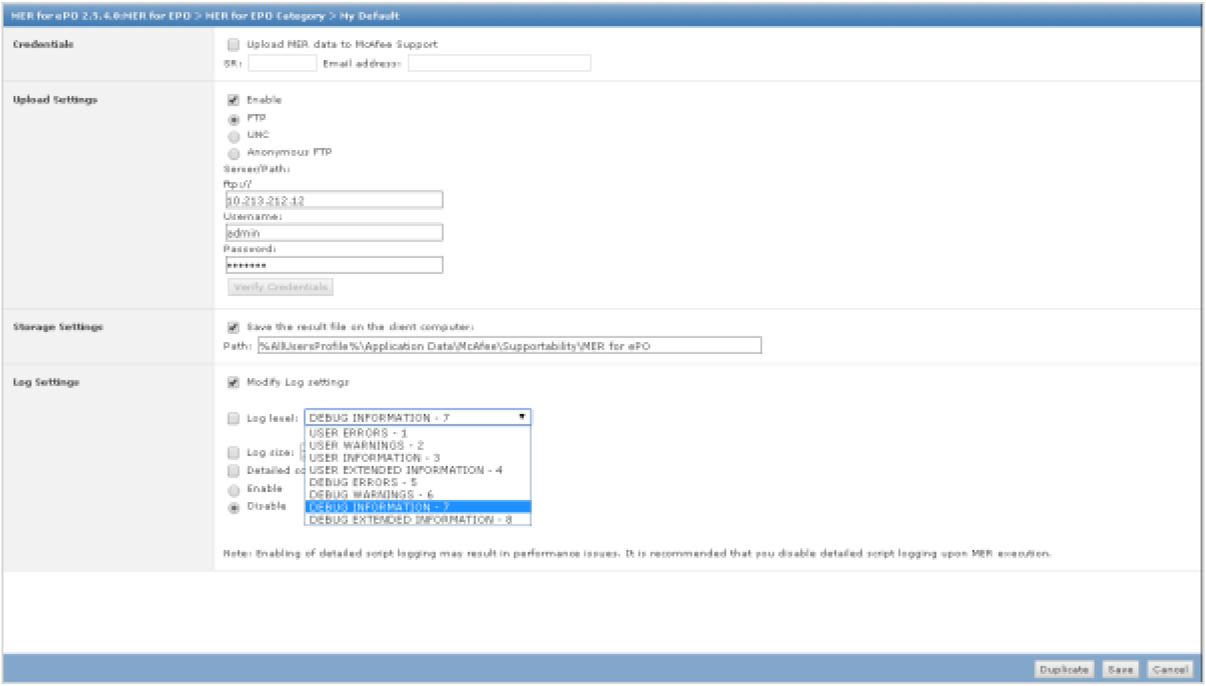
Configure log collection settings

Select policy options to collect logs from endpoints.

1. From the **Policy Catalog**, click the hyperlink for the MER policy.

2. In **Credentials**, select the **Upload MER data to McAfee Support** if you want to upload logs to the support team at scheduled intervals.

3. Enter the SR details and email address.



MER for ePO 2.5.4.0:MER for EPO > MER for EPO Category > My Default

Credentials
□ Upload MER data to McAfee Support
SR: Email address:

Upload Settings
☑ Enable
● FTP
○ UNC
○ Anonymous FTP
Server/Path:
ftp://
10.213.212.12
Username:
admin
Password:
•••••••
Verify Credentials

Storage Settings
☑ Save the result file on the client computer:
Path: %AllUsersProfile%\Application Data\McAfee\Supportability\MER for ePO

Log Settings
☑ Modify Log settings
□ Log level: DEBUG INFORMATION - 7
□ Log size:
□ Detailed sc
○ Enable
● Disable

Note: Enabling of detailed script logging may result in performance issues. It is recommended that you disable detailed script logging upon MER execution.

