

SOPHOS

simple + secure

Sophos Endpoint Security and Control 9.7 policy setup guide

Document date: April 2011



Contents

1 About this guide.....	3
2 General policy recommendations.....	4
3 Setting up an updating policy.....	5
4 Setting up anti-virus and HIPS policies.....	6
5 Setting up firewall policies.....	9
6 Setting up application control policies.....	13
7 Setting up device control policies.....	14
8 Setting up data control policies.....	16
9 Setting up tamper protection policies.....	21
10 Setting up NAC policies.....	22
11 Scanning recommendations.....	24
12 Using on-access scans.....	25
13 Using scheduled scans.....	26
14 Using on-demand scans	27
15 Excluding items from scanning.....	28
16 Technical support.....	29
17 Legal notices.....	30

1 About this guide

This guide describes the policy setup guidelines for Sophos Endpoint Security and Control software.

In particular, it provides advice to help you:

- Understand policy recommendations.
- Set up and roll out each policy by type.
- Use scanning options to discover items.
- Determine what items to exclude from scanning.

This guide is for you if:

- You are using Enterprise Console.
- You want advice on the best options for policy setup and rollout.

See the *Sophos Endpoint Security and Control quick startup guide* prior to reviewing this guide.

All Enterprise Console documents are available at

www.sophos.com/support/docs/Enterprise_Console-all.html.

2 General policy recommendations

When you install Enterprise Console, default policies are created for you. These policies are applied to any groups you create. The default policies are designed to provide effective levels of protection. If you want to use features like application control, device control, data control, tamper protection, or network access control, you need to create new policies or change the default policies. When setting up policies, consider the following:

- Use default settings within a policy when possible.
- Consider the role of the computer when changing default policy settings or creating new policies (e.g. desktop or server).
- Use Enterprise Console for all central policy settings, and set options in Enterprise Console instead of on the computer itself when possible.
- Set options on the computer itself only when requiring temporary configuration for that computer or for items that cannot be configured centrally, such as advanced scanning options.
- Create a separate group and policy for computers that require long-term special configuration.

3 Setting up an updating policy

The updating policy specifies how computers receive new threat definitions and updates to Sophos software. A software subscription specifies which versions of endpoint software are downloaded from Sophos for each platform. The default updating policy enables you to install and update the software specified in the "Recommended" subscription. When setting up your updating policy, consider the following:

- You should normally subscribe to the "Recommended" versions of the software to ensure that it is kept up to date automatically. However, if you want to evaluate new versions of the software before placing them on your main network, you may want to consider using fixed versions of the software on the main network while evaluating the new versions. Fixed versions are updated with new threat detection data, but not with the latest software version each month.
- Ensure that the number of groups using the same updating policy is manageable. You should normally have no more than 1,000 computers updating from the same location. The optimum number updating from the same location is 600-700.

Note: The number of computers that can update from the same directory depends on the server holding that directory and on the network connectivity.

- By default, computers update from a single primary location. However, we recommend that you also always set up an alternative secondary location for updates. If endpoint computers cannot contact their primary location, they will attempt to update from their secondary location if set. For more information, see the Sophos Enterprise Console Help.
- You should allow location roaming on an updating policy for laptop users who roam extensively or internationally within an organization. When this option is enabled, roaming laptops will attempt to locate and update from the nearest location by querying fixed endpoints on the same local network they are connected to, which minimizes update delays and bandwidth costs. If multiple locations are returned, the laptop determines which is nearest and uses that location. If none work, the laptop uses the primary (then secondary) location defined in its updating policy. Location roaming is only supported if you are using Sophos Update Manager, and will only work if the roaming endpoint is updating from a location that is managed by the same Enterprise Console instance that manages the endpoint. For more information, see the Sophos Enterprise Console Help.
- If you are concerned about performance on low specification computers, you can subscribe to a fixed version of the software and manually change the software subscription when you are ready to update the software for those computers. This option will ensure that those computers are updated with new threat detection data. Alternatively, you can perform updates for low specification computers less often (such as two or three times daily) or consider updating at select times outside of typical user hours (such as during evenings or on weekends).



Caution: Be aware that minimizing updates increases security risk.

