Product Guide
Revision A

McAfee® Rogue System Detection 4.7.1

For use with ePolicy Orchestrator 4.6.3-5.0.0 Software

Detecting rogue systems

Unprotected systems, referred to as *rogue systems*, are often the weak spot of any security strategy, creating entry points that viruses and other potentially harmful programs can use to access your network.

Rogue System Detection provides near real-time discovery of rogue systems through the use of a Rogue System Sensor installed throughout your network. The sensor listens to network broadcast messages and DHCP responses to detect systems connected to the network.

When a sensor detects a system on the network, it sends a message to the McAfee ePO server. The server then checks whether the detected system has an active agent installed. If the detected system is unknown to the server, Rogue System Detection provides information to ePolicy Orchestrator to allow you to take remediation steps, which include alerting administrators and automatically deploying an agent to the system.

What are rogue systems

Rogue systems are systems that access your network, but are not managed by your McAfee ePO server. Even in a managed network environment, some systems might not have an active McAfee Agent on them. These might be systems that frequently log on and off the network, like test servers, laptops, or wireless devices.

A rogue system is any device on your network with a network interface card (NIC). On systems with multiple NICs, each resulting interface is identified as a separate system. When these interfaces are detected, they appear as multiple rogue interfaces.

You can specify how the systems with multiple interfaces are matched in the same manner you use to specify how detected systems are matched. Identifying these systems and their interfaces, and managing them with Rogue System Detection help provide the network security your organization needs.

Rogue System Detection interface and system definitions

For Rogue System Detection, each of these terms has a unique meaning and should not be used interchangeably.

- **Interface** — Rogue System Detection binds to an interface; a single system can have multiple interfaces because it has multiple NIC cards, or because the system is connected to multiple subnets and the same NIC is given multiple IP addresses.
- **System** — In Rogue System Detection, a system has a specific DNS Name and OS Platform, which appears in the Detected Systems Details.

Each system can have multiple interfaces in the Detected System Interfaces list.

Rogue System Detection states

Rogue System Detection uses different states to categorize systems, sensors, and subnets, making it easier to monitor and manage your network.

These states determine the following:

- Overall system status
- Rogue System Sensor status
- Subnet status

The Detected Systems page displays information on each of these states through corresponding status monitors. This page also displays the 25 subnets with the most rogue system interfaces in the **Top 25 Subnets** list and the adjacent **Detected System Interfaces by Subnet** table. See *Subnet status* for additional monitor details.

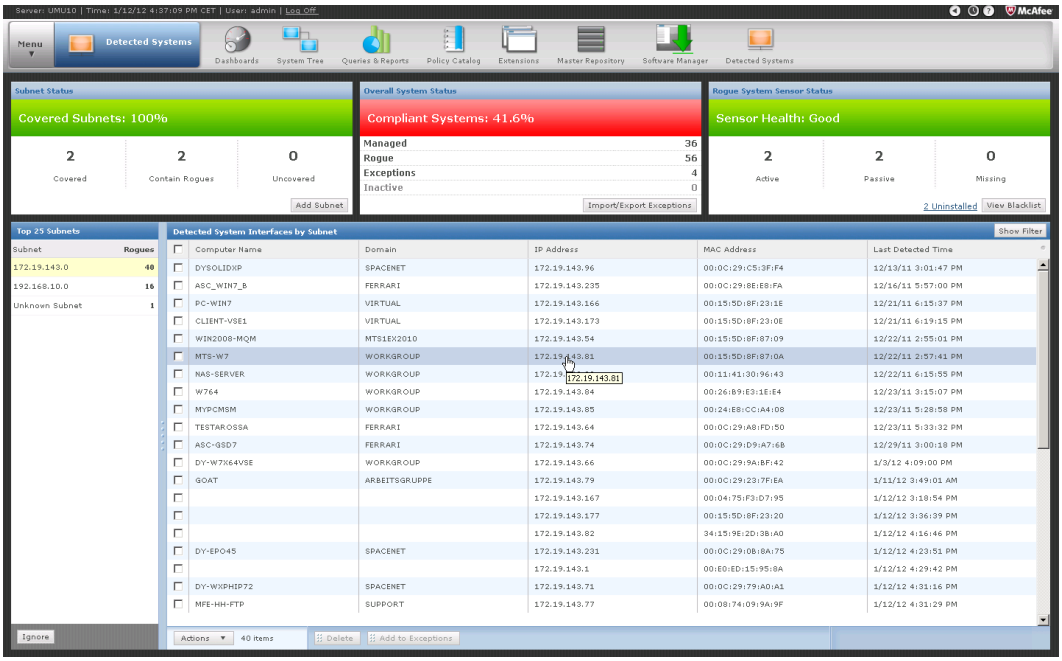

Figure 1 Detected Systems page

The **Top 25 Subnets** list and **Detected System Interfaces by Subnet** table are linked together. The list on the left, **Top 25 Subnets**, is the top 25 most rogue-infested subnets. It is a not a complete list because you could have many more subnets with rogue systems. In the list, you can click **Ignore** to ignore a subnet. This doesn't delete the subnet, it means *I know I can get detections on this subnet, but I don't want to see them*.

McAfee recommends you *not* choose to ignore subnets. If you ignore subnets you have decided that a subnet *can* have rogue systems connected.

The **Detected System Interfaces by Subnet** table allows you to monitor and take actions on the detected interfaces. For example, you can:

- Monitor the **Last Detected Time** to determine when the last detected the system NIC on the McAfee ePO managed network. A system whose interface has not been detected for a very long time might have been disconnected from the network.
- Click the system row to display the **Detected Systems Details** page and see all the interfaces associated with this system.
- Select a system and click **Actions** to add the system interface to exceptions, to system tree, deploy agents, and more.

Subnet status

Subnet status displays how many detected subnets on your network are covered, or have a Rogue System Sensor monitoring the subnet. Coverage is determined by the ratio of covered subnets to uncovered subnets on your network. Subnet states are categorized into these groups:

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

To fall into one of these categories, subnets must be known by the McAfee ePO server or be seen by a sensor. Once a subnet has been detected, you can mark it **Ignore** to prevent receiving further reporting about its status.

Contains Rogues

Subnets that contain rogue systems are listed in the Contains Rogues category to make it easier to take action on them.

Covered

Covered subnets have installed sensors that actively report information about detected systems to the McAfee ePO server. This category also includes the systems listed in the **Contains Rogues** category. For example, the **Covered** subnets category contains subnets A, B, and C. Subnet B contains rogues, while A and C don't. All three are listed in the **Covered** category; only subnet B is listed in the **Contains Rogues** category.

Uncovered

Uncovered subnets don't have any active sensors on them. Subnets that are uncovered do not report information about detected systems to the McAfee ePO server. However, there might be managed systems on this subnet that are being reported on through other means, such as agent-server communication.

Overall system status

Overall system status is displayed in the Overall System Status monitor as a percentage of compliant systems.

Systems' states are separated into these categories:

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

The percentage of compliant systems is the ratio of systems in the **Managed** and **Exceptions** categories to those in the **Rogue** and **Inactive** categories.

Exceptions

Exceptions are systems that don’t need a McAfee Agent, such as routers, printers, or systems from which you no longer want to receive detection information. Identify these systems and mark them as exceptions to prevent them from being categorized as rogue systems. Mark a system as an exception only when it doesn't represent a vulnerability in your environment.

Inactive

Inactive systems are listed in the McAfee ePO database, but have not been detected by a detection source in a specified time, which exceeds the period specified in the Rogue category. Most likely these are systems that are shut down or disconnected from the network, for example, a laptop or retired system. The default time period for marking systems as inactive is 45 days.

Managed

Managed systems have an active McAfee Agent that has communicated with the McAfee ePO server in a specified time. To ensure security, the majority of detected systems on your network should be managed.

Systems on your network with an installed active agent are displayed in this list, even before you deploy sensors to the subnets that contain these systems. When the agent reports to the McAfee ePO database, the system is automatically listed in the **Managed** category.

Rogue

Rogue systems are systems that are not managed by your McAfee ePO server. There are three rogue states:

- **Alien agent** — These systems have a McAfee Agent that is not in the local McAfee ePO database, or any database associated with additional McAfee ePO servers you have registered with the local server.
- **Inactive agent** — These systems have a McAfee Agent in the McAfee ePO database that has not communicated in a specified time.
- **Rogue** — These systems don’t have a McAfee Agent.

Systems in any of these three rogue states are categorized as Rogue systems.

See *Rogue System Sensor status* for monitor details.

Top 25 Subnets

The Top 25 Subnets list provides the subnet list, by name or IP address, for the 25 subnets that contain the most rogue system interfaces on your network. When a top 25 subnet is selected, the

rogue system interfaces it contains are displayed in the adjacent Rogue System Interfaces by Subnet table.

How rogue systems are detected

To configure and manage Rogue System Detection, it is important to understand which components are used and how the rogue systems are detected.

McAfee Agent

The ideal ePolicy Orchestrator managed network has a McAfee Agent installed on all systems in the network. Using the McAfee Agent, those systems actively communicate their status back to the McAfee ePO server on a regular basis. To eliminate rogue systems, when systems are added to the ePolicy Orchestrator managed network, they should have the McAfee Agent installed:

- As part of the image installed on the system before connection
- Automatically when synchronized with Active Directory
- As an automatic response associated to an ePolicy Orchestrator **System Tree**
- Manually by the administrator from the **System Tree**

Rogue System Detection components

Rogue System Detection uses the following to discover and report rogue systems:

- Rogue System Detection extension — Installed on the McAfee ePO server
- Rogue System Detection server settings — Configured as part of the advanced server settings
- Rogue System Sensors — Configured as policy and server settings
- Automatic Responses — Automatically adds the McAfee Agent to the rogue system or notifies the administrator of the rogue system

Optionally, you can configure a Rogue System group in the **System Tree** — This is a place to move the rogue systems to until the McAfee Agent is deployed and the system can be moved to an appropriate group.

Rogue System Sensors

Rogue System Sensors can reside on either the DHCP server, or as a Rogue System Sensors deployed to the local subnet.

Sensors can be installed on the subnet:

- Using the DHCP server — A partial solution that doesn't find systems with static IP addresses

If the DHCP server operating system doesn't support installing the McAfee Agent you must use one of the other sensor installation solutions.

- By deploying to specific systems — By using a **System Tree** action or a client task to deploy the sensor to selected systems
- Using all systems in a subnet and configuring the Rogue System Sensor election feature to determine which sensors are active and which are passive

Rogue System Detection active sensors are configured on subnets depending on, for example:

- The type of traffic on the subnet — If the subnet is a broadcast network managed with a DHCP server, that DHCP server is the best place to install the active sensor.

  If the DHCP server can't support the sensor, you can install sensors on all the systems and configure the systems to elect which system or systems are active during a specific time, or install the sensors on specific systems and let the McAfee ePO server determine which are active.

- The size of the managed network — If the managed network is small, you can configure the McAfee ePO server to determine which sensors are active.
- The type of systems on the subnet — If the subnet is a server farm with mission-critical systems, you can install the sensor on a system with the least traffic and the least down time.

  Mission-critical systems can also be blacklisted to ensure they are not used as active sensors.

Types of Rogue System Detections

It is important to understand that Rogue System Detection server and sensor configuration varies depending on the type of systems and subnets being listened to and how they appear in the Detected Systems page.

Here is a look at the four most common types of rogue systems that appear on the **Detected Systems** page.

