



# Deep Security Best Practices Guide

## Deep Security Health Check

Prepare for:  
Trend Test

Created on: October 20th of 2020 for [app.deepsecurity.trendmicro.com](https://app.deepsecurity.trendmicro.com)



## High-level Technical Summary

This high-level summary is intended to provide an overview of the current status of your Deep Security deployment compared with the recommendations of Deep Security Best Practices Guide. Detailed instructions, business impacts and references can be found in the individual sections of the full report.

### Computer Protected Mode Distribution

Agent	Agentless mode	Combined mode	Total Activated Computers
3	0	0	3

### Computers Compliance Score Distribution

Total Activate Computers	High Compliance	Medium Compliance	Low Compliance	Caution
3	2	0	0	1

### Security Modules Compliance

Module	Full Compliance	Compliance Score
Anti Malware	2	67%
Application Control	0	0%
Firewall	0	0%
Integrity Monitoring	1	33%
Intrusion Prevention	2	67%
Log Inspection	1	33%
Web Reputation	3	100%
Anti-Malware Scan Setting [Real-Time Scan]	2	67%
Anti-Malware Scan Setting [Manual Scan]	0	0%
Anti-Malware Scan Setting [Scheduled Scan]	0	0%

# 1. Report Overview

The primary objective of this report is to outline the current status of computers protected by Deep Security and suggest recommendations specifically targeted at increasing the overall security posture for your environment. This report provides the following information:

- An overview of the compliance level of Deep Security.
- A per-module breakdown of their use and compliance score
- A high-level technical overview, including the main Operating Systems in use, DS Agent Versions.

All results provided should be analysed in the context of the needs and particularities of the environment in question, as configuration checks may prove to be more or less critical for it's security and operational integrity.

## Computer Compliance Distribution

The graph below shows the breakdown of all managed computers by their compliance score. Computers with High compliance have scores between 75-100% and are the expected standard. Medium and Low compliance have scores between 50-74% and 25-49%, respectively. Computers with scores between 0-24% are considered to be in a 'Caution' state. Appropriate measures should be taken to improve their scores.



## Deep Security Computers Details

Version	Managed ratio	Compliance
12.0.0.1090	100%	77%
12.0.0.1186	100%	4%
20.0.0.877	100%	85%

## 2. Environment modules overview

This section shows an overall score for each of the used modules, if a module is turned off, the score will be considered as zero.

### 2.1 Modules overview

#### Anti Malware (2/3)

The Deep Security anti-malware module provides agent computers with both real-time and on-demand protection against file-based threats, including malware, viruses, Trojans, and spyware. To identify threats, the anti-malware module checks files on the local hard drive against a comprehensive threat database. The anti-malware module also checks files for certain characteristics, such as compression and known exploit code.

Note: Portions of the threat database are hosted on Trend Micro servers or stored locally as patterns. Deep Security Agents periodically download anti-malware patterns and updates to ensure protection against the latest threats.

A newly installed Deep Security Agent cannot provide anti-malware protection until it has contacted an update server to download anti-malware patterns and updates. Ensure that your Deep Security Agents can communicate with a Deep Security Relay or the Trend Micro Update Server after installation.

The anti-malware module eliminates threats while minimizing the impact on system performance. The anti-malware module can clean, delete, or quarantine malicious files. It can also terminate processes and delete other system objects that are associated with identified threats.

#### Application Control (0/3)

Application control continuously monitors for software changes on your protected servers. Based on your policy configuration, application control either prevents unauthorized software from running until it is explicitly allowed (whitelisted), or allows unauthorized software until it is explicitly blocked (blacklisted). Which option you choose depends on the level of control you want over your environment.

Warning: Application control continuously monitors your server and logs an event whenever a software change occurs. It is not intended for environments with self-changing software or that normally creates executables, such as some web or mail servers.unauthorized applications.

#### Firewall (0/3)

The firewall module provides bidirectional stateful inspection of incoming and outgoing traffic. Firewall rules define what actions to take on individual packets in that traffic. Packets can be filtered by IP and MAC address, port and packet flag across all IP-based protocols and



Compliance Score



Compliance Score

frame types. The firewall module can also help prevent denial of service attacks and detect and prevent reconnaissance scans.

### Integrity Monitoring (1/3)

The integrity monitoring module scans for unexpected changes to registry values, registry keys, services, processes, installed software, ports and files on Deep Security Agents. Using a baseline secure state as a reference, the integrity monitoring module performs scans on the above and logs an event (and an optional alert) if it detects any unexpected changes.

### Intrusion Prevention (2/3)

The Intrusion Prevention module protects your computers from known and zero-day vulnerability attacks as well as against SQL injections attacks, cross-site scripting attacks, and other web application vulnerabilities.

When patches are not available for known vulnerabilities in applications or operating systems, Intrusion Prevention rules can intercept traffic that is trying to exploit the vulnerability. It identifies malicious software that is accessing the network and it increases visibility into, or control over, applications that are accessing the network. Therefore your computers are protected until patches that fix the vulnerability are released, tested, and deployed.