Figure 5-4 Log settings

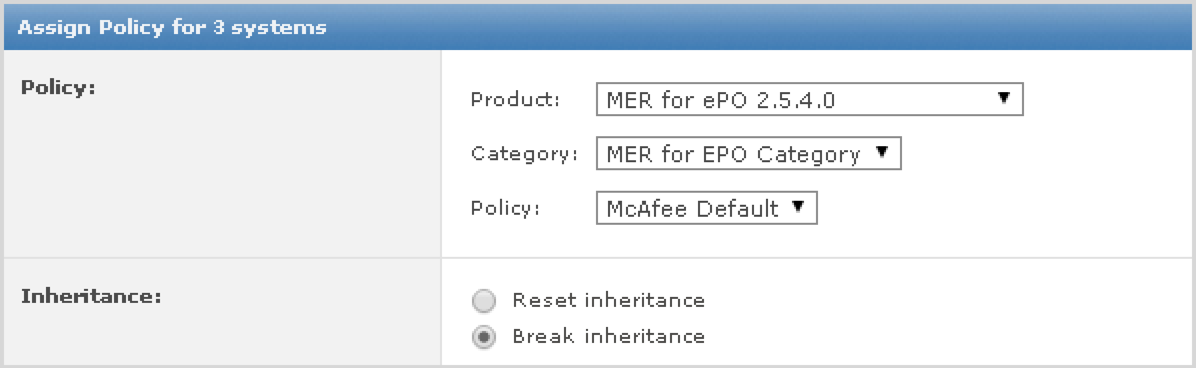
4. In **Upload Settings**, select **Enable** to provide FTP, UNC, or any server details where logs can be stored. Click **Verify credentials** to confirm connectivity.

5. In **Storage Settings**, specify the path on the endpoint where logs are stored. By default, logs are stored in %AllUsersProfile%\Application Data\McAfee\Supportability\MER for ePO.

6. In **Log Settings**, select **Modify Log settings** to specify the log level, log size, and detail script logging.

7. Click **Save**.

From the **System Tree**, select the managed endpoints and apply the configured MER policy.



Assign Policy for 3 systems

Policy:

Product: MER for ePO 2.5.4.0 ▼

Category: MER for EPO Category ▼

Policy: McAfee Default ▼

Inheritance:

○ Reset inheritance
● Break inheritance

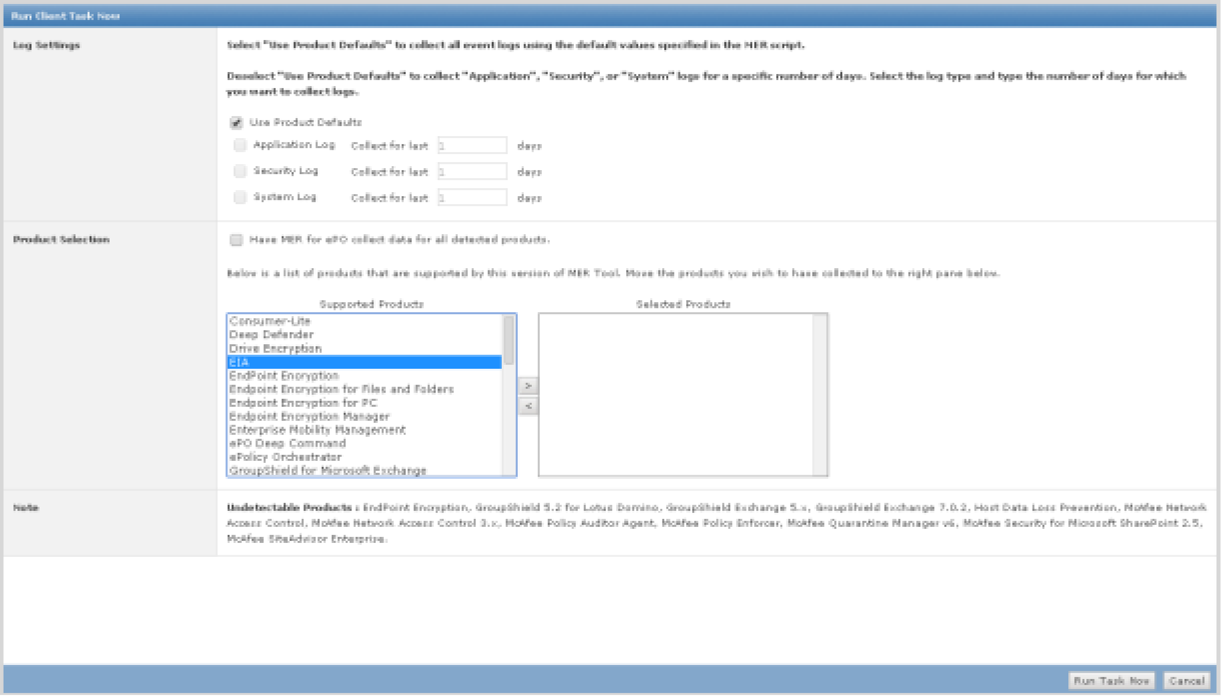
Figure 5-5 Apply MER policy

Run a system scan

Whenever an issue occurs, you can run the scan task to collect system data for analysis.

1. In the ePolicy Orchestrator console, select **System Tree**.
2. Select the managed endpoints from which you want to collect details.
3. Select **Actions | Agent | Run Client Task Now**.
4. From the**Product** drop-down list, select **MER for ePO <version>**.
5. From the **Task Type** drop-down list, click **ScanTask**.
6. Click **Create New Task**. The Run Client Task Now page is displayed.
7. In the **Log Settings** pane, select the logs you want ePO-MER to collect from endpoints. You can either select **Use Product Defaults** or specify the number of days to collect specific logs.

8 In the **Product Selection** pane, select **EIA** from the **Supported Products** list.



Log Settings

Select "Use Product Defaults" to collect all event logs using the default values specified in the MER script.

Deselect "Use Product Defaults" to collect "Application", "Security", or "System" logs for a specific number of days. Select the log type and type the number of days for which you want to collect logs.

☑ Use Product Defaults
☐ Application Log Collect for last 1 days
☐ Security Log Collect for last 1 days
☐ System Log Collect for last 1 days

Product Selection

☐ Have MER for ePO collect data for all detected products.

Below is a list of products that are supported by this version of MER Tool. Move the products you wish to have collected to the right pane below.

Note

Undetectable Products : EndPoint Encryption, GroupShield 5.2 for Lotus Domino, GroupShield Exchange 5.x, GroupShield Exchange 7.0.2, Host Data Loss Prevention, McAfee Network Access Control, McAfee Network Access Control 3.x, McAfee Policy Auditor Agent, McAfee Policy Enforcer, McAfee Quarantine Manager v6, McAfee Security for Microsoft SharePoint 2.5, McAfee SiteAdvisor Enterprise.

Figure 5-6 Run Client Task Now page

9 Click **Run Task Now**. The **Running Client Task Now** page displays the **Status** bar in green when the logs are collected.

Go to %AllUsersProfile%\Application Data\McAfee\Supportability\MER for ePO to view logs and analyze issues.

ePO-MVT

ePO-MVT is an ePO deployable version of McAfee Virtual Technician.

McAfee Virtual Technician (MVT) is a diagnostic tool that can find and resolve many of the most common issues with McAfee products. You can select whether to only detect and report issues found to the ePO server, or detect and automatically resolve issues in your environment, and reporting the outcome to the ePO server.

ePO-MVT supports two client tasks that can be created on ePO:

- MVT Diagnostic task — This task can be configured either to diagnose or to diagnose and resolve issues in the supported products.
- MVT Remediate task — This task can be configured to diagnose and resolve issues in the supported products or required components.

For more information on configuration, see the *ePO-MVT Walkthrough Guide*.

6 Maintenance and troubleshooting

You can use various reports and logs to monitor the status of host agents and troubleshoot communication or operational problems.

Contents

View ePolicy Orchestrator reports

ePolicy Orchestrator provides reports to check the connections of Endpoint Intelligence Agent on managed endpoints.

Tasks

- *View the Endpoint Intelligence reports* on page 49
  The Endpoint Intelligence: Connections reports lists all managed endpoints and their details for a time period with an active Endpoint Intelligence Agent.

