

Using Symantec Endpoint Protection 12.1 to Protect Against Advanced Persistent Threats (APTs)

Configuration guidelines for endpoint protection against APTs

Protecting Endpoints from APTs with Symantec Endpoint Protection 12.1

Configuration guidelines for endpoint protection against APTs

Introduction.....	4
The challenge of Advanced Persistent Threats	4
Symantec Endpoint Protection 12.1	6
Virus and Spyware Protection.....	7
Why should you use Virus and Spyware Protection?	7
How to implement Virus and Spyware Protection	8
How to monitor Virus and Spyware Protection for malicious activity.....	10
How to test that Virus and Spyware Protection is functioning	11
Intrusion Prevention (IPS)	11
Why should you use Intrusion Prevention (IPS)?.....	11
How to implement IPS	12
How to monitor Intrusion Prevention attacks.....	14
How to test Intrusion Prevention	14
Download Insight (Advanced Download Protection)	16
Why should you use Download Insight (Advanced Download Protection)?.....	16
How to implement Download Insight	16
How to monitor Download Insight for malicious activity	19
How to test that Download Insight Protection is functioning	20
SONAR	22
Why should you use SONAR?	22
How to implement SONAR	22
How to monitor SONAR for malicious activity	26
How to test that SONAR is functioning?	26
Rule-based policy options for additional protection	28

Application Control	28
Why should you use Application Control?	28
How to implement Application Control	29
How to monitor Application Control for activity	30
How to test that application control is functioning	31
Application Learning	32
Why should you use Application Learning?	32
How to implement Application Learning	32
How to monitor Application Learning for malicious activity	34
How to test that Application Learning is functioning	34
System Lockdown	36
Why should you use System Lockdown?	36
How to implement System Lockdown	36
How to monitor System Lockdown for malicious activity	36
How to test that System Lockdown is functioning	36
False Positive Mitigation	37
Preventing False Positives	37
Correcting False Positives	37
Adding Exceptions	38
Appendices	39
Remediation	39
Summary: Layered Protection in SEP 12.1	41
Additional Symantec Offerings to Protect against Advanced Persistent Threats	43

Introduction

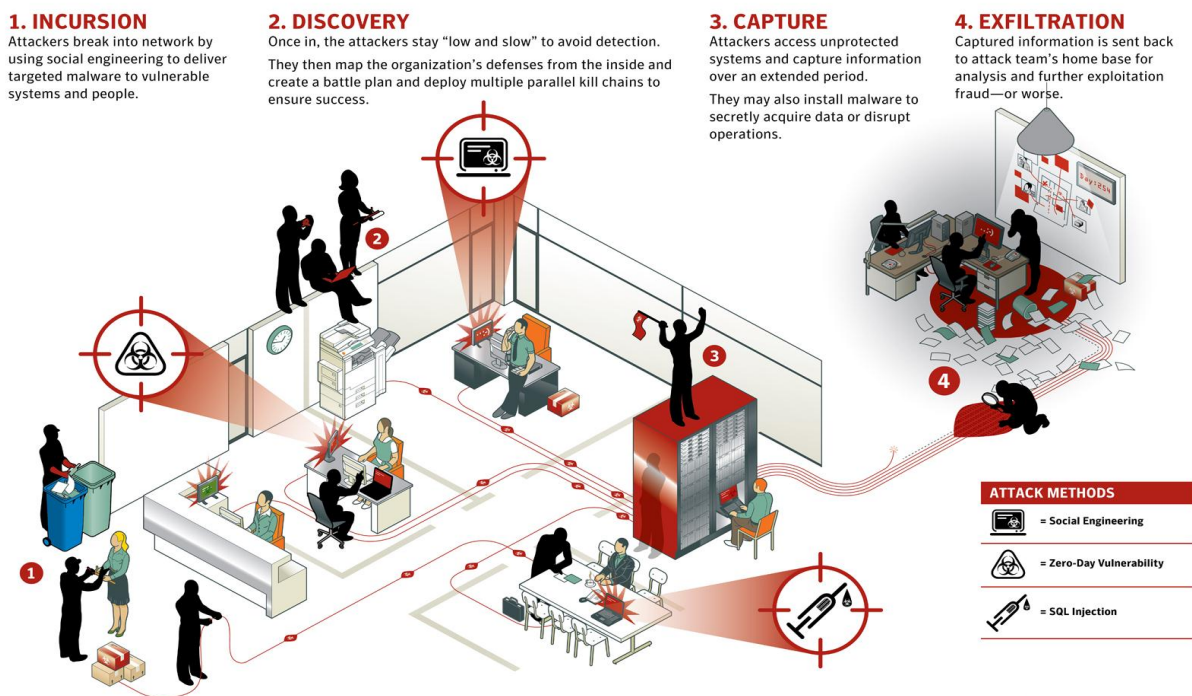
Advanced persistent threats (APTs) pose serious challenges for organizations of all sizes. Challenges related to advanced persistent threats include cyber attacks that are designed to do anything from steal sensitive data for financial gain, corporate espionage, etc., to sabotage of critical infrastructure. These attacks are specifically targeted and are often carried out using sophisticated malware. The effectiveness of traditional file-based antivirus scanning technology is not by itself sufficient protection because a given malware associated with an APT will have extremely low prevalence, that is, will not be widely seen on the Internet. Traditional antivirus signature-based scanning is reactive in that a signature can only be written to detect a threat that has already been seen.

Symantec Endpoint Protection 12.1 (SEP 12.1) includes protection technologies that go beyond traditional antivirus scanning to provide effective protection of endpoints against the sophisticated malware used by APTs. This paper provides guidelines on how to ensure that SEP protection technologies are enabled and functioning in order to provide best protection for endpoints.

The challenge of Advanced Persistent Threats

Advanced persistent threats often use malware that is difficult to detect using traditional antivirus scanning and are designed specifically to run for long periods of time without being noticed. These threats are targeted and as such do not have wide distribution on the Internet. They are generally intended for specific targets and designed to evade detection in order to steal data. The type of data that is targeted for attacks varies by attacker and target, (financial gain, usernames/passwords, intellectual property, etc.)

Even though the motives and targets used by APTs can vary greatly, they often operate in stages that are common across attacks. They are: Incursion, Discovery, Capture, and Exfiltration and are briefly described in the illustration below:



Symantec Endpoint Protection (SEP 12.1) offers advanced protection by using multiple technologies to combat many targeted attack methods that are prevalent in the current threat landscape. While this document details the configurations

and best practices in the use of SEP 12.1 against modern threat vectors, these details are only part of an overall security strategy. Many organizations have some sort of endpoint security solution installed and deployed. Breaches and intrusions can occur when these technology-based safeguards are not supported by sound, realistic, and effective security processes and procedures. For example:

- Has an effort been made to classify the organization's data using the potential damage of exposure as a guide?
- Are policies (both technology-based and operational) in place that reflect an individuals' or systems' access to sensitive data?
- Is there an awareness program to educate end users about social engineering methods that are prevalent in targeted attacks?
- Does the organization have an awareness of the principals of Operational Security and has an examination or audit been done on the amount of information available online, throughout social media or via search engines?
- Is sensitive data encrypted both at rest and in transit?
- Has a bring your own device (BYOD) and remote user strategy been vetted not only for productivity, but for security and compliance as well?

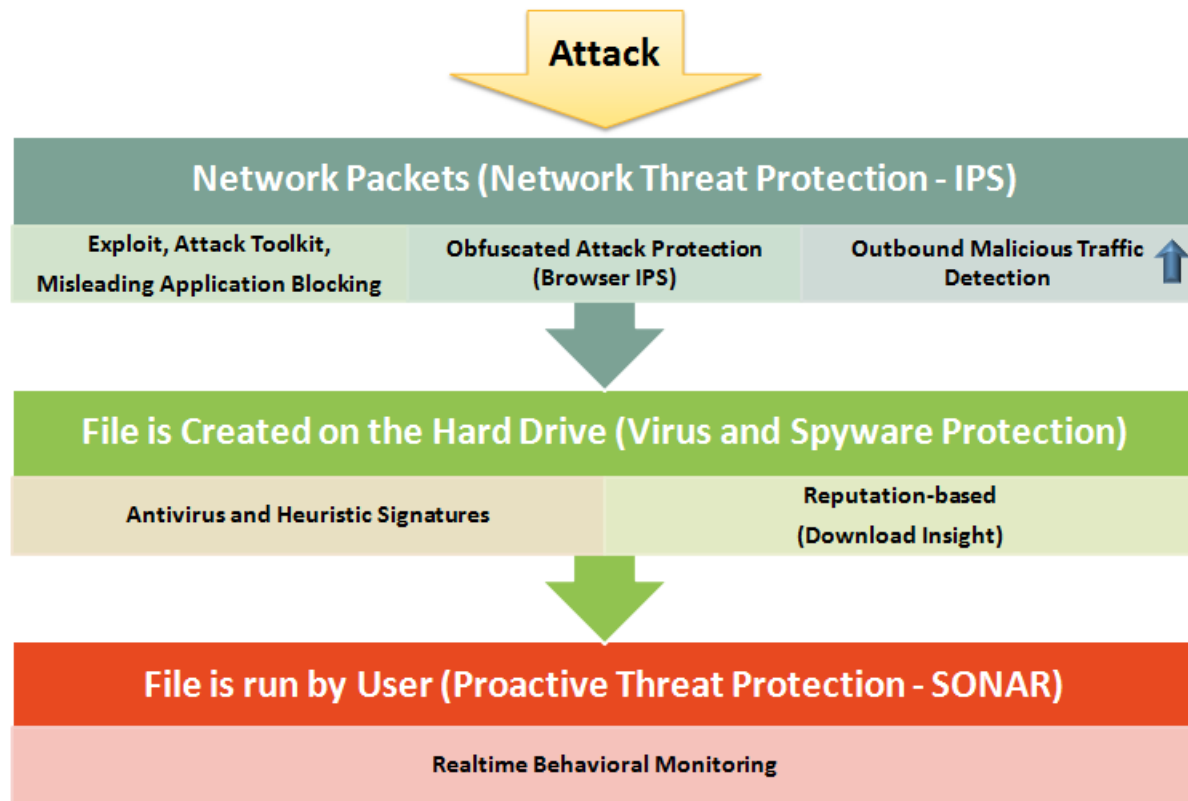
All of this sounds like a lot of work, and the reality is it can be. These are serious questions that reflect the reality of today's operating environment. There are more questions as well and an in-depth examination of these aspects is beyond the scope of this document. However, as breaches and exposures commonly reported in the press indicate, the risk that is accepted by not answering or addressing these questions and others can result in serious damage to reputation, confidence, and productivity. The guidance that follows is designed to be part of a security policy-based methodology that is both information centric and technology based.

For additional reading, see the following article:

http://www.symantec.com/threatreport/topic.jsp?id=best_practices

Symantec Endpoint Protection 12.1

SEP 12.1 uses a multi-layered approach to provide advanced protection against new and unknown malware used by APTs on endpoints. In addition to traditional file-based antivirus, SEP 12.1 provides protection technologies that use Intrusion Prevention (network packet scanning), Download Insight (advanced download protection with reputation), and SONAR (real-time behavior-based scanning). These technologies are developed by Symantec Security Technology and Response (STAR) and are installed and enabled by default in SEP 12.1.



For more information about Symantec Security Technology and Response see:

<http://www.symantec.com/page.jsp?id=star>

Since these STAR technologies are installed and enabled by default, the following sections are intended to help administrators review their SEP 12.1 design and implementation to confirm they are getting the benefit from these out-of-the-box SEP 12.1 protection technologies.

In addition to the protection technologies developed by STAR, SEP 12.1 includes additional rule-based protection that requires some configuration to enable. These protections include Application and Device Control, System Lockdown, and Host Integrity, and are covered in more detail in later sections.

Please note that this document focuses on protection technologies available for Windows clients. Symantec Endpoint Protection is also available for Macintosh and Linux clients, but are not covered in this document. Please see the following Knowledge Base articles for more information regarding protection for Mac and Linux:

Overview for Symantec Endpoint Protection 12.1.4 for Mac

<http://www.symantec.com/docs/HOWTO92146>

About the Symantec AntiVirus client for Linux

<http://www.symantec.com/docs/HOWTO17995>

Virus and Spyware Protection

File-based Virus and Spyware Protection is the traditional method for identifying malicious files by matching signatures with known malicious files or malicious file families. It remains an important part of an overall protection strategy, however on its own it is not enough to protect against new and unknown malware used by APTs. Virus and Spyware Protection detects malicious files by the following methods:

- 1) **Real-time file protection (Auto-Protect)** – Auto-Protect scans files when they are accessed or modified. Auto-Protect is the real-time scanning component in SEP 12.1 and monitors file I/O in order to detect and block access to any files that are malicious. Files accessed on network shares or removable drives (USB sticks for example) will be scanned by Auto-Protect. Files compressed in archive files (.zip, .rar, etc.) are not scanned by Auto-Protect, however, any file extracted from an archive file will be scanned by Auto-Protect to prevent malicious code from being accessed or executed.
- 2) **Manual and scheduled scans** – Manual and scheduled scans scan files on the local systems' hard drive for malicious code and, depending on the configuration, scan all files on a disk drive (Full Scan), or selected folders, load points, and running processes commonly used by malware (Active Scan). Manual and scheduled scans do scan inside archive files. Network shares can be scanned but for performance reasons this is generally not recommended. Administrators can prevent network shares from being scanned by users by requiring a password to scan network drives.
- 3) **Email plugins** – The SEP client offers optional email scanning components for Exchange/Outlook, Domino/Notes, and Internet/SMTP/POP3. Scanning happens in real time and includes scanning inside archive files. If email plugins are not used, then malicious attachments can potentially appear in a users' inbox, however Auto-Protect will scan any malicious attachments if there is an attempt to run or save the attachment to the drive.
Note: Even though email plugins provide an additional layer of protection on the endpoint, Symantec Mail Security (for Gateways and Groupware servers) should be part of an overall protection strategy for malware scanning in email. See the appendix for more information about additional Symantec solutions that provide additional protection against APTs.