4 Setting up anti-virus and HIPS policies

4.1 Recommended settings

The anti-virus and HIPS policy specifies how the security software scans computers for viruses, Trojans, worms, spyware, adware, potentially unwanted applications (PUAs), suspicious behavior, and suspicious files, and how it cleans them up. When setting up your anti-virus and HIPS policy, consider the following:

- The default anti-virus and HIPS policy will protect computers against viruses and other malware. However, you may want to create new policies, or change the default policy, to enable detection of other unwanted applications or behavior.
- Enable Sophos Live Protection, which uses the Sophos online lookup service to instantly decide whether a suspicious file is a threat and to update your Sophos software in real time. The **Enable Live Protection** option is enabled by default for new software installations only. For software upgrades, you must enable this option. To take full advantage of Sophos Live Protection, we recommend also selecting the **Automatically send sample files to Sophos** option.
- Use the **Alert only** option to only detect suspicious behavior. Initially defining a report only policy enables you to gain a better view of suspicious behavior across your network. This option is enabled by default and should be deselected once policy rollout is complete to block programs and files.

4.2 How to roll out an anti-virus and HIPS policy

We recommend that you roll out anti-virus and HIPS policy as follows:

1. Create different policies for different groups.
2. Set exclusions from on-access scanning for directories or computers with large databases or frequently changing files, and ensure that scheduled scans are performed instead. For example, you may want to exclude particular directories on Exchange servers or other servers where performance might be affected. For more information, see Sophos support knowledgebase article 12421 (<http://www.sophos.com/support/knowledgebase/article/12421.html>).

3. Set Sophos Live Protection options. This feature delivers the most up-to-date threat protection by using the Sophos online lookup service to instantly decide whether a suspicious file is a threat and to update your Sophos software in real time. The following options are available:

- **Enable Live Protection:** If the anti-virus scan on an endpoint computer has identified a file as suspicious, but cannot further identify it as either clean or malicious based on the threat identity (IDE) files stored on the computer, certain file's characteristics (such as its checksum and other attributes) are sent to Sophos to assist with further analysis. The Sophos online lookup service performs an instant lookup of a suspicious file in the SophosLabs database. If the file is identified as clean or malicious, the decision is sent back to the computer and the status of the file is automatically updated.

This option is enabled by default for new software installations only. For software upgrades, you must enable this option.

- **Automatically send sample files to Sophos:** If a file is deemed potentially malicious but cannot be positively identified as malicious based on the file characteristics alone, Sophos Live Protection allows Sophos to request a sample of the file. If the Automatically send sample files to Sophos option is enabled and Sophos does not already hold a sample of the file, the file will be submitted automatically. Submission of such file samples helps Sophos to continuously enhance detection of malware without the risk of false positives.

Important: You must ensure that the Sophos domain to which the file data is sent is trusted in your web filtering solution. For details, see Sophos support knowledgebase article 62637 (<http://www.sophos.com/support/knowledgebase/article/62637.html>). If you use a Sophos web filtering solution, such as the WS1000 Web Appliance, you do not need to do anything. Sophos domains are already trusted.

4. Detect viruses and spyware.
 - a) Ensure that on-access scanning is enabled or schedule a full system scan to detect viruses and spyware. On-access scanning is enabled by default. For more information, see [Using on-access scans](#) (page 25) or [Using scheduled scans](#) (page 26).
 - b) Select cleanup options for viruses/spyware.
5. Detect suspicious files.

Suspicious files contain certain characteristics that are common to malware but not sufficient for the file to be identified as a new piece of malware.

 - a) Enable on-access scanning or schedule a full system scan to detect suspicious files.
 - b) Select the **Suspicious files (HIPS)** option.
 - c) Select cleanup options for suspicious files.
 - d) As appropriate, authorize any files that are allowed to run.
6. Detect suspicious behavior and buffer overflows.

Suspicious behavior and buffer overflow detections monitor running processes continuously to determine if a program exhibits suspicious behavior. These detections are useful for stopping security flaws.

- a) Use the **Alert only** option to only detect suspicious behavior and buffer overflows. This option is enabled by default.
- b) Authorize any programs or files you want to continue to run in the future.
- c) Configure your policy to block programs and files that are detected by clearing the **Alert only** option.

This approach avoids blocking programs and files that your users may need. For more information, see Sophos support knowledgebase article 50160 (<http://www.sophos.com/support/knowledgebase/article/50160.html>).

7. Detect adware and PUAs.

When you first scan for adware and PUAs, the scan may generate large numbers of alerts for applications that are already running on your network. By initially running a scheduled scan, you can deal safely with applications that are already running on your network.

