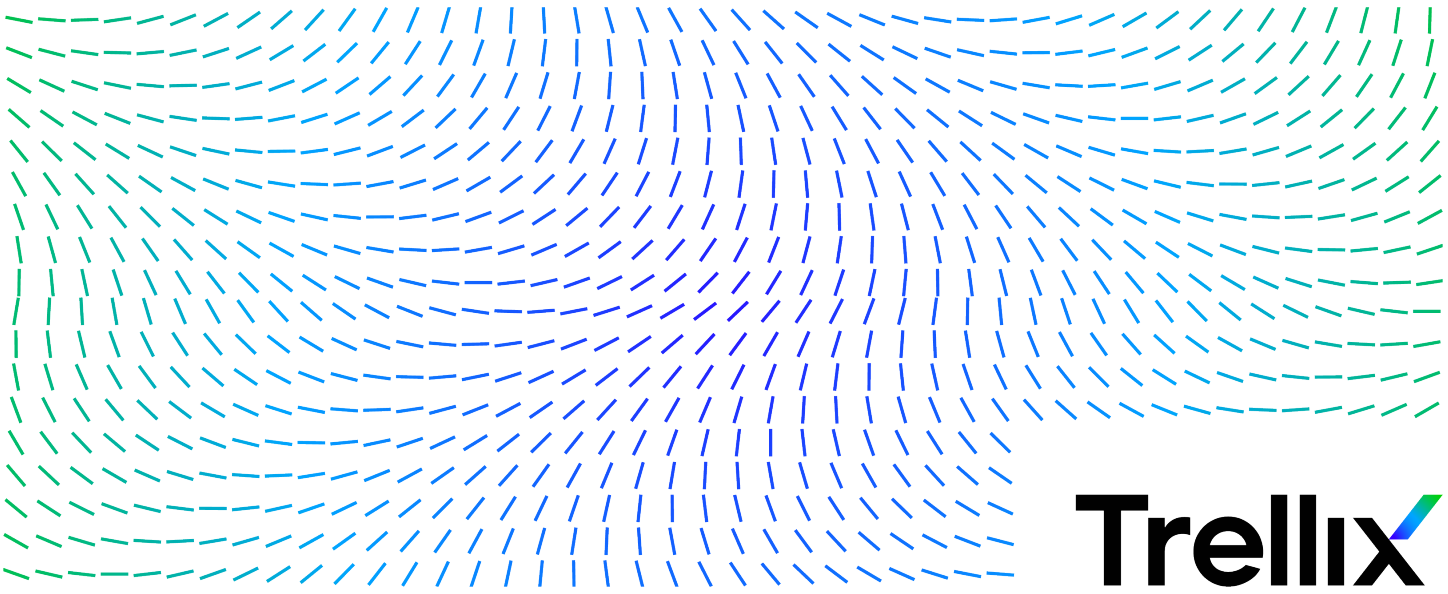
McAfee Rogue System Detection 5.0.6 Interface Reference Guide



Contents

Interface Reference

Add Subnets page

Use this page to add subnets to your network.

Option definitions

Option	Definition
Choose method of adding	Provides options for adding subnets to the **McAfee ePO** server, including: • **Add a single subnet** — Adds individual subnets by name, network address, and network mask. Subnet names are user-configured text strings, such as `Engineering Lab 1`. • **Add a list of subnets** — Adds multiple subnets. • **Import a file with a list of subnets to add** — Adds subnets listed in an external file. Use the following formats when importing: • **Subnet names** — `Name,xxx.xxx.xxx.xxx/yy` • **Subnet addresses** — `xxx.xxx.xxx.xxx/yy`

Communication page (Rogue System Detection policy pages)

Use this page to set the intervals used for sensor communication times, and configure optional active sensor election.

Option definitions

Option	Definition
Sensor's detected system cache lifetime	Specifies how long detected systems remain in the sensor's memory cache. The maximum value for this field is 168 hours, or 7 days. The default is 5 minutes. **Note:** Systems in the sensor's memory cache are not considered new detections and the software does not scan them again for their **McAfee Agent**.

Option	Definition
Reporting time for active sensors	Specifies how often the active sensors report to the server and send their detected data. Type the number and click **hour(s)**, **minute(s)**, or **second(s)** in the list. The maximum value for this field is 168 hours, or 7 days. The default is 5 minutes.
Active sensor election	Specifies which method to use to determine the active sensors. • Click **Use ePO server to determine active sensors**. The default method. **Note:** The maximum number of active sensors is set in the server settings. ▫ **Communication time for inactive sensors** — Specify how often the inactive sensors report to the server to check whether to become active. Type the number and click **minute(s)** or **second(s)** in the list. The maximum value for this field is 1 hour. Default is 1 hour. • Click **Use Local Sensor Election** to configure the sensors and election process. ▫ Configure active sensors, either: ▫ Type the number of **active sensor(s)**. ▫ Click to set **All sensors active**. ▫ Type **Wait time for an election result** and click **second(s)** or **minute(s)**. The default is 300 seconds, or 5 minutes. ▫ Type **Wait time between active sensor elections** and click **second(s)**, **minute(s)**, or **hour(s)**. The default is 3,600 seconds or 1 hour. **Note:** This section is relevant for 4.x sensors only. ▫ Set the multicast group to receive the active sensors. Either:

Option	Definition
	▫ Type **Ipv4 multicast group** address. The default address is 239.5.6.7. ▫ Type **Ipv6 multicast group** address. The default address is ff12::1. **Note:** This section is relevant for 4.x sensors only. **Note:** You might need to change one of these default addresses if another feature is using the default. ▫ Type the **Sensor-to-Sensor communication port** number. The default is port 19001.

