

McAfee Global Threat Intelligence: Turn It On

How to enable McAfee® Global Threat Intelligence™ in your
McAfee product

You have McAfee security products in your environment. You have heard of McAfee Global Threat Intelligence, our cloud-based, real-time threat intelligence service. Did you know that McAfee Global Threat Intelligence is already integrated in most McAfee products, is available at no charge, and is simple to enable? All you have to do is turn it on.

For more information about any product feature, visit the [McAfee Enterprise Support page](#) for product documentation and “how to” videos.

How do I enable McAfee Global Threat Intelligence?

Please select your product:

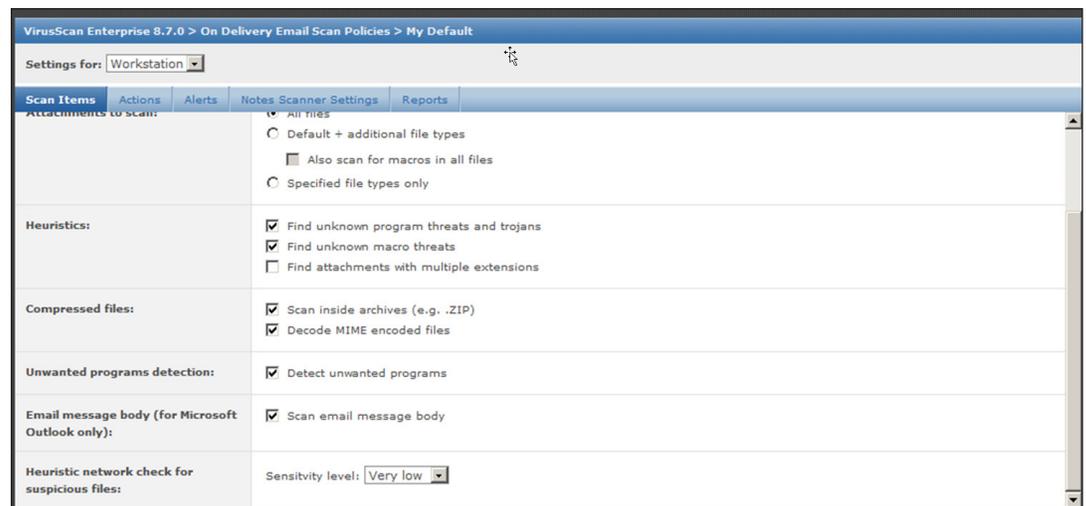
McAfee VirusScan Enterprise	1
McAfee SiteAdvisor Enterprise	4
McAfee Host Intrusion Prevention System	5
McAfee Firewall Enterprise	6
McAfee Network Security Platform	7
McAfee Network Threat Response	10
McAfee Network Threat Behavior Analysis	11
McAfee Email Gateway	12
McAfee Web Gateway	13
McAfee Email and Web Security Appliance	15
McAfee SaaS Email Protection	21
McAfee SaaS Web Protection	21

McAfee VirusScan Enterprise (8.5 or later)

McAfee VirusScan® Enterprise is integrated with McAfee Global Threat Intelligence file reputation. You can enable this service for On-Delivery Email Scan, On Demand Scan, or On Access Scan.

To enable McAfee Global Threat Intelligence file reputation for On-Delivery Email Scan:

1. In the McAfee ePolicy Orchestrator® (McAfee ePO™) Policy Catalog, select your product and version and On Delivery Email Scan Policies.
2. Select the option to edit the policy for Server or Workstation.
3. Under the Scan Items tab, under Heuristic network check for suspicious files (or, in 8.8, under McAfee Artemis® heuristic network check for suspicious files), select Sensitivity level.
4. Save the policy.



McAfee VirusScan Enterprise (Continued)

To enable McAfee Global Threat Intelligence file reputation for On-Demand Scan:

1. In the Systems Tree Menu of McAfee ePO, select Client Tasks and New Task.
2. Type a new name and select your product and version, then On Demand Scan task type, click Next.
3. Under the Performance tab, under Heuristic network check for suspicious files (or, in 8.8, under McAfee Artemis heuristic network check for suspicious files), choose Sensitivity level.
4. To schedule the task to run, click Next.
5. To review and save the task, click Save.

The screenshot shows the 'Client Task Builder' interface in the 'Configuration' step. The 'Performance' tab is selected, and the 'Heuristic network check for suspicious files' section is expanded. The 'Sensitivity level' is set to 'Very low'. Other options include 'When to defer' (with three unchecked checkboxes) and 'How long to defer' (set to 1 hour).

Client Task Builder	
1 Description	
2 Configuration	
3 Schedule	
4 Summary	
What do you want this task to do?	
Scan Locations Scan Items Exclusions Actions Performance Reports Task	
Specify performance options for the scan.	
When to defer:	<input type="checkbox"/> Defer scan when using battery power. <input type="checkbox"/> Defer scan during presentations. <input type="checkbox"/> User may defer scheduled scans.
How long to defer:	Defer at most <input type="text" value="1"/> hours (0=forever)
System utilization:	<input type="text" value="30%"/>
Heuristic network check for suspicious files:	Sensitivity level: <input type="text" value="Very low"/>
Back Next Cancel	

McAfee VirusScan Enterprise (Continued)

To enable McAfee Global Threat Intelligence file reputation for On-Access Scan:

1. In the McAfee ePO Policy Catalog select your product and version and On Access General Policies.
2. Select the option to edit the policy for Server or Workstation.
3. Under the General tab, under Heuristic network check for suspicious files (or, in 8.8, under McAfee Artemis heuristic network check for suspicious files), select the Sensitivity level.
4. Save the policy.

VirusScan Enterprise 8.7.0 > On-Access General Policies > My Default

Settings for: Workstation

General ScriptScan Blocking Messages Reports

Configure the general policy that applies to all on-access scanning.

Scan:	<input checked="" type="checkbox"/> Boot sectors <input checked="" type="checkbox"/> Floppy during shutdown <input type="checkbox"/> Processes on enable
Enable on-access scanning:	<input checked="" type="checkbox"/> Enable on-access scanning at system startup <input checked="" type="checkbox"/> Enable on-access scanning when the policy is enforced.
Maximum scan time:	Maximum archive scan time (seconds): 15 <input checked="" type="checkbox"/> Enforce a maximum scanning time for all files Maximum scan time (seconds): 45
Cookies	<input checked="" type="checkbox"/> Scan cookie files
Heuristic network check for suspicious files:	Sensitivity level: Very low

» Select another product.

McAfee SiteAdvisor Enterprise (3.0 or later)

McAfee SiteAdvisor® Enterprise is integrated with McAfee Global Threat Intelligence file reputation, web reputation, and web categorization.

To enable this service:

1. Launch McAfee ePO and Slick Menu, then Policy, then Policy Catalog.
2. Select Product—McAfee SiteAdvisor Enterprise 3.0 or later.
3. Click Enable or Disable from the policy menu.