- a) Schedule a full system scan to detect all adware and PUAs.
- b) Authorize or uninstall any applications that are detected by the scan.
- c) Select the **Adware and PUAs** on-access scanning option to detect future adware and PUAs.

For more information, see Sophos support knowledgebase article 13815 (<http://www.sophos.com/support/knowledgebase/article/13815.html>).

8. Detect threats in web pages.

- a) Ensure that the **Block access to malicious websites** option is set to **On** to ensure that malicious websites are blocked. This option is turned on by default.
- b) Set the **Download scanning** option to **On** or **As on access** to scan and block malicious downloaded data. **As on access**, which is the default setting, enables download scanning only when on-access scanning is enabled.
- c) As appropriate, authorize any websites that are allowed.

For more information on setting up anti-virus and HIPS policy, see the Sophos Enterprise Console Help.

5 Setting up firewall policies

5.1 Recommended settings

The firewall policy specifies how the firewall protects computers. When setting up your firewall policy, consider the following:

- When Sophos Client Firewall is installed, the Windows firewall setting is turned off; therefore, if you were using the Windows firewall, make a note of existing configurations and move them to Sophos Client Firewall.
- Use the **Allow by default** mode to detect but not block traffic, applications, and processes. Initially defining a report only policy enables you to gain a better view of network activity.
- Use the firewall Event Viewer to view which traffic, applications, and processes are being used. The Event Viewer also allows you to easily create rules that allow or block reported traffic, applications, and processes. You can access the Event Viewer by clicking **View > Firewall Events**.
- Use the **Interactive** mode on test computers to view learning dialogs, configure and recognize the applications you use, and import and edit rules established by that process.
- For **Interactive** mode, we recommend that you clear the **Display an alert in the management console if local changes are made to the global rules, applications, processes or checksums** option to avoid "Differs from policy" warnings when users respond to learning dialogs.
- Allow the use of a web browser, email, file and printer sharing.
- We recommend that you do not change the default ICMP settings, global rules, and application rules unless you are knowledgeable about networking.
- We recommend that you create application rules rather than global rules when possible.

5.2 Configure the firewall for dual location

The single location option is intended for computers that are always on a single network, such as desktops. The dual location option is available if you want the firewall to use different settings according to the location where computers are used, such as in the office and out of the office. You may want to set up dual location for laptops.

If you select dual location, we recommend you set up primary and secondary location configuration options as follows:

- Set up your primary location to be the network you control (e.g. office network) and your secondary location to be locations outside of your control.
- Set up your primary location to have more open access and your secondary location to have more restricted access.

- When configuring your primary location detection options, we generally recommend DNS detection for larger, more complicated networks and gateway detection for smaller, simpler ones. DNS detection requires a DNS server, but is typically easier to maintain than gateway detection. If hardware used for gateway detection fails, reconfiguration of MAC addresses is necessary and computers may incorrectly receive the secondary location configuration until the hardware configuration issues are resolved.
- If you use DNS detection, we recommend that you add a specific DNS entry to your DNS server that has an unusual name and returns a localhost IP address, also called a loopback address (i.e. 127.x.x.x). These options make it highly unlikely that some other network you connect to is incorrectly detected as your primary network.
- In the advanced firewall policy configuration "Applied location" section, select the firewall configuration you want to apply to the computer. If you want the configuration applied to be dependent upon the computer's location, select the **Apply the configuration for the detected location** option. If you want to manually apply either the primary or secondary configuration, select the appropriate option.



Caution: We strongly advise caution when using local subnet rules as part of secondary configurations. If the computer is a laptop, and it is used out of the office, it may connect to an unknown subnet. If this happens, firewall rules in the secondary configuration that use the local subnet as an address may inadvertently allow unknown traffic.

5.3 When to block or allow traffic, applications, and processes

We recommend blocking or allowing traffic, applications, and processes as follows:

- If the firewall is running the **Interactive** mode, educate users on which traffic, applications, or processes to block or allow.
- If the firewall is running the **Block by default** mode, the user does not get prompted by learning dialogs; instead, the administrator is responsible for blocking or allowing all traffic, applications, or processes from Enterprise Console.
- The **Block...this time only** options on a computer should be used only if the user is unsure whether or not to block the traffic. The options are only available on the computer when the policy is in **Interactive** mode.
- There are some cases in which traffic should **not** be blocked. These include the checksum and application rules that relate to a web browser, email, file and printer sharing, and any other programs that must access the internet.
- Once a computer is set up with the allowed applications, users should only be prompted when installing new applications or patching existing applications (when in **Interactive** mode).

