McAfee Rogue System Detection 5.0.6 Installation Guide

Contents

Considerations for installing Rogue System Detection

When planning your deployment of **Rogue System Detection** 5.x, it is important to consider how it affects existing **McAfee** products and how the policy works.

Deployment of Rogue System Detection 5.x sensors

Although the **Rogue System Detection** 5.x sensor technology continues to support deployment on DHCP servers, **McAfee** recommends that you deploy sensors on every subnet. This provides the best visibility of rogue systems, full coverage of the entire enterprise network, fastest detection time, and best accuracy for determining rogue device attributes, such as OS detection.

Ports used for active detection

Rogue System Detection 5.x uses sensor technology to detect rogue systems. The sensor uses a combination of passive and active detection techniques. For active detection, the Rogue System Sensor (5.x) requires a smaller number of ports than previous releases. It attempts to use ports that are already known to be open or closed. Otherwise, it uses the following ports:

- **TCP** — Ports 22, 80, 443, and 445.
- **UDP** — Ports 65534, 65533, and 65532. The software selects the first unused port.

Interaction with other McAfee products

The Rogue System Sensor integrates with **McAfee Agent** on managed systems. The Rogue System Sensor 4.x integrates with the **McAfee® Rogue Database Detection (RDD)** sensor. The Rogue System Sensor 5.x does not support integration with **RDD**. If you use **RDD**, you can maintain existing 4.x sensors and deploy additional new **Rogue System Detection** 5.x sensors.

Use of WinPCap

You cannot deploy the Rogue System Sensor to a system that is running WinPCap or any software using WinPCap. If WinPCap is installed, the sensor installation stops and logs an error message.

If you install WinPCap on a system that already has a sensor installed, it can cause the sensor to stop functioning properly.

Microsoft KB2563894 security update required on systems running the sensor

Any system you install a sensor on requires the Microsoft KB2563894 security update. If the update is not present, the sensor installation stops and logs an error message. This update is required to fix an issue that can cause the system to stop responding due to network traffic types used by the Rogue System Sensor.

Rogue System Detection policies

Rogue System Detection can simultaneously manage Rogue System Sensor versions 4.x and 5.x. **Rogue System Detection** sends the same policy to all sensors. Some policy settings are relevant only for 4.x sensors, some for 5.x sensors, and some for all sensors. When a sensor receives a **Rogue System Detection** policy from **McAfee ePO**, it uses the policy settings that apply to its version.

A revision number was added to the policy and to the server settings. This number can be used to easily identify which specific policy and server setting versions are applied to a specific sensor.

Internal database

Rogue System Sensor 5.x maintains a state of all detected and profiled systems on the network that is encrypted for security. The encryption key is unique for each **Rogue System Detection** installation.

If you uninstall and then reinstall **Rogue System Detection**, the software generates a new encryption key. This means that all managed sensors drop their existing database, create a new database, and redetect the systems on the network. To prevent the extra load and network traffic, avoid uninstalling and reinstalling **Rogue System Detection** unless required or instructed by **McAfee** support.

Sensor components and log files

Rogue System Sensor 5.x is designed to detect rogue systems for its local subnet only. It runs two components on the systems they are installed on:

- **RSDPP** — A Windows service that is responsible for managing communications with **Rogue System Detection** through the **McAfee Agent**.
- **Balash** — A Windows process that is responsible for discovering and profiling devices operating on the network.

Rogue System Sensor 5.x maintains two log files that can be used to solve issues:

- **rsdpp.log** — The log file of the RSDPP service contains information about the sensor installation process and communications with **ePolicy Orchestrator** through the **McAfee Agent**.
- **balash.log** — The log file of the Balash process contains information about the network detection performed by the sensor and the devices that were discovered and profiled.

The **balash.log** file can contain sensitive information, such as the media access control addresses (MAC) and IP addresses of systems on the network. By default, the file contains only messages tagged with **Error** and **Critical** priority. For troubleshooting, you can gather more detailed information by setting the **Log File Settings** configuration on the policy's **General** tab to **Log all messages (recommended for troubleshooting and debugging)**. It is important to reset this configuration to the default level once you finish troubleshooting.