» Select another product.

McAfee Host Intrusion Prevention System (8.0 or later)

McAfee Host Intrusion Prevention System (IPS) is integrated with McAfee Global Threat Intelligence file and network connection reputation.

To enable this service:

1. Launch McAfee ePO and go to the Policy Catalog.
2. Select Host Intrusion Prevention System 8.0 or later: Firewall under Product.
3. Select Firewall Options under Categories.
4. Click Edit corresponding to the policy for which you want to enable McAfee Global Threat Intelligence.
5. Select a value from the drop-down list for Incoming/Outgoing McAfee TrustedSource® Block Threshold.

The screenshot shows the 'Host Intrusion Prevention 8.0 > Firewall Options (Windows) > My Default' configuration window. It is divided into several sections:

- Firewall status:** Includes a checked 'Enabled' checkbox, radio buttons for 'Regular protection' (selected), 'Adaptive mode (rules are learned automatically)', and 'Learn mode (rules are learned after user interaction)'. There are also checkboxes for 'Allow traffic for unsupported protocols' and 'Allow bridged traffic', and 'Incoming' and 'Outgoing' checkboxes.
- Firewall client rules:** Includes a checked checkbox for 'Retain existing client rules when this policy is enforced'.
- Startup protection:** Includes an unchecked checkbox for 'Allow only outgoing traffic until the Host IPS service has started'.
- Protection options:** Includes a checked checkbox for 'Enable IP spoof protection' and an unchecked checkbox for 'Send events to ePO for TrustedSource violations'. It also features two dropdown menus for 'Incoming TrustedSource block threshold' and 'Outgoing TrustedSource block threshold', both currently set to 'Do not block'. A dropdown menu is open for the outgoing threshold, showing options: 'High Risk', 'Medium Risk', 'Unverified', and 'Do not block' (highlighted).
- Stateful firewall settings:** Includes a checked checkbox for 'Use FTP protocol inspection', a text input field with '30' for 'TCP connection timeout (in seconds)', and another text input field with '30' for 'UDP and ICMP echo virtual connection timeout (in seconds)'.

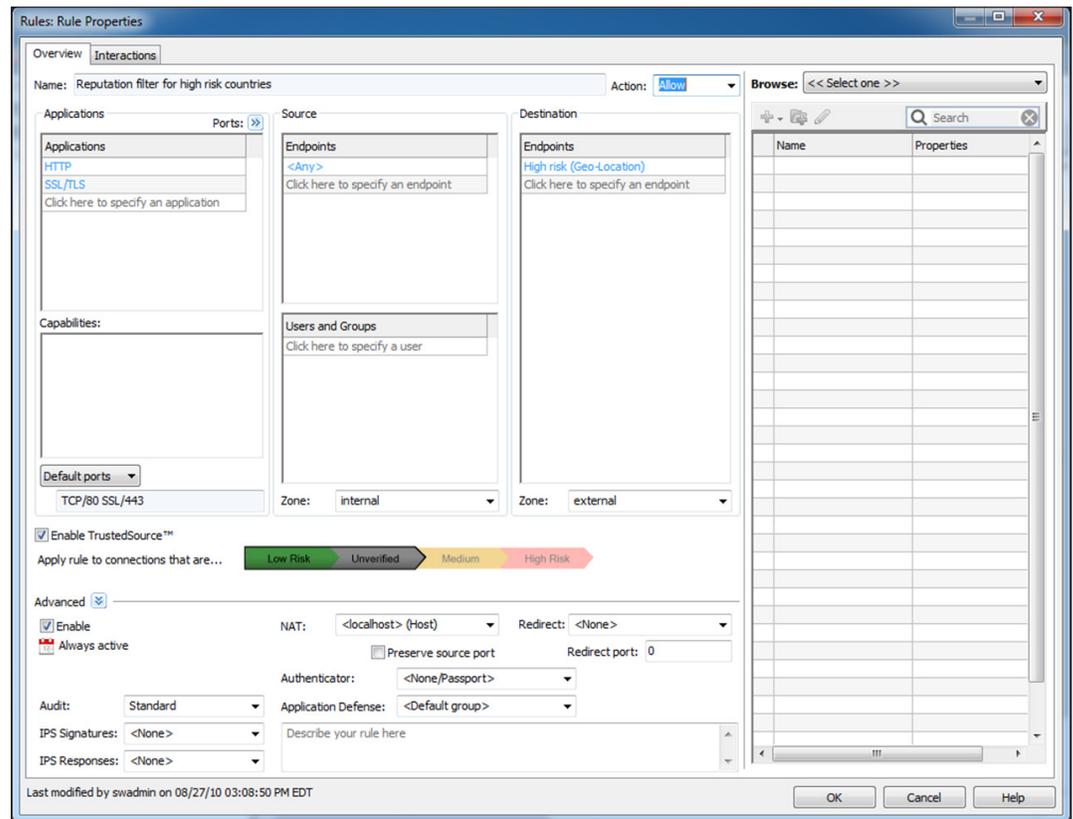
» Select another product.

McAfee Firewall Enterprise (7.0 or later)

McAfee Firewall Enterprise is integrated with McAfee Global Threat Intelligence network connection reputation.

To enable this service:

1. From the Administrative Console, on the resource tree on the left, select a specific Firewall, then select Policy, then Access Control Rules.
2. Create a new rule by clicking on the green plus sign at the top or select an existing rule from the list.
3. In the Rule Properties screen, select Enable TrustedSource.
4. Adjust network connection reputation level for the rule.



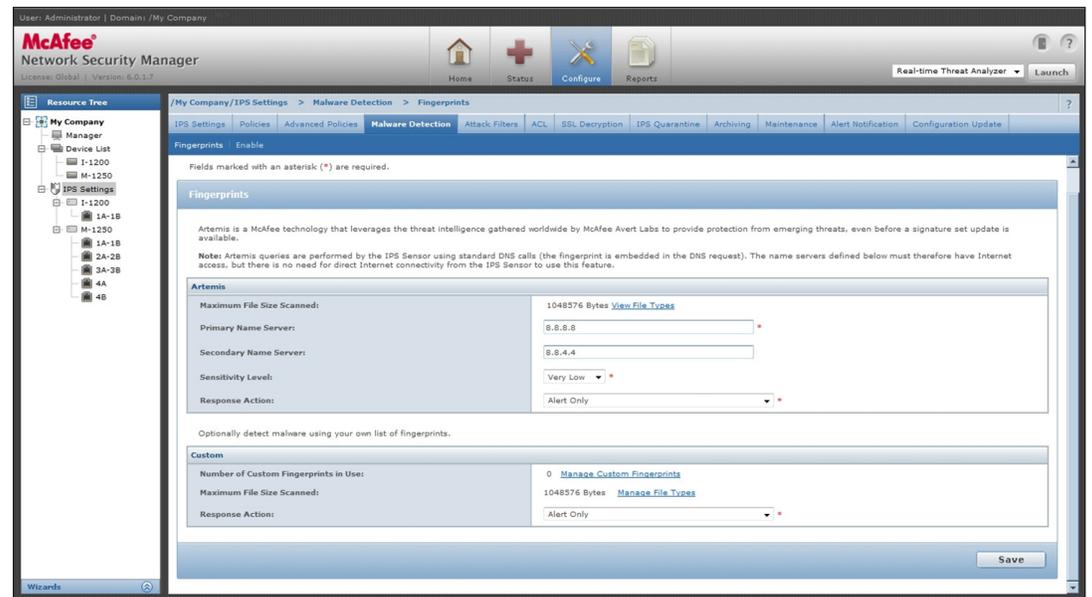
» Select another product.