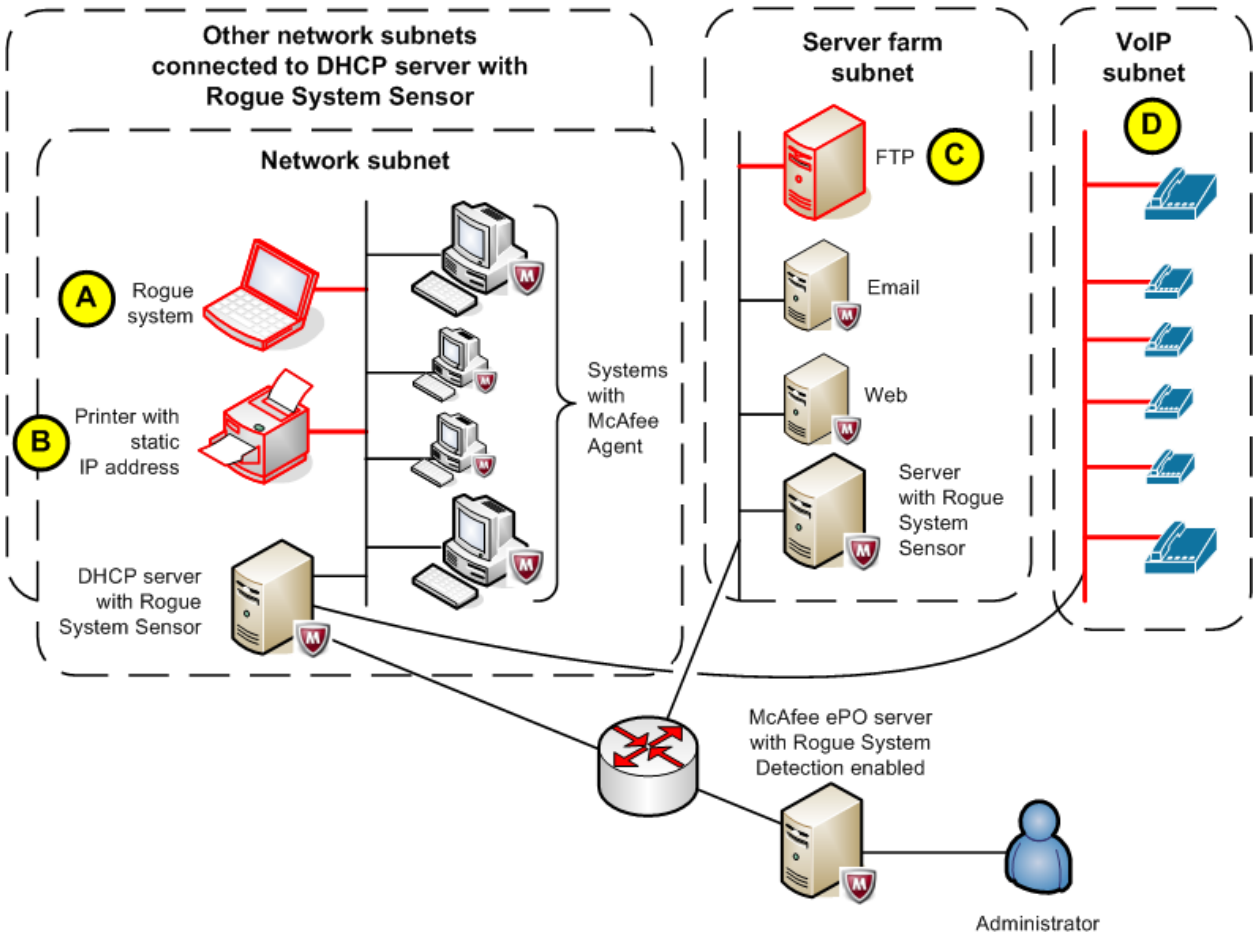

Figure 2 Rogue System Detection examples

The four most common rogue system detections are:

A Broadcast network rogue system detections — These are DHCP-enabled systems that are missing the McAfee Agent. These are the most common rogue systems.

B Rogue systems whose operating systems don't support McAfee Agent installation — For example, printers and mainframe computers.

C Static IP address rogue systems' detections — These are mission-critical servers connected to a subnet with a static IP address.

D Subnets where all the systems' operating systems don't support McAfee Agent installation — For example, Voice Over Internet Protocol (VoIP) and mainframe computer subnets.

Detecting DHCP network rogue systems

DHCP networks are the simplest networks to configure for Rogue System Detection. You can install the McAfee Agent automatically on the rogue system or install the agent manually as a **System Tree** action.

This process will probably account for the majority of the rogue systems detected on your ePolicy Orchestrator managed subnets.

Here is a look at a simple broadcast network subnet and the steps that occur when a rogue system connects to the subnet.

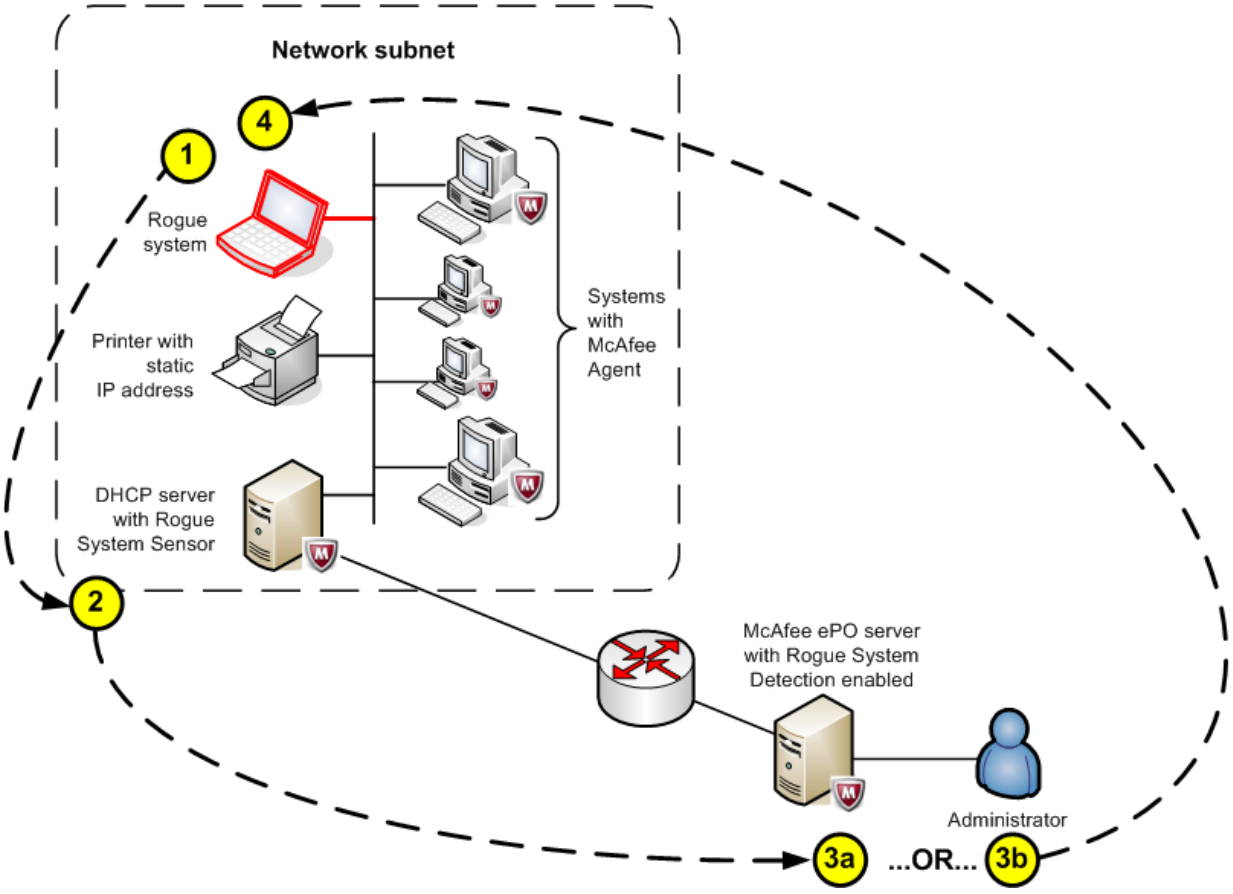

Figure 3 Rogue System Detection on a broadcast network

When a DHCP-enabled rogue system connects to a broadcast network:

1 The DHCP-enabled system connects to the network and sends a DHCP request for an IP address to the DHCP server.

2 The DHCP server, if it has the Rogue System Sensor installed or on a span port, automatically sends the connection event, OS fingerprints, and more to the McAfee ePO server.

If the DHCP server can't support the sensor, you can install sensors on all the systems and configure them to elect which sensors are active during a specific time, or install the sensors on specific systems and let the McAfee ePO server determine which are active.

3 When the McAfee ePO server receives the event and determines the interface is a rogue system, you can either:

   a Use an automatic response to install the McAfee Agent on the rogue system.

   b Use an automatic response to move the system to a special folder in the System Tree then manually install the McAfee Agent using an action.

4 One of the following occurs:

- If the McAfee Agent is installed successfully on the rogue system, it's listed as a managed system and left in the Rogue systems folder of the **System Tree**. The administrator can move the system to its correct **System Tree** folder later.
- If the McAfee Agent installation fails, the system is left as a rogue system. An automatic response can be configured to send a notification to the administrator to manually disconnect the system from the network, or add it as an exception and allow it to remain connected to the network.

The Overall System Status is updated in the Detected Systems page of the McAfee ePO server.

See *Rogue System Detection configuration initial tasks* for the detailed steps needed to configure broadcast network rogue system detection.

Detecting systems that can't host the agent

Some rogue systems on your managed network are systems whose operating systems don't support installation of the McAfee Agent. These systems can be added to the network as exceptions because their operating systems aren't likely to pose a security threat to the managed network.

Examples of unmanageable systems are printers and mainframe computers.

Here is a look at a simple broadcast network and what happens when a rogue system that can't support McAfee Agent installation. In this example a printer, connects to the managed subnet.

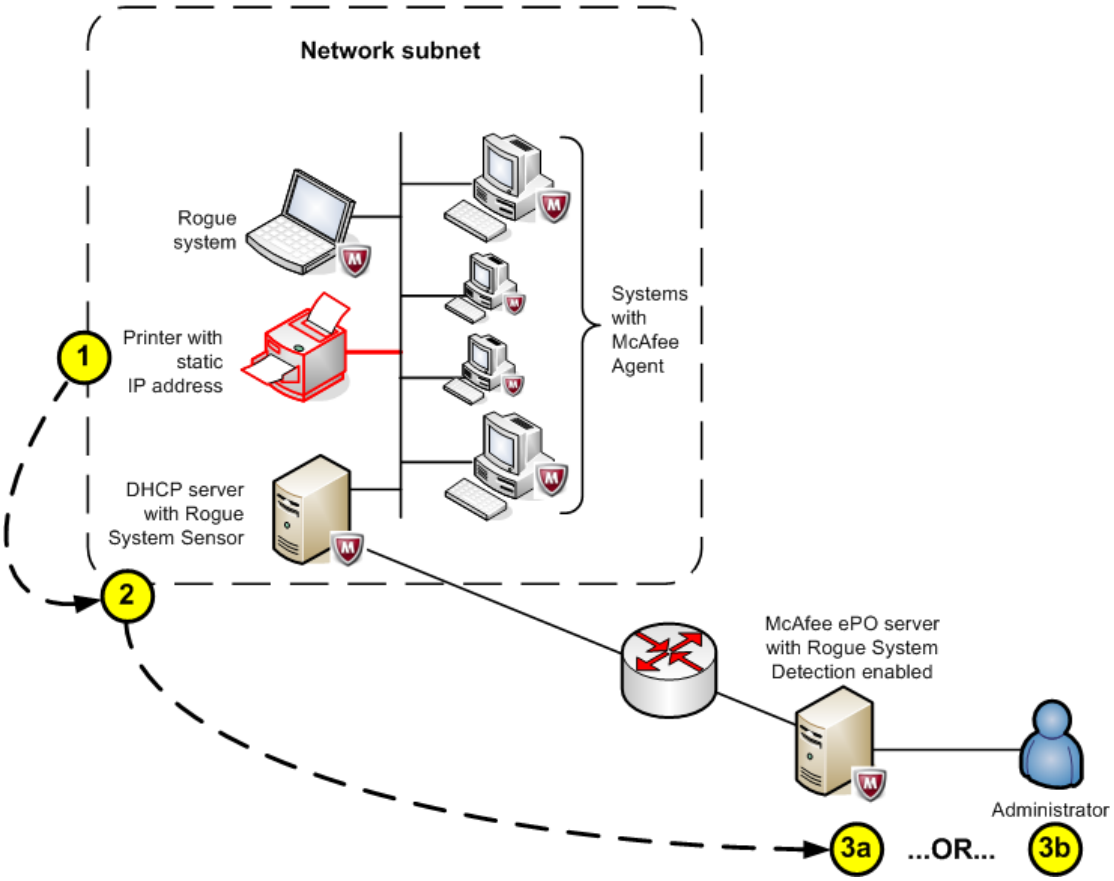

Figure 4 Rogue System Detection exception example

When the rogue system that can't support McAfee Agent installation connects to a managed broadcast network:

1 The printer with a static IP address connects to the network and sends a broadcast to all systems on the local subnet.

2 The broadcast is seen by the Rogue System Sensor installed on the DHCP server and it sends a connection event to the McAfee ePO server.

> If the DHCP server can't support the sensor you can install sensors on all the systems and configure the systems to elect which system or systems are active during a specific time, or install the sensors on specific systems and let the McAfee ePO server determine which are active.

3 When the McAfee ePO server receives the event and determines the interface is a rogue system, you can either:

   a Use an automatic response to move the system to the exceptions list.

   b Use an automatic response to notify the administrator, who can then manually move the system to the exceptions list.

See *Add systems to the Exceptions list* for the detailed steps needed to configure system detections that can't host the agent.

Detecting static IP address systems

Static IP addresses are typically used for mission-critical servers that must have the same IP address at all times to ensure connectivity. To find these rogue systems you must install a Rogue System Sensor on one or more systems on the subnet.

Here's what happens when a rogue system with a static IP address connects to the subnet.