Protection is available for file sharing and messaging software such as Skype, but also web applications with vulnerabilities such as SQL injection and cross-site scripting (XSS). In this way, Intrusion Prevention can also be used as a lightweight web application firewall (WAF).

### Log Inspection (1/3)

The log inspection protection module helps you identify important events that might be buried in your operating system and application logs. These events can be sent to a security information and event management (SIEM) system or centralized logging server for correlation, reporting, and archiving. All events are also securely collected in the Deep Security Manager.

The log inspection module lets you:

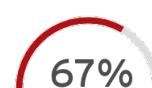
- \* Meet PCI DSS log monitoring requirements.
- \* Detect suspicious behavior.
- \* Collect events across heterogeneous environments containing different operating systems and diverse applications.
- \* View events such as error and informational events (disk full, service start, service shutdown, etc.).
- \* Create and maintain audit trails of administrator activity (administrator login or logout, account lockout, policy change, etc.).



Compliance Score



Compliance Score



Compliance Score

The log inspection feature in Deep Security enables real-time analysis of third party log files. The log inspection rules and decoders provide a framework to parse, analyze, rank and correlate events across a wide variety of systems. As with intrusion prevention and integrity monitoring, log inspection content is delivered in the form of rules included in a security update. These rules provide a high level means of selecting the applications and logs to be analyzed.

### Web Reputation (3/3)

The web reputation module protects against web threats by blocking access to malicious URLs. Deep Security uses Trend Micro's Web security databases from Smart Protection Network sources to check the reputation of websites that users are attempting to access. The website's reputation is correlated with the specific web reputation policy enforced on the computer. Depending on the security level being enforced, Deep Security will either block or allow access to the URL.

Note: The web reputation module does not block HTTPS traffic.

### Anti-Malware Scan Setting [Real-Time Scan] (2/3)

Real-time scans continuously monitor for malware. Every time a file is received, opened, downloaded, copied, or modified, a real-time scan occurs. (In comparison, manual and scheduled scans only detect malware at specific times, when you run them.) If Deep Security detects no security risk, the file remains in its location and users can proceed to access the file. If Deep Security detects a security risk, it displays a notification message, showing the name of the infected file and the specific security risk.

### Anti-Malware Scan Setting [Manual Scan] (0/3)

Manual Scan is an on-demand scan and starts immediately after a user runs the scan on the computer. The time it takes to complete scanning depends on the number of files to scan and the computer's hardware resources.

### Anti-Malware Scan Setting [Scheduled Scan] (0/3)

Scheduled scans run automatically on the configured date and time. Use scheduled scan to automate routine scans and improve scan management efficiency.



Compliance Score



Compliance Score



Compliance Score



Compliance Score



Compliance Score

## 2.2 Setting Compliance

The settings & compliance report (the **client\_detailed\_report.html** in archive) will allow you to drill into agent details to easily ID devices you may want to target for upgrades, or groups you may want to zero in on policy enhancements. The password of the report is as follows.

1ib69AaFpN0gSh36

### Anti Malware

Anti Malware State	67 %
--------------------	------

### Application Control

Application Control State	0 %
---------------------------	-----

### Firewall

Firewall State	0 %
----------------	-----

### Integrity Monitoring

Integrity Monitoring State	33 %
----------------------------	------

### Intrusion Prevention

Intrusion Prevention State	67 %
----------------------------	------

### Log Inspection

Log Inspection State	33 %
----------------------	------

### Web Reputation

Web Reputation State	100 %
----------------------	-------

#### **Anti-Malware Scan Setting [Real-Time Scan]**

---

Alert when this Malware Scan Configuration logs an event	67 %
Real-Time Scan	67 %
Scan Compressed Files	67 %
Scan Embedded Microsoft Office Objects	67 %
Scan Settings: Directories to scan	67 %
Scan Settings: Files to scan	67 %
Spyware/Grayware Protection	67 %

#### **Anti-Malware Scan Setting [Manual Scan]**

---

Alert when this Malware Scan Configuration logs an event	0 %
Scan Compressed Files	67 %
Scan Embedded Microsoft Office Objects	67 %
Scan Settings: Directories to scan	67 %
Scan Settings: Files to scan	67 %
Spyware/Grayware Protection	67 %

#### **Anti-Malware Scan Setting [Scheduled Scan]**

---

Alert when this Malware Scan Configuration logs an event	0 %
Scan Compressed Files	67 %
Scan Embedded Microsoft Office Objects	67 %
Scan Settings: Directories to scan	67 %
Scan Settings: Files to scan	67 %
Spyware/Grayware Protection	67 %



## 3. Environment Details

### Ratio of managed computers: High

A great number (80% or more) of computers registered in the Deep Security Manager have Deep Security Agents installed, properly activated, and are being actively protected according to their configurations.

