

# McAfee Global Threat Intelligence: Turn It On

How to enable McAfee<sup>®</sup> Global Threat Intelligence<sup>™</sup> 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<sup>®</sup> 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<sup>®</sup> (McAfee ePO<sup>™</sup>) 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<sup>®</sup> heuristic network check for suspicious files), select Sensitivity level.
- 4. Save the policy.

VirusScan Enterprise 8.7.0 > On Deliv	rery Email Scan Policies > My Default	
Settings for: Workstation 💌	it.	
Scan Items Actions Alerts N Actachments to scan:	Otes Scanner Settings     Reports       Im Tries     C       Default + additional file types       Im Also scan for macros in all files       C     Specified file types only	-
Heuristics:	<ul> <li>✓ Find unknown program threats and trojans</li> <li>✓ Find unknown macro threats</li> <li>□ Find attachments with multiple extensions</li> </ul>	
Compressed files:	<ul> <li>✓ Scan inside archives (e.gZIP)</li> <li>✓ Decode MIME encoded files</li> </ul>	
Unwanted programs detection:	✓ Detect unwanted programs	
Email message body (for Microsoft Outlook only):	✓ Scan email message body	
Heuristic network check for suspicious files:	Sensitvity level: Very low	-



#### 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.

Client Task Builder	1 Description	2 Configuration	3 Schedule	4 Summar	y	
What do you want this task to do?						
Scan Locations Scan Items Excl	usions Actions Performance	Reports Task				
Specify performance options for the	at do you want this task to do?     at coations   Scan Items   Exclusions   Actions   Performance   Reports   Task    Task    Coations   Scan Items   Exclusions   Actions   Performance options for the scan.     Image: Coations   Image: Coations					
When to defer:	<ul> <li>Defer scan when using batte</li> <li>Defer scan during presentation</li> <li>User may defer scheduled so</li> </ul>	ry power. ions. cans.				
How long to defer:	Defer at most 1 hours (0=	=forever)				
System utilization:						
Heuristic network check for suspicious files:	Sensitvity level: 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-Acce	ess General Policies > My Default
Settings for: Workstation 💌	
General ScriptScan Blocking	Messages Reports
Configure the general policy that ap	plies to all on-access scanning.
Scan:	<ul> <li>✓ Boot sectors</li> <li>✓ Floppy during shutdown</li> <li>□ Processes on enable</li> </ul>
Enable on-access scanning:	<ul> <li>Enable on-access scanning at system startup</li> <li>Enable on-access scanning when the policy is enforced.</li> </ul>
Maximum scan time:	Maximum archive scan time (seconds): 15 Forforce a maximum scanning time for all files Maximum scan time (seconds): 45
Cookies	☑ Scan cookie files
Heuristic network check for suspicious files:	Sensitvity level: Very low



#### McAfee SiteAdvisor Enterprise (3.0 or later)

McAfee SiteAdvisor<sup>®</sup> 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.

iteAdvisor Enterprise Plus 3.5.0 > Enable/Disable > My Default			
Vhen SiteAdvisor Enterprise is disabled, site ratings do not appear, polices are not enforced, and events are not tracked.			
SiteAdvisor policy enforcement:	Enable If you deselect this option, SiteAdvisor protection is disabled on all systems to which this policy is applied.		



#### 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<sup>®</sup> Block Threshold.

Host Intrusion Prevention 8.0 > Firew	vall Options (Windows) > My Default
Firewall status:	✓ Enabled
	<ul> <li>Regular protection</li> <li>Adaptive mode (rules are learned automatically)</li> <li>C Learn mode (rules are learned after user interaction) I Incoming Outgoin</li> </ul>
	<ul> <li>Allow traffic for unsupported protocols</li> <li>Allow bridged traffic</li> </ul>
Firewall client rules:	Retain existing client rules when this policy is enforced
Startup protection:	☐ Allow only outgoing traffic until the Host IPS service has started
Protection options:	<ul> <li>Enable IP spoof protection</li> <li>Send events to ePO for TrustedSource violations</li> <li>Incoming TrustedSource block threshold: Do not block</li> <li>Outgoing TrustedSource block threshold: Do not block</li> <li>High Risk</li> </ul>
Stateful firewall settings:	Use FTP protocol inspection 30 TCP connection timeout (in seconds)
	30 UDP and ICMP echo virtual connection timeout (in seconds)