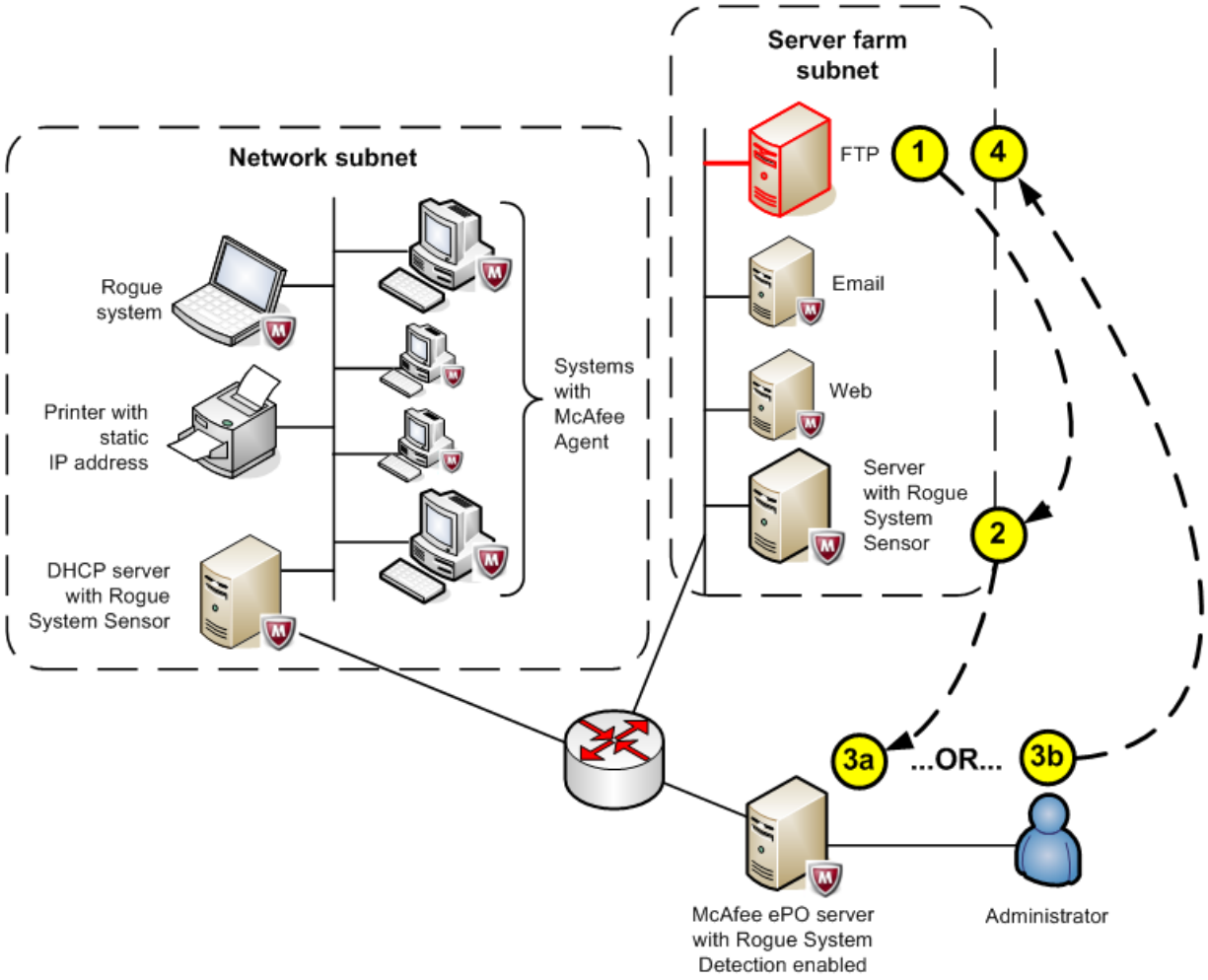

Figure 5 Rogue System Detection on a static IP network

When a rogue system with a static IP address connects to the subnet:

> In the previous figure the rogue system is the FTP server and the Rogue System Sensor is installed on another server.

1 The rogue system connects to the network and sends a broadcast to all systems on the subnet.

2 The server, configured as the Rogue System Sensor, receives the broadcast and sends a connection event to the McAfee ePO server.

3 When the McAfee ePO server receives the event and determines the interface is a rogue system, you can either:

   a Use an automatic response to install the McAfee Agent on the rogue system using a specific IP address range filter.

   b Use an automatic response to notify the administrator, who can then manually deploy the McAfee Agent to the system with a static IP address.

4 One of the following occurs, then the Overall System Status is updated in the Detected Systems page of the McAfee ePO server.

   - If the McAfee Agent is installed successfully on the rogue system, it is listed as a managed system and left in the Rogue systems folder of the System Tree. This allows the administrator to move the system into its correct **System Tree** folder later.
   - If the McAfee Agent installation fails, the system is left as a rogue system and if, configured to do so, an automatic response is sent to the administrator to manually disconnect the system from the network, or add it as an exception and allow it to remain connected to the network.

See *Configure Rogue System Detection Automatic Responses* and *Deploy agent manually from the Detected Systems page* for the detailed steps needed to configure static IP network rogue system detection.

Detecting a subnet of systems that can’t host agents

Some subnets and individual systems on your managed network don't allow you to install the McAfee Agent. The individual systems could have proprietary operating systems, such as printers, mainframe computers, or VoIP telephones.

Also the subnets these individual systems connect to will appear as uncovered subnets with multiple rogue systems in the **Subnet Status** monitor in the **Detected Systems** page of the McAfee ePO server.

Heres what happens when a subnet with many VoIP phones, whose operating systems don't support installation of the McAfee Agent, connect to an ePolicy Orchestrator managed network.

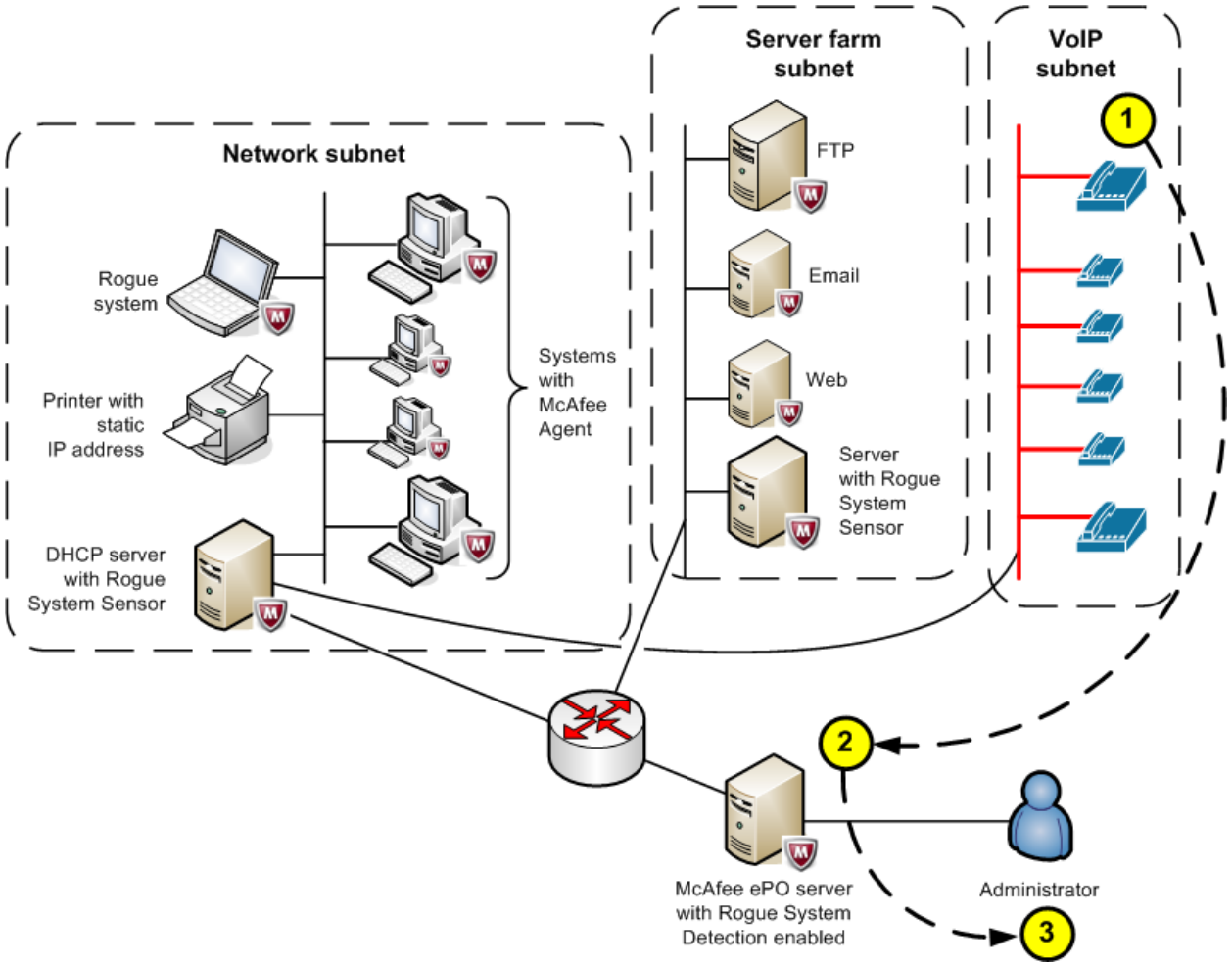

Figure 6 Subnet with special VoIP phone systems

When a subnet of VoIP phones connects to the ePolicy Orchestrator managed network:

1 The uncovered subnet with rogue systems connects to the ePolicy Orchestrator managed network and many broadcasts are sent to the Rogue System Sensor and forwarded to the McAfee ePO server.

2 The subnet appears in the **Detected Systems** dialog as:

- A covered subnet in the **Subnet Status** monitor
- An increase in the number of rogue systems in the **Overall System Status** monitor

3 If an automatic response is configured, the administrator receives a notification that many rogue system have connected to the managed network.

The administrator can configure either:

- The sensor to not scan a specific list of system MAC addresses or the Organizationally Unique Identifiers (OUIs) of the VoIP phones, in this example
- A policy to not listen on interfaces whose IP addresses are included in a specific range

See *Manage subnets* for the detailed steps needed to configure rogue system subnet detection.

How the Rogue System Sensor works

Rogue System Sensors detect devices that are connected to your network, then gather information about the devices and forward it to the McAfee ePO server.

The sensor is a Win32 native executable application that runs on the following Windows NT-based operating systems:

- Windows XP
- Windows Server 2003
- Windows 2008
- Windows Vista
- Windows 7

The Rogue System Sensor can be installed on systems throughout your network. A sensor reports on systems in the broadcast segment where it is installed. A sensor installed on a DHCP server reports on all systems or subnets using DHCP.

To maintain coverage in networks or broadcast segments that don't use DHCP servers, you must install at least one sensor on each broadcast segment using static IP addresses. DHCP deployment can be used with segment-specific deployment of the Rogue System Sensor for the most comprehensive coverage.

The ePolicy Orchestrator 4.7 software supports Rogue System Sensors from version 2.0, 4.5, 4.6, and 4.7.

To protect the system from failing due to a lack of memory, the Rogue System Sensor 4.7 periodically checks the available memory. If it drops below five percent, the sensor shuts down. Once the available memory increases, the sensor restarts.

Passive listening to layer-2 traffic

To detect systems on the network, the sensor uses WinPCap, a packet capture library.

It captures layer-2 broadcast packets sent by systems that are connected to the same network broadcast segment. It also listens passively to all layer-2 traffic for Address Resolution Protocol (ARP), Reverse Address Resolution Protocol (RARP), IP traffic, and DHCP responses.

To obtain additional information, the sensor also performs NetBIOS calls and OS fingerprinting on systems that were already detected. It does this by listening to the broadcast traffic of all devices in its broadcast segment, and by using NetBIOS calls, actively probing the network to gather additional information about the devices connected to it, such as the operating system of a detected system.

The sensor doesn't determine whether the system is a rogue system. It detects systems connected to the network and reports these detections back to the McAfee ePO server, which determines whether the system is rogue based on user-configured settings.

Intelligent filtering of network traffic

The sensor filters network traffic "intelligently" — it ignores unnecessary messages and captures only what it needs, which is Ethernet and IP broadcast traffic.

By filtering out unicast traffic, which might contain non-local IP addresses, the sensor focuses only on devices that are part of the local network.

To optimize performance and minimize network traffic, the sensor limits its communication to the server by relaying only new system detections, and by ignoring any re-detected systems for a user-configured time. For example, the sensor detects itself among the list of detected systems. If the sensor sent a message every time it detected a packet from itself, the result would be a network overloaded with sensor detection messages.

The sensor further filters on systems that were already detected:

- The sensor reports any system the first time it is detected on the network.
- For each detected system, the sensor adds the MAC address to the packet filter, so that it is not detected again, until the user-configured time elapses.
- The sensor implements aging on the MAC filter. After a specified time, MAC addresses for systems already detected are removed from the filter, causing those systems to be re-detected and reported to the server. This process ensures that you receive accurate and current information about detected systems.

Data gathering and communications to the server

When the sensor detects a local network system, that is not already in the cache or blocked by a policy, it gathers information about that system by actively listening to NetBIOS calls and OS fingerprinting.