### Environment Overview

Platform	Managed	Unmanaged	Total	Platform Distribution	Compliance Rating
Microsoft Windows 10 (64 bit)	1	0	1	1 / 3	77%
Red Hat Enterprise 7 (64 bit)	1	0	1	1 / 3	4%
Ubuntu Linux 18 (64 bit)	1	0	1	1 / 3	85%

### Deep Security Agent Version Distribution

All agents in the environment are using the same major version. To further improve your security, make sure the the agents are properly updated. Please note that Feature releases are interim releases that provide early access to new features, and are only supported for six months after the next major release. Note that the number of agents does not equal the actual number of managed computers. An agent (Such as DSVA) can protect multiple computers, which are protected under agentless mode.

Version	Activated Agents
12.0.0.1090	1
12.0.0.1186	1
20.0.0.877	1

## 4. Appendix

### 4.1 Settings

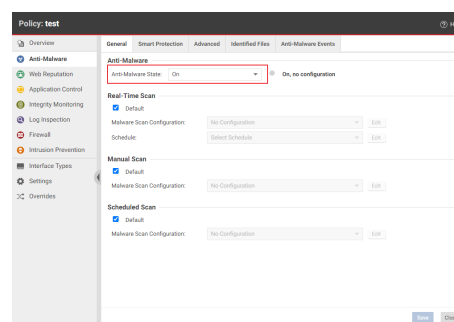
#### Anti Malware

##### Anti Malware State

The Deep Security anti-malware module provides agent computers with both real-time and on-demand protection against file-based threats, including malware, viruses, Trojans, and spyware. To identify threats, the anti-malware module checks files on the local hard drive against a comprehensive threat database. The anti-malware module also checks files for certain characteristics, such as compression and known exploit code. Note: Portions of the threat database are hosted on Trend Micro servers or stored locally as patterns. Deep Security Agents periodically download anti-malware patterns and updates to ensure protection against the latest threats. A newly installed Deep Security Agent cannot provide anti-malware protection until it has contacted an update server to download anti-malware patterns and updates. Ensure that your Deep Security Agents can communicate with a Deep Security Relay or the Trend Micro Update Server after installation. The anti-malware module eliminates threats while minimizing the impact on system performance. The anti-malware module can clean, delete, or quarantine malicious files. It can also terminate processes and delete other system objects that are associated with identified threats.

##### [RECOMMENDATION]

Enabled



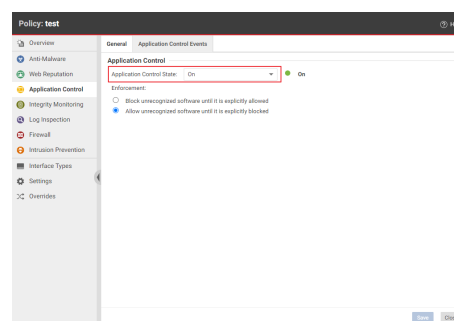
## Application Control

### Application Control State

Application control continuously monitors for software changes on your protected servers. Based on your policy configuration, application control either prevents unauthorized software from running until it is explicitly allowed (whitelisted), or allows unauthorized software until it is explicitly blocked (blacklisted). Which option you choose depends on the level of control you want over your environment. Warning: Application control continuously monitors your server and logs an event whenever a software change occurs. It is not intended for environments with self-changing software or that normally creates executables, such as some web or mail servers.unauthorized applications.

#### [RECOMMENDATION]

Enabled



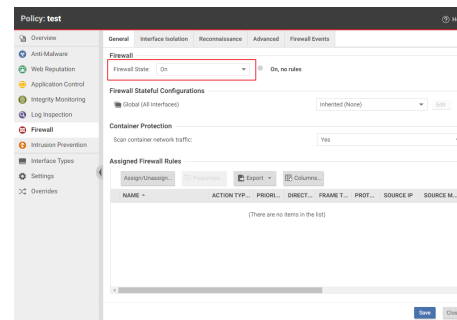
## Firewall

### Firewall State

The firewall module provides bidirectional stateful inspection of incoming and outgoing traffic. Firewall rules define what actions to take on individual packets in that traffic. Packets can be filtered by IP and MAC address, port and packet flag across all IP-based protocols and frame types. The firewall module can also help prevent denial of service attacks and detect and prevent reconnaissance scans.

#### [RECOMMENDATION]

Enabled



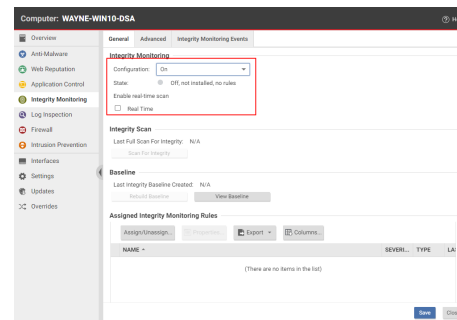
## Integrity Monitoring

### Integrity Monitoring State

The integrity monitoring module scans for unexpected changes to registry values, registry keys, services, processes, installed software, ports and files on Deep Security Agents. Using a baseline secure state as a reference, the integrity monitoring module performs scans on the above and logs an event (and an optional alert) if it detects any unexpected changes.