McAfee Network Security Platform (6.0 or later for file, and 6.0.7 for network connection reputation)

McAfee Network Security Platform is integrated with McAfee Global Threat Intelligence file and network connection reputation.

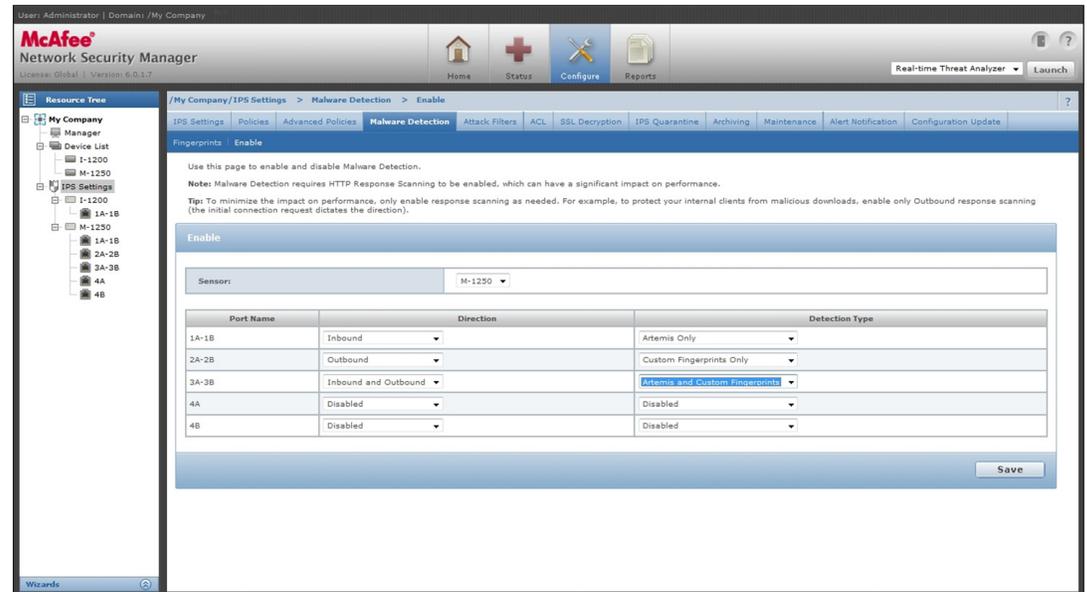
To enable McAfee Global Threat Intelligence file reputation:

1. In the Network Security Manager Resource Tree, select IPS Settings and select the Malware Detection tab.
2. Set the McAfee Global Threat Intelligence file reputation (Artemis) specific options for the sensor, including DNS servers, Sensitivity Level, and Response Action.
3. From here, you can also manage options related to the use of custom fingerprints.
4. Click save.



McAfee Network Security Platform (Continued)

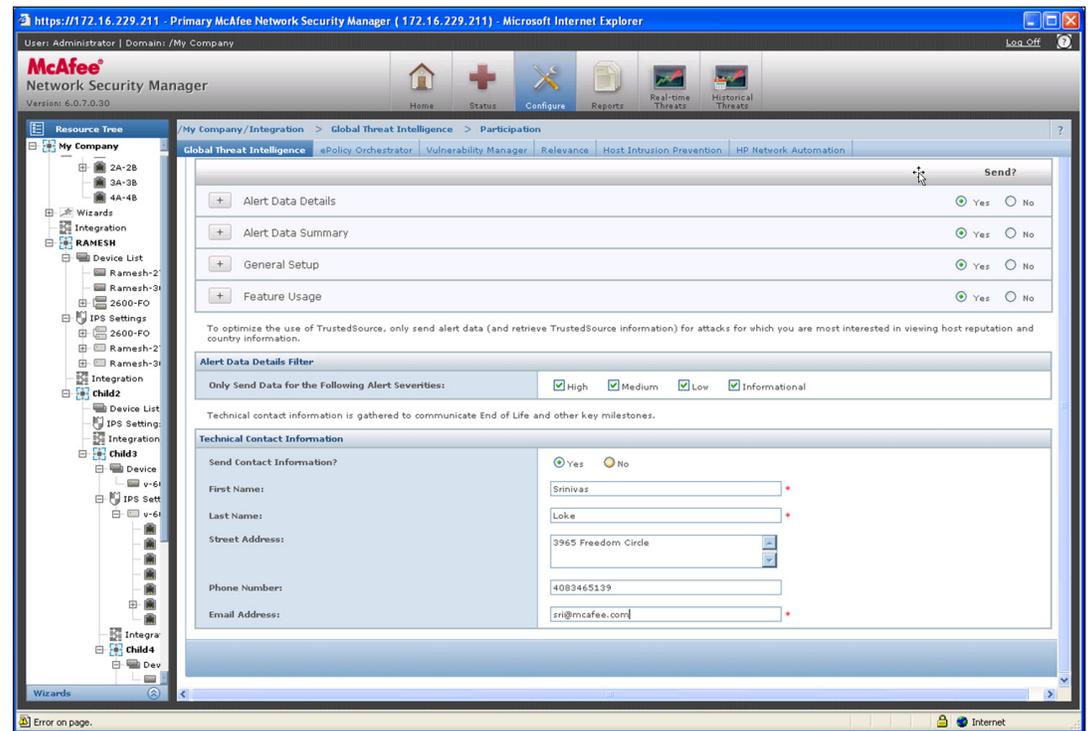
5. Select Enable options.
6. Set the Enable options per sensor and port or port pair.
7. For each port or port pair, choose a direction and detection type.
8. Click Save, then select Configuration Update for the changes to take effect.



McAfee Network Security Platform (Continued)

To enable McAfee Global Threat Intelligence network connection reputation:

1. In the Network Security Manager Resource Tree, select IPS Settings and select the Malware Detection tab.
2. In the Network Security Manager, navigate to My Company/Integration, then Global Threat Intelligence.
3. Once there, you can choose your participation levels, alert details, and technical information.