Detected Subnet Details page

Use this page to view the list of detected subnets in your network. Detected subnets are grouped in the following categories:

- **Contains Rogues**
- **Covered**
- **Ignored**
- **Uncovered**

From this location, select the checkbox next to subnets to perform actions on them. You can also click an individual subnet to view more details.

Option definitions

Option	Definition
Actions	Specifies the actions you can take on this **Detected Systems** table, including: • **Choose Columns** — Opens the **Select the Columns to Display** page. Use this page to select the columns of data to display on the **Detected Subnets** page. • **Export** — Opens the **Export** page. Use this page to specify the format and the package of files to

Option	Definition
	be exported. You can save or email the detected subnets. • **Detected Systems** — Specifies different actions you can perform on the selected detected system, including: ▫ **Delete** — Removes the selected subnets from the **Detected Subnets** list. Deleting subnets removes all references to them, including any rogue systems whose only interfaces are in this subnet. The next time **ePolicy Orchestrator** detects the systems in the deleted subnet, they are detected as new systems. ▫ **Ignore** — Designates the selected subnets as ignored. **ePolicy Orchestrator** disregards ignored subnets. ▫ **Include** — Includes the subnet in the **Detected Subnets** list. When a subnet has been ignored, click **Include** to bring it back into the **Detected Subnets** list. ▫ **Rename** — Changes the name of the selected subnet. ▫ **View Managed Systems** — Opens the **Managed Systems for Subnet** page. Use this page to view the systems managed by the selected subnet.
Detected Subnets Information	Specifies information about detected subnets, including: • **Contains Rogue** — Specifies whether the subnet contains rogue systems. • **Covered** — Indicates whether a Rogue System Sensor covers the displayed subnet. • **Ignored** — Indicates whether the displayed subnet is designated as ignored. • **IP Address** — Specifies the IP address of the displayed subnet. • **Subnet Mask** — Specifies the subnet mask (IP address netmask) for the displayed subnet.

Option	Definition
	• **Subnet Name** — Specifies the name of the displayed subnet. The default name for a subnet is its IP address.
Sensor Information	Specifies the IP address of the sensor, whether it is active, its last communication time, and provides a link to the **Rogue System Sensor Details** page.

Detected Subnets page

Use this page to view detected subnets. From this location, you can view details about the sensors installed on detected subnets, if any. To view subnet details, click the subnet row.

Option definitions

Option	Definition
Actions	Specifies the actions that can be performed on selected entries in the **Master Repository**, including: • **Delete** — Removes the selected subnets from the **Detected Subnets** list. Deleting subnets removes all references to them, including any rogue systems whose only interfaces are in this subnet. The next time **ePolicy Orchestrator** detects the systems in the deleted subnet, they are detected as new systems. • **Ignore** — Designates the selected subnets as ignored. **ePolicy Orchestrator** disregards ignored subnets. • **Include** — Includes the subnet in the **Detected Subnets** list. When a subnet has been ignored, click **Include** to bring it back into the **Detected Subnets** list. • **Rename** — Changes the name of the selected subnet. • **View Managed Systems** — Opens the **Managed Systems for Subnet** page.

Detected System Interfaces Details page

Use this page to view details of detected system interfaces.

Option definitions

Option	Definition
Detected System Interfaces Information	Specifies the details of the detected system interface, including: • **Last Detected Time** — Specifies the date and time of the last detection of the interface. • **IP Address** — Specifies the IP address of the interface. • **IPv6 Address** — Specifies the IPv6 address of the interface. • **MAC Address** — Specifies the MAC address of the interface. • **Organization Name (OUI)** — Specifies the manufacturer of the interface as identified by the MAC address, which includes the organizationally unique identifier. • **Organizationally Unique ID (OUI)** — Specifies the portion of the MAC address that identifies the manufacturer of the device. • **Source** — Specifies the source of the last detection of the interface.
Related Items	Provides links to information related to the detected system interface, including: • **Go to related Detected Subnets** — Links to the **Detected Subnets Details** page for the subnet on which the interface is located. • **Go to related Detected Systems** — Links to the **Detected Systems Details** page that provides details about the system associated with the interface.

Detected Systems Details page

Use this page to view the details of an individual detected system.

Option definitions

Option	Definition
Actions	Specifies the actions that can be performed on selected entries in the master repository, including: • **Add to Exceptions** — Moves the selected systems to the **Exceptions** list. This tells **ePolicy Orchestrator** not to manage the system. For example, printers or routers. • **Add to System Tree** — Displays the **Add to System Tree** page, where you can add specific systems to selected groups in your **McAfee ePO System Tree**. • **Delete** — Removes the selected systems from the **Detected Systems** list. Deleting systems removes all references to them. The next time **ePolicy Orchestrator** detects the systems, they are detected as new rogue systems. • **Edit Comment** — Opens the **Edit Comment** dialog box. User-supplied comments are displayed in detected system details. • **Merge Systems** — Opens the **Merge Systems** page. Select between two and six systems to be merged into a single detected system. Use this option to combine multiple detected systems or system interfaces into a single detected system. For example, when you have a system in your network that has multiple NICs (Network Interface Cards) that are being detected as separate systems, but have not been automatically matched and merged. • **Deploy Agents** — Opens the **Deploy McAfee Agents** page, where you specify, configure, and run agent deployment server tasks. • **Query Agent** — Opens the **Query McAfee Agent Results** page, which provides the name or IP address of the detected system and details about the agent installed on it. • **Remove from Exceptions** — Removes the selected systems from the **Exceptions** list. This list tells **ePolicy Orchestrator** to manage the systems, and returns them to their original category. For