View the Endpoint Intelligence reports

The Endpoint Intelligence: Connections reports lists all managed endpoints and their details for a time period with an active Endpoint Intelligence Agent.

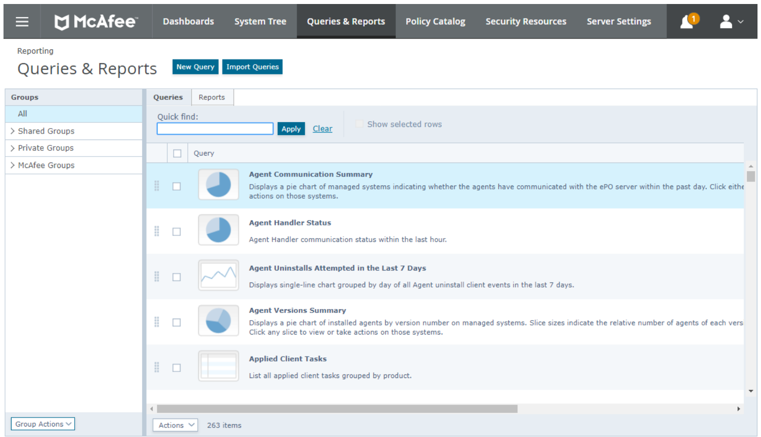
Task

1. From the ePolicy Orchestrator console, click on the menu icon (≡) and select **Reporting** | **Queries & Reports**.
   The **Queries & Reports** page is displayed.

2. In **Quick Find** field, type Endpoint Intelligence and click **Apply**. Select the report you want to view and click **Run**.
   The reports are listed as follows:

   - Endpoint Intelligence: Connections from Malware in Last hour
   - Endpoint Intelligence: Connections from Malware in Last 24 hours
   - Endpoint Intelligence: Connections from Malware in Last 30 days
   - Endpoint Intelligence: Connections from Malware in Last 90 days
   - Endpoint Intelligence: Connections in Last hour
   - Endpoint Intelligence: Connections in Last 24 hours
   - Endpoint Intelligence: Connections in Last 30 days

- Endpoint Intelligence: Connections in Last 90 days
- Endpoint Intelligence: New executables seen is last hour
- Endpoint Intelligence: New executables seen is last 24 hours
- Endpoint Intelligence: New executables seen is last 30 days
- Endpoint Intelligence: New executables seen is last 90 days
- Endpoint Intelligence: New Malware seen is last hour
- Endpoint Intelligence: New Malware seen is last 24 hours
- Endpoint Intelligence: New Malware seen is last 30 days
- Endpoint Intelligence: New Malware seen is last 90 days
- Endpoint Intelligence: All Endpoint Executables



Agent Communication Summary
Displays a pie chart of managed systems indicating whether the agents have communicated with the ePO server within the past day. Click eithe actions on those systems.

Agent Handler Status
Agent Handler communication status within the last hour.

Agent Uninstalls Attempted in the Last 7 Days
Displays single-line chart grouped by day of all Agent uninstall client events in the last 7 days.

Agent Versions Summary
Displays a pie chart of installed agents by version number on managed systems. Slice sizes indicate the relative number of agents of each vers Click any slice to view or take actions on those systems.

Applied Client Tasks
List all applied client tasks grouped by product.