#### 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.

Increations				
ame: Reputation filter for high risk countries	5	Action: Allow	Browse: << Select or	ne >>
Applications Ports: >>>	Source	Destination	+- 🛱 🖉	Q Search
Applications	Endpoints	Endpoints	Name	Properties
HTTP	<any></any>	High risk (Geo-Location)		
SSL/TLS	Click here to specify an endpoint	Click here to specify an endpoint		
Click here to specify an application				
apabilities:	Users and Groups			
	Click here to specify a user			
Default ports				
TCP/80 SSL/443	Zone: internal	Zone: external 🗸		
<pre>/ Enable TrustedSource™ pply rule to connections that are dvanced S Table Always active</pre>	NAT: <a>docalhost&gt; (Host)</a>	High Risk  Redirect: <none></none>		
	Authoritizatory	t Redirect port: 0		
udit: Standard -	Application Defense: <default group=""></default>	• •		
PS Signatures: <none></none>	Describe your rule here			
		1		



# 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.

User: Administrator   Domain: /	My Company	
McAfee Network Security M License: Global   Version: 6.0.1.7	anager Real-time Threat Analyzer V Law	?
E Resource Tree	/My Company/IPS Settings > Malware Detection > Fingerprints	?
■       Hy Company         ■       Protec List         ■       Protec List <td< td=""><td>Part bettings Palations Advanced Databies Malaware Databies Attack Filter ACL SSL Decryption Pile Quarantine Attaching Malamanare Allert Hothifeation Configuration Lipdate   Testions Fails marked with an asterisk (*) are required. Fingerprints Faters is a MoRee technology that leverageses the threat intelligence gathered worldwide by MoRee Avent Labs to provide protection from emerging threats, even before a signature set update is accounted and the databies of the</td><td></td></td<>	Part bettings Palations Advanced Databies Malaware Databies Attack Filter ACL SSL Decryption Pile Quarantine Attaching Malamanare Allert Hothifeation Configuration Lipdate   Testions Fails marked with an asterisk (*) are required. Fingerprints Faters is a MoRee technology that leverageses the threat intelligence gathered worldwide by MoRee Avent Labs to provide protection from emerging threats, even before a signature set update is accounted and the databies of the	
Wizards 🛞		1



# 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.

User: Administrator   Domain: /M McAfee° Network Security Ma License: Global   Version: 6.0.1.7	y Company	_	Home Status	Configure Reports	_	Real-time Threat Analyzer + Launch
Resource Tree	/Hy Company/IPS Settings > IPS Settings Policies Advance Fingerprints Enable Use this page to enable and o	Malware Detection > Enable red Policies Malware Detection	n Attack Filters ACL 1	SSL Decryption IPS Quarantine	Archiving Maintenance Alert Notifi	?
TPS Stettings     T-1200     M-1250     M-1250	Tip: To minimize the impact of (the initial connection request the initial connection request Enable Sensor:	rea n1 P Response Scanning to in performance, only enable res dictates the direction).	M-1230 V	I a significant impact on performan	ree. 1al clients from malicious downloads, en	able only Outbound response scanning
L 💼 48	Port Name		Direction		Detection Type	
	1A-1B 2A-2B	Inbound • Outbound •		Artemis Only Custom Fingers	▼ prints Only	
	3A-3B 4A	Inbound and Outbound   Disabled		Artemis and Cu Disabled	stom Fingerprints 🔻	
	48	Disabled 👻		Disabled	•	
						Save
Wizards 🛞						