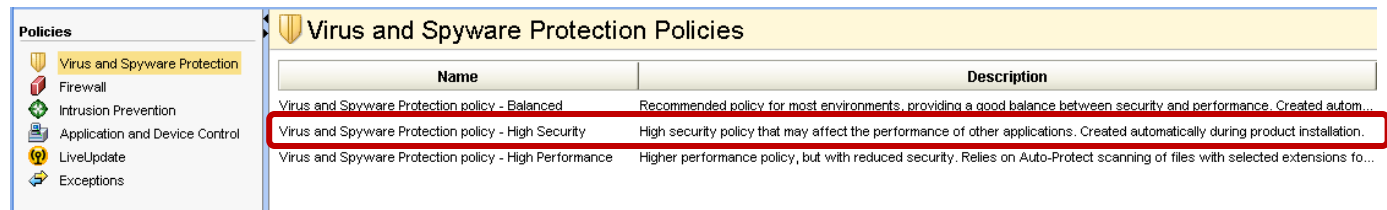
Why should you use Virus and Spyware Protection?

Even though Virus and Spyware Protection is not sufficient by itself to protect against today's threats, it remains an important way of identifying and blocking known malware. In addition to blocking malware, Virus and Spyware Protection provides detection and prevention capabilities that can help administrators identify infected systems that try to download additional malware.

How to implement Virus and Spyware Protection

Virus and Spyware Protection is a key component that is installed and enabled by default. It is important that Virus and Spyware Protection is up-to-date in order to ensure the best possible protection against the latest threats.

SEP 12.1 comes with several Virus and Spyware Protection policies in the management console that are created automatically during product installation. The default policy is balanced between security and performance for most environments. However, there is also a High Security Virus and Spyware policy that is recommended for better security.

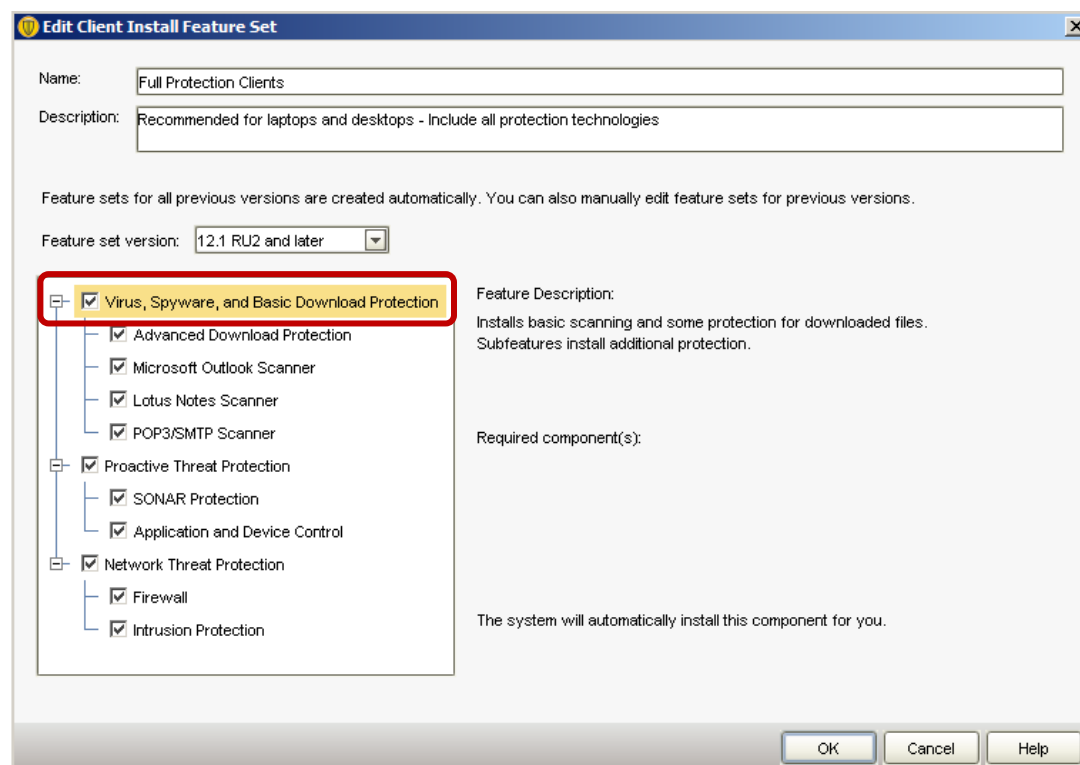


Note that configuration settings in the High Security policy are locked and cannot be changed by end users for Virus and Spyware Protection, Download Insight, and SONAR.

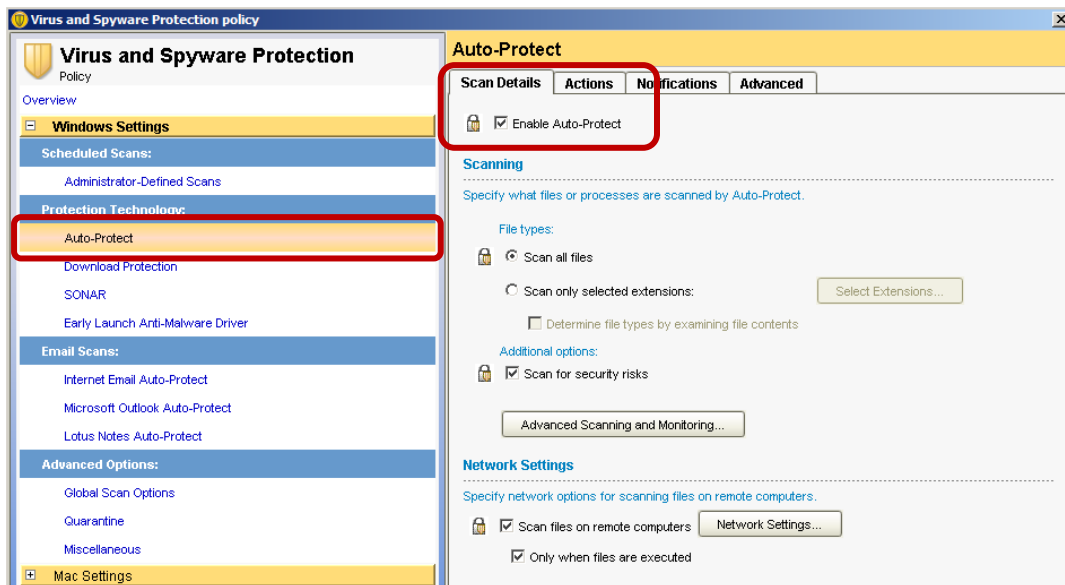
See the following knowledge base article for more details about the available options in the default Virus and Spyware Protection policies, including the High Security policy. For better protection use the High Security policy:

<http://www.symantec.com/business/support/index?page=content&id=TECH173752>

- 1) **Installation:** Virus and Spyware Protection is selected by default during installation or when creating a SEP 12.1 installation package. Make sure that the Virus and Spyware Protection component is selected when installing or creating a client installation package.



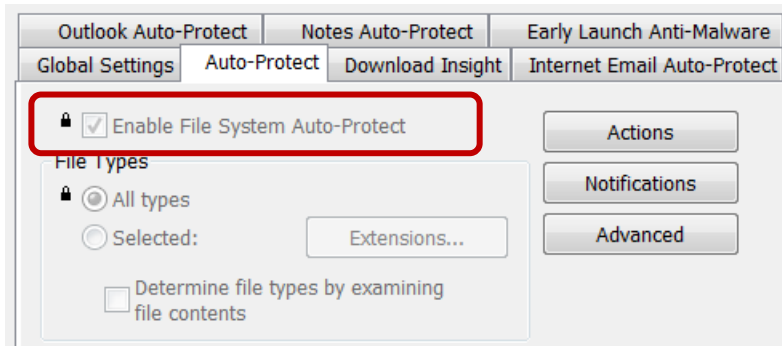
- 2) **Virus and Spyware Protection policy:** Auto-protect is a key component for real-time file scanning. It is enabled by default for a managed SEP client. To confirm it is enabled, in the Symantec Endpoint Protection Manager, select the relevant Virus and Spyware Protection policy for the client group you would like to verify and select **edit policy**. Within the policy select **Auto-Protect** and confirm there is a check next to **Enable Auto-Protect** option as show here:



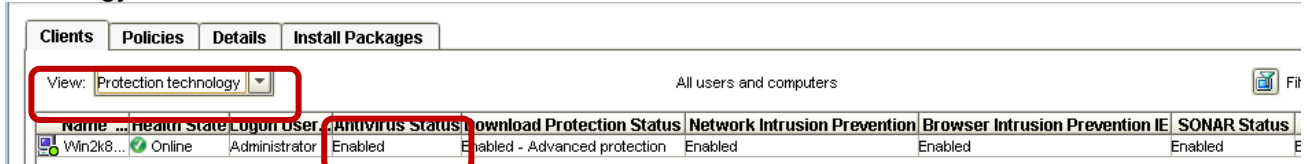
- 3) **Client User Interface:** Virus and Spyware Protection status appears in the client user interface as shown here. Definition date and revision number are also shown. On average Symantec releases three definition revisions per day.



In order to confirm that Auto-Protect is enabled, click **Options** next to Virus and Spyware Protection and select **Change Settings**. Select the **Auto-Protect** tab and confirm that there is a check next to **Enable File System Auto-Protect** as shown here:



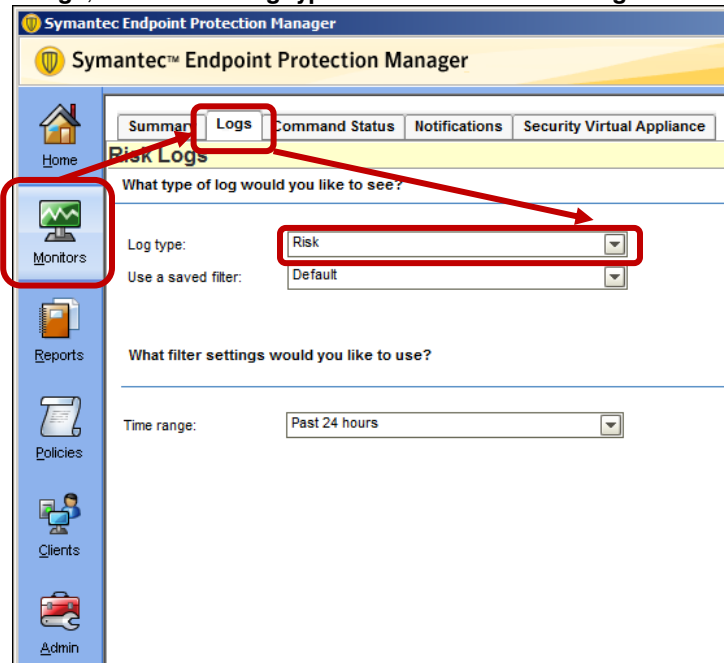
- 4) **Symantec Endpoint Protection Manager:** In the console, go to the **Clients** page and select the **Protection technology** view as shown here:



How to monitor Virus and Spyware Protection for malicious activity

When Virus and Spyware Protection detects malicious files, the SEP 12.1 client logs the events and forwards them to the Symantec Endpoint Protection Manager. To view virus and spyware events in the management console, go to **Monitors**

> **Logs**, then choose **Log type > Risk** and click **View Log**.



When a malicious file is detected, SEP 12.1 will take action on the file. SEP uses a primary action or if the primary action cannot be taken, a secondary action. Possible actions include:

- Delete
- Quarantine
- Clean
- Leave Alone (log only)

Generally, if the action taken is Delete, Quarantine, or Clean, the malicious file was blocked and appropriately remediated. It is not necessary for administrators to take further steps on the endpoint that had a detection. When reviewing Risk logs in the management console, an important field to review is the **Action taken** field.

Some Virus and Spyware Protection detections can indicate that a computer has been compromised and should be investigated. Following a detection, in some cases SEP 12.1 may not be able to fully remediate or remove all traces of a threat. The following examples describe behavior that may indicate that SEP 12.1 was not able to completely remove a threat and that the computer might require further investigation:

- 1) The action taken as recorded in the Risk log does not match the configured primary or secondary actions. This might indicate that SEP 12.1 was unable to properly block the file and the computer might be compromised.
- 2) A system repeatedly detects new malware. This might indicate that an unknown threat is on a computer and is acting as a “dropper,” which tries to download additional malware that is then detected by antivirus signatures.

How to test that Virus and Spyware Protection is functioning

Virus and Spyware detection capabilities can be tested with the Eicar test file eicar.com. The Eicar test file does not contain a malicious payload, but antivirus vendors detect eicar as a way of ensuring virus protection is in place. The Eicar test file can be downloaded from the following website: www.eicar.org

Note: The link is provided as a convenience, Symantec is not associated with Eicar and takes no responsibility for the website or test file.

Intrusion Prevention (IPS)

Why should you use Intrusion Prevention (IPS)?

One way APTs are able to infiltrate systems is through web-based attacks (for example, drive-by-download, watering hole, malicious link in an email, etc.). Intrusion Prevention, part of the Network Threat Protection component in SEP 12.1, is a key protection technology and is particularly effective at the incursion phase of an APT attack. Network Intrusion Prevention is a layer of defense that keeps known and unknown threats from ever reaching users' systems by scanning and blocking network packets that attack endpoints.