Option	Definition
	example, managed systems return to the managed category.
Additional Detail for Managed Systems	Links to the **ePolicy Orchestrator System Details** page for this system.
Detected System Interfaces	Specifies the detected system interface by number and details about each interface, including: • **IP Address** — Specifies the IP address of the interface. • **Last Detected Time** — Specifies the date and time of the last detection of the interface. • **MAC Address** — Specifies the MAC address of the interface. • **Organization Name (OUI)** — Specifies the manufacturer of the interface as identified by the first three digits of the MAC address, which are the organizationally unique identifier (OUI). • **Source** — Specifies the source of the last detection of the interface.
Detected Systems Information	Specifies information about the detected system you are viewing, including: • **Agent GUID** — Specifies the globally unique identifier (GUID) of the agent deployed to the system. • **Agent Version** — Specifies the version of the agent deployed to the system. • **Canonical Name** — Displays the friendly name of the system. • **Comments** — Displays user comments about the system. • **Computer Name** — Specifies the name of the system. • **DNS Name** — Specifies the domain name of the system. • **Domain** — Specifies the domain the system is on.

Option	Definition
	• **McAfee ePO Server Name** — Specifies the name of the **McAfee ePO** server that manages this detected system. • **Exception** — Specifies whether the system is marked as an exception. • **Exception Category** — Specifies which exception category this system belongs to. • **Is New Detection** — Specifies whether this system is a new detection. • **Last Agent Communication** — Specifies the date and time of the last communication from the agent deployed to the system. • **Last Detected IP Address** — Specifies the last detected IP address of the system. • **Last Detected MAC Address** — Specifies the last detected MAC address of the system. • **Last Detected Time** — Specifies the date and time of the last detection of the system. • **Last Detected Organization Name** — Specifies the organization name of the system at its last detection, for example, Dell. • **NetBIOS Comment** — Specifies the NetBIOS comment for the detected system, if any. • **OS Family** — Specifies the family of the operating system. • **OS Platform** — Specifies the operating system installed on the system. • **OS Version** — Specifies the version number of the operating system installed on the system. • **OUI** — Specifies the Organizationally Unique Identifier of the detected system. The OUI identifies the manufacturer of the detected system, for example, Dell. • **Recorded Time** — Specifies the time this system was first detected and recorded in the **McAfee ePO** database. • **Rogue Action** — Specifies the action being performed on a rogue system, for example, **Agent Push in Progress**. • **Rogue State** — Specifies the rogue state of a detected system, for example, Inactive Agent.

Option	Definition
	• **Source** — Specifies the source of the last detection of the system, such as Broadcast or DHCP. • **Users** — Specifies the users currently associated with the system as defined by the NetBIOS call, which is typically the currently logged-on user.

Detected Systems page

This is the main page for monitoring detected systems in your network. Use this page to monitor and manage the detected systems, subnets, and sensors on your network by using the following monitors and table:

- **Subnet Status** monitor
- **Overall System Status** monitor
- **Rogue System Sensor Status** monitor
- **Top 25 Subnets** table

Option definitions

Option	Definition
Show/Hide Filter	Shows or hides the filter options
Quick Find	Allows you to type search strings to find detected systems. Click **Apply** to perform the search. You can search for detected systems based on their IP address and MAC address. **Note:** • Don't include colons when searching for detected systems based on their MAC address. • Use the **starts with** filter to search for detected systems based on their IP address. For example, to search for detected systems whose IP address start with 172.60, type `172.60` in the **Quick Find** text box.
Clear	Removes any text from the **Quick find** text entry box.

Option	Definition
Show selected rows	Displays only the rows you have selected.
Actions	Specifies the actions you can perform on the selected rogue systems, including: • **Add to Exceptions** — Allows you to optionally assign a category to each item you designate as an exception. • **Add to System Tree** — Allows you to add an item to the **System Tree**. • **Choose Columns** — Opens the **Select the Columns to Display** page. Use this to select the columns of data to display on the **Server Task Log** page. • **Delete** — Deletes the selected systems from the **Rogue System Interfaces by Subnet** table. Systems deleted from this table reappear the next time a sensor detects them. • **Deploy Agent** — Launches the **Deploy Agents** page, where you configure the deployment settings with which to deploy agents to the systems of the selected group. • **Export Table** — Opens the **Export** page. Use this page to specify the format and the package of files to be exported. You can save or email the exported file. • **Query Agent** — Displays only the rows you have selected.

Detected Systems page

Use this page to view the list of detected systems on your network by category. Detected systems are grouped in the following categories:

- **Exceptions**
- **Inactive**
- **Managed**
- **Rogue**

From this location, select the checkbox next to systems to perform actions on them. You can also click an individual system to view more details.

Option definitions

Option	Definition
Actions	Specifies the actions you can perform on detected systems, including: • **Choose Columns** — Opens the **Select the Columns to Display** page. Use this to select the columns of data displayed in the **Detected Systems** page. • **Detected Systems** — Specifies the actions you can perform on the selected detected systems, including: ▫ **Add to Exceptions** — Moves the selected systems to the **Exceptions** list. This tells **ePolicy Orchestrator** not to manage the system. For example, printers or routers. ▫ **Add to System Tree** — Displays the **Add to System Tree** page, where you can add specific systems to selected groups in your **McAfee ePO System Tree**. ▫ **Delete** — Removes the selected systems from the **Detected Systems** list. Deleting systems removes all references to them. The next time **ePolicy Orchestrator** detects the systems, they are detected as new rogue systems. ▫ **Deploy Agents** — Opens the **Deploy McAfee Agent** page, where you specify, configure, and run agent deployment server tasks. ▫ **Merge Systems** — Opens the **Merge Systems** page. Select between 2 and 6 systems to be merged into a single detected system. Use this option to combine multiple detected systems or system interfaces into a single detected system. For example, when you have a system in your network that has multiple NICs (Network Interface Cards) that are detected as separate systems, but have not been automatically matched and merged. ▫ **Ping** — Sends an ICMP echo to the selected system to verify that it can be reached.