The gathered information includes:

- DNS name
- Operating system version, family, and platform
- Device type
- NetBIOS information (domain membership, system name, and the list of currently logged-on users)

For IPv6 networks, NetBIOS is detected using Link-local Multicast Name Resolution (LLMNR).

All NetBIOS and LLMNR-related information that is gathered is subject to standard limitations of authorization, and other limitations documented in the Microsoft management API.

The Rogue System Sensor listens on the ports shown in the following table.

This is a list of all ports, for example OS fingerprints and more.

Table 1 Rogue System Sensor ports

Description	Type	Ports
Host discovery	UDP ports	53 67 69 123 137 161 500 1434
Host discovery	TCP ports	21 22 23 25 79 80 110 113 139 264 265 443 1025 1433 1723 5000
Service discovery	UDP ports	53 68-69 123 135 137-138 161 260 445 500 514 520 1434 1645-1646 1812-1813 2049 31337 43981
Service discovery	TCP ports	7 9 11 13 15 19 21-23 25 43 49 53 66-68 79-81 88-89 98 109-111 113 118-119 135 139 143 150 156 256-259 264 389 396 427 443 445 465 512-515 524 563 593 636 799 900-901 1024-1040 1080 1214 1243 1313 1352 1433 1494 1498 1521 1524-1525 1541-1542 1720 1723 1745 1755 1813 2000-2001 2003 2049 2080 2140 2301 2447 2766 2998 3128 3268 3300 3306 3372 3389 4045 4321 4665 4899 5222 5556 5631-5632 5800-5802 5900 6000 6112 6346 6666-6667 7000-7001 7070 7777 7947 8000-8001 8010 8080-8081 8100 8888 10000 12345 20034 30821 32768-32790 49152-49157

The sensor packages the gathered information into an XML message, then sends the message using a secure data channel to the ePolicy Orchestrator server for processing. The server then uses the ePolicy Orchestrator data to determine whether the system is a rogue system.

Bandwidth use and sensor configuration

To save bandwidth in large deployments, you can configure how often the agent sends detection messages to the server. You can configure the agent to cache detection events for a given time period, such as one hour, then to send a single message containing all the events from that time period. For more information, see *Configuring Rogue System Detection policy settings*.

Systems that host sensors

Install sensors on systems that are likely to remain on and connected to the network at all times, such as servers. If you don’t have a server running in a given broadcast segment, install sensors on several workstations to ensure that at least one sensor is connected to the network at all times.

To guarantee that your Rogue System Detection coverage is complete, you must install at least one sensor on each broadcast segment of your network. Installing more than one sensor on a broadcast segment doesn't create issues around duplicate messages because the server filters any duplicates. However, additional active sensors on each subnet result in traffic sent from each sensor to the server. While maintaining as many as five or ten sensors in a broadcast segment should not cause any bandwidth issues, you should not maintain more sensors on a broadcast segment than is necessary to guarantee coverage.

DHCP servers

If you use DHCP servers in your network, you can install sensors on them. Sensors installed on DHCP servers, or on systems connected with a span port, report on all connected subnets by listening for DHCP responses. Using sensors on DHCP servers reduces the number of sensors you need to install and manage on your network to ensure coverage, but it doesn't eliminate the need to install sensors to network segments that use static IP address.

Installing sensors on DHCP servers can improve coverage of your network. However, it is still necessary to install sensors in broadcast segments that use static IP address, or that have a mixed environment. A sensor installed on a DHCP server doesn't report on systems covered by that server if the system uses a static IP address.

Rogue System Sensor status

Rogue System Sensor status is the measure of how many of the sensors installed on your network are actively reporting to the McAfee ePO server, and is displayed in terms of health. Health is determined by the ratio of active sensors to missing sensors on your network.

Sensor states are categorized into these groups:

- **Active** — Active sensors report information about their broadcast segment to the McAfee ePO server at regular intervals, over a fixed time. Both the reporting period and the active period are user-configured. All of the sensors on a subnet use a voting algorithm to determine which sensor is active and which change to passive. The next sensor voted active on the subnet takes over communicating with the McAfee ePO server.

You can use the ePolicy Orchestrator Sever Settings to configure multiple active sensors on a subnet.

- **Missing** — Missing sensors have not communicated with the McAfee ePO server in a user-configured time. These missing sensors could be on a system that has been turned off or removed from the network.
- **Passive** — Passive sensors check in with the McAfee ePO server, but don't report information about detected systems. They wait until they are voted active by the voting algorithm to communicate the state of the broadcast segment to the McAfee ePO server.

Rogue System Sensor election

You can determine the active Rogue System Sensors on a subnet using either the McAfee ePO server or allowing the sensors in the subnets themselves to elect which sensors are active or passive.

Using the McAfee ePO server to set active sensors

You can use the McAfee ePO server to deploy Rogue System Sensors on a subnet from the System Tree and configure the sensor numbers and communication using the sever settings.

For example, you can use:

- A manual process of installing sensors on specific systems
- Client tasks to install sensors

The drawbacks to these methods include:

- Deploying the sensors individually from the McAfee ePO server can be time consuming.
- You need to determine before-hand which systems to configure as Rogue System Sensors and manage them to insure they are always online or have redundant sensors.
- Systems added to the subnets after the initial configuration are not eligible to be active sensors.
- These methods don't scale well for large managed networks.

Allowing Rogue System Sensor elections to set active sensors

Configuring Rogue System Detection to use the local sensor election feature allows Rogue System Sensors in the local subnets to elect the active sensors in the group and reduce sensor traffic back to the McAfee ePO server. This also allows you to automatically deploy a Rogue System Sensor to all nodes on your subnets.

Allowing the Rogue System Sensors that are on a subnet themselves to elect which sensors are active or passive has these advantages:

- You can install the Rogue System Sensor on every system and not worry about selecting individual active sensors.
- If a system running as the active Rogue System Sensor is shut down or removed from the network, another system takes over after a configured time.
- It eliminates some of Rogue System Sensor traffic through the McAfee ePO server.

If you install Rogue System Sensors on a large number of nodes on many subnets and configure the policy to **Use Local Sensor Election**, then later change the policy to **Use ePO server to determine active sensors**, all of those previously installed sensors could overwhelm the McAfee ePO server when they ask if they should become active.

How Rogue System Sensor elections work

The Rogue System Detection local sensor election is configured using the Rogue System Detection policy settings on the **Communications** tab.

The local sensor election feature works like this:

1 A Rogue System Sensor is deployed to every node on the subnet.

2 An active sensor election starts if the number of active sensors communicating to the network subnet group is less than the number of configured active sensors, or the configured time between active sensor elections has passed.

3 Each sensor in the subnet uses an election algorithm using GUIDs to determine which sensors are active.

4 The sensor checks if its own GUID is one of the active sensors. If it is, it sends out a message telling the other sensors it is now an active sensor. If not, it becomes passive and waits for the next election cycle.

Rogue Sensor Blacklist

The Rogue Sensor Blacklist is the list of managed systems where you don't want sensors installed. These can include systems that would be adversely affected if a sensor were installed on them, or systems you have otherwise determined should not host sensors.

For example:

- Mission critical servers where peak performance of core services is essential, such as database servers or servers in the DMZ (demilitarized zone)
- Systems that might spend significant time outside your network, such as laptops

The Rogue Sensor Blacklist is different than the Exceptions list. The systems on the Exceptions list can’t have an agent on them, or you don’t want them categorized as rogue systems, such as printers or routers.

Rogue System Detection policy settings

Rogue System Detection policy settings allow you to configure and manage the instances of the Rogue System Sensor installed throughout your network. Settings can be applied to individual systems, groups of systems, and IP address ranges.

You can configure policy settings for all sensors deployed by the server. This is similar to managing policies for any deployed product, such as VirusScan Enterprise. The Rogue System Detection policy pages are installed on the McAfee ePO server at installation.

Configure the sensor policy settings in the Rogue System Detection policy pages the same way you would for any managed security product. Policy settings that you assign to higher levels of the **System Tree** are inherited by lower level groups or individual systems. For more information about policies and how they work, see *Managing your Network with Policies and Client Tasks*.

McAfee recommends that you configure policy settings before you deploy sensors to your network to make sure that the sensors work according to your intended use. For example, DHCP monitoring is disabled by default. As a result, if you deploy sensors to DHCP servers without enabling DHCP monitoring during your initial configuration, those sensors report limited information to the McAfee ePO server. If you deploy sensors before you configure your policies, you can update them to change sensor functionality.

Considerations for policy settings

Policy settings configure the features and performance of the Rogue System Sensor.

These settings are separated into four groups:

- Communication settings
- Detection settings

- General settings
- Interface settings

Communication settings

Communication settings determine:

- Active sensor election
- Communication time for inactive sensors
- Reporting time for active sensors
- Sensor's detected system cache lifetime

The active sensor election settings determine if the active sensors are set using the McAfee ePO server or allowing the sensors in the subnets themselves to elect which sensors are active or asleep. To configure the active sensors see *Configuring Rogue System Detection policy settings* for details.

If you install Rogue System Sensors on a large number of nodes on many subnets and configure the policy to Use Local Sensor Election and later change the policy to Use ePO server to determine active sensors, all of those previously installed sensors could overwhelm the McAfee ePO server asking if they should become active.

The communication time for inactive sensors determines how often passive sensors check in with the server.

The Reporting time for active sensors determines how often active sensors report to the McAfee ePO server. Setting this value too low can have the same effect as setting the value for the sensor's detected system cache lifetime.

The sensor's detected system cache lifetime is the amount of time a detected system remains in the sensor's cache. This value controls how often the sensor reports that a system is newly detected. The lower the value, the more often the sensor reports a system detection to the server. Setting this value too low can overwhelm your server with system detections. Setting this value too high prevents you from having current information on system detections.

McAfee recommends that you set the same value for the sensor's detected system cache lifetime and for the reporting time for active sensors settings.

Detection settings

Detection settings determine whether:

- Device details detection is enabled
- DHCP monitoring is enabled
- Reporting on self-configured subnets is enabled

If you use DHCP servers on your network, you can install sensors on them to monitor your network. This allows you to use a single sensor to report on all subnets and systems that connect to it. DHCP monitoring allows you to cover your network with fewer sensors to deploy and manage, and reduces the potential for missed subnets and systems.

Device details detection allows you to specify the type of information the Rogue System Sensor scans systems for.

- Operating System (OS) details — This option allows the sensor to determine detailed information about a device's operating system. If you enable OS details scanning, you can also choose to scan the systems you have marked as exceptions.
- OS detection by choosing to scan all networks or only specific networks — You can limit OS detection to specific subnets by included or excluding specific IP addresses.

The Rogue System Sensor uses NetBIOS calls and OS fingerprinting to provide more detailed information about the devices on your network. You can enable active probing on your entire network, or include or exclude specific subnets.

This feature provides accurate matching of detected system interfaces and should be disabled only if you have specific reasons to do so.

General settings

General settings determine:

- Sensor-to-server communication port
- Server IP address or DNS name
- Whether the Rogue System Sensor is enabled

The server IP address default value is the address of the McAfee ePO server that you are using to install sensors. Rogue System Detection reports system detections to the specified server. When this server detects a system that has an agent deployed by a McAfee ePO server with a different IP address, that system is detected as a rogue because the agent is considered an alien agent.

The sensor-to-server communication port server setting can be changed only during installation. Whichever port you have specified during installation must also be specified on the General tab of Rogue System Detection policies.

Interface settings

Interface settings determine whether sensors:

- Don't listen on interfaces whose IP addresses are included in specific networks.
- Only listen on an interface if its IP address is included on a network found during installation.
- Only listen on interfaces whose IP addresses are included in specific networks.

Specifying these settings allows you to choose the networks that the sensor reports on.

How detected systems are matched and merged

When a system connects to your network, Rogue System Detection automatically checks the McAfee ePO database to determine whether the incoming system is new or corresponds to a previously detected system. If the system has been previously detected, Rogue System Detection automatically matches it to the existing record in the McAfee ePO database. When a detected system is not matched automatically, you can manually merge the system with an existing detected system.

Matching detected systems

Automatic matching of detected systems is necessary to prevent previously detected systems from being identified as new systems on your network. By default, systems are first matched against an agent’s GUID. If this GUID doesn't exist, the McAfee ePO database uses attributes specified in the Rogue System Matching server settings. You can specify which attributes the database uses for matching, based on which attributes are unique in your environment.

If a system on your network has multiple NICs, each system interface can result in separate interface detections. Use the Detected System Matching Server Setting to match multiple interfaces to an existing detected system in order to eliminate duplicate systems. See *Editing Detected Systems Matching* to configure your server settings to automatically match detected systems with multiple NICs.

Merging detected systems

When the McAfee ePO server can't automatically match detected systems, you can merge them manually using Merge systems. For example, the McAfee ePO server might not be able to match a detected system interface that was generated by a system with multiple NICs, based on the matching attributes you have specified. See *Merging detected systems* to manually merge a system with multiple NICs.