Intrusion Prevention protects against common infection vectors for enterprise and consumer endpoints, including:

- Malware post-infection system detection (System Infected)
- Base operating system threat prevention (OS Attack)
- Drive-by download and Web-attack threat prevention (Web Attack)
- Social engineering and misleading application threat prevention (Fake App Attack)
- Malicious domain, website and IP-blocking prevention (Malicious Site)

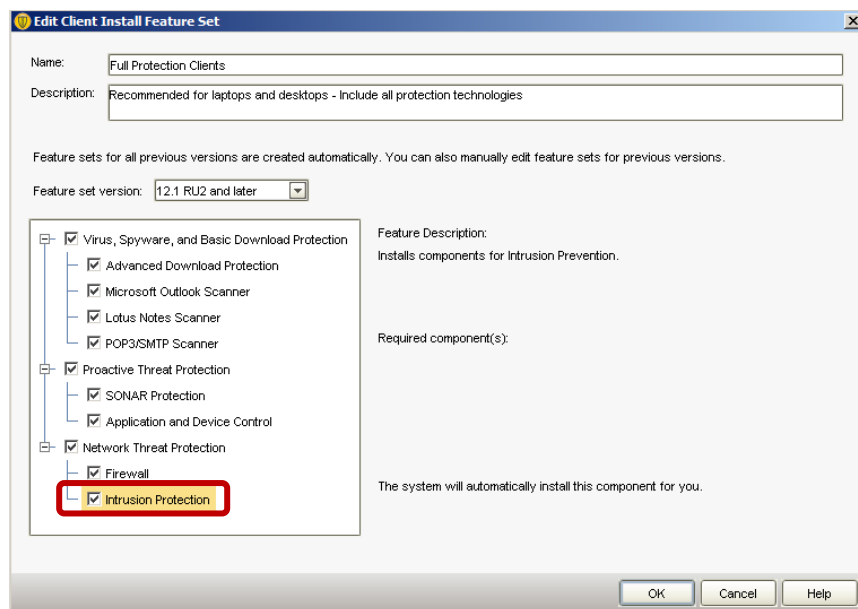
The Intrusion Prevention policy includes a subcomponent called Browser Intrusion Prevention. This component works similarly to the core IPS component, but instead of scanning network packets in the TCP/IP stack, Browser Intrusion Prevention is a browser plugin that can detect attacks that are obfuscated at the network level and then rendered by browsers (Internet Explorer and Firefox). Overall detections by Browser Intrusion Prevention are much fewer than the core IPS component, but it does add an extra layer for specific obfuscated browser attacks.

Browser Intrusion Prevention is still effective in blocking network-based attacks even with unsupported browsers like Chrome. Additionally, if Browser Intrusion Prevention is disabled, Network Intrusion Prevention, Download Insight, and SONAR are all fully functional in protecting systems.

How to implement IPS

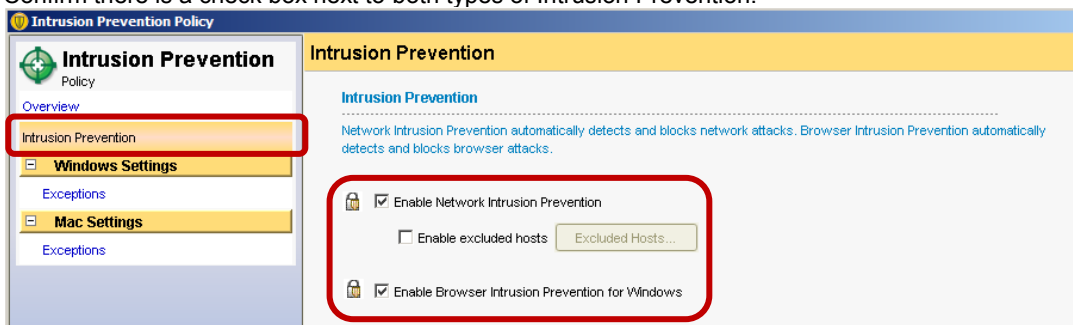
Intrusion Prevention is a key component that is installed and enabled by default. In order to confirm that you have Intrusion Prevention installed and enabled, check the following:

- 1) **Installation:** Intrusion Prevention is selected by default during installation or when creating a SEP 12.1 installation package. Make sure that the Intrusion Prevention component is not deselected when installing or creating a client installation package.



Note: In SEP 12.1 Intrusion Protection is part of Network Threat Protection. Even though the SEP Firewall is also part of Network Threat Protection, the two components can be installed independently of each other.

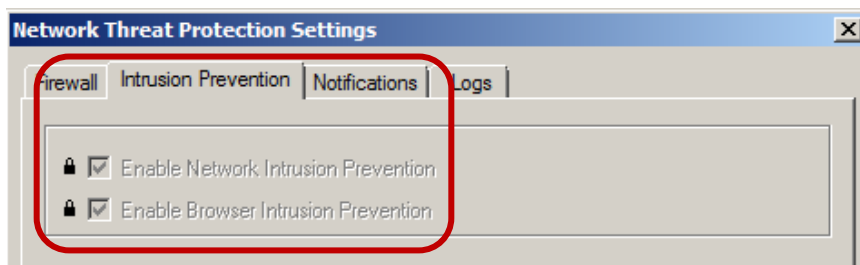
- 2) **Intrusion Prevention policy:** The Intrusion Prevention policy is enabled by default for a managed SEP client. Make sure that it is enabled. To confirm it is enabled, in the Symantec Endpoint Protection Manager, select the relevant Intrusion Prevention policy for the client group you would like to verify and select **edit the policy**. Confirm there is a check box next to both types of Intrusion Prevention:



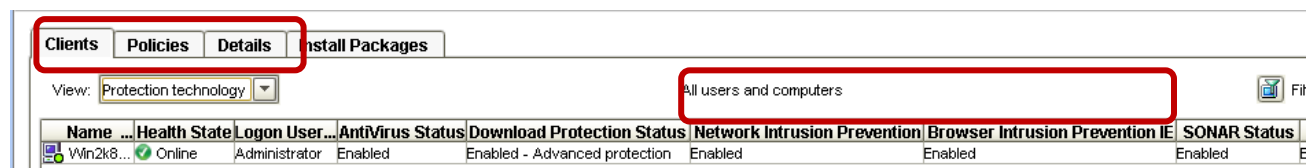
- 3) **Client User Interface:** Intrusion Prevention status can be viewed in the Network Threat Protection stripe of the client user interface as shown here. Definitions are released on as-needed, typically on a daily basis:



In order to confirm that Intrusion Prevention is enabled, click **Options** next to Network Threat Protection and select **Change Settings**. Select the **Intrusion Prevention** tab and confirm that Intrusion Prevention is selected as shown here:



- 4) **Symantec Endpoint Protection Manager:** In the console, go to the **Clients** Page and select the **Protection technology** view as shown here:



Note: The Intrusion Prevention component is an essential component for workstations/laptops users. Although Intrusion Prevention is designed to have minimal impact on network throughput and is supported on server operating systems, it is possible that Intrusion Prevention might impact performance slightly on some servers that require zero-latency network throughput. Symantec recommends installing Intrusion Prevention on servers unless performance is impacted that cannot be resolved after working with Symantec Technical Support.

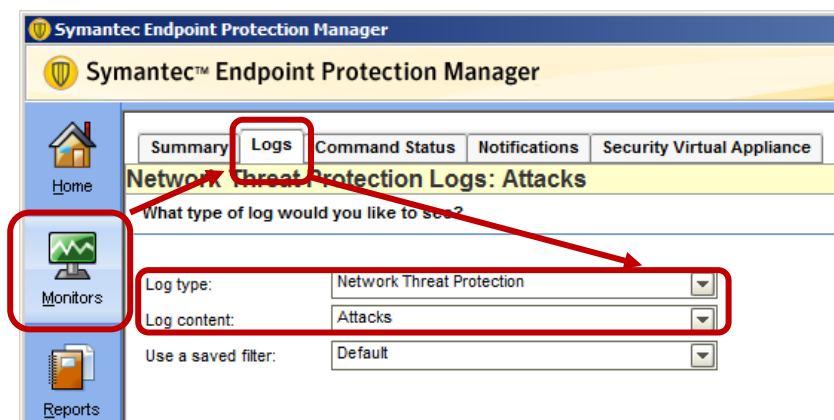
Please see the following knowledge base article for some examples of servers that are not well suited for IPS:

Best Practices for the Intrusion Prevention System component of Symantec Endpoint Protection on high-availability/high bandwidth servers:

<http://www.symantec.com/docs/TECH162135>

How to monitor Intrusion Prevention attacks

When IPS detects malicious network packets, it logs the events in the SEP 12.1 client and forwards these to the Symantec Endpoint Protection Manager. To view Intrusion Prevention events in the management console, go to **Monitors > Logs**, and then choose **Log type > Network Threat Protection** and **Log content > Attacks**. Click **View Log**.



When Intrusion Prevention detects malicious network activity, it logs each detection in one of five categories. The categories are as follows from more critical to less critical:

- **System Infected** – The attack type System Infected is the most critical Intrusion Prevention detection. This means that the system has malware running on it and it is trying to communicate from the compromised system to a C&C server or otherwise as part of a botnet. Rootkit variants, that are difficult to detect with antivirus protection, can be used in an APT attack. Common rootkit families that are detected as System Infected include the ZeroAccess and BlackHole rootkit remote access tool families.
- **OS Attack:** IPS signatures that trigger this type of attack indicate that the endpoint end-system has been protected against an attack and that the connection has been dropped. If the source address is coming from an internal IP address, this may indicate that a computer on the network is infected and is trying to propagate by exploiting vulnerabilities (such as MS RPC and LSASS.) You should check the source IP to find the potentially infected system. Threats such as W32.Downadup/Conficker, Stuxnet, and various bots spread in this manner.
- **Web Attack:** IPS signatures that trigger with a Web Attack prefix indicate that a computer on your network has been protected from a drive-by download and that the connection has been dropped.
- **Fake App Attack:** New variants of malware can succeed at the incursion phase of an attack using social engineering techniques by using misleading applications. These are continually changing with millions of variants, making detection with antivirus alone unfeasible.
- **Malicious Site:** Intrusion Prevention can block known malicious domains, websites, and IP addresses. These sites may include combinations of threats—including drive-by downloads and social-engineering attacks—and have been flagged with Symantec's domain reputation solution as hosting malicious content. An IPS alert with the "Malicious Site" prefix indicates the system blocked traffic from the malicious site and the connection was dropped.

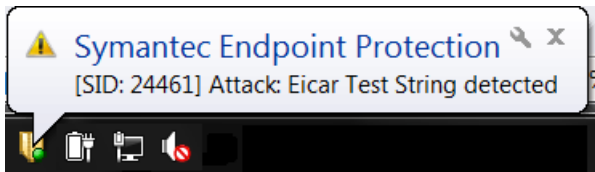
How to test Intrusion Prevention

Intrusion Prevention detection capabilities can be tested with the Eicar test file eicar.com. The Eicar test file does not contain a malicious payload, but antivirus vendors detect eicar as a way of ensuring intrusion prevention protection is in place. The Eicar test file can be downloaded from the following website:

www.eicar.org

Note: Symantec takes no responsibility for the Eicar website or test file. The link is provided solely as a convenience.

When the eicar test file is downloaded to a computer running Intrusion Prevention, the SEP client will log the detection as "Attack: Eicar Test String detected" and a message appears on the endpoint as shown in the following screenshot:



Intrusion Prevention detections have a Security ID (SID) number that can be used to find more information about a given attack on the Symantec Security Technology and Response website at the following link:

http://www.symantec.com/security_response/securityupdates/list.jsp?fid=sep&pvid=sep1213

Download Insight (Advanced Download Protection)

Why should you use Download Insight (Advanced Download Protection)?

Download Insight can block files that have never been seen before on the Internet and is particularly effective protection for stopping new targeted attacks. Download Insight checks the reputation of software files when they are introduced on a computer through typical internet activities and if files have bad or unknown reputation they can be blocked. For example:

- New software files that are downloaded by Internet Explorer, Firefox, Chrome, etc. Download Insight checks both user-downloaded files and drive-by downloads (not initiated by the user).
- File attachments in emails when users save and/or launch these files from their email readers
- Files sent through instant messaging applications before users can save and launch these files on their computers
- Files downloaded by popular file-sharing programs before users can save and launch these files on their computers

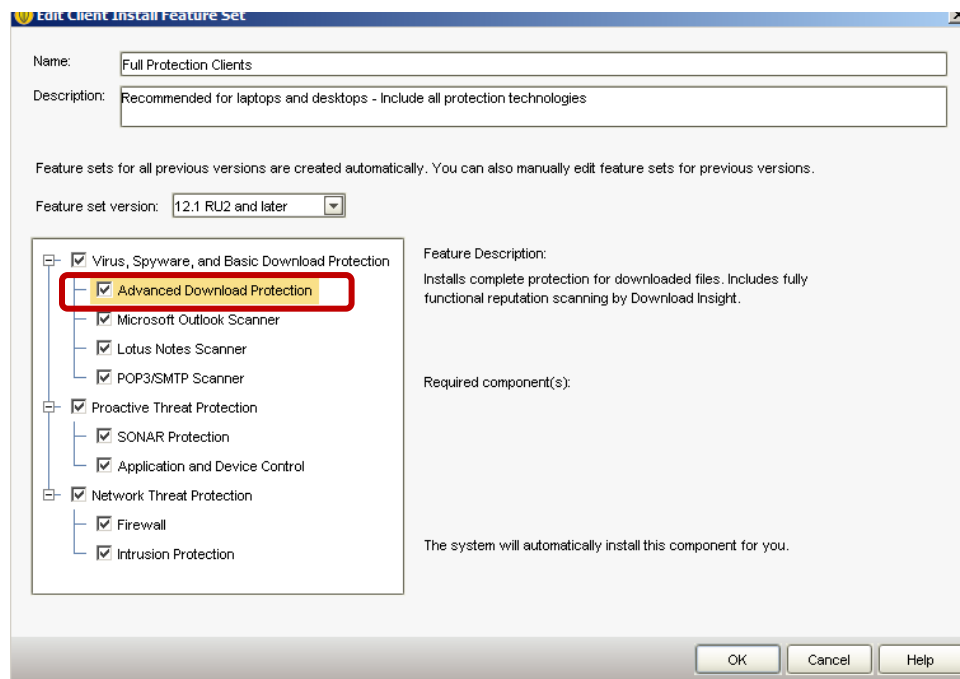
Download Insight does not check other software on protected computers, such as actively running applications that are already installed and running. It only checks new software at the time it is introduced to a computer (e.g., downloaded). The goal is to block a high percentage of new malware before it ever has a chance to run, with minimal false positive implications.

Since Download Insight is configured in the Virus and Spyware Protection policy, it can be applied to an entire enterprise or multiple policies can be assigned to different corporate divisions if different divisions have different risk tolerances.