Getting started

To configure **Rogue System Detection**, you enable and set options on the **Server Settings** page, create policies, and install Rogue System Sensors on systems in the managed subnets.

About policies

A policy is a collection of settings that you create and configure, then enforce.

Policies are organized by product, then by categories within each product. For example, the **McAfee Agent** product includes categories for **General**, **Repository**, and **Troubleshooting**.

To see policies in a specific policy category, select **Menu** → **Policy** → **Policy Catalog**, then select a product and category from the drop-down lists. **On the Policy Catalog page, users can see only policies for products they have permissions to.**

Each category includes two default policies, **McAfee Default** and **My Default**. You can't delete, edit, export, or rename these policies, but you can copy them and edit the copy.

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.

Note

If you install Rogue System Sensors on many 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 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.

Tip

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.

⚠ **Caution**

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.

Note

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.

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 process is similar to managing policies for any deployed product. The **Rogue System Detection** policy pages are installed on the **McAfee ePO** server at installation. Groups or individual systems inherit policy settings that you assign to higher levels of the **System Tree**.

Tip

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. 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.

Configure Rogue System Detection server and policy settings

Confirm the default configuration of the **Rogue System Detection** server settings. These server settings determine what a rogue system is, configure sensor settings, and more.

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

Task

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 policy, click Actions → New Policy.**
3. **On the General tab configure:**
    - **Rogue System Sensor** — Select **Enable** to start a Rogue System Sensor after it is deployed.
    - **Server name or IP address** — Confirm that the default server name or IP address is the **McAfee ePO** server or Agent Handler.
    - **Log File Settings** — You can select whether to log only messages with **Error** and **Critical** priority or, for help in troubleshooting issues, to log all messages.

      Note

      This section is relevant for 5.x sensors only.

    - **Policy Revision ID** — Specifies the revision number of the policy, which is incremented every time you save the policy.

      Note

      This section is relevant for 5.x sensors only.

4. **On the Communications tab, configure:**
    - **Sensor's detected system cache lifetime** — You can increase this setting on large widely dispersed networks to reduce traffic on the subnet.

> **Note**
>
> This section is relevant for 4.x sensors only.

- **Reporting time for active sensors** — You can increase this setting on large widely dispersed networks to reduce traffic back to the **McAfee ePO** server.
- **Active sensor election** — These settings depend 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 setting reduces the traffic that 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.

          > **Caution**
          >
          > Be careful about installing Rogue System Sensors on many nodes on many subnets and configure the policy to **Use Local Sensor Election** and then later changing the policy to **Use ePO server to determine active sensors**. All previously installed sensors can overwhelm the **McAfee ePO** server asking to become active.

        - **Set the number of active sensor(s)** — This is the manual configuration solution.
    - Configure these settings 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 can increase this setting on slow networks to reduce traffic between sensors during the elections.

          > **Note**
          >
          > This setting is relevant for 4.x sensors only.

        - **Wait time between active sensor elections** — You can 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. Only change the default address if another feature is using the default.

      > **Note**
      >
      > This setting is relevant for 4.x sensors only.

    - **Sensor-to-Sensor communication port** — Only 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 voice over IP subnet, you can add that subnet address to the Do not listen on list and the voice over IP phone systems are ignored as rogue systems.**

   Note

   The **Interfaces** tab is relevant for 4.x sensors only.

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.

     Note

     This setting is relevant for 4.x sensors only.

     Note

     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 Section** → **Detected Systems** and click any system that appears in the **Detected System Interfaces by Subnet**.

     Note

     This setting is relevant for 4.x sensors only.

     Important

     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 illogical symbols and characters. It is important to use the **Exceptions List** and to disable 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 many erroneous 32-bit subnets appear in the subnet list. **McAfee** recommends that you enable this feature only when using DHCP detection and not Layer 2 detection.

Note

This setting is relevant for 4.x sensors only.