Rogue System Detection configuration

Configuring Rogue System Detection requires enabling and setting options in the ePolicy Orchestrator Server Settings, policies, and installing Rogue System Sensors on systems in the managed subnets.

Tasks

- *Rogue System Detection configuration initial tasks* on page 20
  To configure Rogue System Detection you must perform these tasks in the ePolicy Orchestrator user interface.
- *Manage sensors* on page 26
  When working with Rogue System Sensors you can remove sensors from systems, add and remove systems from the sensor blacklist, and change permission sets.

Rogue System Detection configuration initial tasks

To configure Rogue System Detection you must perform these tasks in the ePolicy Orchestrator user interface.

These are the initial tasks and the information needed to configure Rogue System Detection.

Tasks

- *Configure Rogue System Detection server and policy settings* on page 20
  You should confirm the default configuration of the Rogue System Detection ePolicy Orchestrator server settings. These server settings determine what a rogue system is, configure sensor settings, and much more.
- *Install sensors* on page 23
  Use any of these tasks to deploy sensors to your network.
- *Configure Rogue System Detection Automatic Responses* on page 25
  Use Rogue System Detection automatic responses to automatically move detected rogue systems to a folder you create in the System Tree and send an email to the administrator notifying them that rogue system has been found.

Configure Rogue System Detection server and policy settings

You should confirm the default configuration of the Rogue System Detection ePolicy Orchestrator server settings. These server settings determine what a rogue system is, configure sensor settings, and much more.

The Rogue System Detection policies are configured with default settings but these settings might not be the best settings to detect rogue systems on your ePolicy Orchestrator server or the most efficient settings for your network.

This task describes those setting and the variables to consider.

See *Using policies to manage products and systems* and *Considerations for policy settings* for policy configuration details.

Task

For option definitions, click **?** in the interface.

1. Click **Menu** | **Policy** | **Policy Catalog**, then from the Product drop-down list select **Rogue System Detection**, and from the Category drop-down list, select **General**. All created policies for Rogue System Detection appear.
2. Click the **My Default** policy to start editing the policy. If you want to create a new policy, click **Actions** | **New Policy** to create one.
3. On the **General** tab, click **Enable** to start a Rogue System Sensor after it is deployed and confirm the default server name or IP address is the McAfee ePO server or Agent Handler.
4. On the **Communications** tab, configure:
   - **Sensor's detected system cache lifetime** — You might increase this setting on large widely dispersed networks to reduce traffic on the subnet.
   - **Reporting time for active sensors** — You might increase this setting on large widely dispersed networks to reduce traffic back to the McAfee ePO server.
   - **Active sensor election** settings are different depending on the size and location of your subnets from the McAfee ePO server.
     - On smaller networks, click **Use ePO server to determine active sensors**. You can probably leave the Communication time for inactive sensors at the default setting.
     - On large networks, click **Use Local Sensor Election**. This reduces the traffic the sensors use to communicate back to the McAfee ePO server or Agent Handler.

       Configure active sensors as either:
       - **All sensors active** — The best selection for large networks with many subnets.

If you install Rogue System Sensors on a large number of nodes on many subnets and configure the policy to **Use Local Sensor Election** and later change the policy to **Use ePO server to determine active sensors**, all of those previously installed sensors could overwhelm the McAfee ePO server asking if they should become active.

       - Set the number of **active sensor(s)** — This is the manual configuration solution.
     - Configure the following depending on the location and speed of the connection between the managed subnets and the McAfee ePO server:
       - **Wait time for an election result** — You might increase this setting on slow networks to reduce traffic between sensors during the elections.
       - **Wait time between active sensor elections** — You might increase this setting if you want elections to occur less frequently.
   - **Ipv4 multicast group** or **Ipv6 multicast group** — Used by the local election feature to send multicast messages. You only need to change the default address if another feature is using the default.
   - **Sensor-to-Sensor communication port** — You only need to change the default if another process is using the port.

5 On the **Interfaces** tab, you can configure specific IP address networks to scan or not to scan for rogue systems. For example, if you have a VoIP subnet, you can add that subnet address to the **Do not listen on** list and those VoIP phone systems are not detected as rogue systems.

See *Rogue System Detection policy settings* for description of this configuration.

6 On the **Detection** tab, configure:

- **DHCP monitoring** — Specifies the settings for Dynamic Host Configuration Protocol (DHCP) monitoring. When DHCP monitoring is enabled, a single sensor installed on a DHCP server can monitor all systems and subnets that it serves.

  

  A DHCP server can't monitor interfaces with static IP addresses.

- **Device details detection** — To access the information captured by this configuration, click **Menu** | **Systems** | **Detected Systems** and click any system that appears in the Detected System Interfaces by Subnet.

  

  Enabling this feature might cause Security Alerts on local Firewalls, for example OS Fingerprint equals Port Scan. Network devices might react unexpectedly, for example network printers might print pages with not logical symbols and characters. It is important to use the Exception list and to not enable the option "Scan systems marked as exceptions."

- **Report on self-configured subnets** — This is disabled by default. Enabling this feature reports all subnets with a netmask of /32 (or /128 in IPv6). With Layer 2 detections, you might see a large number of erroneous 32-bit subnets appear in the subnet list. McAfee recommends you enable this feature only when using DHCP detection and not Layer 2 detection.

After you have configured Rogue System Detection server and policy settings, see *Install Rogue System Sensors* to continue configuring Rogue System Detection.

Install Rogue System Sensors

After you have configured Rogue System Detection server settings, you must install the Rogue System Sensors. Where and how many Rogue System Sensors are installed can make a difference in how effective Rogue System Detection is and can affect your network performance.

You can install Rogue System Sensors on these different types of systems:

All systems must be managed systems with the McAfee Agent installed.

- DHCP servers — This is the best place to install the Rogue System Sensors because DHCP servers are constantly monitoring multicast traffic and are instantly aware when a new system connects to a subnet.
- DNS servers or any system that is always connected to the subnet and monitoring traffic — These are good places to install Rogue System Sensors because these systems are not often turned off and are seldom disconnected from the network.
- All systems on a subnet — This allows you to configure Active sensor election in the Rogue System Detection policy. Once configured, all systems on a subnet periodically, according to configured settings, run an election algorithm to set some sensors as active and the remainder of the systems as passive.

Before you can install the Rogue System Sensor on an end system, the Rogue System Sensor software must be installed in the ePolicy Orchestrator Master Repository. To add the sensor software, see *Checking in engine, DAT and ExtraDAT update packages manually*. This process is generic and also describes installing the Rogue System Sensor.

To install the sensors on any of these systems, see *Installing sensors* for detailed steps to:

- *Install sensors on specific systems*
- *Use queries and server tasks to install sensors*
- *Use client task to install sensors*

After you have installed the Rogue System Sensors, see *Configure Automatic Responses* to continue configuring Rogue System Detection.

Install sensors

Use any of these tasks to deploy sensors to your network.

Tasks

- *Install sensors on specific systems* on page 23
  Create a deployment task that installs the Rogue System Sensor to the selected systems, then performs an immediate agent wake-up call.
- *Use queries and server tasks to install sensors* on page 23
  Create a query that can run as a server task action, which installs sensors on managed systems.
- *Use client task to install sensors* on page 24
  Create a client task that installs sensors to systems on your network.

Install sensors on specific systems

Create a deployment task that installs the Rogue System Sensor to the selected systems, then performs an immediate agent wake-up call.

This task can be performed from:	Getting there
Systems Details page	Click **Menu** | **Systems** | **System Tree** | **Systems** and click any system.
Managed Systems for Subnet xxx.xxx.xxx.xxx page	Click **Menu** | **Systems** | **Detected Systems**, click **Covered** or **Contains Rogues** in the Subnet Status monitor, then select any subnet and click **Actions** | **Detected Subnet** | **View Managed Systems**.
Systems page	Click **Menu** | **Systems** | **System Tree**.

Task

For option definitions, click **?** in the interface.

1 Select the systems where you want to install sensors, then click **Actions** \| **Rogue Sensor** \| **Add or Remove Rogue Sensor**.

- On the Systems Details page, you can install the sensor only from the system you are viewing.
- On the Managed Systems for Subnet xxx.xx.xx.x page, select the systems where you want to install sensors.
- On the Systems page, select the desired group in the System Tree, and select the systems where you want to install sensors.

2 In the Action pane, click **OK**.

Use queries and server tasks to install sensors

Create a query that can run as a server task action, which installs sensors on managed systems.

Task

For option definitions, click **?** in the interface.

1 Click **Menu** | **Reporting** | **Queries & Reports**, then click **Actions** | **New**. The Query Builder wizard opens.

2 On the **Result Type** page, select **System Management** as **Feature Group**, and **Managed Systems** as **Result Types**, then click **Next**.

3 From the **Display Results As** column on the **Chart** page, expand the **List** display and select **Table**, then click **Next**.

4 From the **Available Columns** pane on the Columns page, click the types of information you want your query to return, then click **Next**.

5 On the **Filter** page, click the properties you want to filter with and specify the values for each, then click **Run**.

6 Click **Save** and specify the name of your query and any notes, then click **Save** again.

McAfee recommends using a product-specific prefix when naming your queries, to keep them organized and make them easier to find. For example, `RSD: QueryName`.

7 Click **Menu** | **Automation** | **Server Tasks**, then click **Actions** | **New Task**. The Client Task Builder wizard opens.

8 On the **Description** page, name and describe the task, specify the Schedule status, then click **Next**.

9 From the drop-down list on the **Action** page, select **Run Query**.

10 From the **Query** list, select the query you created, then from the Language drop-down list, select the language you want for the displayed results.

11 Select **Add or Remove Rogue Sensor** as the subaction to take on the results of the query, then click **Next**.

12 On the **Schedule** page, specify the schedule for the task, then click **Next**.

13 Review the summary of the task, then click **Save**.

Use client task to install sensors

Create a client task that installs sensors to systems on your network.

Task

For option definitions, click **?** in the interface.

1 Click **Menu** | **Policy** | **Client Task Catalog**, select **Rogue System Detection x.x.x** | **Sensor Deployment** as Client Task Types, then click **Actions** | **New Task**. The New Task dialog box appears.

2 Ensure that **Sensor Deployment** is selected, then click **OK**.

3 Type a name for the task you are creating and add any notes.

4 Select **Install**, then click **Save**.

Select **Run at every policy enforcement** if needed.

5 Click **Menu** | **Systems** | **System Tree** | **Systems**, then select the system on which you want to install sensors, then click **Actions** | **Agent** | **Modify Tasks on a single system**.

To install sensors on a group of systems, refer to *Configuring the Deployment task for groups of managed systems*.

6 Click **Actions** | **New Client Task Assignment**. The Client Task Assignment Builder wizard appears.

7 On the Select Task page, select **Product** as **Rogue System Detection** and **Task Type** as **Sensor Deployment**, then select the task you created for installing sensors.

8 Next to **Tags**, select the desired platforms to which you are deploying the packages:

- **Send this task to all computers**
- **Send this task to only computers that have the following criteria** — Use one of the edit links to configure the criteria.

9 Click **Next**.

10 On the Schedule page, select whether the schedule is enabled, and specify the schedule details, then click **Next**.

11 Review the summary, then click **Save**.

Configure Rogue System Detection Automatic Responses

Use Rogue System Detection automatic responses to automatically move detected rogue systems to a folder you create in the System Tree and send an email to the administrator notifying them that rogue system has been found.

> **Before you begin**
>
> You must have already created a System Tree folder, to receive the detected systems, and specified an email server for use with your ePolicy Orchestrator server.

This section describes configuring Automatic Responses specifically for Rogue System Detection. See *Responding to events in your network* for detailed information about other Automatic Responses configuration.

Task

For option definitions, click **?** in the interface.

1 Click **Menu** | **Automation** | **Automatic Responses**, then click **Actions** | **New Response** or **Edit** next to an existing rule.

2 In the **Response Builder** dialog box that appears, click the **Description** tab, type appropriate information in **Name** and **Description**, and select a **Language**.

3 In **Events**, click the following in the lists:

- Event group, click **Detected System Events**.
- Event type, click **System Detection**.

4 In **Status**, click **Enabled**, then click **Next**.

5 On the **Actions** tab, configure two actions.

1 Select **Add to System Tree** from the actions list and configure the following:

- In **System Tree Location**, click **Browse** and select the folder where you want the detected system moved. For example, "Rogue system detections."
- Optionally, you can click **Tag and Sort Systems**, to make systems easier to find, and **Duplicate System Names** to show duplicate entries.

2 Select **Send Email** from the actions list and configure the following:

- In **Recipients**, type the email address of the administrator to receive the notification, or click … to select the email address from the Contacts list.
- In **Importance**, click a value from the list.
- In **Subject**, type a string, or select variables from the Insert variable lists and click **Insert**.
- In **Body**, type a string, or select variables from the Insert variable lists and click **Insert**.

6 Click **Next**, review the **Summary** page, and click **Save**.

After you have configured these processes, Rogue System Detection is configured.