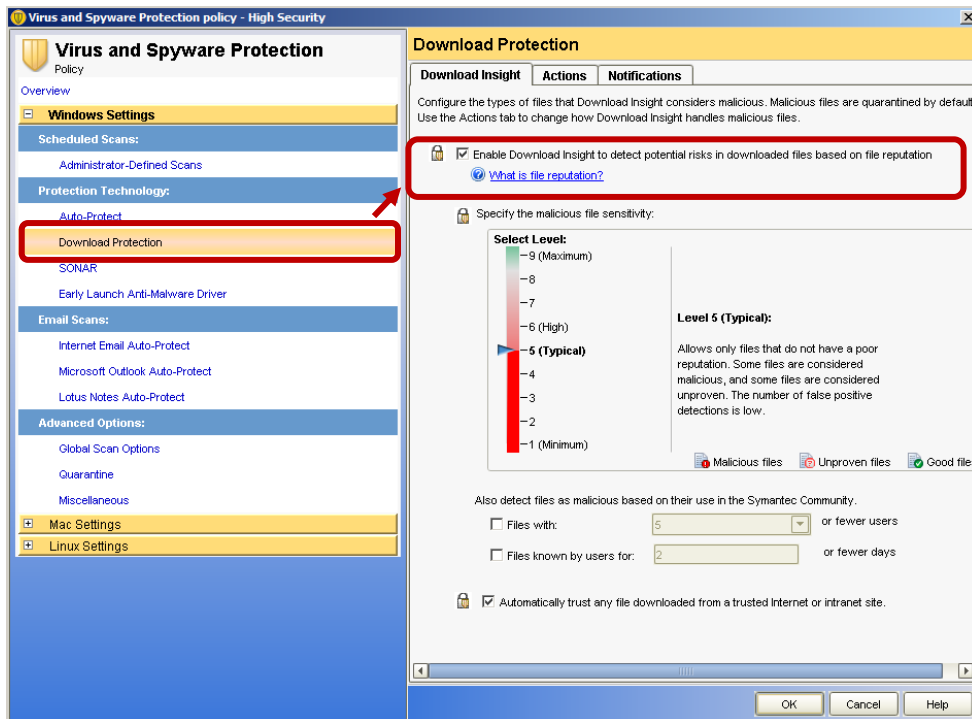
How to implement Download Insight

Download Insight is installed by default and enabled by default in the Virus and Spyware Protection policy. In order to confirm that you have Download Insight installed and enabled confirm the following:

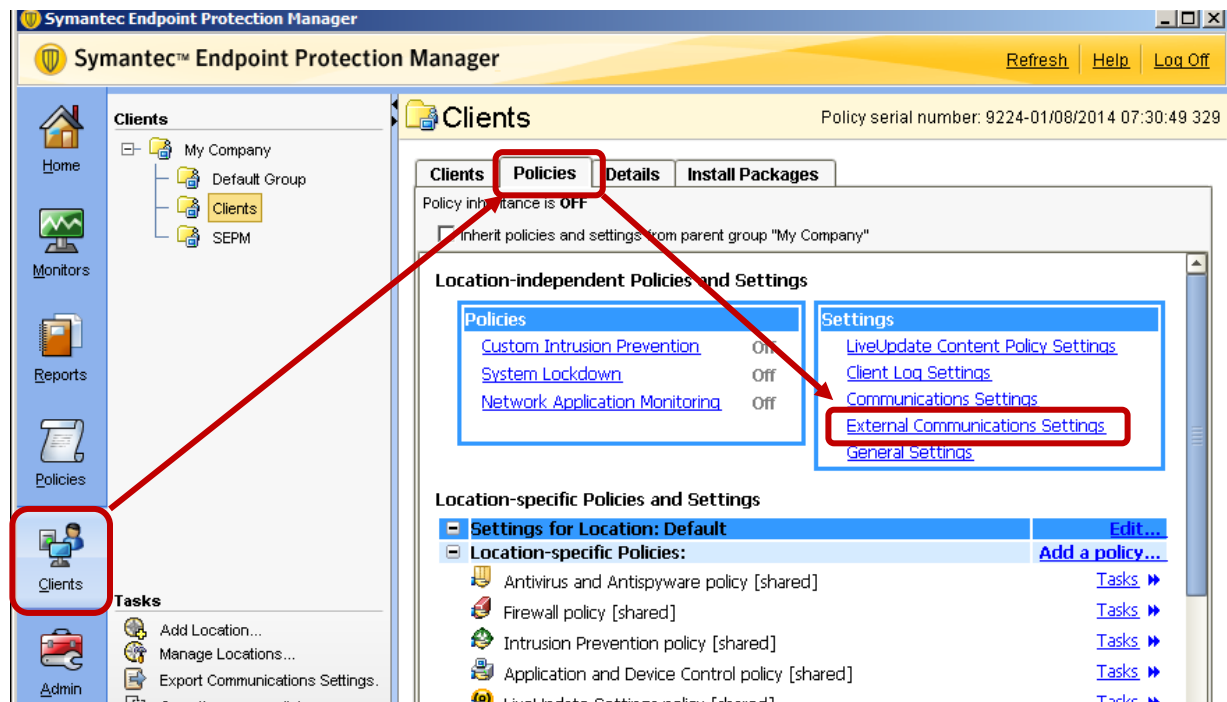
- 1) **Installation:** Download Insight (Advanced Download Protection) is selected by default during installation or when creating a SEP 12.1 installation package. Confirm that the Download Insight (Advanced Download Protection) is selected when installing or creating a client installation package.



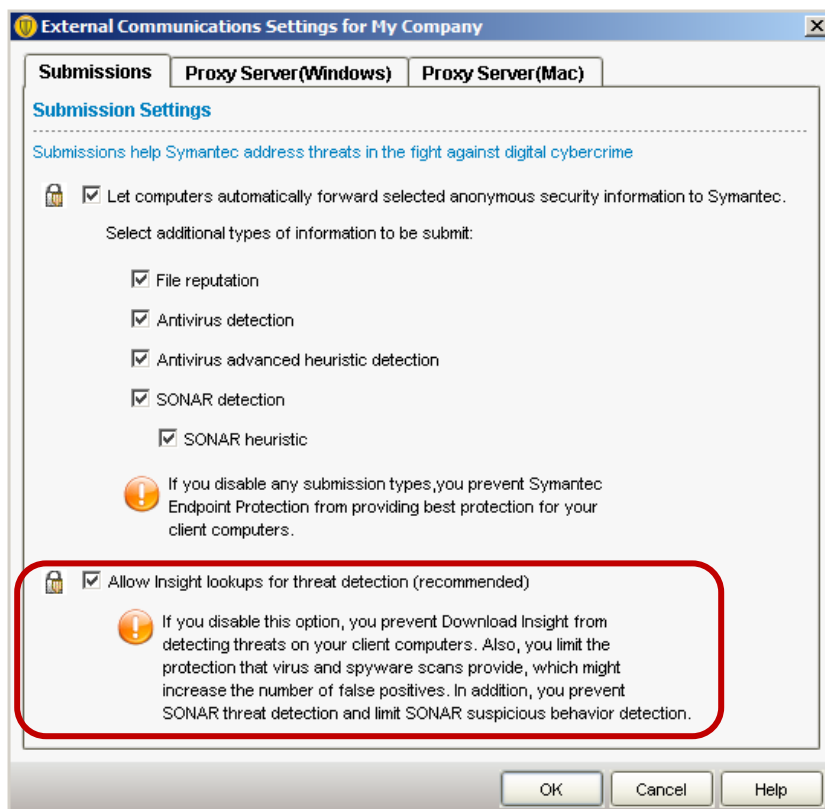
- 2) **Download Insight (Advanced Download Protection) policy:** Download Insight (Advanced Download Protection) is enabled by default for a managed SEP client. To confirm it is enabled, in the Symantec Endpoint Protection Manager, select the relevant Virus and Spyware Protection policy for the client group you would like to verify and select **edit policy**. Select **Download Protection** and confirm that Download Insight is enabled as shown here:



Important! In addition to enabling Download Insight in the Virus and Spyware Protection policy, Insight lookups must be enabled as shown here (enabled by default). Go to the **Clients** page and select the **Policies** tab in each group where Insight should be enabled. Select **External Communications Settings**.



In the **External Communications Settings** dialog box, make sure that **Allow Insight Lookups for threat detection** is enabled. The option is enabled by default.



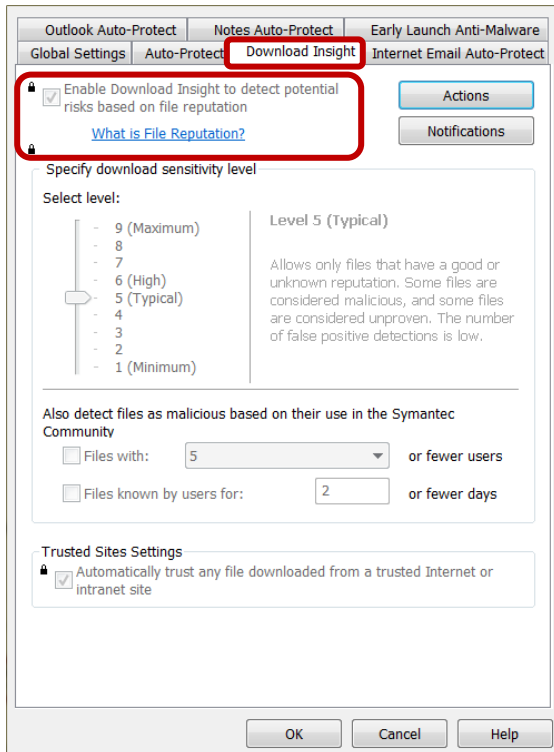
Note that Download Insight requires access to the URLs listed below in order to do a successful lookup on Symantec's Insight database and receive a response about a file's trustworthiness. Make sure that the SEP clients have access to the following URLs:

<https://ent-shasta-mr-clean.symantec.com>

<https://ent-shasta-rrs.symantec.com>

Enabling all submissions types helps provide best protection for SEP clients. At a minimum the highlighted checkbox above must be checked for Download Insight to be able to query the reputation of a given file.

- 3) **Client User Interface:** In the Client UI, in the **Virus and Spyware Protection Settings** dialog box, select the **Download Insight** tab to confirm that Download Insight is enabled as shown here:



- 4) **Symantec Endpoint Protection Manager:** In the management console, on the **Clients** Page select the **Protection technology** view as shown here:

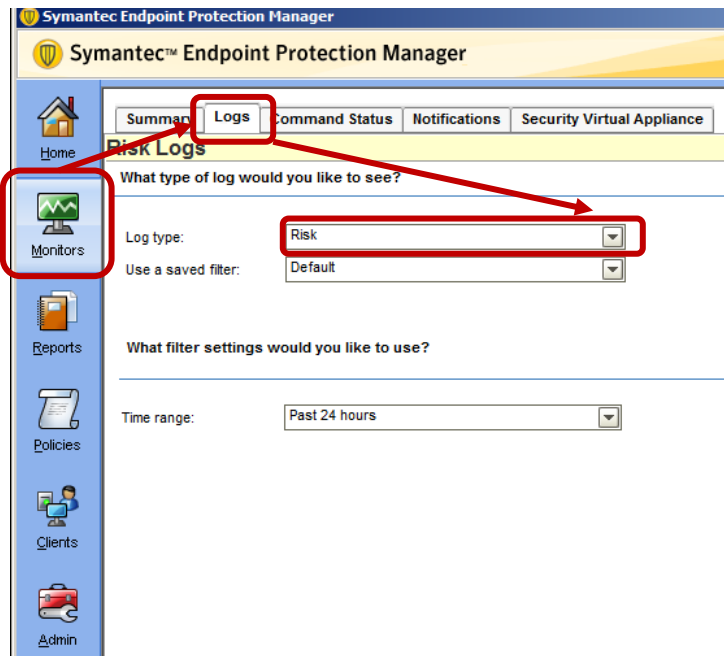


In order to do a successful lookup, SEP 12.1 clients must have Internet access as described in step 2. If a client does not have Internet access, Download Insight will not make detections.

Default configuration settings should provide appropriate protection for malware used by APTs, which tend to be new variants that have not been seen by many users.

How to monitor Download Insight for malicious activity

When Download Insight detects suspicious or unknown files, it logs the events on the SEP 12.1 client, which forwards them to the management console. To view Download Insight events in the management console, go to **Monitors > Logs**, then choose **Log type > Risk** and click **View Log**. Look for events that refer to detections with "reputation" in the threat name.



How to test that Download Insight Protection is functioning

Download Insight can be tested by downloading the test file, **cloudcar.exe**, or by downloading a self-extracting executable that you create.

Cloudcar.exe will be detected as a file with a known bad reputation even though the file itself is not malicious. It can be accessed on the amtso.com website.

<http://www.amtso.org/feature-settings-check-cloud-lookup.html>

A newly created self-extracting executable can also be used to test Download Insight. Creating a self-extracting executable essentially creates an executable that has not yet been seen on the Internet. Download Insight will block and prompt to warn that the file is unproven. This illustrates how effective Download Insight is for detecting and preventing unknown executable files from being saved or run on a user's computer.

Download Insight requires access to the URLs listed below in order to do a successful lookup on Symantec's Insight database and receive a response about the file's trustworthiness. When testing Download Insight, make sure the SEP clients have access to the following URLs:

<https://ent-shasta-mr-clean.symantec.com>

<https://ent-shasta-rrs.symantec.com>

Note: if clients cannot connect to the above URLs based on their default proxy settings as defined in Internet Explorer, you must configure the appropriate settings in the clients communications settings in the Symantec Endpoint Protection Manager. See the following Knowledge Base article for information how to configure proxy settings:

Specifying a proxy server for client submissions and other external communications

<http://www.symantec.com/docs/HOWTO55363>

Download Insight is designed to provide protection against the top attack vector for new and unknown malicious files, namely files that are downloaded to a client system by “portal” applications. Portal applications include browsers, FTP clients, chat clients, mail clients, etc.

Note that Download Insight will NOT do a lookup on the following files:

- 1) Files accessed on the local file system or on network shares.
- 2) Files scanned by a manual or scheduled scan (including when right-clicking a file and selecting Scan Now).
- 3) Files that are not executable (e.g. pdf, docx, etc.)
- 4) Files scanned by doscan.exe
- 5) Malware delivered via vulnerability exploit

For more information about Download Insight please see the following Knowledge Base article:

Managing Download Insight Detections:

<http://www.symantec.com/docs/HOWTO55252>

SONAR

Why should you use SONAR?