» Select another product.

McAfee Network Threat Response (2.1.1 or later)

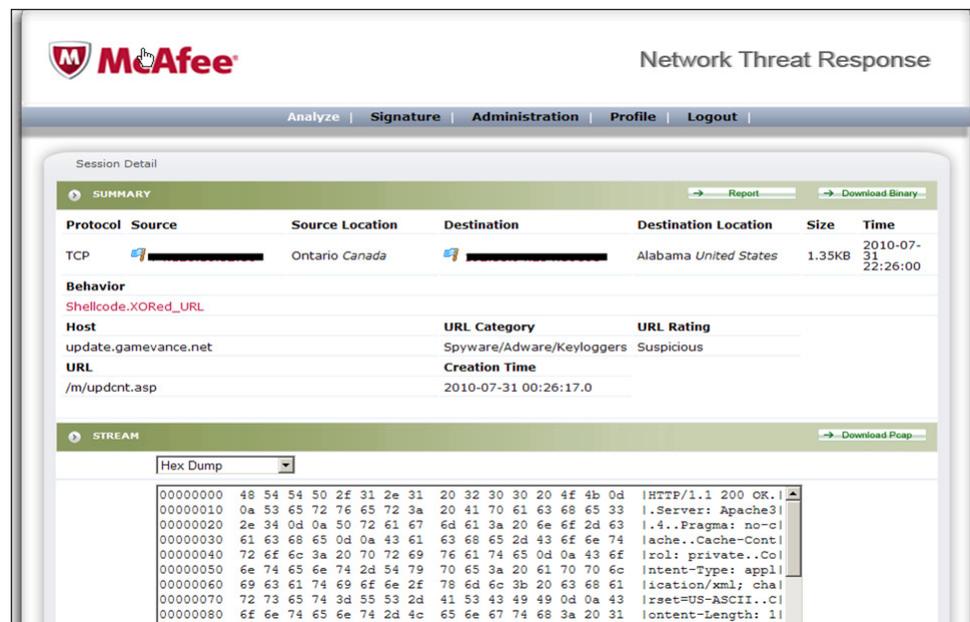
McAfee Network Threat Response is integrated with McAfee Global Threat Intelligence file and network connection reputation.

McAfee Network Threat Response integration with McAfee Global Threat Intelligence is on by default, so no action is necessary. However, it can be disabled if desired. The only setting an administrator may need to set to enable the feature is to set a proxy.

1. Select the drop-down menu Administration Proxy, enter the information, and commit the change.
2. McAfee Global Threat Intelligence file reputation (Artemis) will be updated with McAfee Network Threat Response's analysis and findings.
3. McAfee Global Threat Intelligence network connection reputation (TrustedSource) will be queried to provide event context.



For example, an analyst can quickly determine if a malicious file was downloaded from a suspicious URL before any detailed analysis takes place.



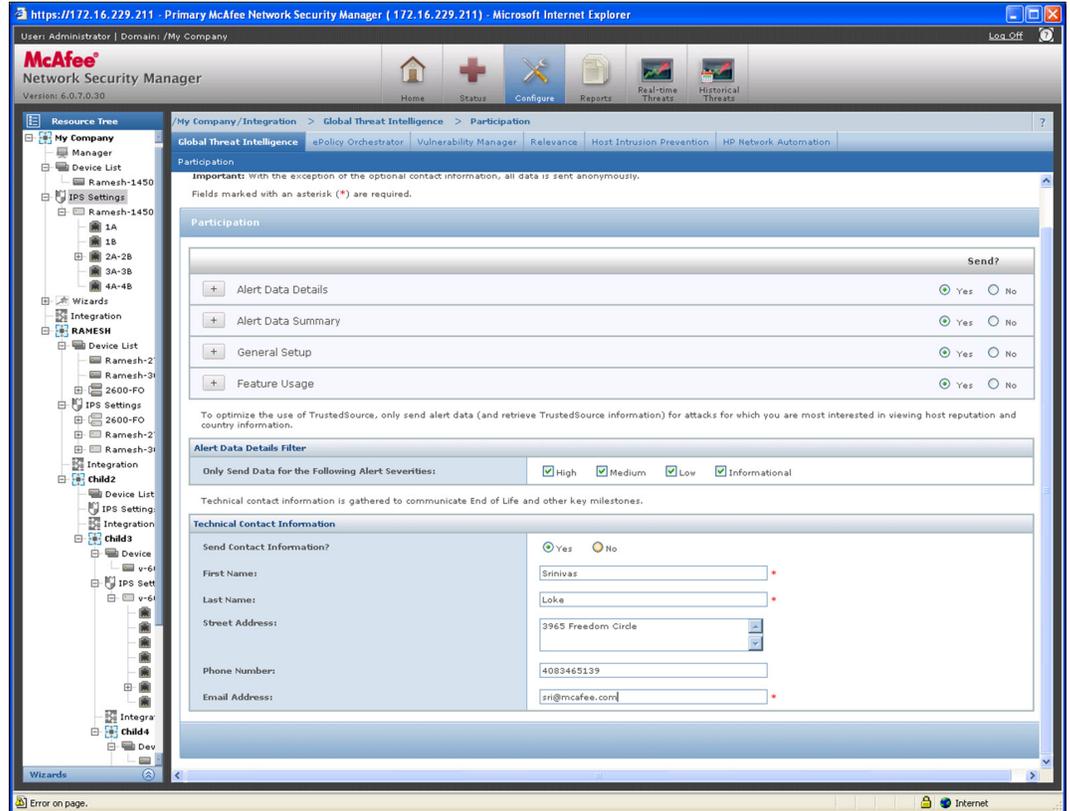
» Select another product.

McAfee Network Threat Behavior Analysis (1.0 or later)

McAfee Network Threat Behavior Analysis is integrated with McAfee Global Threat Intelligence network connection reputation.

To enable this service:

1. In the Network Security Manager, navigate to My Company/Integration, then Global Threat Intelligence.
2. Once there, you can choose your participation levels, alert details, and technical information.