Manage sensors

When working with Rogue System Sensors you can remove sensors from systems, add and remove systems from the sensor blacklist, and change permission sets.

See *Installing sensors* for details on adding sensors to managed systems.

Tasks

- *Edit sensor descriptions* on page 26
  Editing Rogue System Sensor descriptions makes them easier to find and their function easier to understand on the **Rogue System Sensors** page.
- *Add systems to the Rogue Sensor Blacklist* on page 27
  Add systems to the **Rogue Sensor Blacklist** to ensure they are not used as active Rogue System Sensors.
- *Remove systems from the Rogue Sensor Blacklist* on page 27
  Rogue System Detection prevents sensors from being installed on systems that are included in the blacklist. If you want to install a sensor on a system that has been blacklisted, you must remove the system from the list.
- *Remove sensors* on page 27
  Create a deployment task that removes the sensor from the selected systems, then performs an immediate agent wake-up call.
- *Edit Rogue System Sensor settings* on page 28
  Edit the Rogue System Sensor settings to determine how sensors interact with each other and the ePolicy Orchestrator server.
- *Change the sensor-to-server port number* on page 29
  You can change the port that the Rogue System Sensor uses to communicate with the McAfee ePO server.

Edit sensor descriptions

Editing Rogue System Sensor descriptions makes them easier to find and their function easier to understand on the **Rogue System Sensors** page.

This task can be performed from:	Getting there
Rogue System Sensor Details page	Click **Menu** | **Systems** | **Detected Systems**, click any sensor category in the Rogue System Sensor Status monitor, then click any sensor.
Rogue System Sensor page	Click **Menu** | **Systems** | **Detected Systems**, then click any sensor category in the Rogue System Sensor Status monitor.

Task

For option definitions, click **?** in the interface.

1 Select the system whose description you want to edit, click **Actions** | **Rogue Sensor** | **Edit Description**.

2 Type the description, then click **OK**.

Add systems to the Rogue Sensor Blacklist

Add systems to the **Rogue Sensor Blacklist** to ensure they are not used as active Rogue System Sensors.

Task

For option definitions, click **?** in the interface.

1 Click **Menu** | **Systems** | **System Tree** | **Systems** and select the detected systems you want to add to the Rogue Sensor Blacklist.

2 Click **Actions**, then select **Rogue Sensor** | **Add to Sensor Blacklist**.

3 Click **Yes** to confirm the change.

4 To confirm that the system is moved to the Rogue Sensor Blacklist, click **Menu** | **Systems** | **Detected Systems**, then from the Rogue System Sensor Status monitor, click **View Blacklist**.

Remove systems from the Rogue Sensor Blacklist

Rogue System Detection prevents sensors from being installed on systems that are included in the blacklist. If you want to install a sensor on a system that has been blacklisted, you must remove the system from the list.

Task

For option definitions, click **?** in the interface.

1 Click **Menu** | **Systems** | **Detected Systems**.

2 In the Rogue System Sensor Status monitor, click **View Blacklist**.

3 Select the system you want to remove from the Rogue System Blacklist page.

4 Click **Actions**, select **Rogue Sensor** | **Remove from Blacklist**, then click **OK** when prompted.

Remove sensors

Create a deployment task that removes the sensor from the selected systems, then performs an immediate agent wake-up call.

This task can be performed from:	Getting there
Managed Systems for Subnet xxx.xxx.xxx.xxx page	Click **Menu**	**Systems**	**Detected Systems**, click any **Covered** or **Contains Rogues** system in the Subnet Status monitor, then select any subnet and click **View Managed Systems**.
Systems Details page	Click **Menu**	**Systems**	**System Tree**	**Systems**, then click any system.
Systems page	Click **Menu**	**Systems**	**System Tree**.

Task

For option definitions, click **?** in the interface.

1 From the Systems page or Systems Details page, select the systems where you want to remove sensors, then click **Actions** | **Rogue Sensor** | **Remove Rogue Sensor**.

- In the Managed Systems for Subnet xxx.xx.xx.x page, select the systems where you want to remove sensors.
- In the Systems Details page, you can remove the sensor from only the system you are viewing.
- In the Systems page, select a group in the System Tree, then select the systems where you want to remove sensors.

2 In the **Action** pane, click **OK**.

Rogue System Detection permission sets

Permission sets for Rogue System Detection determine what information a user group can view, modify, or create for Rogue System Detection.

One or more permission sets can be assigned. By default, permission sets for global administrators are automatically assigned to include full access to all products and features.

The permission sets and their available privileges for Rogue System Detection are listed in the following table.

Permission set	Rights
Rogue System Detection	• Create and edit Rogue System information; manage sensors. • Create and edit Rogue System information; manage sensors; deploy McAfee Agents and add to System Tree. • No permissions. • View Rogue System information.
Rogue System Sensor	• No permissions. • View and change settings. • View settings.

Edit Rogue System Sensor settings

Edit the Rogue System Sensor settings to determine how sensors interact with each other and the ePolicy Orchestrator server.

Sensor settings are user-configured and specify:

- The amount of time sensors are active
- The maximum number of sensors active on each subnet
- How long the server waits to hear from a sensor before categorizing it as missing

Task

For option definitions, click **?** in the interface.

1 Click **Menu** | **Configuration** | **Server Settings**, then in the Settings Categories list, select **Rogue System Sensor** and click **Edit**.

2 Edit the **Sensor Timeout** field to set the maximum amount of time the server waits for a sensor to call in before marking it as missing.

3 Edit the **Sensors per Subnet** field to set the maximum number of sensors active on each subnet, or select **All sensors active**.

4 Add a list of **Sensor Scanning** MAC addresses and OUIs that the sensors should not actively probe, regardless of the configured policy.

5 Edit the **Active Period** field to set the maximum amount of time that passes before the server tells a sensor to become passive, or to allow a new sensor to become active.

The Active Period setting doesn't set the communication times for the active and inactive sensors. Communication time is configured using communication policy settings for Rogue System Detection.

6 Click **Save**.

Change the sensor-to-server port number

You can change the port that the Rogue System Sensor uses to communicate with the McAfee ePO server.

The port number specified in the Server Settings page can be changed only during installation of ePolicy Orchestrator. If you changed this port number during installation, you must also change it in the Rogue System Detection policy settings, to allow sensors to communicate with the server.

Task

For option definitions, click **?** in the interface.

1 Click **Menu** | **Policy** | **Policy Catalog**, then from the Product drop-down list, select **Rogue System Detection x.x.x**, and from the Category drop-down list, select **General**. All created policies for Rogue System Detection appear in the details pane.

2 Locate the desired policy, then click its name.

3 On the General tab, change the **Sensor-to-Server Communication Port** to the desired port number, then click **Save**.

Manage rogue systems

When working with rogue systems you can, for example, view, ping, and query these detected systems, plus modify the exceptions list, and more.

See *Rogue System Detection configuration initial tasks* for details about the most common rogue system configuration tasks.

Tasks

- *Deploy agent manually from the Detected Systems page* on page 30
  You can manually deploy the McAfee Agent to a rogue system using actions in the Detected Systems page.
- *Manage alien agents and multiple McAfee ePO servers* on page 31
  If you have an ePolicy Orchestrator managed network with multiple McAfee ePO servers, some rogue systems might appear, if configured, as alien agents in the local Detected Systems Details page. To fix this you must add all McAfee ePO servers to the Server Settings for the Detected System Compliance setting categories.
- *View detected subnets and their details* on page 32
  Use this task to view detected subnets and their details. You can view detected subnets details from any page that displays detected subnets.
- *Ping a detected system* on page 32
  Ping a detected system to confirm that it can be reached over the network.
- *Query detected system agents* on page 32
  Query agents installed on detected systems. Not all detected systems have a McAfee Agent installed. The results of this task indicate whether an agent is installed and provides links to details about the system and the agent, if available.
- *Add systems to the Exceptions list* on page 33
  Exceptions are systems that don’t need a McAfee Agent and from which you no longer want to receive detection information. Identify these systems and mark them as exceptions to prevent them from being categorized as rogue systems.
- *Remove systems from the Exceptions list* on page 33
  You can remove detected systems from the Exceptions list if you would like to start receiving detection information about it, or you know that the system is no longer connected to your network.
- *Export or import Exceptions list* on page 34
  You can export information from the Exceptions list or import information into the Exceptions list.
- *Add detected systems to the System Tree* on page 34
  Add detected systems to the System Tree from the Detected Systems pages.
- *Edit system comments* on page 35
  System comments can be useful for noting important "human readable" information to a detected system entry.
- *Merge detected systems* on page 35
  You can manually merge detected systems that can't be automatically matched by the McAfee ePO server.
- *Remove systems from the Detected Systems list* on page 35
  You might want to remove a system from the Detected Systems list when you know it is no longer in service.

Deploy agent manually from the Detected Systems page

You can manually deploy the McAfee Agent to a rogue system using actions in the Detected Systems page.

Task

For option definitions, click **?** in the interface.

1 To select the rogue system where you want to deploy the McAfee Agent:

   a Click the interface in the Detected System Interfaces by Subnet table.

   b Click **Rogue** in the Overall System Status monitor, the rogue systems appear in the Detected Systems page, and click the system.

2 Click **Actions** | **Detected Systems** | **Deploy Agent** and the Deploy McAfee Agent page appears.

3 Configure the options in the Agent Deployment Settings page, then click **OK**.

The McAfee Agent is deployed to the rogue system and it is changed to a managed state.

Manage alien agents and multiple McAfee ePO servers

If you have an ePolicy Orchestrator managed network with multiple McAfee ePO servers, some rogue systems might appear, if configured, as alien agents in the local Detected Systems Details page. To fix this you must add all McAfee ePO servers to the Server Settings for the Detected System Compliance setting categories.

You can have systems managed by a remote McAfee ePO server listed as Rogue in the **Detected Systems** page. To move the systems to Managed run the **Query Agent** action.

Task

For option definitions, click **?** in the interface.

1 Click **Menu** | **Configuration** | **Server Settings**, then from the Settings Categories list select **Detected System Compliance**. The existing Detected System Compliance settings appear in the right-hand pane.

2 Click **Edit**. The Edit Detected System Compliance settings fill the dialog box ready to edit.

3 In the **Other ePO Servers** field of ePO Servers settings, type the name of the McAfee ePO server that manages the alien system, then click **Save**.

   To add multiple McAfee ePO server names, separate them with a comma, whitespace, or on separate lines. For example:

```
ePO1,ePO2
ePO1 ePO2
ePo1
ePo2
```

4 For the Query Agent action to work correctly, click **Menu** | **Policy** | **Policy Catalog**, click **McAfee Agent** from the product list, and select a **General** category policy. Make these changes:

   a Click the **General** tab and disable **Accept connections only from the ePO server**.

   b Click the **Logging** tab and click **Enable Agent Activity Log**.

   c (Optional) Change the **Alternative McAfee Agent ports** found at **Menu** | **Configuration** | **Server Settings**, from Setting Categories select **Detected System Matching** and enter the alternate ports to check for a McAfee Agent.

5 Run the **Query Agent** action on all alien agents. This can be done manually or using a server task or automatic response.

Now the alien system appears as a managed system with an ePO Server Name that's different than the local McAfee ePO server. To confirm the change, click **Menu** | **Systems** | **Detected Systems**. The previous alien system is no longer in the list of detected systems.

View detected subnets and their details

Use this task to view detected subnets and their details. You can view detected subnets details from any page that displays detected subnets.

Task

For option definitions, click **?** in the interface.

1 Click **Menu** | **Systems** | **Detected Systems**.

2 In the Subnet Status monitor, click any category to view the list of detected subnets it contains, such as **Covered**. The Detected Subnets page appears and displays the subnets in that category.

3 Click any detected subnet to view its details. The Detected Subnet Details page appears.

Ping a detected system

Ping a detected system to confirm that it can be reached over the network.

This task can be performed from:	Getting there
Detected Systems Status page	Click **Menu**	**Systems**	**Detected Systems**, then click any category in the **Overall System Status** monitor.
System Tree page	Click **Menu**	**Systems**	**System Tree**.

Task

For option definitions, click **?** in the interface.

1 Select the system you want to ping.

You can only ping one system at a time.

2 Click **Actions** | **Detected Systems** or **Directory Management**, then click **Ping**.

The result is displayed on the **Actions** bar in the notification panel at the bottom right corner of the McAfee ePO console window.

Query detected system agents

Query agents installed on detected systems. Not all detected systems have a McAfee Agent installed. The results of this task indicate whether an agent is installed and provides links to details about the system and the agent, if available.

This task can be performed from:	Getting there
Detected Systems page	Click **Menu**	**Systems**	**Detected Systems**.
Detected Systems Status page	Click **Menu**	**Systems**	**Detected Systems**, then click any category in the **Overall System Status** monitor.

Task

For option definitions, click **?** in the interface.

1 Select the systems whose agents you want to query.

2 Click **Actions** | **Detected Systems** | **Query Agent** or **Actions** | **Query Agent**. The Query McAfee Agent Results page opens.