5.4 How to roll out firewall policy

By default, the firewall is enabled and blocks all non-essential network traffic. Therefore, you should configure it to allow the traffic, applications, and processes you want to use, and test it prior to installing and running the firewall on all computers. We recommend that you introduce firewall policy as follows:

1. Plan your policy and what you want it to do before creating or editing firewall rules (global, application, or other).
2. Use the **Allow by default** mode to detect but not block common traffic, applications, and processes.
3. Use the firewall Event Viewer to view which traffic, applications, and processes are being used. The Event Viewer also allows you to easily create rules that allow or block reported traffic, applications, and processes. You can access the Event Viewer by clicking **View > Firewall Events**.
4. Create custom global rules and application rules as needed.

Note: As an alternative to steps 1-4, you can configure a test computer in **Interactive** mode and then import and edit the rules established by that process. For more information, see the Sophos Endpoint Security and Control Help.

5. You should run a phased rollout of the Sophos Client Firewall across your network. This will avoid flooding your network with traffic in the initial stages. You should first roll out Sophos Client Firewall to a small number of computers that can be easily monitored. These computers should be representative of the various roles in your network.



Caution: Do not deploy across your entire network until the configuration has been thoroughly checked and tested.

- a) Install and configure Sophos Client Firewall on the test computers.
 - b) Run all of your usual programs and procedures on those computers.
 - c) Check for any weaknesses in the test configuration (e.g. giving too much access to some users).
 - d) Where needs differ, subdivide the group and create extra configurations as needed.
 - e) Once you've tested the rules, change the policy mode to **Block by default**; otherwise, computers will remain insecure.
6. Once you have completed the first stage of your rollout, you can plan the deployment of Sophos Client Firewall across your network.

It is important to avoid flooding the network with too much traffic at any one time. Do not deploy to the entire network at once.

- Split the rest of the network into manageable groups, such as 100 computers at a time.
- Roll out to those groups in stages.

For more information on setting up firewall policy, see the Sophos Enterprise Console Help.

6 Setting up application control policies

6.1 Recommended settings

The application control policy specifies which applications are blocked and which are allowed on your computers. When setting up your application control policy, consider the following:

- Use the **Detect but allow to run** option to detect but not block controlled applications. Initially defining a report only policy enables you to gain a better view of application use across your network.
- Use the application control Event Viewer to audit application use within your company. You can access the Event Viewer by clicking **View > Application Control Events**.
- Use the Report Manager to create trend reports on application control events by computer or user.
- Consider using the "All added by Sophos in the future" option to block all new applications of a specific type that Sophos adds so that you do not have to constantly update your policy. For example, if you currently block all instant messaging applications, you may consider blocking all new instant messaging applications.

6.2 How to roll out application control policy

By default, all applications and application types are allowed. We recommend that you introduce application control as follows:

1. Consider which applications you want to control.
2. Enable on-access scanning, and select the **Detect but allow to run** option to detect but not block controlled applications.
At this time, you have one application control policy for your entire network.
3. Use the application control Event Viewer to view which applications are being used, and determine the applications or application types that you want to block. You can access the Event Viewer by clicking **View > Application Control Events**.
4. To grant access to applications differently for various computer groups, create different policies for different groups. For example, you may not want to allow VoIP for office-based desktop computers, but you may want to authorize its use for remote computers.
5. Determine which applications or application types you want to block and move them to the Blocked list.
6. Configure your policy to block controlled applications that are detected by clearing the **Detect but allow to run** option.

By taking this approach, you avoid generating large numbers of alerts and blocking applications that your users may need. For more information on setting up application control policy, see the Sophos Enterprise Console Help.