#### [RECOMMENDATION]

Enabled, regardless of whether real-time scanning is enabled



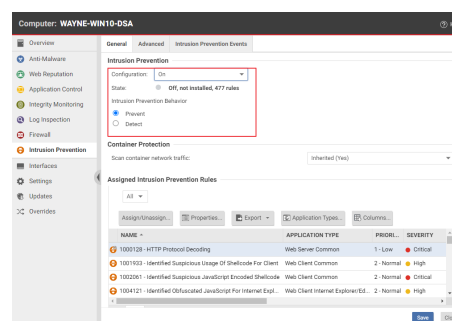
## Intrusion Prevention

### Intrusion Prevention State

The Intrusion Prevention module protects your computers from known and zero-day vulnerability attacks as well as against SQL injections attacks, cross-site scripting attacks, and other web application vulnerabilities. When patches are not available for known vulnerabilities in applications or operating systems, Intrusion Prevention rules can intercept traffic that is trying to exploit the vulnerability. It identifies malicious software that is accessing the network and it increases visibility into, or control over, applications that are accessing the network. Therefore your computers are protected until patches that fix the vulnerability are released, tested, and deployed. Protection is available for file sharing and messaging software such as Skype, but also web applications with vulnerabilities such as SQL injection and cross-site scripting (XSS). In this way, Intrusion Prevention can also be used as a lightweight web application firewall (WAF).

#### [RECOMMENDATION]

Enabled, regardless of whether it is configured as "Prevent" or "Detect".



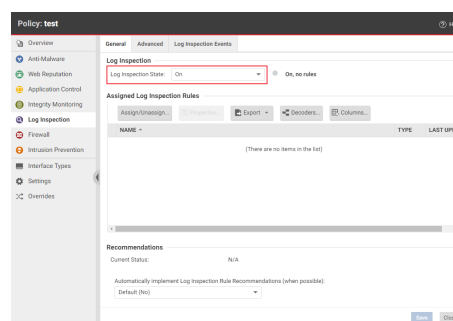
## Log Inspection

### Log Inspection State

The log inspection protection module helps you identify important events that might be buried in your operating system and application logs. These events can be sent to a security information and event management (SIEM) system or centralized logging server for correlation, reporting, and archiving. All events are also securely collected in the Deep Security Manager. The log inspection module lets you:

- \* Meet PCI DSS log monitoring requirements.
- \* Detect suspicious behavior.
- \* Collect events across heterogeneous environments containing different operating systems and diverse applications.
- \* View events such as error and informational events (disk full, service start, service shutdown, etc.).
- \* Create and maintain audit trails of administrator activity (administrator login or logout, account lockout, policy change, etc.).

The log inspection feature in Deep Security enables real-time analysis of third party log files. The log inspection rules and decoders provide a framework to parse, analyze, rank and correlate events across a wide variety of systems. As with intrusion prevention and integrity monitoring, log inspection content is delivered in the form of rules included in a security update. These rules provide a high level means of selecting the applications and logs to be analyzed.



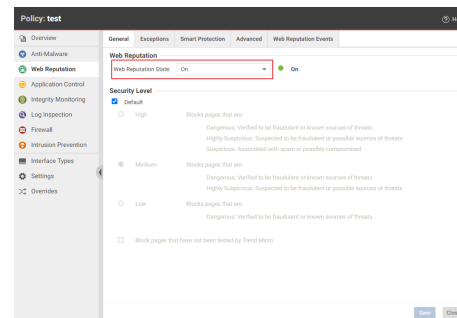
## Web Reputation

### Web Reputation State

The web reputation module protects against web threats by blocking access to malicious URLs. Deep Security uses Trend Micro's Web security databases from Smart Protection Network sources to check the reputation of websites that users are attempting to access. The website's reputation is correlated with the specific web reputation policy enforced on the computer. Depending on the security level being enforced, Deep Security will either block or allow access to the URL. Note: The web reputation module does not block HTTPS traffic.

#### [RECOMMENDATION]

Enabled





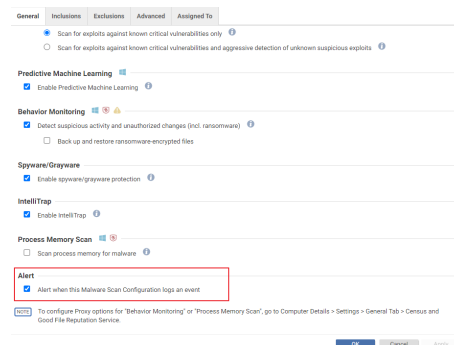
## Anti-Malware Scan Setting [Real-Time Scan]

Alert when this Malware Scan Configuration logs an event

When Deep Security detects malware, you can generate an alert.

### [RECOMMENDATION]

Enable it for real-time scanning tasks.