Option	Definition
	▫ **Query Agent** — Opens the **Query McAfee Agent Results** page, which provides the name or IP address of the detected system and details about the agent. ▫ **Remove from Exceptions** — Removes the selected systems from the **Exceptions** list. This list tells **ePolicy Orchestrator** to manage the systems, and returns them to their original category. For example, managed systems return to the managed category. • **Rogue Sensors** — Specifies the actions you can perform on the selected rogue sensor, including: ▫ **Edit Comment** — Opens the **Edit Comment** dialog box. User-supplied comments are displayed in **Detected System** details. • **Export Table** — Opens the **Export** page. Use this page to specify the format and the package of files to be exported. You can save or email the detected subnets.

Detection page (Rogue System Detection policy pages)

Use this page to specify detection settings for **Rogue System Detection**.

Option definitions

Option	Definition
DHCP monitoring	Specifies the settings for Dynamic Host Configuration Protocol (DHCP) monitoring. When you enable **DHCP monitoring**, a single sensor installed on a DHCP server can monitor all systems and subnets that it serves: **Note:** This section is relevant for 4.x sensors only. • **Disabled** — Select this box to disable DHCP monitoring.

Option	Definition
	• **Report only systems whose IP address is inside the sensor's network** — Select this box to ignore VLAN traffic. This option is overridden when **DHCP monitoring** is enabled. • **Enabled** — Select this box to enable DHCP monitoring. **Note: DHCP monitoring** is disabled by default.
Device details detection	Specifies the settings for Subnet Port Scanning, which scans the ports your network uses to detect specific information about the devices connected to it: **Note:** This section is relevant for 4.x sensors only. • **Enabled** — Select this box to enable device details detection and allow the sensor to scan your network ports. Then configure the following settings as needed: ▫ **Do not run OS detection against devices on these networks** — Prevents use of OS detection to user-specified subnets. Enter a subnet's network address and click **Add To List** to specify a network. Select a network from the list and click **Remove From List** to permit port scanning on that network. ▫ **Run OS detection only against devices on these networks** — Limits use of OS detection to user-specified subnets. Enter a subnet's network address and click **Add To List** to specify a network. Select a network from the list and click **Remove From List** to stop port scanning on that network. ▫ **Scan detected systems for OS details** — Select this box to allow the sensor to scan detected systems for detailed information about a device's

Option	Definition
	operating system. Then configure the following settings as needed: ▫ **OS scanning interval** — Specify the operating system scanning interval. Type the number and click **hour(s)**, **minute(s)**, or **second(s)** in the list. Default is 30 seconds. ▫ **OS scanning initial delay** — Specify the operating system scanning interval delay. Type the number and click **hour(s)**, **minute(s)**, or **second(s)** in the list. The default is 60 seconds. ▫ **How long to cache OS data** — Specify how long to cache operating system scan data. Type the number and click **second(s)**, **minute(s)**, **hour(s)**, or **day(s)**. Default is 1 day. ▫ **Scan systems marked as exceptions** — Click to scan systems, such as routers and printers, even if they have been designated as exceptions. This setting is disabled default. ▫ **Use OS detection on all networks to determine detailed device information** — Tells sensors to scan all subnets to discover detailed information about detected systems. This setting is the default option.
Report on self-configured subnets	Select the **Enabled** box to enable reporting on self-configured subnets. This setting prevents subnets that have a netmask of /32 from being ignored. **Note:** This section is relevant for 4.x sensors only.
Sensor Scanning	Select **Use active zero-configuration resolution** to enable the sensor to send multicast DNS requests. This setting is enabled by default. Select **Use DNS queries for DNS name resolution** to enable the sensor to query DNS servers for DNS names. This setting is enabled by default.

Option	Definition
	Note: This section is relevant for 5.0 sensors only.

Edit Detected System Compliance page

Use this page to edit the compliance settings for **Rogue System Detection**. Compliance settings affect how **Rogue System Detection** categorizes detected systems, and how coverage information is displayed in status monitors on the **Detected Systems** page.

Option definitions

Option	Definition
Covered Subnets	Specifies the required coverage levels for covered subnets so that the color codes represent your requirements. These color codes affect the **Subnet Status** monitor on the **Detected Systems** page.
Detected System definitions	Defines the categories for detected systems and specifies the time periods used in each category, including: • **Exception** — Systems you have designated as exceptions. • **Inactive** — Systems categorized as rogues that sensors have not detected in a user-configured number of days. • **Managed** — Systems that have an agent in the **McAfee ePO** database that has communicated to the server within a user-configured number of days. • **Rogue** — Systems that don't have an agent, have an agent that is not in the **McAfee ePO** database, or have an agent in the **McAfee ePO** database whose last communication is older than the number of days specified in the managed systems field.