Figure 6-1 Endpoint Intelligence reports

3 When you are finished viewing the report, click **Close**.

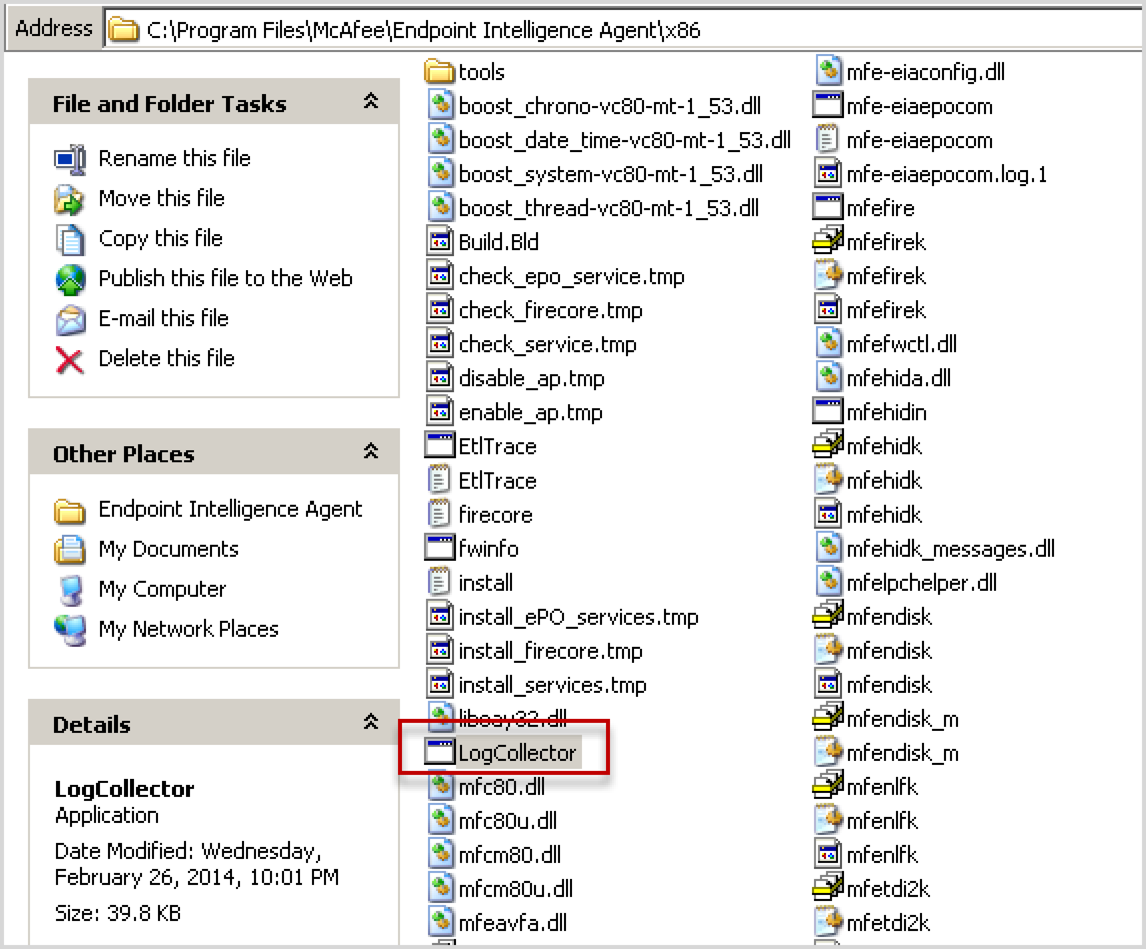
Viewing the Endpoint Intelligence Agent logs

Endpoint Intelligence Agent writes errors and debugging information to several local log files on an endpoint. These log files might be requested when working with McAfee Technical support.

- Installation information is logged to EIAInstallation.log. The location of this file varies depending on the system user, but it is commonly found in C:\Windows\Temp\McAfeeLogs.
- McAfee EIA-ePO communicator service information is logged to mfe-eiaepocom.log. The log files are rotated based on size. After a file reaches 10 MB, it is moved to the consequent number until the count reaches 10. For example, eiaepocom.log becomes eiaepocom.log.2 and can rotate until eiaepocom.log.10.
- Endpoint Baseline Generator information is logged to mfe-ebg.log.

Log Collector tool

You can collect logs by executing the LogCollector.exe that is available in the McAfee EIA installation folder. This file is available in \C:\Program Files\McAfee\Endpoint Intelligence Agent\x86.The logs are generated in the EiaDiagnosisLogs_<month_date_hour_minutes>.CAB folder.