#### 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.

ntps://172.16.229.211 - Pi	rimary MCATEE Network Security Manager (172.16.229.211) - P	Microsoft Internet Explorer	-
: Administrator   Domain: /M	ly Company		Log Of
cAfee° twork Security Mana ion: 6.0.7.0.30	ager 🔒 🔶	Configure Reports Real-time Historical Threats	
Resource Tree	/My Company/Integration > Global Threat Intelligence > Partic	ipation	
🖽 💼 2A-2B			+†+ Send?
₩ 3A-3B ₩ 4A-4B	+ Alert Data Details		• Yes O No
Wizards     Integration     RAMESH	+ Alert Data Summary		⊕ Yes ○ No
Device List     E      Amesh-2	+ General Setup		⊙ Yes ○ No
📟 Ramesh-3 (	+ Feature Usage		⊙ Yes ○ No
IPS Settings IPS Settings III IPS 2600-FO III Ramesh-2 <sup>*</sup>	To optimize the use of TrustedSource, only send alert data (and country information.	retrieve TrustedSource information) for attacks for which you are most interes	ted in viewing host reputation and
🕀 🛄 Ramesh-3i	Alert Data Details Filter		
Integration     Ghild2	Only Send Data for the Following Alert Severities:	V High V Medium V Low V Informational	
— 📟 Device List — 🗓 IPS Setting:	Technical contact information is gathered to communicate End o	f Life and other key milestones.	
- K Integration	Technical Contact Information		
E 🙀 Child 3	Send Contact Information?	⊙ Yes ONo	
- 📟 v-61 - 🙌 IPS Sett	First Name:	Srinivas *	
E- E v-61	Last Name:	Loke	
- 🗰 -	Street Address:	3965 Freedom Circle	
	Phone Number:	4083465139	
	Email Address:	sri@mcafee.com •	
- 🚰 Integra - 🙀 Child4			
🗆 📟 Dev			
ards 🛞	<		
			A Jaharah



#### 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.

Analy	Analyze   Signature   Administration   Profile   Logout		
Enabled			
Proxy host:	127.0.0.1	ex: 127.0.0.1	
Proxy port:	3128 ex: 3128		
Test	Commit		

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

	Analyze   Signature	e   Administration   Pro	ofile   Logout	
Session Detail				
			→ Report	→ Download Binary
Protocol Source	Source Location	Destination	Destination Location	Size Time
тср 🦪	Ontario Canada	9	Alabama United States	1.35КВ 2010-07 31 22:26:00
Behavior				
Shellcode.XORed_URL				
Host		URL Category	URL Rating	
update.gamevance.net		Spyware/Adware/Keyloggers	Suspicious	
URL		Creation Time		
/m/updcnt.asp		2010-07-31 00:26:17.0		
STREAM				→ Download Pcap
Hex Dump	•			
00000000 48	54 54 50 2f 31 2e 31	20 32 30 30 20 4f 4b 0d	HTTP/1.1 200 OK.	
00000010 0a	53 65 72 76 65 72 3a	20 41 70 61 63 68 65 33	.Server: Apache3	
00000030 61	63 68 65 0d 0a 43 61	63 68 65 2d 43 6f 6e 74	acheCache-Cont	
00000040 72	6f 6c 3a 20 70 72 69	76 61 74 65 0d 0a 43 6f	Irol: privateCol	

» Select another product.

1



#### 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 you participation levels, alert details, and technical information.

work Security Man	ager estimates ager e	_
Resource Tree	//Wy Company/Integration         > Global Threat Intelligence         > Participation           Global Threat Intelligence         eBolicy Orchestrator         Vulnerability Managar         Relevance         Host Intrusion Prevention         HP Network Automation           Participation         Important with the exception of the optional contact information, all data is sent anonymously.         Important         Important	
Ramesh 1450     IPS Settings     Ramesh-1450     A     IA     IB	Fields marked vith an asterisk (*) are required. Participation	
⊡ 💼 2A-2B — 💼 3A-3B		Send?
→ 🚔 4A-4B → 🌁 Wizards	+ Alert Data Details	🕑 Yes 🔘 N
RAMESH	+ Alert Data Summary	🖲 Yes 🔘 N
Device List Ramesh-2 <sup>*</sup>	+ General Setup	🕑 Yes 🔘 N
Ramesh-31	+ Feature Usage	🖲 Yes 🔘 N
IPS Settings Control	To optimize the use of TrustedSource, only send alert data (and retrieve TrustedSource information) for attacks for which you are most inte country information.	rested in viewing host reputation and
E Ramesh-3	Alert Data Details Filter	
Integration     Gridd2	Only Send Data for the Following Alert Severities:	
610		
- 📟 Device List - 🖺 IPS Setting:	Technical contact information is gathered to communicate End of Life and other key milestones.	
- 🖶 Device List - \iint IPS Setting: - 🛐 Integration	Technical contact Information is gathered to communicate End of Life and other key milestones. Technical Contact Information	
- Device List - U IPS Setting: - U Integration - Child3 - Device	Technical contact information is gathered to communicate End of Life and other key milestones.           Technical Contact Information         Organization           Send Contact Information?         Organization	
Device List     Difference	Technical contact information is gathered to communicate End of Life and other key milestones. Technical Contact Information? First Name: Sinivas	
Device List UPS Setting: Integration Child 3 Device UPS Sett UPS Sett UPS Sett UPS Sett	Technical contact information is gathered to communicate End of Life and other key milestones.          Technical Contact Information?	
Device List	Technical contact information is gathered to communicate End of Life and other key milestones.          Technical contact Information?         Send Contact Information?         First Name:         Last Name:         Struet Address:	
Device List     Device List     Device     Device     Device     Unlds	Technical contact information is gathered to communicate End of Life and other key milestones.          Technical contact Information?         Send Contact Information?         First Name:         Last Name:         Street Address:         Phone Number:	
Device List     Device List     Device	Technical contact information is gathered to communicate End of Life and other key milestones.          Technical contact information?         Send Contact Information?         First Name:         Last Name:         Street Address:         Phone Number:         4003465139         Email Address:	
Device List     Device List     Device     Childs     Device	Technical contact information is gathered to communicate End of Life and other key milestones.          Technical contact information?         Send Contact information?         First Name:         Last Name:         Street Address:         Phone Number:         4003465139         Email Address:	