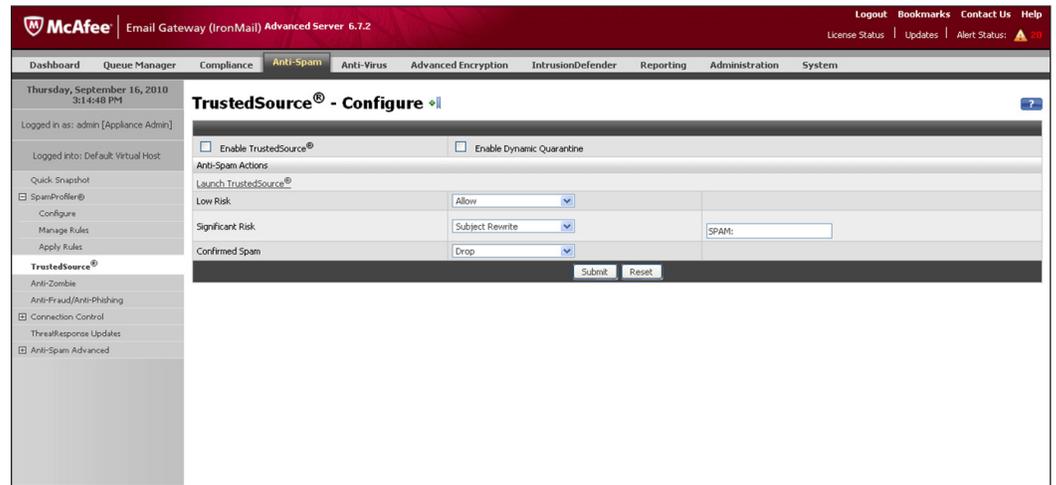
» Select another product.

McAfee Email Gateway (6.7.2 or later)

McAfee Email Gateway is integrated with McAfee Global Threat Intelligence message reputation.

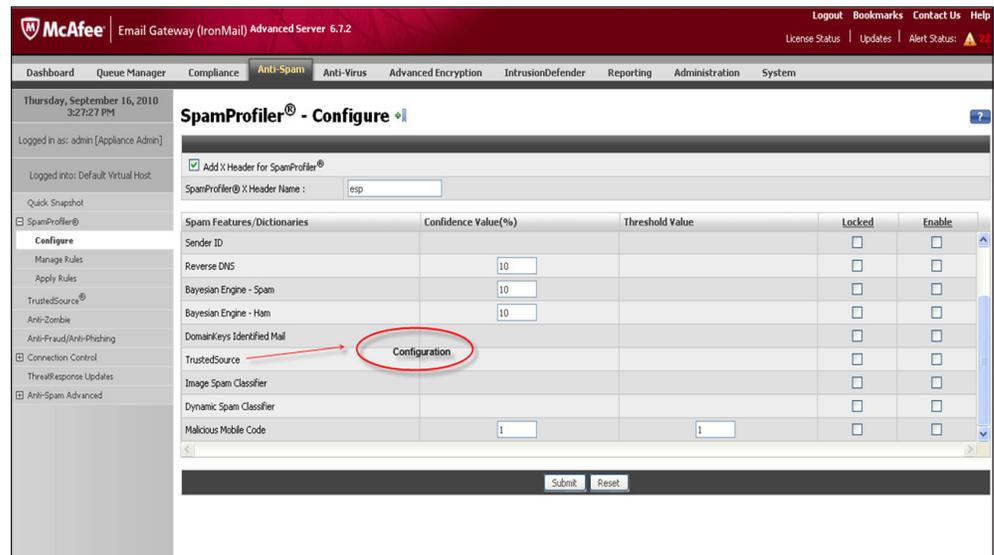
To enable this service:

1. Select Anti-Spam, TrustedSource.
2. Click Enable TrustedSource and set additional configuration if needed.



To enable McAfee Global Threat Intelligence message reputation in the Spam Profiler:

1. Select Anti-Spam, Spam Profiler, Configure.
2. Click Enable Trusted Source under Spam Features/Dictionaries.



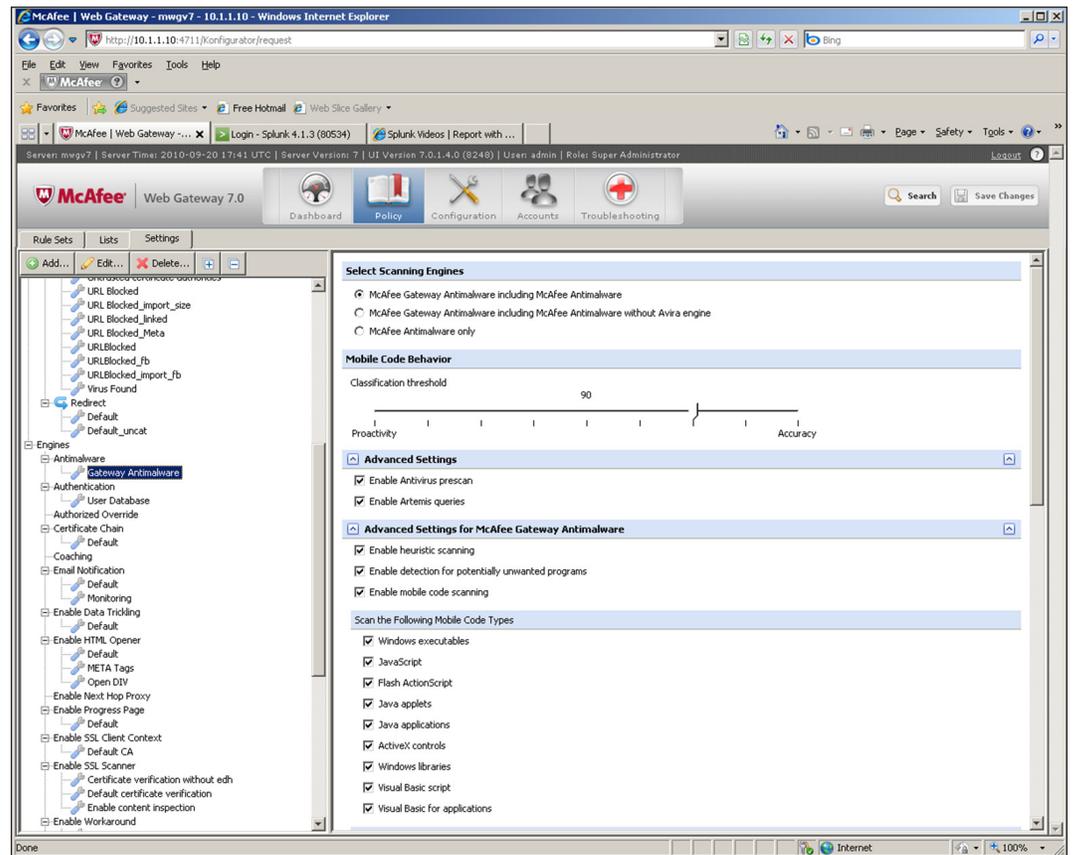
» Select another product.

McAfee Web Gateway (7.0 or later)

McAfee Web Gateway is integrated with McAfee Global Threat Intelligence file reputation, web categorization, and web reputation.