7 Setting up device control policies

7.1 Recommended settings

The device control policy specifies which storage and networking devices are authorized for use on computers. When setting up your device control policy, consider the following:

- Use the **Detect but do not block devices** option to detect but not block controlled devices. To do this, you must first set the status to **Blocked** for each device type you want to detect. The software will not scan for any device types you have not specified. Initially defining a report only policy enables you to gain a better view of device use across your network.
- Use the device control Event Viewer to quickly filter block events for investigation. You can access the Event Viewer by clicking **View > Device Control Events**.
- Use the Report Manager to create trend reports on device control events by computer or user.
- Consider providing tighter access control for computers of users with access to sensitive information.
- Plan a list of device exemptions prior to rolling out a policy that blocks devices. For example, you may want to allow the use of optical drives within the art team.
- The "Secure Removable Storage" category can be used to automatically authorize hardware-encrypted USB storage devices from various supported vendors. A full list of supported vendors is available on the Sophos website. For a list of supported secure removable storage devices, see Sophos support knowledgebase article 63102 (<http://www.sophos.com/support/knowledgebase/article/63102.html>).
- When adding device exemptions to the device control policy, identify the reason for a device exemption or who requested it in the **Comment** field.
- Use the custom desktop messaging options to provide users with additional guidance when a controlled device is discovered. For example, you could provide a link to your company's device use policy.
- If you want a network device to become enabled (i.e. Wi-Fi adapters) when the computer is physically disconnected from the network, select the **Block bridged** option when setting access levels for network devices.

Note: The Block bridged mode significantly reduces the risk of network bridging between a corporate network and a non-corporate network. The mode is available for both wireless and modem types of devices. The mode works by disabling either wireless or modem network adapters when an endpoint is connected to a physical network (typically through an Ethernet connection). Once the endpoint is disconnected from the physical network, the wireless or modem network adapters are seamlessly re-enabled.

- Ensure you are certain about blocking a device prior to rolling out your policy. Be aware of all users scenarios, especially in relation to WiFi and network devices.



Caution: Policy changes are made from the Enterprise Console server to the computer through the network; therefore, once the network is blocked, it cannot be unblocked from Enterprise Console since the computer cannot accept additional configuration from the server.

7.2 How to roll out device control policy

By default, device control is turned off and all devices are allowed. We recommend that you introduce device control as follows:

1. Consider which devices you want to control.
2. Enable device control scanning, and select the **Detect but do not block devices** option to detect but not block controlled devices. To do this, you must first set the status to **Blocked** for each device type you want to detect. The software will not scan for any device types you have not specified.

At this time, you have one device control policy for your entire network.

3. Use the device control Event Viewer to view which devices are being used, and determine the device types that you want to block. You can access the Event Viewer by clicking **View > Device Control Events**.
4. To grant access to devices differently for various computer groups, create different policies for different groups. For example, you may not want to allow removable storage devices for human resources and finance departments, but allowing them for IT and sales departments is acceptable.
5. Exempt the instances or model types that you do not want to block. For example, you can exempt a specific USB key (instance) or all Vodafone 3G modems (model type).
6. Determine which devices you want to block and change their status to **Blocked**. You can also allow read-only access to certain storage devices.
7. Configure your policy to block controlled devices that are detected by clearing the **Detect but do not block devices** option.

By taking this approach, you avoid generating large numbers of alerts and blocking devices that your users may need. For more information on setting up device control policy, see the Sophos Enterprise Console Help.

8 Setting up data control policies

8.1 Defining data control policy

The data control policy enables you to manage the risks associated with the accidental transfer of sensitive data from computers.

Each company will have its own definition of sensitive data. Common examples include:

- Customer records containing personally identifiable information.
- Financial data such as credit card numbers.
- Confidential documents.

When the data control policy is enabled, Sophos monitors user actions at common data exit points:

- Transfer of files onto storage devices (removable storage, optical media, and disk-based media).
- Upload of files into applications (corporate web browsers, email clients, and IM clients).

A data control rule is made up of three elements:

- Items to match: Options include file content, file types, and file names.
- Points to monitor: Monitoring points include storage types and applications.
- Actions to take: Available actions include "Allow file transfer and log event" (monitor mode), "Allow transfer on acceptance by user and log event" (training mode), and "Block transfer and log event" (restricted mode).

For example, data control rules can be defined to log the uploading of any spreadsheet using Internet Explorer or to allow for the transfer of customer addresses onto a DVD once the transfer is confirmed by the user.

Defining sensitive data based on content can be complex. Sophos has simplified this task by providing a pre-built library of sensitive data definitions, known as Content Control Lists. The library covers a wide range of personally identifiable and financial data formats and is kept up-to-date by Sophos. As necessary, you can also define custom Content Control Lists.