#### 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.

McAfee Email Gate	way (IronMail) Advanced Serv	er 6.7.2			Logout License Status	Bookmarks Contact Us Help
Dashboard Queue Manager	Compliance Anti-Spam	Anti-Virus Advanced Er	ncryption IntrusionDefende	r Reporting Administra	tion System	
Thursday, September 16, 2010 3:14:48 PM	TrustedSource <sup>®</sup> ·	Configure 📲				7.
Logged in as: admin [Appliance Admin]						
Logged into: Default Virtual Host	Enable TrustedSource®		Enable Dynamic Quarantine			
Quick Snapshot	Launch TrustedSource®					
E SpamProfiler®	Low Risk	All	w v			
Configure						
Manage Rules	Significant Risk	Su	bject Rewrite 💌	SPAM:		
Apply Rules	Confirmed Spam	Dri	op 🗸			
TrustedSource®			Submit	Reset		
Anti-Zombie			- Contra			
Anti-Fraud/Anti-Phishing						
Connection Control						
ThreatResponse Updates						
Anti-Spam Advanced						

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.

McAfee Email Gate	way (IronMail) Advanced Serve	er 6.7.2	AL IN				Logou	t Bookmark	5 Contact Us	Help
•							License Status	I Updates I	Alert Status:	A 22
Dashboard Queue Manager	Compliance Anti-Spam	Anti-Virus	Advanced Encryption	IntrusionDefender	Reporting	Administration	System			
Thursday, September 16, 2010 3:27:27 PM	SpamProfiler <sup>®</sup> - C	Configure	e •I							?
Logged in as: admin [Appliance Admin]										
Logged into: Default Virtual Host	Add X Header for SpamProfiler®	9 esp								
Quick Snapshot			664	- (6) )	where the t	1			e . 11.	
Configure	Spam Features/Dictionaries		Confidence Valu	e(%)	Inreshol	d Value			Enable	~
Manage Rules	Devices DMC			10						
Apply Rules	Reverse DND			10						
TrustedSource®	Bayesian Engine - Spam			10						
Anti-Zombie	Bayesian Engine - Ham			10						
Anti-Fraud/Anti-Phishing	DomainKeys Identified Mail	- 6								
Connection Control	TrustedSource	- (	Configuration							в
ThreatResponse Updates	Image Spam Classifier									
Anti-Spam Advanced	Dynamic Spam Classifier									
	Malicious Mobile Code			1		1				~
	<u>&lt;</u>									>
				Cubrok	Decet					
				SUDMIC	Reset					