To enable McAfee Global Threat Intelligence file reputation:

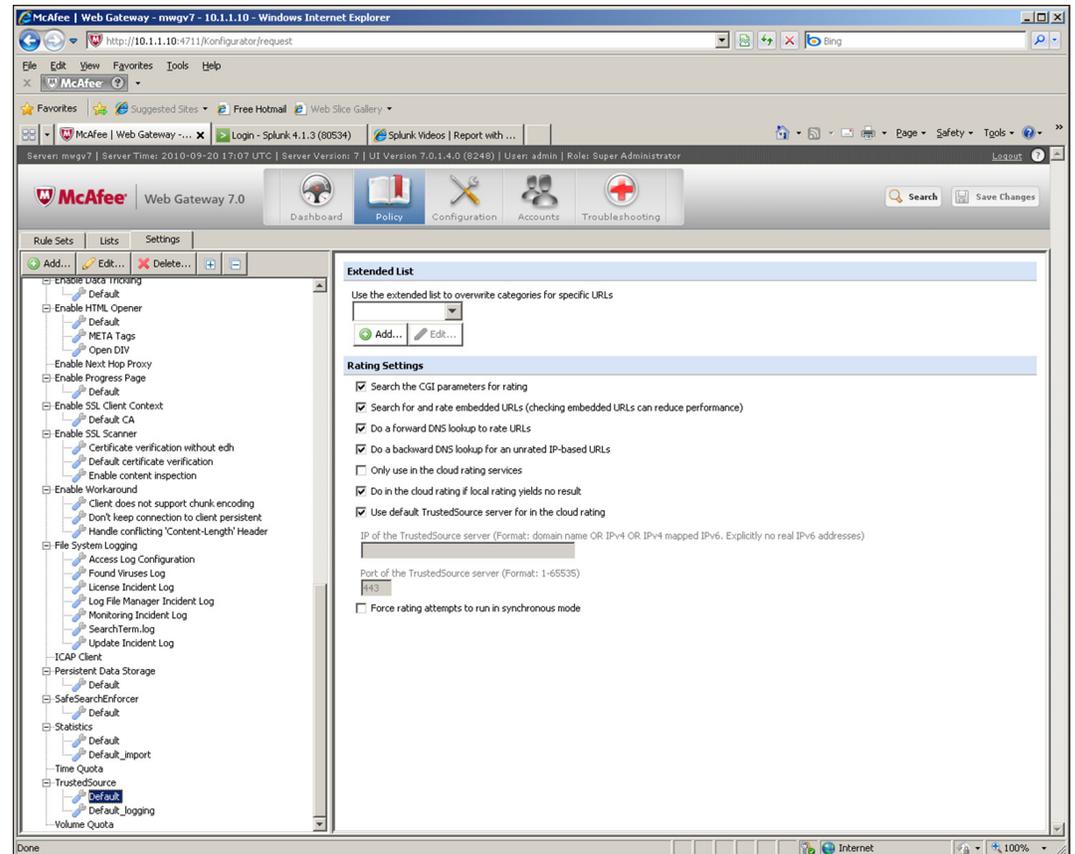
1. In the policy screen, in the settings tab to the left, drill down on engines, anti-malware, and gateway anti-malware.
2. Under Advanced Settings, click Enable Artemis Queries.



McAfee Web Gateway (Continued)

To enable McAfee Global Threat Intelligence web categorization and reputation:

1. Staying in the policy screen and settings tab on the left, drill down to TrustedSource, Default.
2. To the right, select “Do in the cloud rating if local rating yields no result” for web categorization and “Use default TrustedSource server for in the cloud rating” for web reputation. Geo-location information is only available through cloud look-ups. To enable, select “Only use in the cloud rating services.”



» Select another product.

McAfee Email and Web Security Appliance (5.5 or later)

McAfee Email and Web Security Appliance is integrated with McAfee Global Threat Intelligence file, web, and message reputation.

To enable McAfee Global Threat Intelligence file reputation:

1. Under Email, Scanning Policies, Select Anti-Virus policy.

User: System Administrator | Change Password | Log Off

McAfee Email and Web Security Virtual Appliance v5.5

Dashboard Reports Email Web System Troubleshoot

Email Overview Email Configuration **Email Policies** Quarantine Configuration Quarantine Queued Email

Email Policies (SMTP)

Scanning Policies Dictionaries

Select a protocol: SMTP

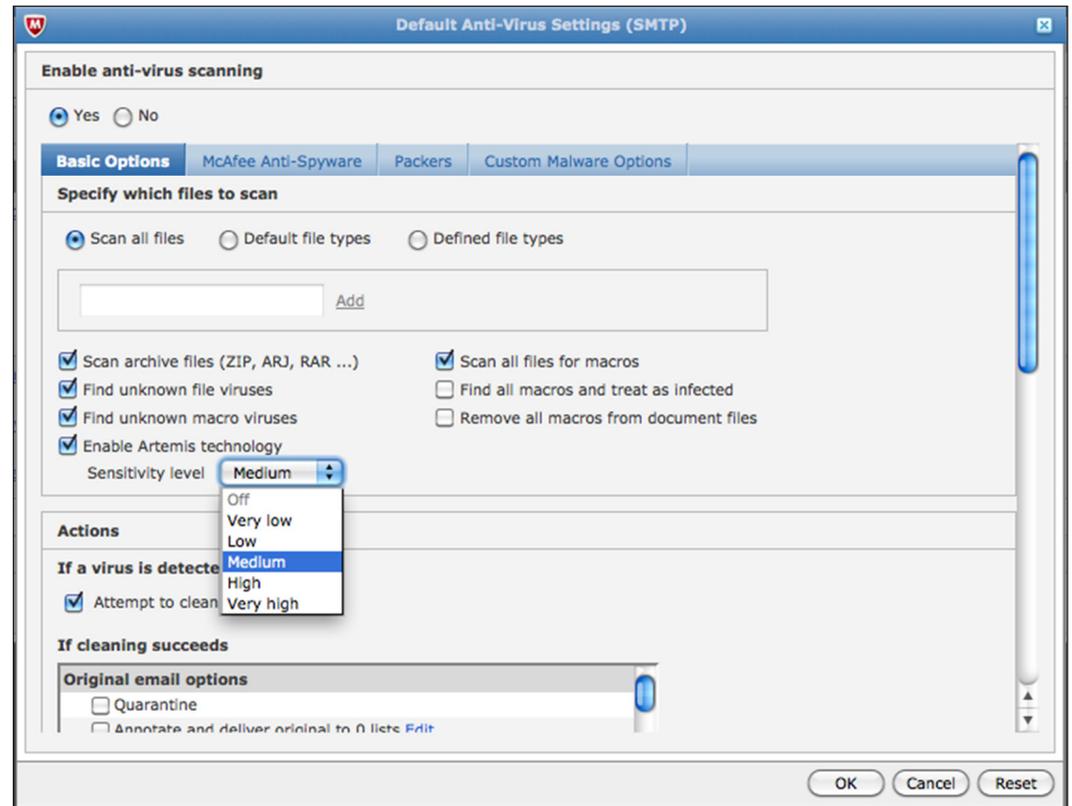
Policy List and Evaluation Order

Order	Policy Name	Anti-Virus	Spam	Content	Scanner Options	Move	Delete
1	Marketing Policy Email is inbound	Anti-Virus: Use default policy	Spam: Use default policy Phish: Use default policy Sender authentication: Use default policy	File filtering: Use default policy Mail size filtering: Use default policy Content scanning: Use default policy	Scanning limits: Use default policy Content handling: Use default policy Alert settings: Use default policy Notification and routing: Use default policy	↑ ↓	🗑️
2	Default policy Email is outbound	Viruses: Clean or Replace with an alert McAfee Anti-Spyware: Replace with an alert Packers: Replace with an alert	Spam: Mark when score >= 5 Score >= 10: Drop the data Phish: Mark, Drop the data Sender authentication: Enabled McAfee TrustedSource™: Enabled	File filtering: 2 custom rules Default action: Allow through Mail size filtering: Enabled Content scanning: 1 rule	Scanning limits: 500 MB or 8 minutes Content handling Alert settings: Use HTML alerts Notification and routing	N/A	🗑️