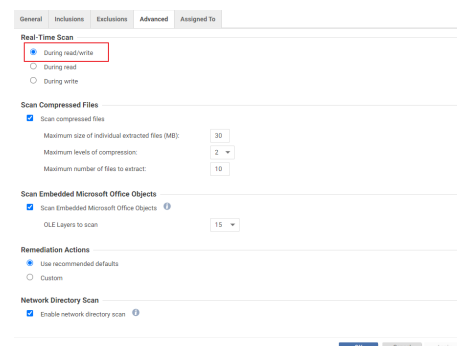
The screenshot shows the 'Advanced' tab of the Malware Scan Configuration settings. The 'Alert' section is highlighted with a red box, showing the option 'Alert when this Malware Scan Configuration logs an event' which is checked. Other settings visible include 'Predictive Machine Learning', 'Behavior Monitoring', 'Spyware/Grayware', 'IntelliTrap', and 'Process Memory Scan'.

### Real-Time Scan

To specify when to scan the files, select "During read/write", "During read" or "During write". (real-time scan only)

### [RECOMMENDATION]

Configured it as "During read/write" for real-time scanning tasks.



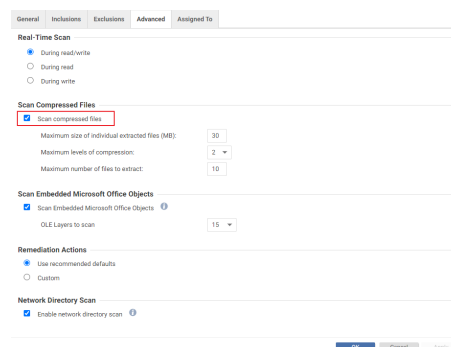
The screenshot shows the 'Advanced' tab of the Malware Scan Configuration settings, specifically the 'Real-Time Scan' section. The 'During read/write' option is selected and highlighted with a red box. Other settings visible include 'Scan Compressed Files', 'Scan Embedded Microsoft Office Objects', 'Remediation Actions', and 'Network Directory Scan'.

### Scan Compressed Files

Extract compressed files and scan the contents for malware. When you enable the scan, you specify the maximum size and number of files to extract (large files can affect performance). You also specify the levels of compression to inspect so that you can scan compressed files that reside inside compressed files. Level 1 compression is a single compressed file. Compressed files inside that file are level two. You can scan a maximum of 6 compression levels, however higher levels can affect performance.

#### [RECOMMENDATION]

Enable it for real-time scanning tasks.

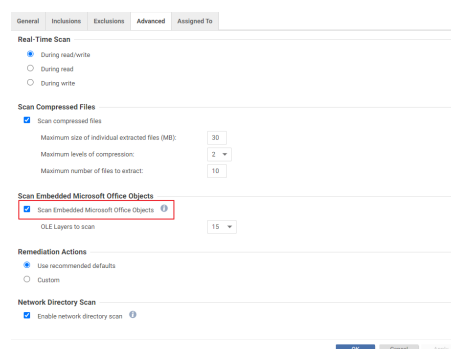


### Scan Embedded Microsoft Office Objects

Certain versions of Microsoft Office use Object Linking and Embedding (OLE) to insert files and other objects into Office files. These embedded objects can contain malicious code. Specify the number of OLE layers to scan to detect objects that are embedded in other objects. To reduce the impact on performance, you can scan only a few layers of embedded objects within each file.

#### [RECOMMENDATION]

Enable it for real-time scanning tasks.

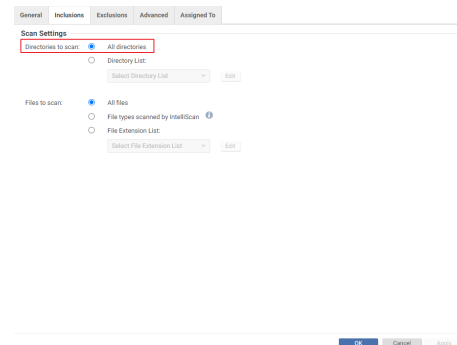


### Scan Settings: Directories to scan

To specify the directories to scan for malware, select All directories or Directory List.

#### [RECOMMENDATION]

Configured it as "All directories" for real-time scanning tasks.



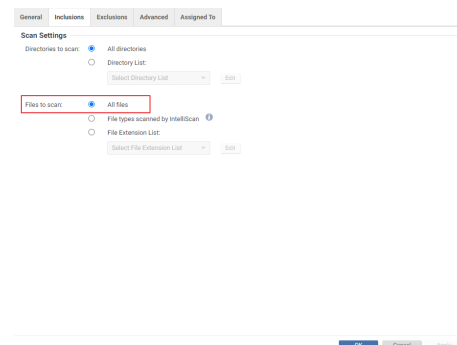
The screenshot shows the 'Scan Settings' dialog box with the 'Exclusions' tab selected. Under 'Directories to scan', the 'All directories' radio button is selected. Below it, there is a 'Select Directory List' button and a 'Scan' button. Under 'Files to scan', the 'All files' radio button is selected. Below it, there are two other options: 'File types scanned by IntelliScan' and 'File Extension List', each with a 'Select File Extension List' button and a 'Scan' button.

### Scan Settings: Files to scan

To specify the files to scan, select either All files, File types scanned by IntelliScan, or File Extension List.

#### [RECOMMENDATION]

Configured it as "All files" for real-time scanning tasks.