SONAR technology detects threats based on their behaviors, with no reliance on file signatures. It is effective even against brand-new variants of sophisticated malware such as Duqu, StuxNet and Hydraq/Aurora, and malware-embedding rootkits from sources like TidServ and ZeroAccess. To minimize performance impacts on the system, rules of suspect behaviors are created using exhaustive machine and human analysis, and distributed via LiveUpdate.

SONAR combines the following features:

- Real-time behavioral monitoring of all processes running on a computer
- Exhaustive automated and human classification of behaviors
- Removal or blocking, depending on threat behavior and likely system impact

As real-time behavior-based protection, SONAR monitors the behaviors of processes as they run, for example, attempts to change a browser home page, install a browser toolbar, monitor keystrokes, and almost 1,400 others. It puts each behavior in full context by also considering the following factors:

- Origin—was the original file downloaded from a trusted site, copied from a network share, installed from portable media, etc.?
- Contents—was the original file encrypted and “packed” and disguised using high-entropy encryption? What Windows functions does it import? Was the code compiled using a commercial solution or one of the low-end, non-mainstream compilers hackers favor?
- Relationships—has the process created any executables that were identified as malicious?
- Behavior sequences—Is the process part of a behavior sequence that identifies threat families for example members of the “PC Scout” fake antivirus software family, all of which launch from the Temp folder, write “AVE” to the Windows Registry, create a “hostinfo.txt” file, and modify the Browser Home Page, in that order.

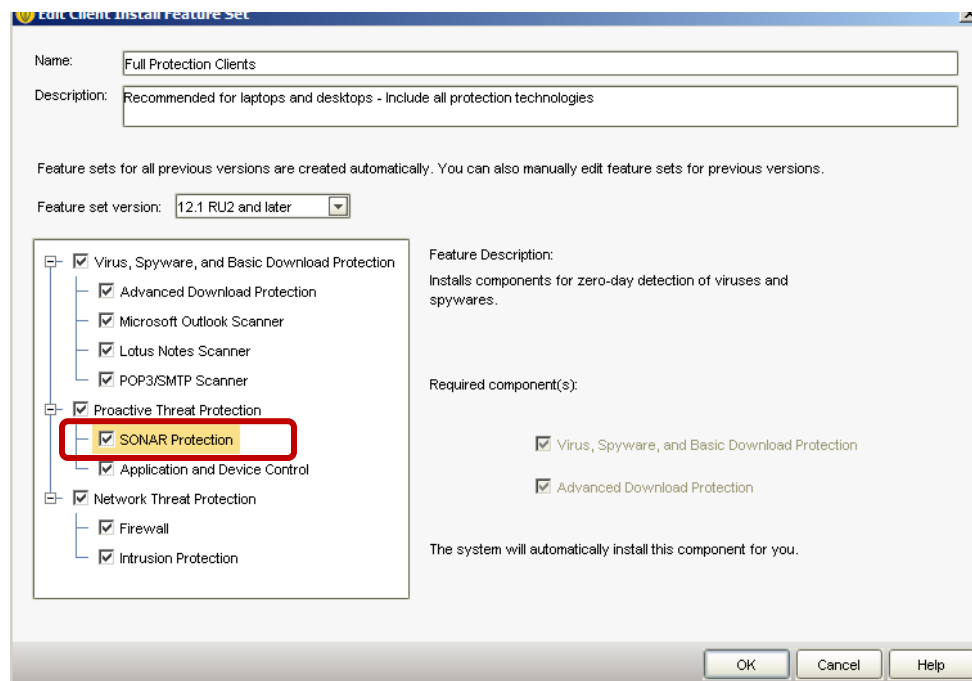
Human classification improves response time because it is faster to test, analyze, and release rules family-by-family than instance-by-instance. It also reduces false positives since each rule is backed not only by a greater volume of evidence, but by the know-how and experience of seasoned Symantec security professionals.

Incidental characteristics like signatures, packing, and even reputation all help streamline identification and removal of malware—but process behaviors define it. Because SONAR monitors and blocks process behaviors in real time, it provides a final line of defense against threats to endpoints. Because SONAR classification rules monitor behavior in real time, SONAR is immune to obfuscation techniques used to evade traditional signature-based scanning.

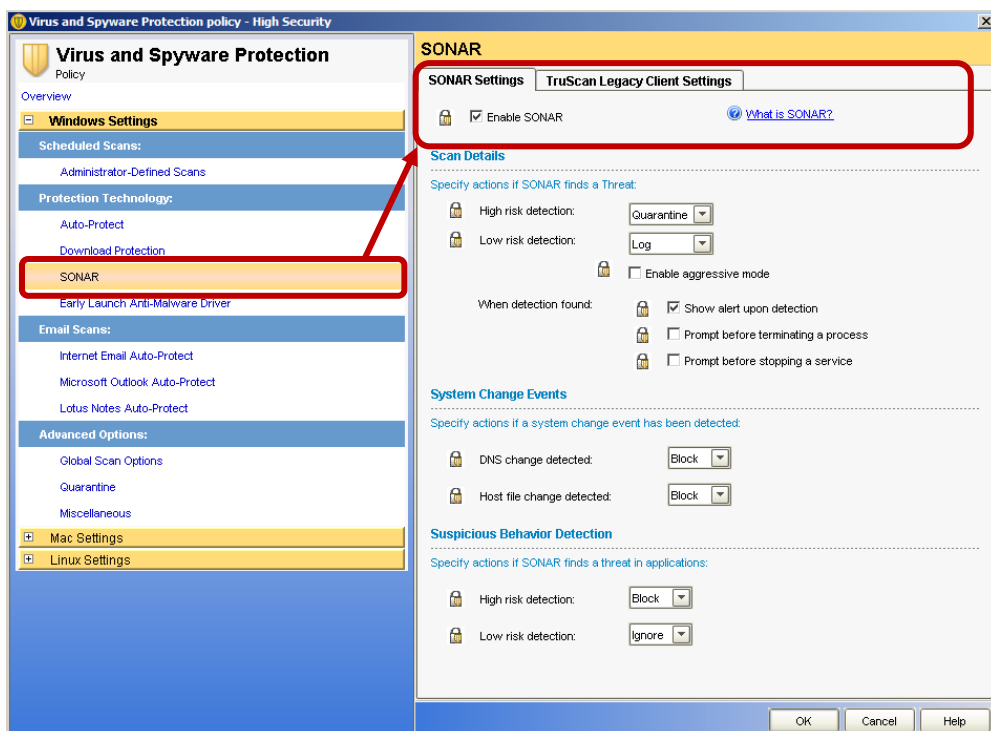
How to implement SONAR

SONAR is installed by default. It is enabled by default in the Virus and Spyware Protection policy. In order to confirm that you have SONAR installed and enabled confirm the following:

- 1) **Installation:** SONAR is selected by default during installation or when creating a SEP 12.1 installation package. Confirm that SONAR is selected in the client install feature set when installing or creating a client installation package.

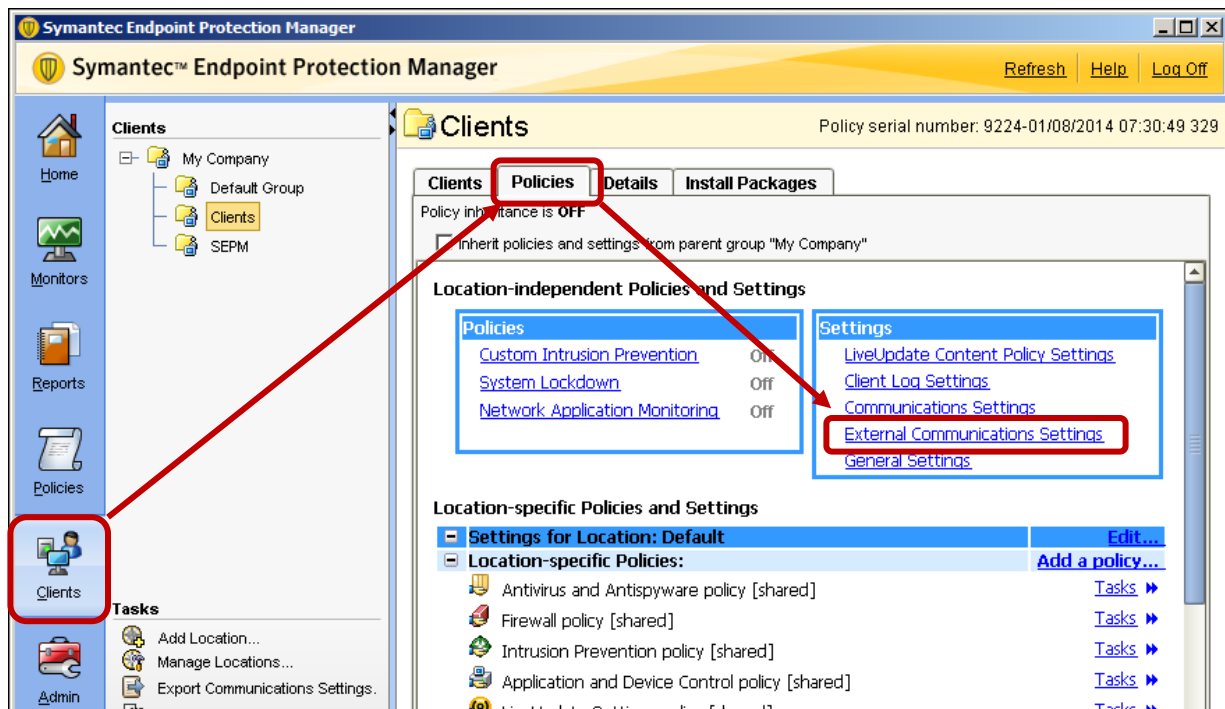


- 2) **SONAR policy:** SONAR is enabled by default for a managed SEP client. Make sure it is enabled in the Symantec Endpoint Protection Manager. To confirm it is enabled, in the Symantec Endpoint Protection Manager, select the relevant Virus and Spyware Protection policy for the client group you would like to verify and select **edit the policy**. Select **SONAR** and confirm there is a check box next to **Enable SONAR** as shown here:

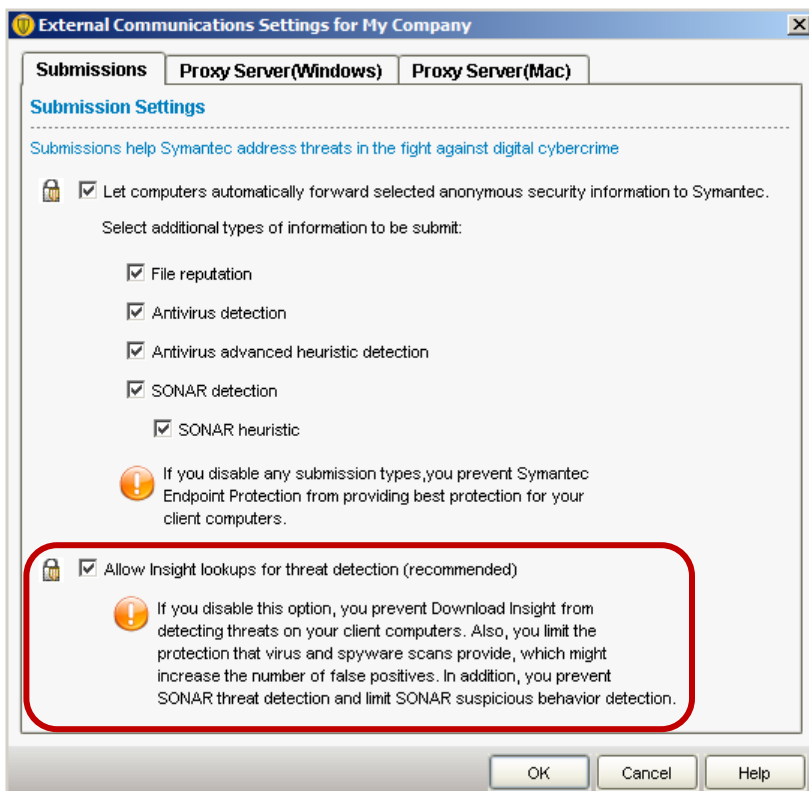


The default settings provide strong protection for unknown threats and should detect malicious files based on behavior. The **Enable Aggressive Mode** option may increase the conviction rate of files considered low risk, but may also increase false positives. In case of false positives see the chapter below regarding False Positive Mitigation.

Important! In addition to enabling SONAR in the Virus and Spyware Protection policy, Insight lookups must be enabled as described in the Download Insight section of this document. Go to the **Clients** page and select the **Policies** tab in each group that should have SONAR enabled. Select **External Communications Settings** as shown here:



In the **External Communications Settings** dialog box, make sure that **Allow Insight Lookups for threat detection** is selected. This option is selected by default.



Important! Like Download Insight, SONAR requires access to the below listed URLs in order to do a successful lookup on Symantec's Insight database and receive a response about the file's trustworthiness.

<https://ent-shasta-mr-clean.symantec.com>

<https://ent-shasta-rrs.symantec.com>

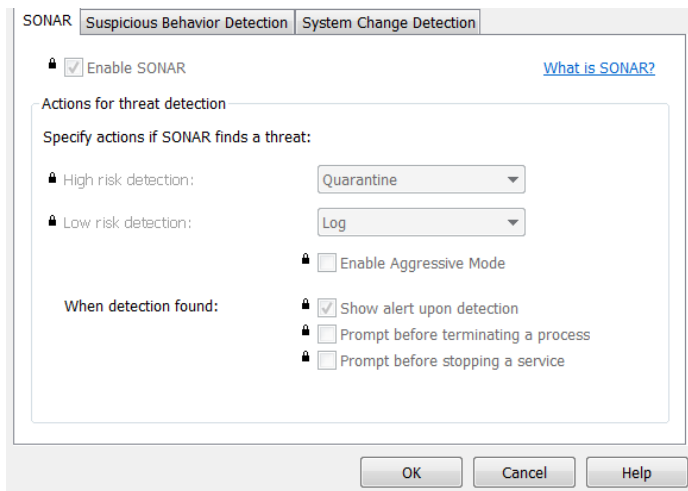
Since SONAR requires access to the same URLs as Download Insight, testing Download Insight can help you verify that SONAR has the appropriate Internet access to correctly detect and convict malware. Enabling additional submissions helps provide the best protection for SEP clients.