Option	Definition
	Note: The maximum number of days for managed systems must be shorter than the number of days specified for Inactive systems. The greatest value for either field is 999 days. Set these values to time periods short enough to provide realistic information about your network. The default values are 20 days and 45 days, respectively.
ePO Servers	Allows you to specify additional **McAfee ePO** servers whose systems might come onto your network, that you don't want to be detected as rogue systems.
Sensor Health	Specifies the ratio of active to missing sensors for sensor health, so that the color codes represent your requirements. These color codes affect the **Rogue System Sensor Status** monitor on the **Detected Systems** page.
System Compliance	Specifies the required levels for compliant systems so that the color codes represent your requirements. These color codes affect the **Overall System Status** monitor on the **Detected Systems** page.

Edit Detected System Matching page

Use this page to edit the matching settings for **Rogue System Detection**. Matching settings affect how **Rogue System Detection** determines if newly detected interfaces are on an existing system, and how **Rogue System Detection** handles them when they are found.

Option definitions

Option	Definition
Alternative McAfee Agent Ports	Specifies alternate ports to use when querying a detected system for a **McAfee Agent**.

Option	Definition
Matching Detected Systems	Defines the properties that determine when to match newly detected system interfaces to an existing detected system.
Matching Managed Systems	Defines the properties that determine when to match newly detected system interfaces to an existing managed system.
Static IP Ranges for Matching	Specifies the static IP address ranges for use when matching static IP addresses. **Note:** The IP addresses in the range can be either IPv4 or IPv6 addresses.

Edit Detected System OUIs page

Use this page to specify how your OUI (Organizationally Unique Identifier) file is updated. The OUI file allows **ePolicy Orchestrator** to identify product information about managed systems, such as manufacturer.

Option definitions

Option	Definition
Last Updated	Specifies the last time **McAfee ePO** server updated your OUI file.
Update from	Specifies the source used to update the OUI file, including: • **File Upload** — Use this option to manually upload a text file (.txt) containing an updated OUI list. Choosing this option disables the ability to save default settings for this page. • **Server location** — Specifies a location on the **McAfee ePO** server that contains an updated OUI file. • **URL** — Specifies a website or other resource that contains an updated OUI file.

Edit Detected Systems Exceptions Categories page

Use this page to edit, add, or remove detected system exception categories.

Option definitions

Option	Definition
Categories	**Add new categories** — Allows you to add new exception categories for detected systems. **Note:** The Rogue System Sensor cannot be installed on a detected system that has been added to an exception category.
	Name — Displays the name of any previously configured exception categories for detected systems.
	Description — Displays the description of any previously configured exception categories for detected systems.
	Change — Edits the detected system exception category.
	Delete — Deletes the detected system exception category.

Edit Permission Set: Rogue System Detection page

Use this page to select permissions for **Rogue System Detection**.

Option definitions

Option	Definition
Create and edit Rogue System information; manage Rogue Sensors	Grants the ability to deploy sensors, create and edit **Rogue System Detection** configuration, and other data.

Option	Definition
Create and edit Rogue System information; manage Rogue Sensors; Deploy Agents and Add to System Tree	Grants full access to **Rogue System Detection**. **Note:** The **Deploy Agents** and **System Tree** permissions affected by this permission set apply only to detected systems.
No permissions	Grants no access to **Rogue System Detection**. A user with this level of permissions cannot access any **Rogue System Detection** assets.
View Rogue System information	Grants only the ability to view **Rogue System Detection** information. A user granted this level of permissions cannot create, edit, or modify information.

Edit Permission Set: Rogue System Sensor page

Use this page to select permissions for the Rogue System Sensor.

Option definitions

Option	Definition
Rogue System Detection : Policy	Controls access to the Rogue System Sensor. Choose from the following access levels: • **No permissions** — Grants no access to policies. • **View Settings** — Grants only the ability to view sensor policies. • **View and change settings** — Grants full access to sensor policies.
Rogue System Detection : Tasks	Controls access to tasks generated by the Rogue System Sensor. Choose from the following access levels: • **No permissions** — Grants no access to **Rogue System Detection** tasks.

Option	Definition
	• **View Settings** — Grants only the ability to view **Rogue System Detection** tasks. • **View and change settings** — Grants full access to **Rogue System Detection** tasks.

Edit Rogue System Sensor page

Use this page to edit the settings for the Rogue System Sensor.

Sensor settings affect how many sensors can be active on a subnet at one time, how long sensors stay active, and how long the **McAfee ePO** server waits for a sensor to call in before designating it as missing.

Option definitions

Option	Definition
Active Period	Specifies the maximum amount of time before the server asks a sensor to sleep, to allow a new sensor to become active. The maximum active period for a sensor is 24 hours (1,440 minutes).
Sensors per Subnet	Specifies the maximum number of active sensors on a subnet at any time. Active sensors report system detections and other information during their active period.
Sensor Scanning	Specifies a list of MAC addresses or OUIs that sensors do not scan, regardless of the sensor's policy. For version 5.0 sensors, you can add a list of IP addresses or subnet masks that sensors do not scan actively. The sensor does not scan these systems regardless of the sensor's policy settings.
Sensor Timeout	Specifies the maximum amount of time a sensor can be out of contact before being designated as missing. The maximum sensor timeout period is 7 days (168 hours or 10,080 minutes).

Option	Definition
Server Settings Revision ID	Specifies the revision number of the setting. The ID is incremented every time the **Server Settings** are saved.

Deploy McAfee Agent page

Use this page to send and install agents to selected managed systems.