Add systems to the Exceptions list

Exceptions are systems that don't need a McAfee Agent and from which you no longer want to receive detection information. Identify these systems and mark them as exceptions to prevent them from being categorized as rogue systems.

Candidates for exceptions include routers, printers, mainframe computers, and VoIP telephones.

Mark a system as an exception only when it does not represent a vulnerability in your environment.

This task can be performed from:	Getting there
Detected Systems page	1 Click **Menu** | **Systems** | **Detected Systems**. 2 From **Detected System Interfaces by Subnet** pane, click any system. 3 Click **Actions** | **Add to Exceptions**. The Add to Exceptions dialog box appears. 4 Click **Detected Systems** | **Exceptions** to display the **Add to Exceptions** dialog box.
Detected Systems Details page	1 Click **Menu** | **Systems** | **Detected Systems**. 2 From **Overall System Status** monitor pane, click any detected system category 3 From the **Detected Systems Details** page, click any system. 4 Click **Actions** | **Detected Systems** | **Add to Exceptions** to display the **Add to Exceptions** dialog box.

Task

For option definitions, click **?** in the interface.

1 Use one of the processes in the previous table to display the **Add to Exceptions** dialog box.

2 Select one of the following to configure the exception category:

- **No Category** — Displayed without a category entry.
- **New Category** — Displayed with the new category name you type.
- **Select Category** — Displayed with the category selected from the list.

To configure categories, see *Editing Detected System Exception Categories*.

3 click **OK**.

Remove systems from the Exceptions list

You can remove detected systems from the Exceptions list if you would like to start receiving detection information about it, or you know that the system is no longer connected to your network.

Task

For option definitions, click **?** in the interface.

1 Click **Menu** | **Systems** | **Detected Systems**.

2 In the Overall System Status monitor, click the **Exceptions** category, then select the system you want to remove.

3 Click **Actions**, select **Detected Systems** | **Remove from Exceptions**, then click **OK** when prompted.

Export or import Exceptions list

You can export information from the Exceptions list or import information into the Exceptions list.

Both the export and import data processes modify MAC address data stored in the Rogue System Detection Exceptions list.

Task

For option definitions, click **?** in the interface.

1 Click **Menu** | **Systems** | **Detected Systems** and click **Import/Export Exceptions** from the Overall System Status monitor. The Import/Export Exceptions dialog box appears.

2 Do one of the following:

- On the **Export Exceptions** tab, click the link, then save the file.

  Files are exported in the Comma Separated Value format. The file name for your Exceptions list is predefined as RSDExportedExceptions.csv. You can change the name of the file when you download it to your local system.

- Click **Import Exceptions** tab and choose the method you want to use to import, specify the systems or file, then click **Import Exceptions**.

  When importing systems, only MAC addresses are recognized. MAC addresses can be separated by whitespace, commas, or semicolons. The MAC address can include colons, but they are not required.

Add detected systems to the System Tree

Add detected systems to the System Tree from the Detected Systems pages.

This task can be performed from:	Getting there
Detected Systems page	Click **Menu**	**Systems**	**Detected Systems**.
Detected Systems Status page	Click **Menu**	**Systems**	**Detected Systems**, then click any category in the **Overall System Status** monitor.

Task

For option definitions, click **?** in the interface.

1 Select the detected systems you want to add to the System Tree.

2 Click **Actions** | **Detected Systems** | **Add to System Tree**. The Add to System Tree page opens.

3 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.

4 Specify one of these options:

- **Tag and Sort Systems** — Applies tags and sorts system immediately after adding the systems to the System Tree.
- **Duplicate System Names** — Allows duplicate entries to be added to the System Tree.

Edit system comments

System comments can be useful for noting important "human readable" information to a detected system entry.

This task can be performed from:	Getting there
Detected Systems Details page.	Click **Menu**	**Systems**	**Detected Systems**, click any detected system category in the Overall System Status monitor, then click any system.
Detected Systems page.	Click **Menu**	**Systems**	**Detected Systems**, then click any detected system category in the Overall System Status monitor.

Task

For option definitions, click **?** in the interface.

1 Select the system whose comment you want to edit, then click **Actions** | **Detected Systems** | **Edit Comment**.

2 Type your comments, then click **OK**.

Merge detected systems

You can manually merge detected systems that can't be automatically matched by the McAfee ePO server.

See *How detected systems are matched and merged* for more information.

Task

For option definitions, click **?** in the interface.

1 Click **Menu** | **Systems** | **Detected Systems**, then from Overall System Status monitor, select **Rogue**. The rogue systems appear in the display.

2 Select the systems you want to merge.

3 Click **Actions**, then select **Detected Systems** | **Merge Systems**. The Merge Systems page appears.

4 Click **Merge**.

5 When the merge warning message appears, click **OK**.

Remove systems from the Detected Systems list

You might want to remove a system from the Detected Systems list when you know it is no longer in service.

Once a system has been removed, it doesn't appear in the Detected Systems list until the next time the system is detected.

Task

For option definitions, click **?** in the interface.

1 Click **Menu** | **Systems** | **Detected Systems**.

2 In the Overall System Status monitor, click any detected system category, then click the system you want to remove.

3 Click **Actions** | **Detected Systems** | **Delete**, then click **OK** when prompted.

Manage subnets

When working with subnets in Rogue System Detection you can add, delete, and include previously ignored subnets.

Tasks

- *Viewing detected systems and their details* on page 36
  You can view detected system details from any page that displays detected systems.
- *Add subnets* on page 36
  You can add subnets to Rogue System Detection.
- *Delete subnets* on page 37
  You can delete subnets from Rogue System Detection.
- *Ignore subnets* on page 37
  You can ignore subnets that you don't what to receive information about from Rogue System Detection.
- *Include subnets* on page 38
  Include subnets that have previously been ignored by Rogue System Detection.
- *Rename subnets* on page 38
  You can rename subnets from the default IP address, to make them easier to find or understand their use.

Viewing detected systems and their details

You can view detected system details from any page that displays detected systems.

Task

For option definitions, click **?** in the interface.

1 Click **Menu** | **Systems** | **Detected Systems**.

2 In the Overall System Status monitor, click any category to view the list of detected systems it contains, such as **Managed**. The Detected Systems page appears.

3 Click any detected system to view its details.

The System Details page is different than the Detected Systems Details page. The Detected Systems Details page displays some information that is unique to Rogue System Detection.

Add subnets

You can add subnets to Rogue System Detection.

Task

For option definitions, click **?** in the interface.

1 Click **Menu** | **Systems** | **Detected Systems**, then in the Subnet Status monitor, click **Add Subnet**. The Add Subnets page appears.

2 Choose the method you want to use to add subnets, specify the subnets you want to add, then click **Import**.

Delete subnets

You can delete subnets from Rogue System Detection.

This task can be performed from:	Getting there
Detected Subnets Details page	Click **Menu**	**Systems**	**Detected Systems**, click any category in the Subnet Status monitor, then click any subnet.
Detected Subnets page	Click **Menu**	**Systems**	**Detected Systems**, then click any category in the Subnet Status monitor.

Task

For option definitions, click **?** in the interface.

1 Select the subnets you want to delete, click **Actions**, then select **Detected Systems** | **Delete**.

2 In the **Delete** confirmation pane, click **Yes**.

Ignore subnets

You can ignore subnets that you don't what to receive information about from Rogue System Detection.

This task can be performed from:	Getting there
Detected Subnets Details page	Click **Menu**	**Systems**	**Detected Systems**, click any category in the Subnet Status monitor, then click any subnet.
Detected Subnets page	Click **Menu**	**Systems**	**Detected Systems**, then click any category in the Subnet Status monitor.
Detected Systems page	Click **Menu**	**Systems**	**Detected Systems**.

Ignoring a subnet deletes all detected interfaces associated with that subnet. All further detections on that subnet are also ignored. To view the list of ignored subnets, click the **Ignored** link in the **Subnet Status** monitor. This link appears only when there are subnets being ignored.

Task

For option definitions, click **?** in the interface.

1 Select the subnets you want to ignore, click **Actions**, then select **Detected Systems** | **Ignore**.

2 In the Ignore dialog box, click **OK**.

When ignoring a subnet on the Detected Systems page in the Top 25 Subnets list, a dialog box opens. Click **OK**.

Include subnets

Include subnets that have previously been ignored by Rogue System Detection.

This task can be performed by querying ignored subnets using the steps below, or you can include subnets from the **Ignored Subnets** page.

Task

For option definitions, click **?** in the interface.

1 Click **Menu** | **Reporting** | **Queries & Reports**, and query for any ignored subnets. For more information on working with queries, see *Reporting on System Status.*

2 On the Unsaved Queries page, click **Include**.

3 In the Include dialog box, click **OK**.

Rename subnets

You can rename subnets from the default IP address, to make them easier to find or understand their use.

This task can be performed from:	Getting there
Detected Subnets Details page	Click **Menu**	**Systems**	**Detected Systems**, click any subnet category in the Subnet Status monitor, then click any subnet.
Detected Subnets page	Click **Menu**	**Systems**	**Detected Systems**, then click any subnet category in the Subnet Status monitor.

Task

For option definitions, click **?** in the interface.

1 Select the subnet you want to rename, then click **Actions** and select **Detected Systems** | **Rename**.

2 In the Rename dialog box, type the new name for the subnet, then click **OK**.

Rogue System Detection command-line options

You can run command-line options from the client system.

You can start the sensor manually from the command-line instead of starting it as a Windows service. You might want to do this if you are testing functionality, or to check the sensor version. The following table lists the run-time command-line options for the sensor.

Switch	Description
`--console`	Forces the sensor to run as a normal command-line executable; otherwise it must be run as an NT service.
`--help`	Prints the Help screen and lists available command-line options.
`--install`	Registers the sensor with the Windows Service Control Manager.
`--port`	Overrides the Server Port configuration setting in the registry that you specified during installation. This parameter takes effect only when running in command-line mode, which also requires the `--console` command-line switch. **Sample syntax:** `sensor.exe --port "8081" --console`

Switch	Description
`--server` "[server name]" or "[IP address]"	Overrides the Server Name configuration setting in the registry that you specified during installation. This parameter takes effect only when running in command-line mode, which also requires the `--console` command-line switch. **Sample syntax:** `sensor.exe --server "MyServerName" --console`
`--uninstall`	Unregisters the sensor with the Windows Service Control Manager.
`--version`	Prints the version of the sensor and exits.

Default Rogue System Detection queries

Rogue System Detection provides default queries that you can use to retrieve specific information from your network.

These queries can be modified or duplicated in the same manner as other queries in ePolicy Orchestrator. You can also create custom queries, display query results in dashboard monitors, and add those dashboard monitors to the Dashboards section in ePolicy Orchestrator.

For more information on using dashboards, see *Assessing Your Environment With Dashboards*.

Rogue System Detection query definitions

Query	Definition
Active Sensor Response (Last 24 Hours)	Returns the details of active sensors installed on your network in the last 24 hours, in pie chart format.
Passive Sensor Response (Last 24 Hours)	Returns the details of passive sensors installed on your network in the last 24 hours, in pie chart format.
Rogue Systems, By Domain (Last 7 Days)	Returns the details of systems detected on your network as rogue systems in the last seven days, grouped by domain, in table format.
Rogue Systems, By OS (Last 7 Days)	Returns the details of systems detected on your network as rogue systems in the last seven days, grouped by operating system, in pie chart format.
Rogue Systems, By OUI (Last 7 Days)	Returns the details of systems detected on your network as rogue systems in the last seven days, grouped by organizationally unique identifier, in pie chart format.
Subnet Coverage	Returns the details of detected subnets on your network, in pie chart format.

Configuring Rogue System Detection server settings

Rogue System Detection server settings determine how information about subnets and detected systems is displayed in the Detected Systems page within your ePolicy Orchestrator console.

Configuring server settings for Rogue System Detection

These server settings allow you to customize Rogue System Detection to meet the specific needs of your organization.

These settings control important behavior, including:

- Whether a detected system is compliant (based on last agent communication).
- The categories for system exceptions (systems that don't need an agent).
- How detected system interfaces are matched.
- The list of OUIs used to identify vendor specific NICs used by systems connecting to your network.
- How your Rogue System Sensors are configured.

Use these tasks to configure server settings for Rogue System Detection.

Tasks

- *Editing Detected System Compliance* on page 40
  Use this task to edit the Detected System Compliance settings. These settings are user-configured and have two important functions:
- *Editing Detected System Exception Categories* on page 41
- *Editing Detected Systems Matching* on page 41
  Use this task to edit the matching settings for Rogue System Detection. Matching settings are user-configured and have these important functions:
- *Editing Detected System OUIs* on page 42
  Use this task to edit the settings that specify the method and location used to update Detected System OUIs (Organizationally Unique Identifiers). Rogue System Detection uses OUIs to provide details about the systems on your network.
- *Edit Rogue System Sensor settings* on page 28
  Edit the Rogue System Sensor settings to determine how sensors interact with each other and the ePolicy Orchestrator server.