- 3) **Client User Interface:** SONAR status appears in the Proactive Threat Protection status of the client user interface as shown here. Definitions for SONAR refer to the human-authored rules for malicious sequences of behaviors, and updates occur on a less frequent basis than virus protection and IPS.

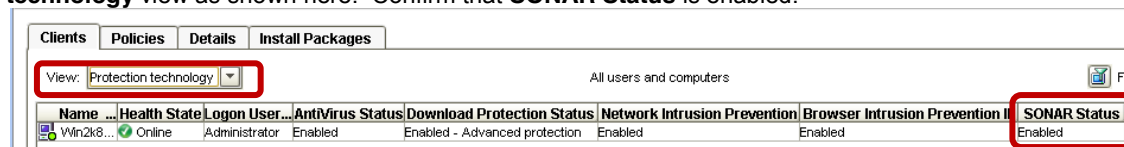


Note: SONAR does not use signatures to identify malware the way traditional antivirus scanning does. However, SONAR does use human-authored rules that allow SONAR to monitor applications for known malicious behavior sequences as with the "PC Scout" fake AV family described earlier.

SONAR configuration settings can be confirmed in the client user interface by clicking **Options** next to Proactive Threat Protection and selecting **Change Settings**. Confirm that SONAR is enabled as shown here:



- 5) **Symantec Endpoint Protection Manager:** In the console, go to the **Clients** page and select the **Protection technology** view as shown here. Confirm that **SONAR Status** is enabled.



The default settings should be appropriate for detecting an Advanced Persistent Threat. However, you can enable aggressive mode to increase SONAR's sensitivity to detecting suspicious activity. Note that enabling aggressive mode can also increase the chance of a false positive. See the chapter on mitigating false positives for more information.

In addition to SONAR-specific configurations, submissions are an important way that Symantec is able to tune SONAR technologies for maximum accuracy.

How to monitor SONAR for malicious activity

When SONAR detects suspicious or unknown files it logs the events in the SEP 12.1 client and forwards these to the Symantec Endpoint Protection Manager. To view SONAR events in the management console, select **Monitors > Logs**, then choose **Log Type > SONAR**, and click **View Log**.



How to test that SONAR is functioning?

SONAR detects malicious files that have been executed in real time based on the files behavior when executed. Running an antivirus scan on a file will not trigger a SONAR detection.

SONAR can be tested by executing the test file, **socar.exe**. The file can be downloaded from the following Knowledge Base article:

<http://www.symantec.com/business/support/index?page=content&id=TECH216647>

Note that the SONAR must be able to make an Insight lookup to get the full benefit of SONAR's protection. If the SEP client is unable to query Insight, SONAR will not convict in order to prevent false positives.

To ensure Insight lookups function correctly, make sure the SEP clients have access to the following URLs:

<https://ent-shasta-mr-clean.symantec.com>

<https://ent-shasta-rrs.symantec.com>

Rule-based policy options for additional protection

In addition to the protection technologies discussed above, SEP 12.1 provides additional protection technologies that can help prevent new and unknown malware from compromising the computers in your network. These are primarily rule-based technologies that are installed by default but must be enabled and configured to take effect.

These protection technologies include:

- Application Control
- Application Learning
- System Lockdown
- Host Integrity (part of the Symantec Protection Suite)

Application Control

Why should you use Application Control?

In addition to signature or Symantec-defined rule-based protection, administrators can also choose to add more protection to their endpoints by creating protection rules that they define themselves. These rules can range from the simple task of blocking access to autorun.inf files on all removable devices, to the more complicated tasks of preventing browser helper objects from being registered, or making USB devices read only in a specific location.

By default, the Application and Device Control policy contains a number of example rules, all of which could be turned on and tuned very easily if required. For example:

- Block applications from running
- Block programs from running from removable drives
- Make all removable drives read-only
- Block writing to USB drives
- Log files written to USB drives
- Block modifications to hosts file
- Block access to scripts
- Stop software installers
- Block access to Autorun.inf
- Block Password Reset Tool
- Block File Shares
- Prevent changes to Windows shell load points
- Prevent changes to system using Internet Explorer or Firefox
- Prevent modification of system files
- Prevent registration of new Browser Helper Objects
- Prevent registration of new Toolbars

The application control technology in Symantec Endpoint Protection is capable of controlling registry, file and folder access, launching and termination of processes, and attempts to load DLLs. Advanced rules can be written to control any combination of these activities. Any attempted change can be allowed or prevented with full logging and monitoring capabilities should the administrator want to know what a process is doing on the endpoint.

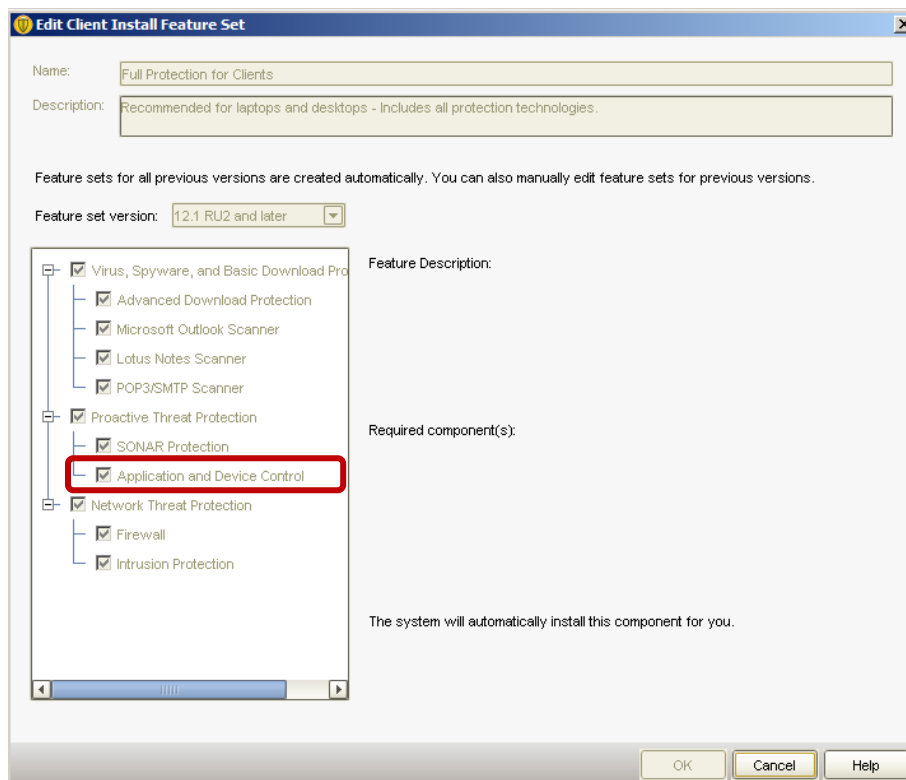
One very powerful component of application control is its ability to control applications by their hash. This ability allows you to create rules to blacklist or block applications that may be malicious but are not yet contained in an antivirus definition set, or have been submitted to Symantec for further analysis. To control applications by their hash, you use the built-in **Block applications from running** rule.

Application Control offers advanced protection capability and can be very powerful in preventing access to files, registry keys, and processes depending on the configuration. Because of this it is important to test policies before activating them to monitor for unexpected behavior. Application Control policies have a test and production mode to make it easier for administrators to monitor events where application control rules are triggered.

How to implement Application Control

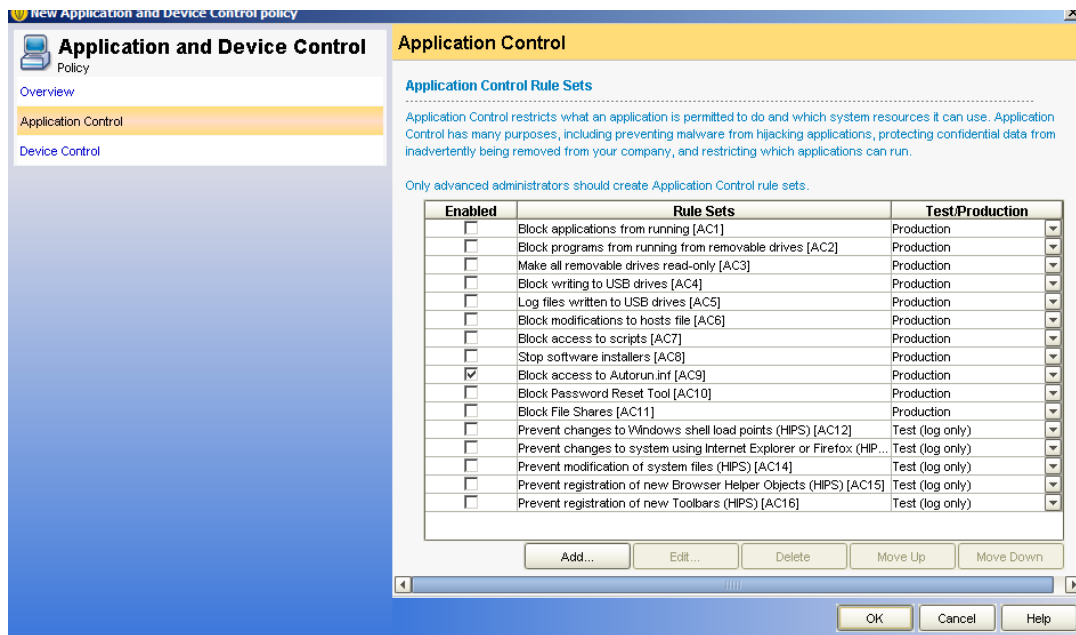
In order to make sure that application control is installed and enabled, follow the steps here:

- 1) **Installation:** Application Control is selected by default during installation or when creating a SEP 12.1 installation package. Ensure that the **Application and Device Control** checkbox is selected when installing or creating a client installation package.



- 2) Application Control is configured in the Application and Device Control policy. By default, application control is enabled and blocks **autorun.inf** files on all removable devices. Administrators can choose to edit the existing policy or create a new one if they wish to do so. Application control rules are best written with the focus on preventing unwanted behavior rather than addressing known malicious behavior, which requires knowledge of a threat.

The screenshot below shows the built-in Application Control rules:



In order to provide improved protection against the downloading and execution of advanced threats, it is recommended that customers enable the following rules in the default application control policy:

- Block modifications to hosts file (this can also be implemented using SONAR)
- Block access to scripts (if scripts are used for administration, you can create an exception folder in the policy and execute admin scripts from here)
- Block access to Autorun.inf
- Prevent changes to Windows shell load points
- Prevent changes to system using Internet Explorer or Firefox
- Prevent modification of system files
- Prevent registration of new Browser Helper Objects
- Prevent registration of new Toolbars

Note: The screenshot shows the default SEP 12.1 RU4 Application Control policy. Previous versions of SEP 12.1 have fewer built-in rules.

How to monitor Application Control for activity

Application control can be monitored from both the SEP client interface and also from the Symantec Endpoint Protection Manager. In the management console, to see all the events select **Monitors > Logs**, and then choose **Log Type > Application and Device Control** and **Log content > Application Control**. Click **View Log**.

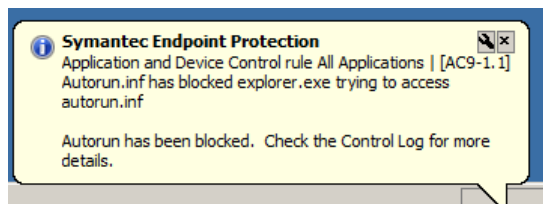


In advanced filtering options, you can then choose from a number of different criteria to narrow your search. Additional filters include Severity, whether a rule was triggered in test mode, Event Type, and Action. Events are not necessarily a sign of malicious activity, but it is more than possible malicious processes will be blocked by these rules.

In the client interface, go to **View Logs**, then next to **Client Management**, click **View Logs** and select the **Control Log** to view all the application control events.

How to test that application control is functioning

If a default Application and Device Control policy is applied to an endpoint, you can test its functionality by creating or copying a file called **autorun.inf** to removable storage. The file can be empty. Application control is only looking for the name. You should then receive a client notification and the file will be blocked. This event will be forwarded to the Symantec Endpoint Protection Manager and can be viewed there as well.



Application Learning

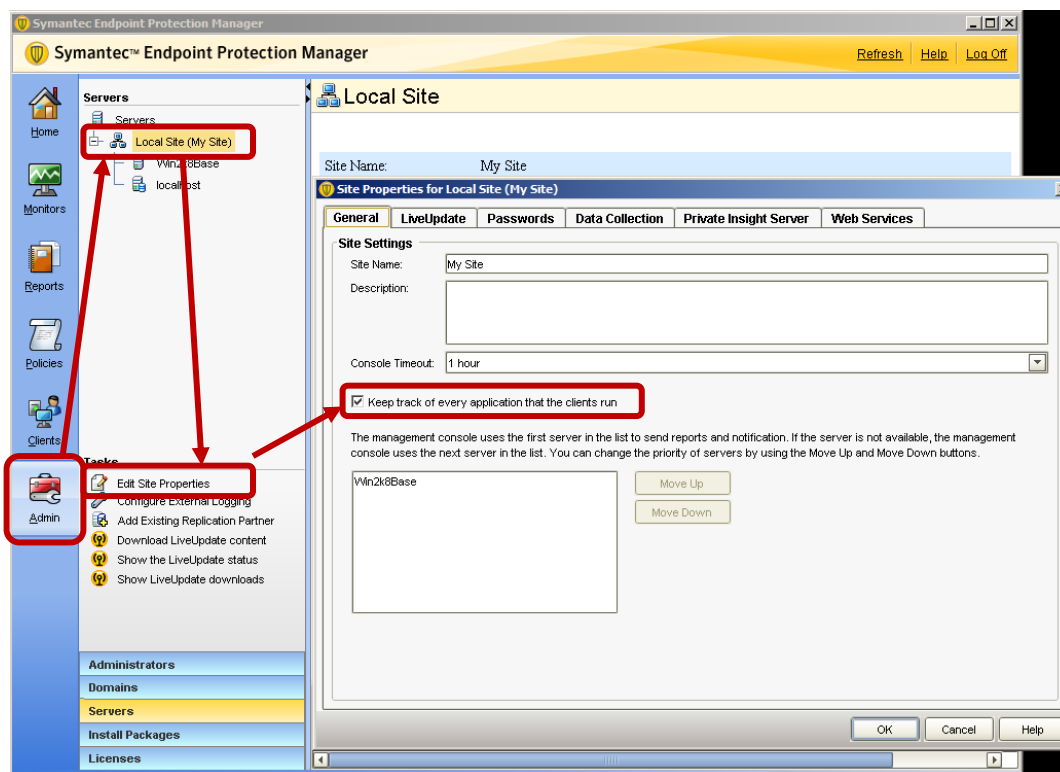
Why should you use Application Learning?