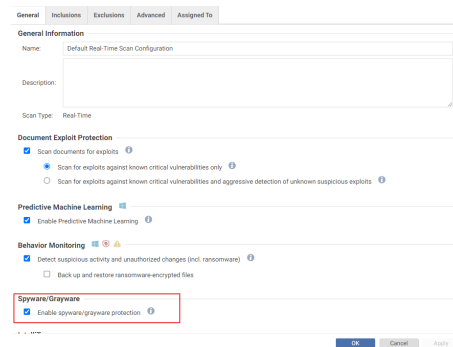
The screenshot shows the 'Scan Settings' dialog box with the 'Exclusions' tab selected. Under 'Files to scan', the 'All files' radio button is selected. Below it, there are two other options: 'File types scanned by IntelliScan' and 'File Extension List', each with a 'Select File Extension List' button and a 'Scan' button.

### Spyware/Grayware Protection

When spyware and grayware protection is enabled, the spyware scan engine quarantines suspicious files when they are detected.

#### [RECOMMENDATION]

Enable it for real-time scanning tasks.



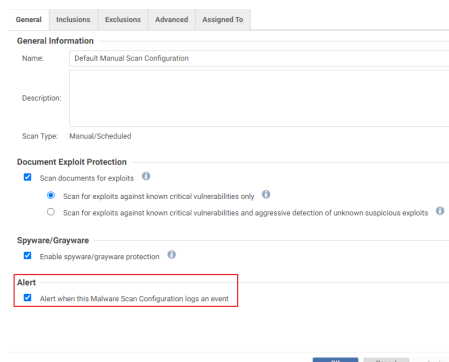
## Anti-Malware Scan Setting [Manual Scan]

Alert when this Malware Scan Configuration logs an event

When Deep Security detects malware, you can generate an alert.

### [RECOMMENDATION]

Enable it for manual scanning tasks.



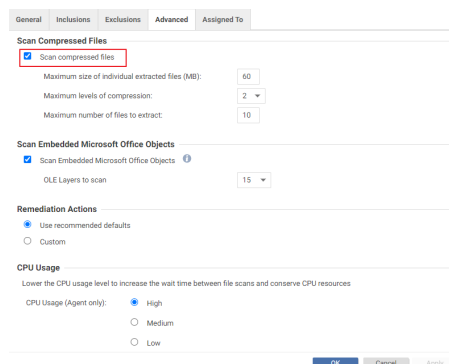
The screenshot shows the 'General' tab of the Malware Scan Configuration window. The 'Name' field is 'Default Manual Scan Configuration'. The 'Scan Type' is 'Manual/Scheduled'. Under 'Document Exploit Protection', the 'Scan documents for exploits' checkbox is checked. Under 'Spyware/Grayware', the 'Enable spyware/grayware protection' checkbox is checked. In the 'Alert' section, the 'Alert when this Malware Scan Configuration logs an event' checkbox is checked and highlighted with a red box. The 'OK', 'Cancel', and 'Apply' buttons are at the bottom right.

### Scan Compressed Files

Extract compressed files and scan the contents for malware. When you enable the scan, you specify the maximum size and number of files to extract (large files can affect performance). You also specify the levels of compression to inspect so that you can scan compressed files that reside inside compressed files. Level 1 compression is a single compressed file. Compressed files inside that file are level two. You can scan a maximum of 6 compression levels, however higher levels can affect performance.

### [RECOMMENDATION]

Enable it for manual scanning tasks.



The screenshot shows the 'Advanced' tab of the Malware Scan Configuration window. Under 'Scan Compressed Files', the 'Scan compressed files' checkbox is checked and highlighted with a red box. The 'Maximum size of individual extracted files (MB)' is set to 60. The 'Maximum levels of compression' is set to 2. The 'Maximum number of files to extract' is set to 10. Under 'Scan Embedded Microsoft Office Objects', the 'Scan Embedded Microsoft Office Objects' checkbox is checked. The 'OLE Layers to scan' is set to 15. Under 'Remediation Actions', the 'Use recommended defaults' radio button is selected. Under 'CPU Usage', the 'High' radio button is selected. The 'OK', 'Cancel', and 'Apply' buttons are at the bottom right.

### Scan Embedded Microsoft Office Objects

Certain versions of Microsoft Office use Object Linking and Embedding (OLE) to insert files and other objects into Office files. These embedded objects can contain malicious code. Specify the number of OLE layers to scan to detect objects that are embedded in other objects. To reduce the impact on performance, you can scan only a few layers of embedded objects within each file.