- **Sensor Scanning** — Select **Use active zero-configuration resolution** to enable the sensor to send multicast DNS requests and select **Use DNS queries for DNS name resolution** to resolve IP Addresses using DNS servers.

Note

This setting is relevant for 5.x sensors only.

Results

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

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

Edit Detected System Compliance

Edit the **Detected System Compliance** settings. These settings are user-configured.

The settings 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.

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.**

Note

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
   - **System Compliance** — Required compliance status
   - **Sensor Health** — Ratio of active to missing sensors
5. **Use ePO Servers to configure additional McAfee ePO servers whose detected systems are not considered rogue systems.**
6. **Click Save.**

Edit Detected System Exception Categories

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

Task

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 -.**

   Note

   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 printers on your network in your company's Northwest regional offices. This way you can track these systems without receiving reports about them being rogue.

4. **Click Save.**

Edit Detected System OUIs

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

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 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

Determine how sensors interact with each other and the **ePolicy Orchestrator** server.

Sensor settings are user-configured and specify:

- The amount of time that 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

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 specifying 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. **Edit the Sensor Scanning section to specify systems you do not want to scan. This setting is useful for saving resources and lessening network traffic.**
   - Add a list of **Sensor Scanning** MAC addresses and OUIs that the sensors do not actively probe, regardless of the configured policy.
   - For version 5.x sensors, you can add a list of IP addresses or subnet masks that sensors do not scan actively. These systems are not scanned regardless of the policy settings for the sensor.
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 allows a new sensor to become active.**

   Note

   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. **The Server Settings Revision ID field specifies the revision number of the setting. The ID is incremented every time the Server Settings are saved.**

   Note

   This section applies only to version 5.x sensors.

7. **Click Save.**

Results

The new **Server Settings** take effect after the next agent-server communication interval.

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 administrators automatically include full access to all products and features.

This table shows the **Rogue System Detection** permission sets and their available rights.

Rogue System Detection permissions

Name	Possible 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	• **Rogue System Detection : Policy** □ No permissions □ View settings □ View and change settings • **Rogue System Detection : Tasks** □ No permissions □ View settings □ View and change settings

This table shows the default **ePolicy Orchestrator** permission sets and their rights.

Default Permission Sets and their Rights

Permission set	Rights
Executive Reviewer	No permissions
Global Reviewer	• View sensor policy settings • View sensor task settings

Permission set	Rights
Group Admin	No permissions
Group Reviewer	No permissions

Install sensors

After you configure **Rogue System Detection** server settings, install the **Rogue System Detection** sensors. Where you install the sensors and how many sensors you install affects how effective **Rogue System Detection** is and can affect your network bandwidth.

Before you begin

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

You can install **Rogue System Detection** sensors on these types of systems:

- **DNS or any system that is always connected to the subnet and monitoring traffic** — These systems are the best place to install **Rogue System Detection** sensors because they are not often turned on or off and are seldom disconnected from the network.
- **DHCP servers on multicast subnets** — DHCP servers constantly monitor multicast traffic and instantly detect when a new system connects to the subnet.
- **All systems on a multicast subnet** — This allows you to configure **Active sensor election** in the **Rogue System Detection** server settings. Once configured, all systems on a multicast subnet run an election algorithm to set some system sensors as active and the remainder as passive. The configuration settings control how often the software runs the algorithm.

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.

Task

1. **Click Menu → Systems Section → System Tree → Systems and click any system.**

Tip

You can use the **Managed Systems for Subnet xxx.xxx.xxx.xxx** page to select systems. Click **Menu → Systems Section → Detected Systems**, click **Covered** or **Contains Rogues** in the **Subnet Status** monitor, then select any subnet and click **Actions → Detected Subnet → View Managed Systems**.

Tip

You can also use the **Systems** page to select systems. Click **Menu** → **Systems Section** → **System Tree**.

2. **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 a group in the **System Tree**, and select the systems where you want to install sensors.
3. **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

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.**

Tip

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.**

Results

At every scheduled run, the query installs the latest sensor package to systems that meet the specified criteria.