Option definitions

Option	Definition
Target systems	Displays the names of the systems that were selected when you clicked **Deploy Agents**.
Agent version	Specifies the version of the agent to send and install on the selected systems. Agent versions that are available depends on which agent installation packages are checked in to the Master Repository. **Note:** To deploy agents to non-Windows systems, the target systems must be configured to support SSH network protocol. For more information on configuration, see the product documentation provided with your target systems Operating System (OS).
Installation options	Specifies the agent installation options available, including: • **Install only on systems that do not have an agent** — Sends the agent installation package only to systems without an agent installed. When deselected, sends the agent installation package to all selected systems, regardless of whether the agent is already installed on them. • **Force installation over existing version** — Replaces existing agents within the selected group

Option	Definition
	with the selected versions. This option is not available when you select **Install only on systems that do not have an agent**.
Installation path	Specifies the path on the client system (default is **<system_drive>\McAfee\Common Framework**) where you want to install the agent. The location you specify must exist on managed systems.
Credentials for agent installation	Specifies the domain name, user name, and password of the user account with which to install the agent on selected systems.
Number of attempts	Specifies the number of deployment attempts before it quits. Type **0** for continuous attempts.
Retry interval	Specifies the interval in seconds between deployment attempts.
Abort after	Specifies the number of minutes after the start of the attempted agent deployment before the deployment quits.
Push Agent Using	Select the connection used for the deployment as either: • **Selected Agent Handler** — Select the server from the list. • **All Agent Handlers**.

Import/Export Exceptions page

Use this page to import or export exceptions. From this location, you can import exceptions by MAC address or from a file, and export exceptions to a file.

Option definitions

Option	Definition
Import Exceptions tab	**Choose method of Importing** — Specifies the method used for importing systems to the exceptions category in different formats, including: • **By Text** — Imports exceptions by MAC address. Format MAC addresses using unseparated hexadecimal characters, colons, or hyphens. For example, xx:xx:xx:xx:xx:xx. • **By File** — Files imported must be formatted as a single column list of MAC addresses.
Export Exceptions tab	**Exporting** — Exports a list of systems, categorized as exceptions, to a file.

Add to System Tree page

Use this page to add a system to the **ePolicy Orchestrator System Tree**.

Option definitions

Option	Definition
Systems to Add	Specifies the detected systems that you have selected to be added to the **System Tree**.
System Tree Location	Specifies the location on the **System Tree** where you want to add the selected systems. Click **Browse** to open the **Select System Tree Group** dialog box, which allows you to navigate to the location where you want to add the selected systems.
Duplicate System Names	Allows duplicate entries to be added to the **System Tree**. For example, you might have two systems with the same name. Allowing duplicate entries permits you to add the system with the duplicate name to the **System Tree**.

Managed System for Subnet page

View the list of managed systems on the selected subnet. From this location, select the checkbox next to systems to perform actions on them. You can also click an individual system to view more details.

Option definitions

Option	Definition
Apply Tag	Applies tag names that are used for sorting systems on your network. • **Server** • **Workstation**
Assign Policy	Opens the **Assign Policy** page for the selected systems.
Change Sorting Status	Allows you to disable or enable **System Tree** sorting on the selected systems.
Clear Tag	Removes previously applied tags from the selected systems.
Delete	Removes the selected systems from the **Detected Systems** list. Deleting systems removes all references to them from the **McAfee ePO** database. The next time **ePolicy Orchestrator** detects the systems, they are detected as new systems.
Deploy Agents	Opens the **Deploy McAfee Agent** page for the selected systems.
Edit Description	Allows you to edit the user-defined description of the selected systems.
Exclude Tag	Specifies system tags that can be used to exclude groups of systems when sorting. • **Server** • **Workstation**

Option	Definition
Export Systems	Exports the selected systems to an external file.
Filter	Specifies which managed systems in this subnet are shown in the table. • **In Blacklist** — Shows the managed systems in this subnet listed in the **Sensor Blacklist**. • **Show All** — Shows all managed systems in this subnet. • **With Sensors** — Shows the managed systems in this subnet with sensors installed. • **Without Sensors** — Shows the managed systems in this subnet without sensors installed.
Modify Policies on a Single System	Opens the **Policy Assignment** page for the selected system.
Modify Tasks on a Single System	Opens the **Client Tasks** page for the selected system.
Move Systems	Opens the **Select the New Group** page to move the selected systems.
Options	Specifies the available options. • **Choose Columns** — Choose the columns of data to display on the **Covered Subnets** page. • **Export Table** — Exports the table of data to a user-specified format and location.
Show Agent Log	Opens the **Agent Log** page.
Sort Now	Sorts the selected systems according to their tags.
Test Sort	Performs a test sort on the selected systems, and opens the **Test Sort** page.
Wake Up Agents	Opens the **Wake Up McAfee Agent** page.

Merge Systems page

Use this page to manually merge detected systems into a single detected system. The detected systems listed in the **Source System** columns are combined into a single record with the properties listed in the **Target System** column.

Option definitions

Option	Definition
Agent GUID	Specifies the globally unique identifier (GUID) of the agent deployed to the system.
Canonical Name	Displays the friendly name of the system. The friendly name of a system is the least complex unique name available to identify the system. For example, a DNS name is less complex than an MAC address. Therefore, the DNS name is displayed instead of the MAC address, if it is available.
Close	Cancels the merge operation and reopens the previous page.
Comments	Displays user comments about the system.
Computer Name	Specifies the name of the system.
DNS Name	Specifies the domain name of the system.
Domain	Specifies the domain the system is on.
Exception	Specifies whether the system is selected as an exception.
Ignored	Specifies whether the system has been ignored.
Last Detected IP Address	Specifies the last detected IP address of the system.
Last Detected IPv6 Address	Specifies the last detected IPv6 address of the system.