#### [RECOMMENDATION]

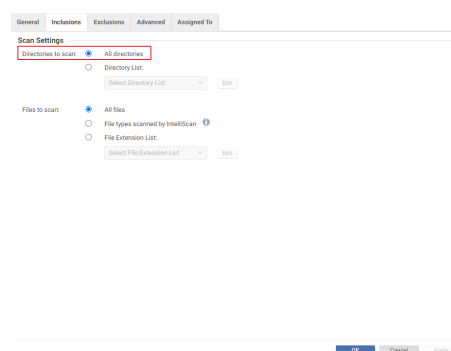
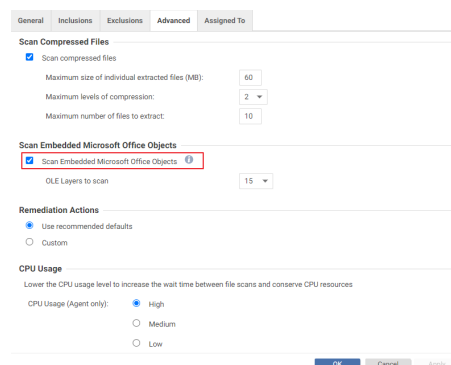
Enable it for manual scanning tasks.

### Scan Settings: Directories to scan

To specify the directories to scan for malware, select All directories or Directory List.

#### [RECOMMENDATION]

Configured it as "All directories" for manual scanning tasks.

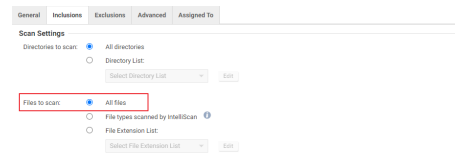


### Scan Settings: Files to scan

To specify the files to scan, select either All files, File types scanned by IntelliScan, or File Extension List.

#### [RECOMMENDATION]

Configured it as "All files" for manual scanning tasks.



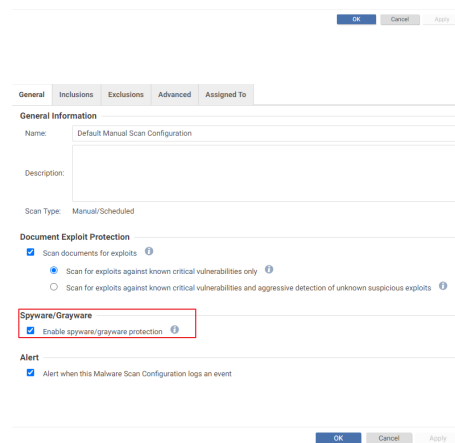
The screenshot shows the 'Files to scan' tab in the Scan Settings dialog. The 'Directories to scan' section has 'All directories' selected. The 'Files to scan' section has 'All files' selected, which is highlighted with a red box. Other options include 'File types scanned by IntelliScan' and 'File Extension List'.

### Spyware/Grayware Protection

When spyware and grayware protection is enabled, the spyware scan engine quarantines suspicious files when they are detected.

#### [RECOMMENDATION]

Enable it for manual scanning tasks.



The screenshot shows the 'General Information' tab in the Scan Settings dialog. The 'Name' field is 'Default Manual Scan Configuration'. The 'Scan Type' is 'Manual/Scheduled'. Under 'Document Exploit Protection', 'Scan documents for exploits' is checked. Under 'Spyware/Grayware', 'Enable spyware/grayware protection' is checked and highlighted with a red box. The 'Alert' section has 'Alert when this Malware Scan Configuration logs an event' checked.

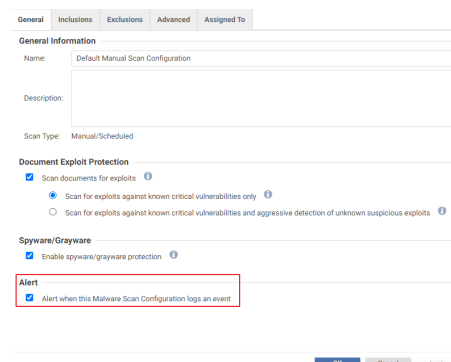
## Anti-Malware Scan Setting [Scheduled Scan]

Alert when this Malware Scan Configuration logs an event

When Deep Security detects malware, you can generate an alert.

### [RECOMMENDATION]

Enable it for scheduled scanning tasks.



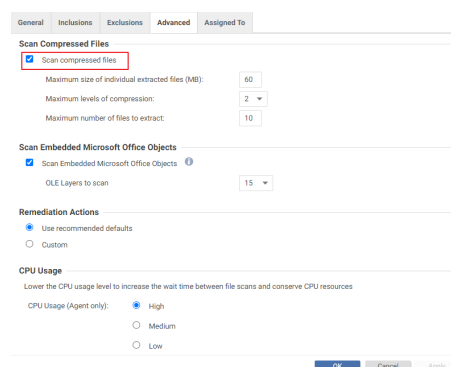
The screenshot shows the 'General' tab of a Malware Scan Configuration. The 'Name' field is 'Default Manual Scan Configuration'. The 'Scan Type' is 'Manual/Scheduled'. Under 'Document Exploit Protection', the 'Scan documents for exploits' checkbox is checked. Under 'Spyware/Grayware', the 'Enable spyware/grayware protection' checkbox is checked. In the 'Alert' section, the 'Alert when this Malware Scan Configuration logs an event' checkbox is checked and highlighted with a red box. The 'OK', 'Cancel', and 'Apply' buttons are at the bottom right.