Application learning allows an administrator to understand what applications are launching within their environment. APTs are designed to be “low and slow” and undetectable. In some situations, threats are discovered that may have been present and dormant on customer’s networks for many months. Application learning allows you to quickly find out whether you have these applications on your endpoints or not, and then deal with them accordingly. Application learning collects application data from any enabled endpoint. The administrator can then search on the hash of the application, its executable name, publisher, etc., and see which clients have the code present. Once this is known, other protection technologies can be used to remove or quarantine the files as desired.

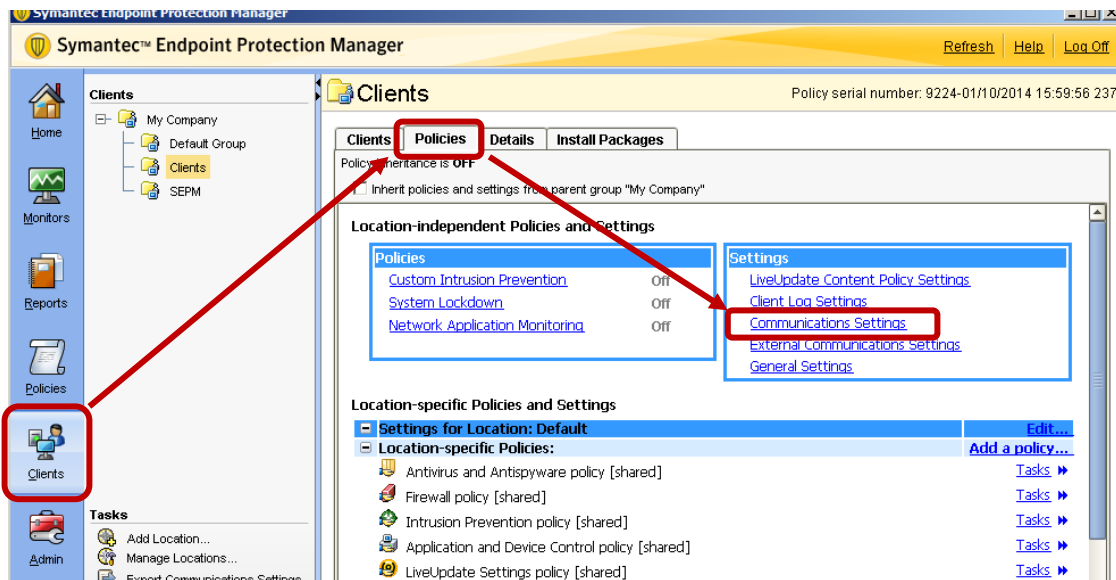
How to implement Application Learning

Application learning can be controlled from the Symantec Endpoint Protection Manager. By default, the feature is disabled globally and administrators need to make sure they enable it at both the site level and also the individual group level.

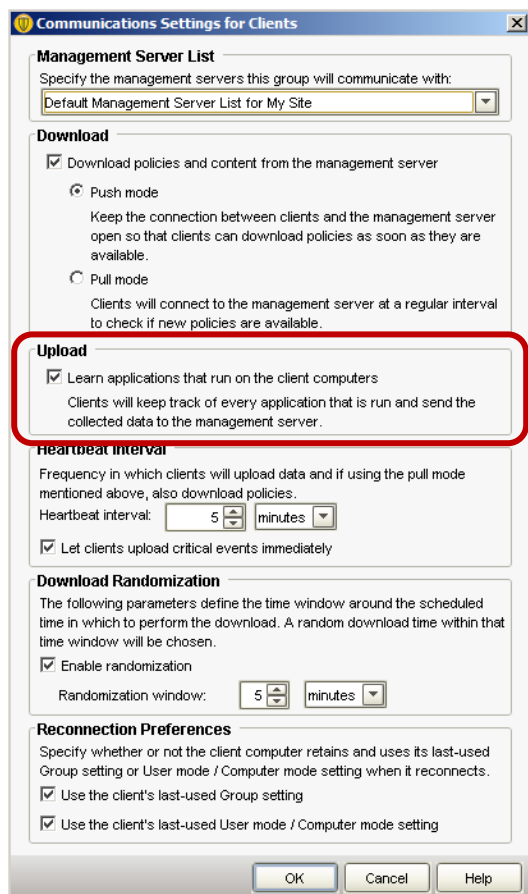
To enable application learning at the SEP site level, in the console, go to **Admin > Servers > Local Site > Edit Site Properties** and make sure the option **Keep track of every application that the clients run** is enabled. This option is enabled by default, but it should be confirmed as shown in the screenshot here:



Once the site is enabled for application learning, you can then choose to selectively enable the function on a per group setting. In each group you want to enable application learning, select the group, and then on the **Policies** tab within the group panel, choose **Communications Settings** as shown here:



Enable the option **Learn applications that run on the client computers** as shown here (this is not enabled by default):



Important note: Application learning requires more storage space in the SEP database. You should plan for this and should consider only enabling it for certain locations or areas of the business. Due to their nature, the application learning tables are not purged, and will grow quite quickly after the feature is initially enabled. See the following knowledge base article for some best practices when enabling application learning:

<http://www.symantec.com/docs/TECH134367>

How to monitor Application Learning for malicious activity

The application learning data can be searched by hash and a variety of different application characteristics, such as application path, name, size, etc. Applications that don't have a version, description, or recent modified date might warrant further analysis.

How to test that Application Learning is functioning

Once application learning is enabled, you should wait for at least two heartbeat cycles. From that point onwards, you will see all learned applications. On the **Policies** page, under **Tasks**, click **Search for Applications** as shown here:



In the **Search for Applications** dialog box, search the entire group structure with selected criteria. In the screenshot here, no search criteria returns a list of all applications that have been seen within the environment to date.

Search for Applications

Query

You can search for information about an application that clients in a specified group run. You can search for applications based on a specific computer or a specific application.

Search for applications in:

My Company

Browse...

☒ Search subgroups

Search Criteria:

☒ Based on client/computer information

☐ Based on applications

Search Field	Comparison Operator	Value
--------------	---------------------	-------

Search

Stop

Query Results

Export...

Clear All

Page 1 of 2

< Previous

Next >

Name	Path	Description	Version	Size	Last Modified Time
cmd.exe	c:\windows\system32\	Windows Command Processor	5.1.2600.5512 (xpsp.080413-2111)	389120	April 14, 2008 2:12:14 AM CEST
ieexplore.exe	c:\program files\internet explorer\	Internet Explorer	7.00.6000.16791 (vista_gdr.081217-16...	634024	December 19, 2008 6:25:25 AM CE
ping.exe	c:\windows\system32\	TCP/IP Ping Command	5.1.2600.5512 (xpsp.080413-0852)	17920	April 14, 2008 2:12:31 AM CEST
notepad.exe	c:\windows\system32\	Notepad	5.1.2600.5512 (xpsp.080413-2105)	69120	April 14, 2008 2:12:29 AM CEST
infectedprompt.exe	c:\documents and settings\symcuser\...	Self-Extracting Custom Command Laun...	1.2.3.926 RELEASE	86333	January 9, 2014 4:36:43 PM CET
savui.exe	c:\program files\symantec\symantec e...	Symantec Endpoint Protection	12.1.2015.2015	200656	November 3, 2012 7:22:24 AM CET
sonar_test[1].exe	c:\documents and settings\symcuser\...			1508687	January 10, 2014 10:17:04 AM CE
cloudcar.exe	c:\temp\			7178	June 22, 2011 9:43:22 PM CEST

View Details

Close

Help

System Lockdown

Why should you use System Lockdown?

System Lockdown is a powerful technology that allows advanced administrators to have full control over what applications can and cannot launch in their environment. By taking a trusted image and check-summing every portable executable within it, SEP can then be configured to allow only those trusted processes to launch on an endpoint.

System Lockdown is best used in environments where the client platform changes rarely, or changes in a controlled environment. It is ideal for virtual desktop environments, or systems that are rarely updated or are disconnected from the Internet and unable to update themselves. System Lockdown is not intended for environments where legitimate applications and patches need to be updated regularly, as System Lockdown will block new applications that are not included in the list of trusted applications.

System Lockdown can be configured either in whitelisting mode, where all the checksums in the list are trusted or in blacklisting mode, where all the checksums in the list are blocked. Blacklisting mode is typically used with government-provided application block lists where CERTs provide lists of known bad files and their checksums.

How to implement System Lockdown

Implementing System Lockdown is a four-step process:

1. Make sure that the SEP client has Application and Device Control installed.
2. Checksum a gold image or client that you want to lock down.
 - a. The SEP client installation folder contains the checksum.exe application, which can be used to create the file list and their respective checksums.
3. Upload the checksum list to the Symantec Endpoint Protection Manager.
 - a. Lists are added in the console on the **Policies** tab, under **Policy Components > File Fingerprint Lists**.
4. Enable System Lockdown on the groups where you need it.
 - a. On the **Clients** page, select the group. On the **Policies** tab, click **System Lockdown**.
 - b. Choose to enable System Lockdown.
 - c. Choose an application list.

How to monitor System Lockdown for malicious activity

Similar to Application Control, System Lockdown does not specifically block malicious activity, rather it blocks any application that you have not deemed as trusted and which may or may not be malicious. System Lockdown can be monitored on the client in the Control Log and in the Symantec Endpoint Protection Manager on the **Monitors** page in the Application Control Log view.

How to test that System Lockdown is functioning

System Lockdown can be tested by trying to execute any application that is not in the trusted application list. The user will receive a Windows error message and the SEP client will log a blocked entry in the Control Log.

For more information about System Lockdown, see the following knowledge base article:

Configuring System Lockdown

<http://www.symantec.com/docs/HQWT055130>

False Positive Mitigation

Preventing False Positives

SEP 12.1 will not detect known good files as malware. There are several ways to make sure that your good files are known as “good.” The following steps will help prevent false positives when using SEP 12.1.

Step 1 – Use Digital Signatures

One of the easiest ways to identify that a file is good is to know where it came from and who created it. An important factor in building confidence in a file being good is to check its digital signature. Executable files without a digital signature have a higher chance of being identified as unknown or low-reputation.

- Custom or home-grown applications should be digitally signed with Class 3 digital certificates.
- Customers should insist that their software vendors digitally sign their applications.

Step 2 - Add to the Symantec Whitelist

Symantec has a growing whitelist of over 25 million good files. These files are used in testing signatures before they are published. Their hash values are also stored online and used to avoid false positives on the SEP client by using real-time cloud lookups whenever a file is detected by any of our client security technologies (for example, SONAR behavioral technology, a fingerprint, etc.). This whitelist is a powerful tool for avoiding false positives. Customers and vendors can add files to this list.

Software vendors can request that their executable be added to the Symantec whitelist at the following link:

<https://submit.symantec.com/whitelist/>

Step 3 - Test

The initial deployment of SEP 12.1 during a pilot should include test machines with representative images of the software that you run in your environment, including common third-party applications. You should monitor for potential issues during piloting.

Step 4 - Feedback

Each security technology in SEP 12.1 can collect data that is sent back to Symantec to measure and mitigate false positives through analysis, heuristic comparison against collected data sets, and custom generic whitelisting. You can enable SEP to automatically submit metadata when it makes detection.

Correcting False Positives

Symantec wants to know about and correct false positives. Having information about detections not only allows Symantec to correct current issue, it also allows Symantec to study the causes of the false positive to avoid similar files from having issues in the future.

False positive submissions can be made immediately to Symantec via a Web form. All suspected false positives should be submitted to https://submit.symantec.com/false_positive/.

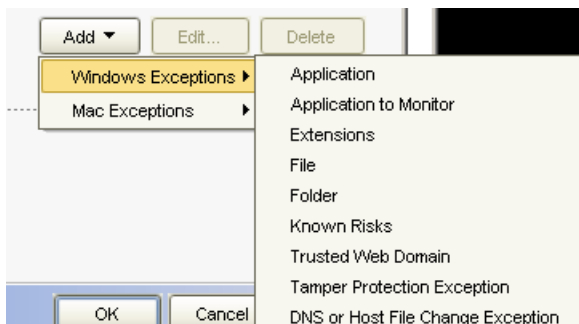
- It is critical for the resolution of reputation (Download Insight) false positives that the file or the SHA256 value of the file be included with the submission. (The hash value of a file is also available in notices on client third-party tools.)
- False positives should not be submitted via the malware submission system. The URL above should be used to report false positives, no matter what Symantec product is involved.

Once the submission has been processed and the file whitelisted by Symantec, the quarantine rescan feature will automatically restore the file out of the quarantine.