Option	Definition
Last Detected MAC Address	Specifies the last detected MAC address of the system.
Last Detected Time	Specifies the date and time of the last detection of the system.
Merge	Merges the systems detailed in the **Source System** columns into one detected system, with the details listed in the **Target System** column.
NetBIOS Comment	Specifies the NetBIOS comment for the detected system.
OS Family	Specifies the family of the operating system.
OS Platform	Specifies the operating system installed on the system.
OS Version	Specifies the version number of the operating system installed on the system.
Users	Specifies the user logged on to the system at the last detected time.

General page (Rogue System Detection policy pages)

Use this page to configure general policy settings for **Rogue System Detection**.

Option definitions

Option	Definition
Rogue System Sensor	Enables sensors when they are deployed.
Server name or IP address	Specifies the name or IP address of the system where your **McAfee ePO** server is installed. **Rogue System Detection** treats agents managed by any

Option	Definition
	other **McAfee ePO** server as alien agents. Therefore, the systems where those alien agents are deployed are identified as rogue systems. The default value in this field is the IP address of the system where **Rogue System Detection** is installed. When changing this value, use standard IP address format (xxx.xxx.xxx.xxx), DNS name, or the FQDN.
Log File Settings	Specifies whether the software logs only messages with **Error** and **Critical** priority or logs all messages. **Note:** This section is relevant for 5.0 sensors only.
Policy Revision ID	Specifies the revision number of the policy, which is incremented every time you save the policy. **Note:** This section is relevant for 5.0 sensors only.

Import Sensor Blacklist page

Use this page to import systems to the **Rogue Sensor Blacklist**.

Option definitions

Option	Definition
Choose method of importing	Specifies the method for importing systems into the **Rogue Sensor Blacklist**, including: • **Manually add systems to the Sensor Blacklist** — Specifies whether to add systems manually by system name, with each system separated by a new line. System names must be formatted as standard system names, for example, xx-100. • **Import file with list of systems to add to the Sensor Blacklist** — Specifies whether to add

Option	Definition
	systems by uploading a text file containing a list of system names. The list separates each system by a new line.

Interfaces page (Rogue System Detection policy pages)

Use this page to specify which interfaces sensors listen to.

Note

This page is relevant for 4.x sensors only.

Option definitions

Option	Definition
Initial Interface Binding	Select this box to tell sensors to listen only to the interfaces whose IP addresses were present at the time of installation.
Listen only on interfaces with IP addresses in these networks	Tells sensors to listen to interfaces only in user-specified networks. Type a network address and click **Add To List** to specify a network. Select a network from the list and click **Remove From List** to stop listening to interfaces on that network. IP addresses must use standard IP address format followed by the two-digit Classless Inter-Domain Routing (CIDR) that specifies the subnet mask.
Do not listen on interfaces with IP addresses in these networks	Tells sensors not to listen to interfaces in user-specified networks. Type a network address and click **Add To List** to specify a network. Select a network from the list and click **Remove From List** to allow sensors to listen to interfaces on that network. IP addresses must use standard IP address format followed by the two-digit CIDR number that specifies the subnet mask.

Overall System Status monitor

Use the **Overall System Status** monitor to view the status of all detected systems on your network by category. From this location, you can view the list of systems that make up a category by clicking it. You can also import or export systems from the **Exceptions** list by clicking **Import/Export Exceptions**.

The color-coded title bar across the top of the status monitor displays the percentage of total systems on your network that are compliant. This percentage represents the ratio of systems that are managed or designated as exceptions, to total detected systems. User-configured options based on this ratio determine the color of the title bar. There are three color codes: green, orange, and red. They represent good, marginal, and poor status, respectively. Only managed systems are compliant.

Option definitions

Option	Definition
Exceptions	Specifies the number of systems on your network that are designated as exceptions. Exceptions are systems that you don't want **ePolicy Orchestrator** to manage.
Import/Export Exceptions	Displays the **Import and Export Exceptions** page.
Inactive	Specifies the number of systems on your network identified as rogues not detected by a sensor in a specified time period.
Managed	Specifies the number of systems on your network that **ePolicy Orchestrator** manages.
Rogue	Specifies the number of systems on your network that **ePolicy Orchestrator** does not manage.

Query McAfee Agent Results page

Use this page to view results from a **McAfee Agent** query.

Option definitions

Option	Definition
Detected System	Specifies the names of systems on which the **McAfee Agent** query was performed.
Agent Details	Specifies details about the agents deployed to selected detected systems, including: • **Computer Name** — Specifies the name of the system the agent is deployed to. • **McAfee ePO Server Name** — Specifies the name of the server that the agent reports to. • **Agent Version** — Specifies the version of the agent deployed to the system. • **Agent GUID** — Specifies the globally unique identifier (GUID) of the agent deployed to the system. When the query is unsuccessful, you can click **Retry**, which performs another query on this agent.

Rogue Sensor Blacklist Details page

Use this page to view details about a sensor in the **Rogue Sensor Blacklist**. From this location, you can view information about the sensor, the system it is on, and remove the sensor from the blacklist.

Option definitions

Option	Definition
Rogue Sensor Blacklist Information	Provides information about the selected system on the **Rogue Sensor Blacklist**, including: • **Agent GUID** — Specifies the globally unique identifier (GUID) of the agent deployed to the system. • **Computer Name** — Specifies the name of the system. • **DNS Name** — Specifies the domain name of the system. • **Domain** — Specifies the domain the system is on.

Option	Definition
	• **IP Address** — Specifies the IP address of the system. • **MAC Address** — Specifies the MAC address of the system.
Actions	Specifies the actions you can perform on the system, including: • **Remove** — Removes the system from the **Rogue Sensor Blacklist**.