Use a client task to install sensors

Create a client task that installs the latest sensor package to systems on your network.

Task

1. **Click Menu → Policy → Client Task Catalog, select Rogue System Detection → Sensor Deployment as Client Task Types, then click Actions → New Task. The New Task dialog box appears.**
2. **Verify 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 Section → System Tree → Systems, then select the system on which you want to install sensors, then click Actions → Agent → Modify Tasks on a single system.**
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 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.**

Results

At every scheduled run, the client task installs the latest sensor package to systems that meet the specified criteria.

Configure a deployment task for groups of managed systems

Configure a product deployment task to deploy products to groups of managed systems in the **System Tree**.

Task

1. **Open the New Task dialog box.**
   a. **Select Menu → Policy → Client Task Catalog.**
   b. **Under Client Task Types, select a product, then click New Task.**
2. **Select Product Deployment, then click OK.**
3. **Type a name for the task you are creating and add any notes.**
4. **Next to Target platforms, select the types of platform to use the deployment.**
5. **Next to Products and components, set the following:**

   - Select a product from the first drop-down list. **The products listed are products that you have checked in to the Master Repository. If you do not see the product you want to deploy listed here, check in the product package.**
   - Set the **Action** to **Install**, then select the **Language** of the package, and the **Branch**.

- To specify command-line installation options, type the options in the **Command line** text field. See the product documentation for information on command-line options of the product you are installing.

Note

You can click **+** or **–** to add or remove products and components from the list displayed.

6. **If you want to automatically update your security products, select Auto Update.**
   This also deploys the hotfixes and patches for your product automatically.

Note

If you set your security product to update automatically, you cannot set the **Action** to **Remove**.

7. **(Windows only) Next to Options, select whether you want to run this task for every policy process, then click Save.**
8. **Select Menu → Systems Section → System Tree → Assigned Client Tasks, then select the required group in the System Tree.**
9. **Select the Preset filter as Product Deployment (McAfee Agent).**
   Each assigned client task per selected category appears in the **details** pane.
10. **Click Actions → New Client Task Assignment.**
11. **On the Select Task page, select Product as McAfee Agent and Task Type as Product Deployment, then select the task you created to deploy your product.**
12. **Next to Tags, select the platforms you are deploying the packages to, then click Next:**
    - **Send this task to all computers**
    - **Send this task to only computers that have the following criteria** — Click **edit** next to the criteria to configure, select the tag group, select the tags to use in the criteria, then click **OK**.

Tip

To limit the list to specific tags, type the tag name in the text box under **Tags**.

13. **On the Schedule page, select whether the schedule is enabled, and specify the schedule details, then click Next.**
14. **Review the summary, then click Save.**

Results

At every scheduled run, the deployment task installs the latest sensor package to systems that meet the specified criteria.

Rogue System Detection command-line options

You can run command-line options on 4.x sensors from the client system to solve issues or override the standard configuration.

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 runtime command-line options for the sensor.

ⓘ **Important**

Command-line options only apply to supported 4.x sensors.

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`
`--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.

Remove sensors

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

Task

1. **To select a system from the Systems page, click Menu → Systems Section → System Tree.**
2. **Select a group in the System Tree, then select the systems that you want to remove sensors from.**

   Tip

   Select systems from the **Managed Systems for Subnet xxx.xxx.xxx.xxx** page by clicking **Menu** → **Systems Section** → **Detected Systems**, clicking any **Covered** or **Contains Rogues** system in the **Subnet Status** monitor, then selecting any subnet and clicking **View Managed Systems** and selecting systems.

   Tip

   You can also select systems from the **Systems Details** page by clicking **Menu** → **Systems Section** → **System Tree** → **Systems**, then clicking any system. You can remove the sensor from only the system you are viewing.

3. **Click Actions → Rogue Sensor → Remove Rogue Sensor.**
4. **In the Action pane, click OK.**

Results

The deployment task removes sensors from the selected systems.

COPYRIGHT