As with all Sophos policies, the data control policy continues to be enforced on computers even when they are disconnected from your company's network.

8.2 Recommended settings

When setting up your data control policy, consider the following:

- Use the **Allow file transfer and log event** action to detect but not block controlled data. Initially defining a report only policy enables you to gain a better view of data use across your network.

- Use the **Allow transfer on acceptance by user and log event** action to alert users about the risks of transferring documents that potentially contain sensitive data. This approach can reduce the risk of data loss without a significant impact on IT operations.
- Use the "quantity" setting within content rules to configure the volume of sensitive data you want to find before a rule is triggered. For example, a rule that is configured to look for one postal address within a document will generate more data control events than a rule looking for 50 or more addresses.

Note: Sophos provides default quantity settings for each Content Control List.

- Use the data control Event Viewer to quickly filter events for investigation. All data control events and actions are logged centrally in Enterprise Console. You can access the Event Viewer by clicking **View > Data Control Events**.
- Use the Report Manager to create trend reports on data control events by rules, computers, or users.
- Use the custom desktop messaging options to provide users with additional guidance when an action is triggered. For example, you could provide a link to your company's data security policy.
- Use the verbose logging mode to gather additional detail on the accuracy of data control rules. Once the evaluation of these rules is complete, disable verbose logging.

Note: Verbose logging must be activated on each computer. All data generated is stored in the computer's local data control log. When the verbose logging mode is active, all strings contained in each file that match the data specified in a rule are logged. The additional detail within the log can be used to identify phrases or strings within a document that triggered a data control event.

8.3 How to roll out data control policy

By default, data control is turned off and no rules are specified to monitor or restrict the transfer of files onto storage devices or into applications. We recommend that you introduce data control as follows:

1. Understand how data control works on your computers:

- **Storage devices:** Data control intercepts all files copied onto monitored storage devices using Windows Explorer (this includes the Windows desktop). However, direct saves from within applications, such as Microsoft Word, or transfers made using the command prompt are not intercepted.

It is possible to force all transfers onto monitored storage devices to be made using Windows Explorer by using either the "Allow transfer on acceptance by user and log event" action or the "Block transfer and log event" action. In either case, any attempt to save directly from within an application or transfer files using the command prompt are blocked by data control, and a desktop alert is displayed to the user requesting that they use Windows Explorer to complete the transfer.

When a data control policy only contains rules with the "Allow file transfer and log event" action, direct saves from within applications and transfers using the command prompt are not intercepted. This behavior enables users to use storage devices without any restrictions. However, data control events are still only logged for transfers made using Windows Explorer.

Note: This restriction does not apply to application monitoring.

- **Applications:** Data control intercepts files and documents uploaded into monitored applications. To ensure only file uploads by users are monitored, some system file locations are excluded from data control monitoring. For more information on the content or actions within applications that are scanned or not scanned, see [Understanding data control scanning within applications](#) (page 19).

Note: If you are monitoring e-mail clients, data control scans all file attachments but does not scan e-mail content. The Sophos Email Security and Data Protection solution can be used if scanning email content is required.

2. Consider what types of information you want to identify and create rules for. Sophos provides a set of sample rules that you can use to help build your data control policy.

Important: Content scanning can be an intensive process and this should be taken into consideration when creating content rules. It is important to test the impact of a content rule prior to rolling it out across a large number of computers.

Note: When creating your first policy, we recommend focusing on the detection of large collections of personally identifiable information within documents. Sophos provides sample rules to meet this requirement.

3. Enable data control scanning, and select the **Allow file transfer and log event** action in your rules to detect but not block controlled data.

Important: We recommend that you configure all rules to use this action for the initial deployment. This will enable you to assess the effectiveness of the rules without impacting user productivity.

4. Deploy your data control policy to a small number of computers to make it easier to analyze data control events triggered by the policy.
5. Use the data control Event Viewer to view data being used, check for any weaknesses in the test configuration (e.g. a rule being too sensitive and generating a higher than anticipated volume of events). You can access the Event Viewer by clicking **View > Data Control Events**.
6. Once the policy has been tested, you can make any required adjustments and roll it out to a larger set of computers within your company. At this stage, you may decide to:
 - Change the actions for some rules as necessary to **Allow transfer on acceptance by user and log event** or **Block transfer and log event**.
 - Create different policies for different groups. For example, you may want to allow computers within the human resources department to transfer personally identifiable information, but prevent all other groups from doing so.