# 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.

CMcAfee   Web Gateway - mwgv7 - 10.1.1.10 - Windows	s Internet Explorer		<u>- 🗆 ×</u>
C		💌 🗟 🐓 🗙 🍋 Bing	P -
File Edit View Favorites Iools Help			
× WhcAfee 😧 -			
🔶 Favorites 🔗 🌈 Suggested Sites 🔹 🖉 Free Hotmail	Web Slice Gallery •		
		🔊 - 🖸 - 🗖 🖶 - Dans - Cafabur, Taskar	. ×
Se V McAree   Web Gateway X Login - Splunk 4.	.1.3 (80534) C Splunk Videos   Report with	· · · · · · · · · · · · · · · · · · ·	<b>.</b>
Server: mwgv7   Server Time: 2010-09-20 17:41 UTC   Serv	er Version: 7   UI Version 7.0.1.4.0 (8248)   User: admin   Role: Super Administr	itor Logout	<u> </u>
Web Gateway 7.0	Schoard Policy Configuration Accounts Troubleshooting	Q Search 🔛 Save Chan	ges
Rule Sets Lists Settings			
🔾 Add 🥜 Edit 💥 Delete ∓ 😑			-
Ontrasted connects damandes	Select Scanning Engines		
	<ul> <li>McAfee Gateway Antimalware including McAfee Antimalware</li> </ul>		
	C McAfee Gateway Antimalware including McAfee Antimalware without A	vira engine	
	C McAfee Antimalware only		
URLBlocked	Mobile Code Bebavior		
URLBlocked_import_fb			
	Classification threshold 90		
E G Redirect			
Default uncat	I I I I I I I		
E-Engines	Produviky	Accuracy	
-Antimalware	Advanced Settings		
Gateway Antimalware	Enable Antivirus prescan		
User Database	Enable Artemis queries		
-Authorized Override			
☐ Certificate Chain	Advanced Settings for McAfee Gateway Antimalware		
Coaching	Enable heuristic scanning		
Email Notification	Enable detection for potentially unwanted programs		
Je Default	Enable mobile code scanning		
E Enable Data Trickling			
	Scan the Following Mobile Code Types		
E-Enable HTML Opener	✓ Windows executables		
META Taps	✓ JavaScript		
	✓ Flash ActionScript		
Enable Next Hop Proxy	V Java applets		
Enable Progress Page			
Enable SSL Client Context			
	ActiveX controls		
-Enable SSL Scanner  Castification without off	✓ Windows libraries		
Default certificate verification	Visual Basic script		
	Visual Basic for applications		
Enable Workaround			-
Done		🐘 🚱 Internet 🥢 🔹 1009	10 -
1			/



#### 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."





# 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 F	Password   Log Off			Abo	ut the Applia	ince   Resources
Email and V Appliance v Email Overvie	Afee Web Security Virtual v5.5 ew Email Configuration	Dashboard Rep	ants Email We	b System Troubl	eshoot		() () () () () () () () () () () () () (
Email Pol	licies (SMTP)						
Scanning	Policies Dictionaries					_	
Select a p	protocol: SMTP	\$					¢
Policy Lis	st and Evaluation Order						
Order	Policy Name	Anti-Virus	Spam	Content	Scanner Options	Move	Delete
1	Marketing Policy	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	08	1
2	Default policy	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 Poli	cy)						



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

	Default Anti-Virus Settings (SMTP)	×
nable anti-virus scanning		
• Yes O No		
Basic Options McAfee Anti-Spyware	Packers Custom Malware Options	<u> </u>
Specify which files to scan		
• Scan all files O Default file type	O Defined file types	
Add		
Scan archive files (ZIP, ARJ, RAR)	Scan all files for macros	
Find unknown file viruses	Find all macros and treat as infected	
Find unknown macro viruses	Remove all macros from document files	
Enable Artemis technology		
Sensitivity level Medium		
Off		
Actions Low		
If a virus is detecte Medium		
High		
Very high		
If cleaning succeeds		
Original email options		
Quarantine	U	A
□ Annotate and deliver original to 0	liete Fdit	
		OK Cancel Reset



To enable McAfee Global Threat Intelligence message reputation:

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

lser: System A	dministrator 🍰   Change I	Password   Log Off			Abo	ut the Applia	ince   Resourc
Email and V Appliance v Email Overview	Afee Veb Security Virtual 5.5 w Email Configuration	Dashboard Re Email Policies Quaran	ports Email We We thine Configuration Quarar	b System Troub tine Queued Email	leshoot	•	) X () **
Email Poli	cies (SMTP)						
Scanning P	olicies Dictionaries			_			
Select a p	rotocol: SMTP	\$					Ð
Policy List	t and Evaluation Order						
Order	Policy Name	Anti-Virus	Spam	Content	Scanner Options	Move	Delete
1	Marketing Policy	Anti-Virus: Use defauit 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	00	1
2	Default policy	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 Polic	y)						