Editing Detected System Compliance

Use this task to edit the Detected System Compliance settings. These settings are user-configured and have two important functions:

- They specify the time-frame that determines the state of detected systems (Managed, Rogue, Exception, Inactive).
- They control the visual feedback of the Rogue System Detection status monitors on the Detected Systems page.

For option definitions, click **?** in the interface.

Task

1 Click **Menu** | **Configuration** | **Server Settings**, then in the Settings Categories list, click **Detected System Compliance**.

2 In the details pane, click **Edit**.

3 Edit the number of days to categorize Detected Systems as Managed or Inactive.

The number of days in **Rogue** | **Has Agent in McAfee ePO Database, but is older than__days** is controlled by the number of days set in the Managed field.

4 Edit the percentage levels for these options, so that the color codes represent your requirements:
   - **Covered Subnets** — Required coverage.
   - **Compliant Systems** — Required compliance status.
   - **Sensor Health** — Ratio of active to missing sensors.

5 **ePO Servers** — Configure additional McAfee ePO servers whose detected systems should not be considered rogue systems.

6 Click **Save**.

Editing Detected System Exception Categories

Use this task to configure and edit the categories to use to manage exception systems in your network. Exceptions are system that you know are unmanaged (don't have a McAfee Agent on them).

Task

For option definitions, click **?** in the interface.

1 Click **Menu** | **Configuration** | **Server Settings**, then from the Settings Categories list, select **Detected System Exception Categories** and click **Edit**.

2 Add or subtract exception categories using **+** and **-**.

Use the **Delete** and **Change** links to modify existing exceptions categories.

3 Specify a name and description for each exception category. For example, you might want to create a category named "Printers-US-NW" to contain all the printers on your network in your company's Northwest regional offices. This way you can keep track of these systems without receiving reports about them being rogue.

4 Click **Save**.

Editing Detected Systems Matching

Use this task to edit the matching settings for Rogue System Detection. Matching settings are user-configured and have these important functions:

- They define the properties that determine how newly detected interfaces are matched with existing systems.
- They specify static IP ranges for matching.
- They specify which ports to check for a McAfee Agent.

For option definitions, click **?** in the interface.

Task

1 Click **Menu** | **Configuration** | **Server Settings**, then in the Settings Categories list select **Detected System Matching** and click **Edit**.

2 Use the **Matching Detected Systems** table to define the properties that determine when to match detected systems.

3 Use the **Matching Managed Systems** table to define the properties that determine when a newly detected interface belongs to an existing managed system.

4 In **Static IP Ranges for Matching**, type the static IP ranges to use when matching on static IP addresses.

5 In **Alternative McAfee Agent Ports**, specify any alternate ports you want to use when querying detected systems to check for a McAfee Agent.

6 Click **Save**.

Editing Detected System OUIs

Use this task to edit the settings that specify the method and location used to update Detected System OUIs (Organizationally Unique Identifiers). Rogue System Detection uses OUIs to provide details about the systems on your network.

Task

For option definitions, click **?** in the interface.

1 Click **Menu** | **Configuration** | **Server Settings**, then from the server settings Categories list, select **Detected System OUIs** and click **Edit**.

2 Choose one of the following options to specify where to update your list of OUIs:

- **URL** — Specifies the location of an OUI.txt file to be read. The McAfee ePO server must have access to this location in order to pull the file directly from the path specified in the URL.
- **Server location** — Specifies a location on this McAfee ePO server where the OUI.txt file is located.
- **File upload** — Type or browse to an OUI.txt file to upload to this McAfee ePO server for processing, then click **Update**.

Edit Rogue System Sensor settings

Edit the Rogue System Sensor settings to determine how sensors interact with each other and the ePolicy Orchestrator server.

Sensor settings are user-configured and specify:

- The amount of time sensors are active
- The maximum number of sensors active on each subnet
- How long the server waits to hear from a sensor before categorizing it as missing

Task

For option definitions, click **?** in the interface.

1 Click **Menu** | **Configuration** | **Server Settings**, then in the Settings Categories list, select **Rogue System Sensor** and click **Edit**.

2 Edit the **Sensor Timeout** field to set the maximum amount of time the server waits for a sensor to call in before marking it as missing.

3 Edit the **Sensors per Subnet** field to set the maximum number of sensors active on each subnet, or select **All sensors active**.

4 Add a list of **Sensor Scanning** MAC addresses and OUIs that the sensors should not actively probe, regardless of the configured policy.

5 Edit the **Active Period** field to set the maximum amount of time that passes before the server tells a sensor to become passive, or to allow a new sensor to become active.

The Active Period setting doesn't set the communication times for the active and inactive sensors. Communication time is configured using communication policy settings for Rogue System Detection.

6 Click **Save**.

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`

Browse for Systems page

Use this page to browse and add systems from the selected domain.

Option definitions

Option	Definition
Domain	Select the required domain from the drop-down list. The client system in the selected domain are listed.
Show/Hide Filter	Shows or hides these options used to find and filter client systems: • **Show selected rows** — Displays only the rows you have selected.
Actions	Specifies the actions you can perform on the selected client systems, including: • **Choose Columns** — Opens the Select the Columns to Display page. Use this to select the columns to display. • **Export Table** — Opens the Export page. Use this to specify the format and the package of files to be exported. You can save or email the list of client systems in the selected domain.

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. Default is 5 minutes. Systems in the sensor's memory cache are not considered new detections and are not scanned again for their McAfee Agent.
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. 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 if they should 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. • Set the multicast group to receive the active sensors. Either: • Type **Ipv4 multicast group** address. The default address is 239.5.6.7. • Type **Ipv6 multicast group** address. The default address is ff12::1. 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 Subnets Details page

Use this page to view detected subnet details. From this location you can view the details of the sensors installed on this subnet, if any, by clicking the details link in the System Information pane.

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** — Marks the selected subnets as ignored. Ignored subnets are no longer recognized by ePolicy Orchestrator. • **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.
Sensor Information	Specifies the IP address of the sensor, whether it is active, its last communication time, and a link to the Rogue System Sensor Details page.
Detected Subnets Information	Specifies information about detected subnets, including: • **Contains Rogue** — Specifies whether the subnet contains rogue systems. • **Covered** — Indicates whether the displayed subnet is covered by a Rogue System Sensor. • **Ignored** — Indicates whether the displayed subnet is marked as ignored. • **IP Address** — Specifies the IP address of the displayed subnet. • **Subnet Mask** — Specifies the subnet mask (IP netmask) for the displayed subnet. • **Subnet Name** — Specifies the name of the displayed subnet. The default name for a subnet is its IP address.

Detected Subnets 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 to select the columns of data to display in this Detected Subnets page.
	• **Export** — Opens the Export page. Use this to specify the format and the package of files to 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** — Marks the selected subnets as ignored. Ignored subnets are no longer recognized by ePolicy Orchestrator.
	  • **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 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 that the system does not need to be managed, 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 tells ePolicy Orchestrator that the systems need to be managed, and returns them to their original category. For example, managed systems return to the managed category.
Additional Detail for Managed Systems	Links to the ePolicy Orchestrator System Details page for this system.

Option	Definition
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. • **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.

Option	Definition
	• **Rogue State** — Specifies the rogue state of a detected system, for example, Inactive Agent. • **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. • Don't include colons when searching for detected systems based on their MAC address. • You can use "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 the item(s) you are marking 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 they are detected by a sensor. • **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 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 that the system does not need to be managed, 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 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.
	  • **Ping** — Sends an ICMP echo to the selected system to verify that it can be reached.
	  • **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 tells ePolicy Orchestrator that the systems need to be managed, 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 rouge 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 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 DHCP monitoring is enabled, a single sensor installed on a DHCP server can monitor all systems and subnets that it serves: • **Disabled** — Select this box to disable DHCP monitoring. • **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.  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:
	• **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 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. 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 marked as exceptions. Default is disabled.
	  • **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 is the default option.

Report on self-configured subnets	Select the **Enabled** box to enable reporting on self-configured subnets. This prevents subnets that have a netmask of /32 from being ignored.

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 marked as exceptions. • **Inactive** — Systems categorized as rogues that have not been detected by a sensor 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. 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.
Matching Detected Systems	Defines the properties that determine when to match newly detected system interfaces to an existing detected system.

Option	Definition
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 ranges for use when matching static IP addresses. 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 Orchestratorto identify product information about managed systems, such as manufacturer.

Option definitions

Option	Definition
Last Updated	Specifies the last time your OUI file was updated.
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 file location on the McAfee ePO server that contains an updated OUI list. • **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 adds new exception categories for detected systems. The Rogue System Sensor cannot be installed on a detected system that has been added to a 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: McAfee Agent page

The McAfee Agent permission set determines if users can view or edit agent policy settings.

Option definitions

Option	Definition
No permissions	Grants no permissions to the McAfee Agent.
View settings	Grants read-only permissions to McAfee Agent policy and tasks settings.
View and change settings	Grants read-write permissions to McAfee Agent policy and tasks settings.

Edit Permission Set: Rogue System Detection page

Use this page to select permissions to Rogue System Detection.

Options 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.
Create and edit Rogue System information; manage Rogue Sensors; Deploy Agents and Add to System Tree	Grants full access to Rogue System Detection.  The Deploy Agents and System Tee 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 to the Rogue System Sensor.

Option definitions

Option	Definition
Rogue System Detection 4.6.0:Rogue System Sensor	Controls access to the Rogue System Sensor. Choose from the following access levels: • **No permissions** — Grants no access to sensors. • **View Settings** — Grants only the ability to view the settings for sensors. • **View and change settings** — Grants full access to the settings for sensors.
Rogue System Detection 4.6.0: 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. • **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 marking 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 (1440 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 should not scan, regardless of the sensor's policy.
Sensor Timeout	Specifies the maximum amount of time a sensor can be out of contact before being marked as missing. The maximum sensor timeout period is seven days (168 hours or 10080 minutes).

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 on which your McAfee ePO server is installed. **Rogue System Detection** treats agents managed by any 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.

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 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 systems by uploading a text file containing a list of system names, with each system separated by a new line.

Interfaces page (Rogue System Detection policy pages)

Use this page to specify which interfaces sensors listen to.

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.
Only listen on interfaces whose IP addresses are included in the following 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 CIDR that specifies the subnet mask.
Do not listen on interfaces whose IP addresses are included in the following 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 that specifies the subnet mask.

Overall System Status monitor

Use the Overall System Status monitor to view the current 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 marked as exceptions, to total detected systems. The color of the title bar is determined by user-configured options based on this ratio. 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 marked 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 that have not been detected by a sensor in a specified time period.
Managed	Specifies the number of systems on your network that are managed by ePolicy Orchestrator.
Rogue	Specifies the number of systems on your network that are not managed by ePolicy Orchestrator.

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 details 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. • **IP Address** — Specifies the IP address of the system. • **MAC Address** — Specifies the MAC address of the system.
Actions	Specifies the actions that can be performed on this 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 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 a managed system is added to the Rogue Sensor Blacklist, it is returned to the Managed list when removed from the blacklist.

Table Actions	Specifies the actions that can be performed on the Rogue Sensor Blacklist page, including:
	• **Choose Columns** — Choose the columns of data to display on the Rogue Sensor Blacklist page.
	• **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	Specifes the actions that can be performed 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 currently installed. • **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 the sensor is installed on, 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. Instances of the Rogue System Sensor installed on your network 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 can be performed 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 Sensors page. • **Export Table** — Exports the table of data to a user-specified format and location.

Rogue System Sensor Status monitor

Use the Rogue System Sensor Status monitor to view the current status of the sensors installed on your network by category. From this location, you can view the list of sensors that make up a category by clicking it. You can also view the list of sensors on the sensor blacklist by clicking **View Blacklist**.

The color-coded title bar across the top of the status monitor displays the health of sensors on your network. This is determined by the ratio of missing sensors to total sensors installed. The color of the title bar is determined by user-configured options based on this ratio. There are three color-codes: green, orange, and red. They represent good, marginal, and poor health, respectively.

Option definitions

Option	Definition
Active	Specifies the number of active sensors on your network. Active sensors report to ePolicy Orchestrator at specified time periods.
Missing	Specifies the number of missing sensors on your network. Missing sensors have not contacted ePolicy Orchestrator in a specified time period.
Passive	Specifies the number of passive sensors on your network. Passive sensors are in contact with ePolicy Orchestrator, but not reporting. These sensors are activated by ePolicy Orchestrator at specified time periods.
View Blacklist	Displays the Rogue Sensor Blacklist page.

Subnet Status monitor

Use the Subnet Status monitor to view the current 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 color-coded title bar across the top of the status monitor displays the percentage of subnets on your network that are covered. This percentage represents the ratio of covered subnets to uncovered subnets. The color of the title bar is determined by user-configured options 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.
Covered	Specifies the number of subnets on your network that are covered. Covered subnets have two 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 system interfaces.

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	Marks the highlighted subnet in the Top 25 Subnets list as ignored. Ignored subnets are no longer monitored by ePolicy Orchestrator.
Selected Row Actions	Specifies the actions that can be performed on entries in Togue 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 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.