Add Policy...

McAfee Email and Web Security Appliance (Continued)

2. Check the box to enable McAfee Global Threat Intelligence file reputation.
3. Select the Sensitivity level.



McAfee Email and Web Security Appliance (Continued)

To enable McAfee Global Threat Intelligence message reputation:

1. Under Email, Scanning Policies, click the Sender Authentication in the Spam column.

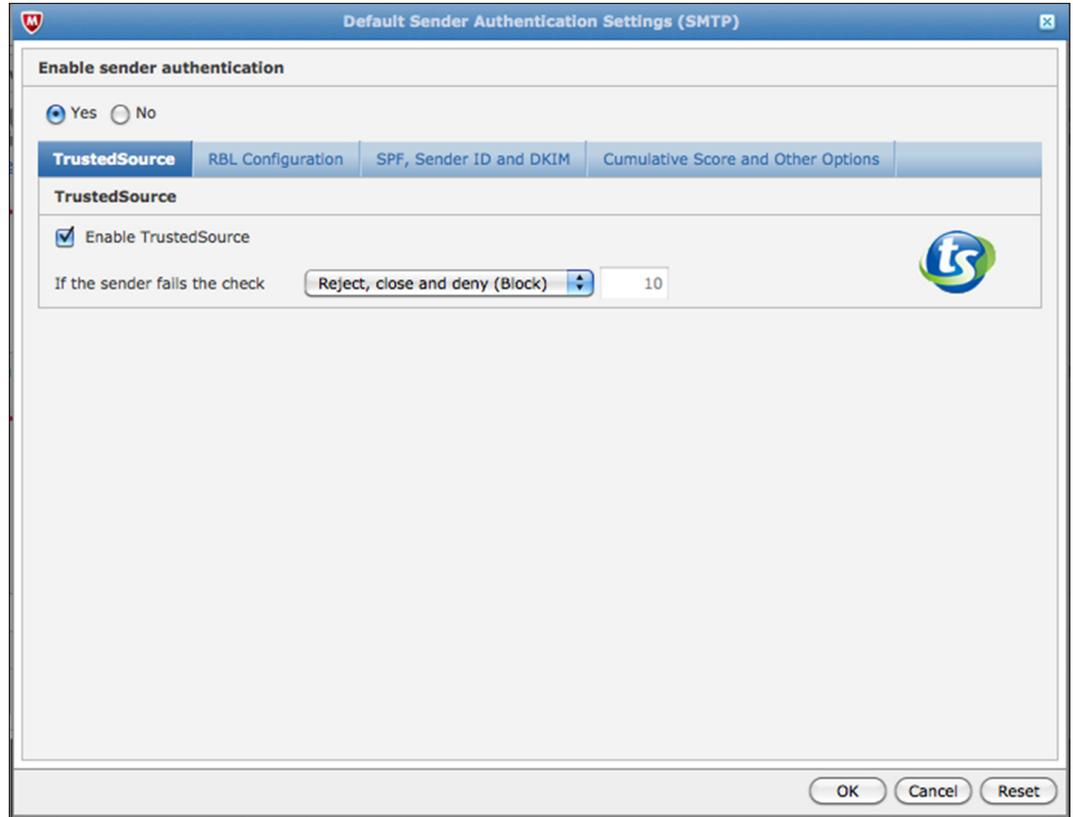
The screenshot shows the McAfee Email and Web Security Virtual Appliance v5.5 interface. The top navigation bar includes 'Email Overview', 'Email Configuration', 'Email Policies', 'Quarantine Configuration', 'Quarantine', and 'Queued Email'. The 'Email Policies (SMTP)' section is active, showing 'Scanning Policies' and 'Dictionaries'. A dropdown menu is set to 'SMTP'. Below this is a table titled 'Policy List and Evaluation Order'.

Order	Policy Name	Anti-Virus	Spam	Content	Scanner Options	Move	Delete
1	Marketing Policy Email is inbound	Anti-Virus: Use default policy	Spam: Use default policy Phish: Use default policy Sender authentication: Use default policy	File filtering: Use default policy Mail size filtering: Use default policy Content scanning: Use default policy	Scanning limits: Use default policy Content handling: Use default policy Alert settings: Use default policy Notification and routing: Use default policy	Move	Delete
2	Default policy Email is outbound	Viruses: Clean or Replace with an alert McAfee Anti-Spyware: Replace with an alert Packers: Replace with an alert	Spam: Mark when score >= 5 Score >= 10: Drop the data Phish: Mark, Drop the data Sender authentication: Enabled McAfee TrustedSource™: Enabled	File filtering: 2 custom rules Default action: Allow through Mail size filtering: Enabled Content scanning: 1 rule	Scanning limits: 500 MB or 8 minutes Content handling Alert settings: Use HTML alerts Notification and routing	N/A	Delete

At the bottom of the table, there is an 'Add Policy...' button.