### Scan Compressed Files

Extract compressed files and scan the contents for malware. When you enable the scan, you specify the maximum size and number of files to extract (large files can affect performance). You also specify the levels of compression to inspect so that you can scan compressed files that reside inside compressed files. Level 1 compression is a single compressed file. Compressed files inside that file are level two. You can scan a maximum of 6 compression levels, however higher levels can affect performance.

### [RECOMMENDATION]

Configured it as "All files" for scheduled scanning tasks.



The screenshot shows the 'Advanced' tab of a Malware Scan Configuration. The 'Scan compressed files' checkbox is checked and highlighted with a red box. Below it, the 'Maximum size of individual extracted files (MB)' is set to 60, 'Maximum levels of compression' is set to 2, and 'Maximum number of files to extract' is set to 10. Under 'Scan Embedded Microsoft Office Objects', the 'Scan Embedded Microsoft Office Objects' checkbox is checked, and 'OLE Layers to scan' is set to 15. Under 'Remediation Actions', the 'Use recommended defaults' radio button is selected. Under 'CPU Usage', the 'High' radio button is selected. The 'OK', 'Cancel', and 'Apply' buttons are at the bottom right.



### Scan Embedded Microsoft Office Objects

Certain versions of Microsoft Office use Object Linking and Embedding (OLE) to insert files and other objects into Office files. These embedded objects can contain malicious code. Specify the number of OLE layers to scan to detect objects that are embedded in other objects. To reduce the impact on performance, you can scan only a few layers of embedded objects within each file.

#### [RECOMMENDATION]

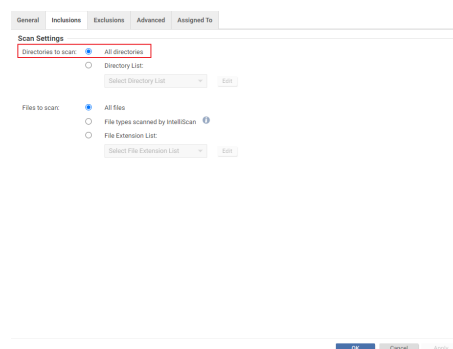
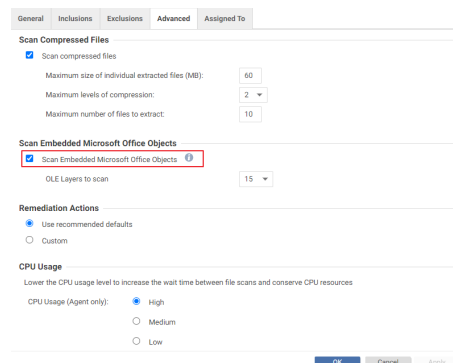
Enable it for scheduled scanning tasks.

### Scan Settings: Directories to scan

To specify the directories to scan for malware, select All directories or Directory List.

#### [RECOMMENDATION]

Configured it as "All directories" for scheduled scanning tasks.

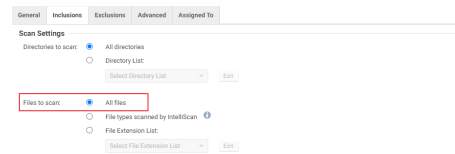


### Scan Settings: Files to scan

To specify the files to scan, select either All files, File types scanned by IntelliScan, or File Extension List.

#### [RECOMMENDATION]

Configured it as "All files" for scheduled scanning tasks.



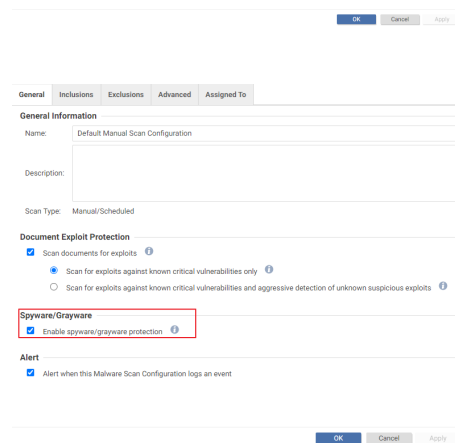
The screenshot shows the 'Files to scan' tab in the Scan Settings dialog. The 'Directories to scan' section has 'All directories' selected. The 'Files to scan' section has 'All files' selected, which is highlighted with a red box. Other options include 'File types scanned by IntelliScan' and 'File Extension List'.

### Spyware/Grayware Protection

When spyware and grayware protection is enabled, the spyware scan engine quarantines suspicious files when they are detected.

#### [RECOMMENDATION]

Enable it for scheduled scanning tasks.



The screenshot shows the 'General Information' tab in the Scan Settings dialog. The 'Name' field is 'Default Manual Scan Configuration'. The 'Description' field is empty. The 'Scan Type' is 'Manual/Scheduled'. The 'Document Exploit Protection' section has 'Scan documents for exploits' checked. The 'Spyware/Grayware' section has 'Enable spyware/grayware protection' checked, which is highlighted with a red box. The 'Alert' section has 'Alert when this Malware Scan Configuration logs an event' checked.