Address C:\Program Files\McAfee\Endpoint Intelligence Agent\x86

LogCollector
Application
Date Modified: Wednesday, February 26, 2014, 10:01 PM
Size: 39.8 KB

Figure 6-2 LogCollector tool

The location of this folder varies depending on the system user; it is found in the x86 folder in the 32-bit operating system and in the x64 folder in the 64-bit operating system.

The following files are copied from the installation directory (different for 32-bit and 64-bit operating systems):

- firecore.log
- mfe-ebg.log
- mfe-eiaepocom.log
- mfe-eiaconfig.log
- Syscore.etl
- cachedReputation.txt
- install.log
- EIAUnInstall.log
- eiaservice.etl

The following files are also copied:

- %systemroot%\Temp\McAfeeLogs\EIAInstallation.log
- %systemroot%\Temp\McAfeeLogs\EIAUninstall.log
- Files under %programdata%HYPERLINK "file:///\\McAfee\Common%20Framework\DB" \McAfee\Common Framework\DB\
- Files under %AppData%HYPERLINK "file:///\\McAfee\Common%20Framework\DB" \McAfee\Common Framework\DB\

Troubleshooting tips

Some troubleshooting tips while using McAfee EIA are given in the following table.

Problem	Solution
Troubleshooting ePO deployments	You cannot do a manual configuration for ePO deployments. On the McAfee EIA configuration dialog box, do not delete the certificates and routes. If deleted, McAfee ePO pushes the policies that have certificates and the routes. It will take some time to update these certificates and routes.
Issues with the installer	Collect the following log files for information: • ePO, eia install log • Use Log Collector to collect logs
Issues with the McAfee EIA service	Go to `C:\<Program Files>\McAfee\EndpointIntelligenceAgent\x86` and execute the *EIAUtil* utility as an administrator. • On the **Endpoint Intelligence Agent Configuration** screen, click **Start Trace**. • Reproduce the issue. • Click **Stop Trace**. Make sure to stop collecting traces, else the logs might consume lot of disk space.
Issues with starting eia service	Go to `C:\Program Files\Common Files\McAfee\SystemCore` and execute the command, `mmsinfo.exe -start eiaservice`
Issues with multiple device support	• Go to`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\McAfee\Endpoint Intelligence Agent\Configured`. Search for the gateway addresses for Firewall and NTBA. These routes are configured as static routes only. • Execute the LogCollector tool in case of multiple gateways configured in the discovery mode. You can see the routes that are discovered in CacheDump file. • Verify that metadata is sent to both the configured network devices using Wireshark for specified service port. Default port is 9008.

Problem	Solution
Issues with the EIM extension	• Provide the policy configuration. • Provide the browser version details. • In case of certificate issues, provide the ePO audit logs.
Issues with the McAfee EIA/ communicator issues	• Collect the crash dump from crashes folder in the installation directory. • Provide the relevant windows event viewer log. • Enable debug logs for McAfee EIA service by changing the log level to debug in the ePO advanced policy. • Use Log Collector to collect all logs. • If possible, provide the relevant crash .exe file, for example, mfe-ebg64.exe or mfe-eiaepocom.exe. • Provide the MA debug logs in case of ePolicy Orchestrator communicator crash.

7 Frequently asked questions

This section answers some of the frequently asked questions about Endpoint Intelligence Agent.

Question 1

When McAfee EIA switches the DTLS connection from one network device to another, the older connection continues to be displayed in the status screen as connected. Why?

Answer 1

When a route is added, McAfee EIA connects to a network device and starts sending metadata. The status screen displays that the connection is up.

Since the connection between McAfee EIA and the network device is UDP connection over TLS, that is, DTLS, McAfee EIA uses heart beat messages to detect the status of the connection. To save bandwidth, heartbeat is sent as part of metadata but not as a separate message. If McAfee EIA does not receive a response, even after sending three heartbeat messages, it declares the peer as dead.

When a route gets changed, McAfee EIA connects to a new network device and starts sending metadata. It does not have any data that needs to be sent to the older device. Since there is no data, there is no way of sending a heartbeat message. So the status of the older connection remains in the same state. The connection status screen shows two rows. One for the previous connection and the other for the current connection.