Rogue Sensor Blacklist page

Use this page to view the list of rogue systems placed on the **Rogue Sensor Blacklist**.

Option definitions

Option	Definition
Show/Hide Filter	Shows or hides the filter options.
Show selected rows	Select this box to display only the rows you have selected.
Selected Row Actions	Specifies the actions that can be performed on selected systems in the **Rogue Sensor Blacklist**, including: • **Remove** — Removes the selected systems from the sensor blacklist and returns them to their previous category. For example, if you add a managed system to the **Rogue Sensor Blacklist**, the software returns it to the **Managed** list when you remove it from the blacklist.
Table Actions	Specifies the actions that you can perform on the **Rogue Sensor Blacklist** page, including: • **Choose Columns** — Choose the columns of data to display on the **Rogue Sensor Blacklist** page.

Option	Definition

	• **Export Table**— Exports the table of data to a user-specified format and location
	• **Rogue Sensor** — Specifies actions you can take on the **Rogue Sensor Blacklist**.
	  ▫ **Export Blacklist** — Downloads a list of the systems in the **Rogue Sensor Blacklist** table in XML format.
	  ▫ **Import Blacklist** — Opens the **Import Sensor Blacklist** page, where you can import systems to the sensor blacklist manually by adding system names, or by selecting a file to import.

Rogue System Sensor Details page

Use this page to view Rogue System Sensor details.

Option definitions

Option	Definition
Action	Specifies the actions that you can perform on this sensor, including: • **Delete Sensor** — Removes the sensor from the system. • **Edit Description** — Changes the description of the Rogue System Sensor.
Rogue System Sensor Information	Specifies details about the Rogue System Sensor installed on this system, including: • **Agent GUID** — Specifies the globally unique identifier (GUID) of the agent deployed to the system. • **Computer Name** — Specifies the name of the system this sensor is installed on. • **Description** — Specifies a user-defined description. • **Installed** — Specifies whether this sensor is installed.

Option	Definition
	• **Last Communication Time** — Specifies the date and time of the last communication from the agent deployed to the system. • **Sensor Name** — Specifies the name of the sensor. • **Sensor Type** — Specifies the type of sensor. • **Sensor Version** — Specifies the version number of the sensor on this system. • **Status** — Specifies the status of this sensor. For example, **Missing**.
Sensor's Managed System Information	Specifies the name of the system where the sensor is installed, and links to the **ePolicy Orchestrator** system details for the system.
Sensor's Subnet Information	Specifies information about systems detected by the sensor, including: • **Covered** — Specifies the detected system coverage. • **Ignored** — Specifies whether the detected system is ignored. • **IP Address** — Specifies the detected system IP address. • **Subnet Mask** — Specifies the detected system subnet mask.

Rogue System Sensor page

Use this page to view the list of Rogue System Sensors on your network, which are grouped in the following categories:

- **Active**
- **Missing**
- **Passive**
- **Uninstalled**

From this location, select the checkbox next to sensors to perform actions on them. You can also click an individual sensor to view more details.

Option definitions

Option	Definition
Selected Row Actions	Specifies the actions that you can perform on Rogue System Sensors, including: • **Delete Sensor** — Removes the selected sensor from the system it is installed on. • **Edit Description** — Changes the user-defined description of the Rogue System Sensor.
Table Actions	Specifies the available options, including: • **Choose Columns** — Choose the columns of data to display on the **Rogue System Sensor** page. • **Rogue System Sensor Export Table** — Exports the table of data to a user-specified format and location.

Subnet Status monitor

Use the **Subnet Status** monitor to view the status of subnets in your network by category. From this location, you can view the list of subnets that make up a category by clicking it. You can also add subnets to your **McAfee ePO** server by clicking **Add Subnet**.

The software displays the percentage of covered subnets using a color-coded title bar across the top of the status monitor. This percentage represents the ratio of covered subnets to uncovered subnets. The software determines the color of the title bar based on this ratio. There are three color-codes: green, orange, and red. They represent good, marginal, and poor status, respectively.

Option definitions

Option	Definition
Add Subnet	Displays the **Add Subnet** page.
Contains Rogues	Specifies the number of covered subnets on your network that contain rogue systems.

Option	Definition
Covered	Specifies the number of subnets on your network that are covered. Covered subnets have 2 active sensors.
Uncovered	Specifies the number of subnets on your system that do not have two active sensors.

Top 25 Subnets table

Use the **Top 25 Subnets** table to view the 25 subnets on your network that contain the most rogue systems.

Note

The systems in the highlighted subnet in the **Top 25 Subnets** list appear to the right in the **Rogue System Interfaces by Subnet** pane.

Option definitions

Option	Definition
Ignore	Designates as ignored the highlighted subnet in the **Top 25 Subnets** list. **ePolicy Orchestrator** does not monitor ignored subnets.
Selected Row Actions	Specifies the actions that can be performed on entries in **Rogue System Interface by Subnet** table, including: • **Add to Exceptions** — Moves the selected rogue systems to the **Exceptions** list. Check the box next to a system to enable this button. • **Add To System Tree** — Displays the **Add To System Tree** page. • **Deploy Agent** — Opens the **Deploy McAfee Agent** page where you specify, configure, and run agent deployment server tasks. • **Query Agent** — Opens the **Query McAfee Agent Results** page, which provides the name or IP

Option	Definition
	address of the detected system and details about the agent installed on it.
Table Actions	Specifies the actions you can take on the **Top 25 Subnets** table, including: • **Choose Columns** — Choose the columns of data to display on the **Covered Subnets** page. • **Export Table** — Exports the table of data to a user-specified format and location.

COPYRIGHT

Trellix