2. Check the box to enable TrustedSource.

Default Sender Authentication Settings (SMTP)						
Enable sender aut	hentication					
💽 Yes 🔘 No						
TrustedSource	RBL Configuration	SPF, Sender ID and DKIM	Cumulative Score and Other Opti	ons		
TrustedSource						
Enable Trustee	dSource					
If the sender fails	the check Rejec	t, close and deny (Block)	10	<b>U</b>		
				Cancel Reset		



To enable McAfee Global Threat Intelligence web reputation:

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

User: System A	Administrator 🍰   Change P	assword   Log Off			Abou	t the Applia	nce   Resource
Email and V Appliance v Web Configure	Afee Neb Security Virtual 15.5 ation Web Policies	Dashboard Repo	orts Email We	b System Trout	eshoot	•	? <b>% ?</b>
Web Delle							
Second Polic							
Select a p	protocol: HTTP	•					Ð
Policy Lis	t and Evaluation Order						
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: SilteAdvisor: Enabled, Categories: (Deny: 14, Allow: 91) Timed setting: Add a new timed setting	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	
Add Polic	cy)						



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

Default URL Filtering Settings (HTTP)					
nable URL filtering					
Yes 🔘 No					
SiteAdvisor Web Reputation	Categories	Categorized URLs	Alerts and Settings		
SiteAdvisor Web Reputation					
Enable					
Classification Code		A	ction		
SiteAdvisor - Untested		0	Allow Through	\$	•
SiteAdvisor - Use caution		0	Coach Access	\$	
SiteAdvisor - Tested OK		0	Allow Through	•	
🔇 SiteAdvisor - Warning		C	Deny Access	÷	
3lteAdvisor - Warning			Deny Access	•	
				ОК (	Cancel (Res



#### 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.

W McAfee <sup>®</sup>	Control Console	Search Users 💌			Go
🚨 Account Management 🛛 📓 Email Protect	tion 📓 Email Archiving 🥥 Web Protection				
🍣 Policies 🚯 Setup 🚺 Reports 🔎	Forensics				
Policy Definition Policy Scheduling					
executive			Save	Cancel	Help
Policy Sets Threat Content Trusted Site	es Blocked Sites				
Enable content filtering     Safe Search Options     Prevent leading search engines from n     Allow all Deny all Expand All     Business     FinanceBanking     Job Search     Stock Treading	eturning sexually explicit search results Collapse All Web pages that provide business-related informatio Web pages that provide financial information or ac Web pages that allow users to purchase, sel, or t Web pages that allow users to purchase, sel, or t		○ C € € C	• • • • • • • •	
Drugs				0	
Alcohol Drugs Tobacco	A web page that has a significant focus on selling Sites in this category provide information on the Web pages that sell, promote, or advocate the use		000	000	
Entertainment/Culture			•	•	
Art/Culture/Heritage Entertainment Humor/Comics Internet Radio/TV Media Downloads Media Sharing Recreation/Hobbies Streaming Media	Web pages that contain virtual art galleries, arti Web pages that provide information about cimema, t Web pages providing content interded to be conical Web pages that provide software or access to conti Web pages that provide audio or video files for do Web pages that allow users to upload, search for, Web pages that provide streaming media, or contain Web pages that provide streaming media, or contain		00000000	00000000	

» Select another product.



McAfee, Inc. 2821 Mission College Boulevard Santa Clara, CA 95054 888 847 8766 www.mcafee.com McAfee, the McAfee logo, McAfee Global Threat Intelligence, McAfee TrustedSource, McAfee Artemis, McAfee VirusScan, McAfee ePolicy Orchestrator, and McAfee ePO are registered trademarks or trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other marks and brands may be claimed as the property of others. The product plans, specifications and descriptions herein are provided for information only and subject to change without notice, and are provided without warranty of any kind, express or implied. Copyright © 2010 McAfee, Inc.

15300wp\_turn-on-gti\_1010\_wh