McAfee Email and Web Security Appliance (Continued)

2. Check the box to enable TrustedSource.



McAfee Email and Web Security Appliance (Continued)

To enable McAfee Global Threat Intelligence web reputation:

1. Under Web, Web Policies, select Enhanced URL filtering: SiteAdvisor in the URL Filtering column.

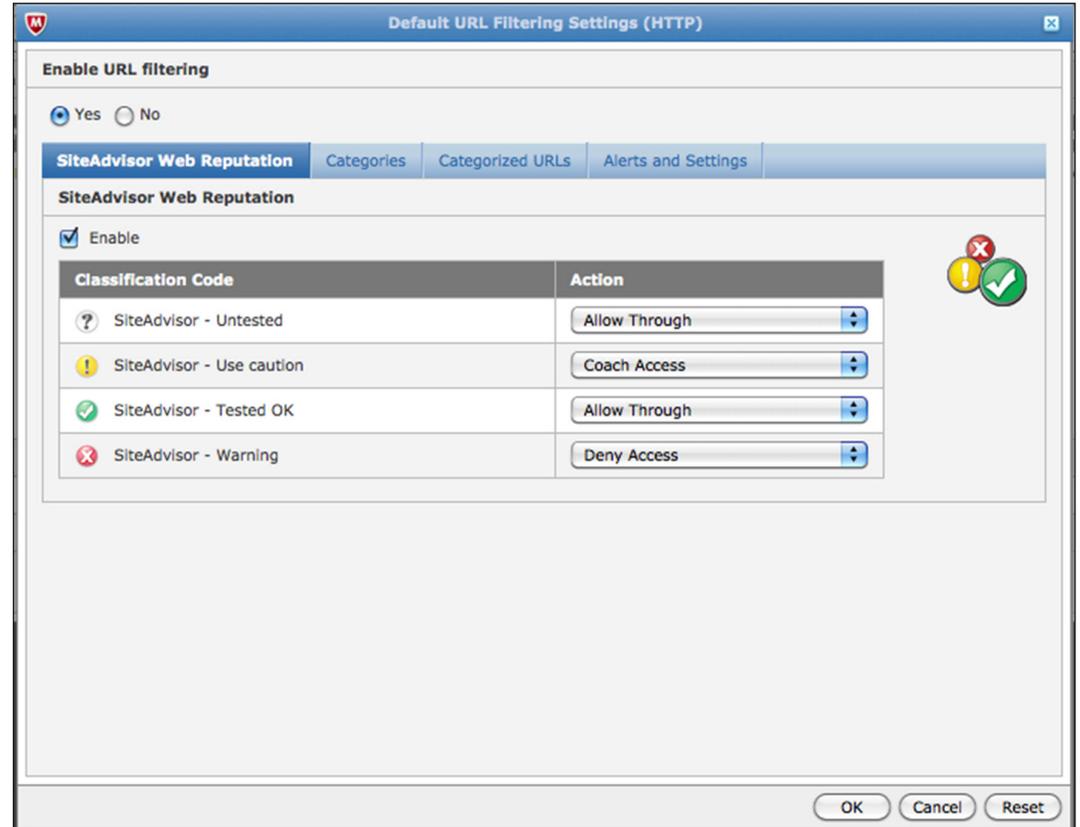
The screenshot shows the McAfee Email and Web Security Virtual Appliance v5.5 Web Policies configuration page. The 'Web Policies (HTTP)' section is active, and the 'Scanning Policies' tab is selected. The 'Policy List and Evaluation Order' table is displayed, showing the 'Default policy' with the following settings:

Order	Policy Name	Anti-Virus	URL Filtering	Content	Scanner Options	Move	Delete
1	Default policy	Viruses: Replace with an alert McAfee Anti-Spyware: Replace with an alert Packers: Detection disabled	HTTPS URL filtering: Enabled Primary URL filtering: Deny: 0, Allow: 0 Enhanced URL filtering: SiteAdvisor: Enabled, Categories: (Deny: 14, Allow: 91) <div style="border: 1px solid black; padding: 2px; width: fit-content;"> Timed setting: Add a new timed setting </div>	Content scanning: Disabled Streaming media: Enabled Instant messaging: Allowed	Scanning limits: 500 MB or 15 minutes Content handling Alert settings: Use HTML alerts HTTP scanning: Requests, Responses	N/A	

An 'Add Policy...' button is located at the bottom left of the table.

McAfee Email and Web Security Appliance (Continued)

2. Under McAfee SiteAdvisor Web Reputation click the Enable box.



» Select another product.

McAfee SaaS Email Protection

McAfee SaaS Email Protection is integrated with McAfee Global Threat Intelligence message reputation.

This service is enabled by default.

» Select another product.

McAfee SaaS Web Protection

McAfee SaaS Web Protection is integrated with McAfee Global Threat Intelligence web categorization.

To enable this service:

1. In the administrative console, select the Web Protection tab.
2. Select the Policies tab.
3. Select the Content tab.
4. Check Enable content filtering.
5. Under Safe Search Options, you may choose to check Prevent leading search engines from returning sexually explicit search results.
6. You may further select website allow/deny options by checking the bubbles in the table below.

The screenshot shows the McAfee Control Console interface. At the top, there's a search bar for users. Below that, navigation tabs include Account Management, Email Protection, Email Archiving, and Web Protection. Under Web Protection, there are sub-tabs for Policies, Setup, Reports, and Forensics. The main area is titled 'Policy Definition' and 'Policy Scheduling'. The policy name is 'executive'. There are 'Save', 'Cancel', and 'Help' buttons. Below this, there are tabs for 'Policy Sets', 'Threat', 'Content', 'Trusted Sites', and 'Blocked Sites'. The 'Content' tab is active. It shows a checkbox for 'Enable content filtering' which is checked. Below that, under 'Safe Search Options', there is a checkbox for 'Prevent leading search engines from returning sexually explicit search results' which is also checked. At the bottom, there are buttons for 'Allow all', 'Deny all', 'Expand All', and 'Collapse All'. A table lists various web categories with radio buttons for selection:

Category	Description	Allow all	Deny all
Business/Services			
Business	Web pages that provide business-related informato...	<input type="radio"/>	<input type="radio"/>
Finance/Banking	Web pages that provide financial information or ac...	<input type="radio"/>	<input type="radio"/>
Job Search	Web pages related to a job search including sites ...	<input type="radio"/>	<input type="radio"/>
Stock Trading	Web pages that allow users to purchase, sell, or t...	<input type="radio"/>	<input type="radio"/>
Drugs			
Alcohol	A web page that has a significant focus on selling...	<input type="radio"/>	<input type="radio"/>
Drugs	Sites in this category provide information on the ...	<input type="radio"/>	<input type="radio"/>
Tobacco	Web pages that sell, promote, or advocate the use ...	<input type="radio"/>	<input type="radio"/>
Entertainment/Culture			
Art/Culture/Heritage	Web pages that contain virtual art galleries, arti...	<input type="radio"/>	<input type="radio"/>
Entertainment	Web pages that provide information about cinema, t...	<input type="radio"/>	<input type="radio"/>
Humor/Comics	Web pages providing content intended to be comical...	<input type="radio"/>	<input type="radio"/>
Internet Radio/TV	Web pages that provide software or access to cont...	<input type="radio"/>	<input type="radio"/>
Media Downloads	Web pages that provide audio or video files for do...	<input type="radio"/>	<input type="radio"/>
Media Sharing	Web pages that allow users to upload, search for, ...	<input type="radio"/>	<input type="radio"/>
Recreation/Hobbies	Web pages for recreational organizations and facil...	<input type="radio"/>	<input type="radio"/>
Streaming Media	Web pages that provide streaming media, or contain...	<input type="radio"/>	<input type="radio"/>

» Select another product.