Adding Exceptions

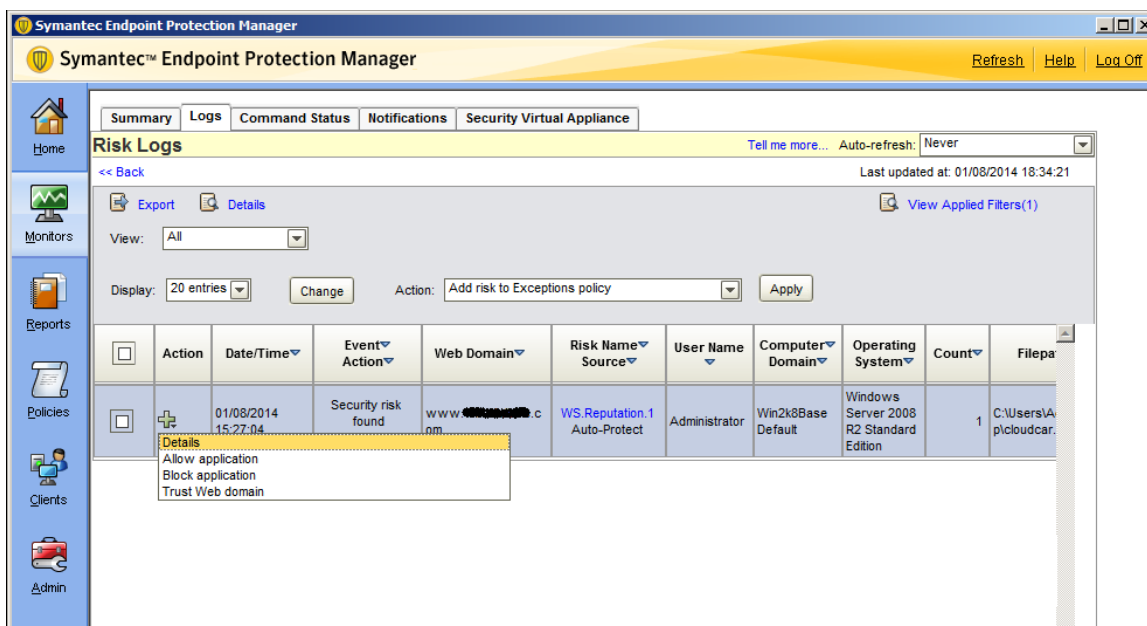
Administrators can whitelist files and domains locally by configuring exceptions. Administrators can add new exceptions for files (for example, "File X is always safe") or domains (for example, "All files downloaded from domain http://somedomain.com are safe") in two ways:

- 1) Add a domain or file exclusion in an Exceptions Policy in the Symantec Endpoint Protection Manager. The Exceptions Policy can be used to add a new exclusion for an internally developed enterprise application or to whitelist the domain of a new enterprise vendor that hosts trusted applications used by employees.



Note: SONAR exceptions can be configured using File, Folder, and Trusted Web Domain exceptions. Download Insight exceptions can be configured using Trusted Web Domain exceptions.

- 2) Files can also be excluded directly in the Logs view of detected events by whitelisting a file or trusting the source domain the file was downloaded from as shown here:



Appendices

Remediation

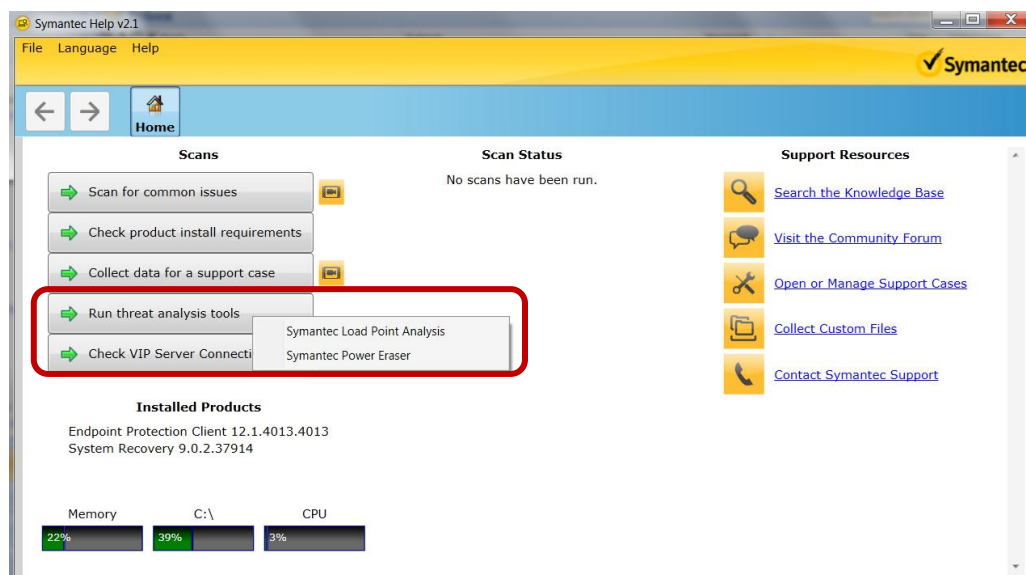
In the event that a system is potentially compromised, Symantec provides some additional tools to assist with remediation steps:

- Symantec Load Point Analysis – Leverages Insight lookups to scan a system in specific areas that are commonly used as load points by malware.
- Symantec Power Eraser – Leverages Insight to do an aggressive scan, including an optional rootkit scan that requires a client restart.

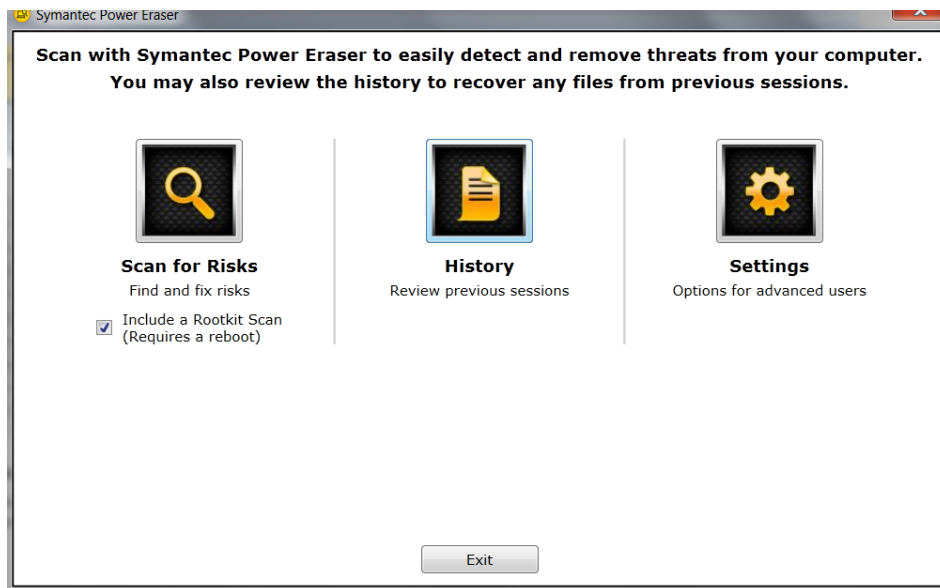
Both of these tools are available in the SymHelp troubleshooting tool. SymHelp is available for download from the Symantec Knowledge base and can be accessed from the SEP client by going to **Help > Download Symantec Help Tool**.

Note that depending on the system that has been potentially compromised, additional forensics might need to be performed before remediation in order to understand how a breach might have occurred and what the impact might be. The tools described here are not intended to provide comprehensive forensics or analysis related to a potential breach.

After downloading the SymHelp tool, run it and accept the EULA on the first screen to continue. As shown here, click **Run threat analysis tools** and select either **Symantec Load Point Analysis** or **Symantec Power Eraser**.



For the more aggressive scan, including Insight lookups on running processes, select **Symantec Power Eraser**. The **Include a Rootkit Scan** option requires a reboot and adds a scan targeted to detect root kits during startup. Click **Scan for Risks**.



Note: Just as with Download Insight and SONAR, access to Symantec Insight URLs in the Internet is required in order to include reputation lookups on running processes and other files of interest. If needed, configure proxy settings as appropriate by selecting “Settings” and entering appropriate proxy information.

For more information about Symantec Power Eraser, see the following knowledge base article:

<http://www.symantec.com/business/support/index?page=content&id=TECH203683>

Summary: Layered Protection in SEP 12.1

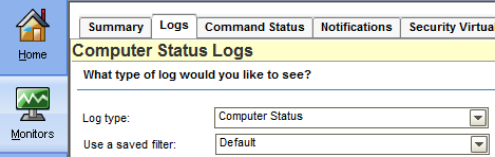
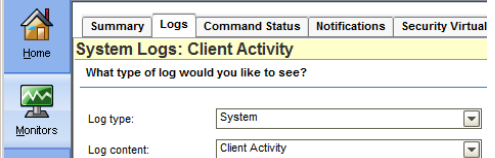
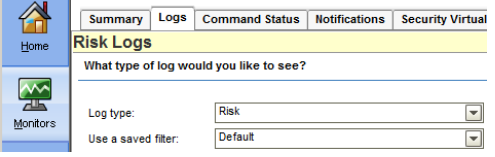
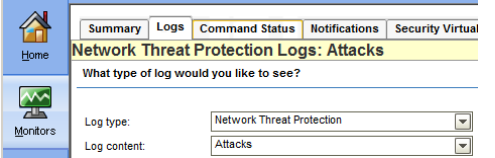
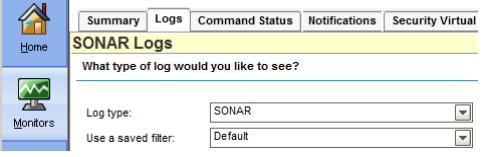

Symantec Security Technology and Response Protection Technologies (highly recommended)

Component	Protection benefit
Virus and Spyware	Signature-based file scanning to detect known threats and threat families <ul style="list-style-type: none">• Real-time scanning on file access• Advanced heuristics requires Internet access
IPS	Inbound and outbound network packet scanning for malicious payloads and activity <ul style="list-style-type: none">• Exploits, attack kits, misleading applications, etc.• Blocks up to 60 percent of all attacks• Detect suspicious outbound traffic (phoning home)
Download Insight	Cloud-based reputation engine detects files with good, bad, or unknown reputation on download. <ul style="list-style-type: none">• Requires internet access for Insight lookups• Applies to executables (exe, dll, sys, ocx, etc)• Queries when executables are downloaded (browser, email, FTP client, etc.)
SONAR	Real-time behavior-based scanning <ul style="list-style-type: none">• Detects malicious behavior in real time to block never-before-seen threats• Requires Internet access for Insight Lookups

Additional Rule-based Protection Technologies (optional, for more advanced use-cases)

Component	Protection Benefit
Application Control and Device Control	Rule-based policies for system hardening <ul style="list-style-type: none">• Application Control: Block autorun.inf, file access, registry access, processes from launching, access to removable drives, loading dlls and many additional options.• Device Control: Block or allow devices by device or class ID, for example, block USB devices except for explicitly allowed models.
Application Learning	Monitor for suspicious applications <ul style="list-style-type: none">• Monitor applications that run in an environment to locate potentially suspicious executables
System Lockdown	System Lockdown <ul style="list-style-type: none">• Define explicit whitelist or blacklist using a file fingerprint list

Some useful logs for monitoring protection status in the Symantec Endpoint Protection Manager

Information	Monitors > Logs	Comment
Client Protection Technologies Enabled and Definitions status	<p>Log type: Computer Status</p> 	<p>Protection technologies installed and enabled status:</p> <ul style="list-style-type: none"> • Auto-Protect • Firewall • SONAR • Download Insight • Intrusion Prevention • IE and Firefox Browser Protection (Browser IPS) • Client product version • Definitions date and revision
Insight Lookup Errors	<p>Log type: System</p> <p>Log content: Client Events</p> 	<p>In the event column look for: “Reputation check timed-out errors”</p> <ul style="list-style-type: none"> • Insight errors could affect Download Insight, SONAR, and Advanced Heuristics effectiveness
Malware: Virus and Spyware Download Insight	<p>Log type: Risk</p> 	<ul style="list-style-type: none"> • Download Insight: detections with Reputation in the risk name, such as “WS.Reputation.1”
Malware: Intrusion Prevention	<p>Log type: Network Threat Protection</p> <p>Log content: Attacks</p> 	<p>Intrusion Prevention from most to least critical:</p> <ul style="list-style-type: none"> • System Infected • OS attack • Web attack • Fake App Attack • Malicious website
Malware: SONAR	<p>Log type: SONAR</p> 	<ul style="list-style-type: none"> • SONAR requires Internet access to successfully complete Insight lookups to prevent false positives.
Application Control	<p>Log type: Application and Device Control</p> <p>Log content: Application Control</p> 	<ul style="list-style-type: none"> • Application Control policies can be set to log only mode for monitoring purposes. • Test Application Control policies before enabling them in production.

Additional Symantec Offerings to Protect against Advanced Persistent Threats

Symantec Endpoint Protection is just one important way to protect against advanced persistent threats. Symantec has additional offerings to help customers stay protected from advanced persistent threats. These include the following:

Symantec Critical System Protection

<http://www.symantec.com/critical-system-protection>

Leading organizations leverage Symantec Critical System Protection to secure their physical and virtual data centers. Delivering host-based intrusion detection (HIDS) and intrusion prevention (HIPS), Symantec provides a proven and comprehensive solution for server security. Achieve complete protection for VMware vSphere, stop zero-day and targeted attacks, and gain real-time visibility and control into compliance with Symantec Critical System Protection.

Symantec Web Gateway

<http://www.symantec.com/web-gateway>

Symantec Web Gateway protects organizations against multiple types of Web-borne malware and gives organizations the flexibility of deploying it as either a virtual appliance or on physical hardware. Powered by Insight, Symantec's innovative reputation-based malware filtering technology, Web Gateway relies on a global network of greater than 210 million systems to identify new threats before they cause disruption in organizations.

Symantec Messaging Gateway

<http://www.symantec.com/messaging-gateway>

Symantec Messaging Gateway enables organizations to secure their email and productivity infrastructure with effective and accurate real-time anti-spam and anti-malware protection, targeted attack protection, advanced content filtering, data loss prevention, and email encryption. Messaging Gateway is simple to administer and catches more than 99 percent of spam with less than one in a million false positives. Defend your email perimeter, and quickly respond to new messaging threats with this market leading messaging security solution.

Symantec Managed Security Services

<http://www.symantec.com/managed-security-services>

Organizations around the world rely on Symantec Managed Security Services to build and sustain a resilient incident management program. Symantec offers the global presence and scale to satisfy even the largest enterprises. Every month, Symantec Managed Security Services:

- Analyzes over 275 billion log entries
- Identifies over 40,000 potential security events
- Escalates over 4,000 validated, severe events

Symantec has been a leading provider of managed security services for over 10 years, and has been recognized by leading industry analysts and publications.

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help businesses and consumers secure and manage their information.

Headquartered in Mountain View, Calif.,

Symantec has operations in 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit

our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation

World Headquarters

350 Ellis Street

Mountain View, CA 94043

+1 650-527-8000

www.symantec.com

Copyright © 2014 Symantec Corporation. All rights reserved. Symantec and the Symantec logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

10/10