For more information on setting up data control policy, see the Sophos Enterprise Console Help.

8.4 Understanding data control scanning within applications

The following is a list of the content or actions that are scanned or not scanned within supported applications.

For a complete list of known limitations with data control, see Sophos support knowledgebase article 63016 (<http://www.sophos.com/support/knowledgebase/article/63016.html>).

Applications	Data Control Scanning Actions
Web browsers	<p>Scanned:</p> <ul style="list-style-type: none"> ■ File uploads ■ Webmail attachments ■ Microsoft SharePoint uploads <p>Not scanned</p> <ul style="list-style-type: none"> ■ Webmail message content ■ Blog entries ■ File downloads

Applications	Data Control Scanning Actions
	<p>Note: In a small number of cases, files may be scanned when downloaded.</p>
Email clients	<p>Scanned</p> <ul style="list-style-type: none"> ■ Email attachments <p>Not scanned</p> <ul style="list-style-type: none"> ■ Email message content ■ Forwarded attachments ■ Attachments made using the "Send" email option within applications (e.g. Windows Explorer and Microsoft Office) ■ Attachments using the "E-mail this file" option within Windows Explorer ■ Attachments copied from one email to another email ■ Saved attachments <p>Note: In a small number of cases, files may be scanned when saved.</p>
Instant messaging (IM) clients	<p>Scanned</p> <ul style="list-style-type: none"> ■ File transfers <p>Note: A file may be scanned twice: once upon upload to the IM client and again upon acceptance by the recipient. Both scans occur on the sender's computer.</p> <p>Not scanned</p> <ul style="list-style-type: none"> ■ IM message content ■ Sent files

9 Setting up tamper protection policies

9.1 Recommended settings

Tamper protection policy enables you to prevent unauthorized users (local administrators with limited technical knowledge) from reconfiguring, disabling, or uninstalling Sophos security software. Unauthorized users are those who do not know the tamper protection password.

Note: Tamper protection is not designed to protect against users with extensive technical knowledge. It will not protect against malware which has been specifically designed to subvert the operation of the operating system to avoid detection. This type of malware will only be detected by scanning for threats and suspicious behavior. For more information, see [Setting up anti-virus and HIPS policies](#) (page 6).

After you enable tamper protection and create a tamper protection password, a user who does not know the password will not be able to reconfigure on-access scanning or suspicious behavior detections in Sophos Endpoint Security and Control, disable tamper protection, or uninstall Sophos Endpoint Security and Control components (Sophos Anti-Virus, Sophos Client Firewall, Sophos AutoUpdate, or Sophos Remote Management System) or Sophos SafeGuard Disk Encryption from Control Panel.

When setting up your tamper protection policy, consider the following:

- Use the tamper protection Event Viewer to audit tamper protection password use and to monitor the rate of tamper attempts in your company. You can view both successful tamper protection authentication events (authorized users overriding tamper protection) and failed attempts to tamper with Sophos security software. You can access the Event Viewer by clicking **View > Tamper Protection Events**.

9.2 How to roll out tamper protection policy

By default, tamper protection is disabled. We recommend that you introduce tamper protection as follows:

1. Enable tamper protection and create a secure tamper protection password.
The password allows only authorized endpoint users to re-configure, disable, or uninstall Sophos security software.
Note: Tamper protection does not affect members of the SophosUser and SophosPowerUser groups. When tamper protection is enabled, these users can still perform all tasks that they are usually authorized to perform, without the need to enter the tamper protection password.
2. If you require the ability to enable or disable tamper protection or create different passwords for various groups, create different policies for different groups.

For more information on setting up tamper protection policy, see the Sophos Enterprise Console Help.

10 Setting up NAC policies

10.1 When to use pre-defined NAC policies

The NAC policy specifies the conditions that computers must comply with before they can access the network. By default, Sophos NAC allows all computers to access the network. You need to configure a NAC policy in order to control access.

Use the pre-defined policies to enforce security compliance for both managed and unmanaged computers. You can edit the pre-defined policies in the NAC Manager to change the policy mode, the profiles that are in the policy, or which network access templates are applied to the policy.

The following policies are available:

- **Default:** This policy is used if a computer has the Compliance Agent installed and no other policy has been assigned. By default, the policy mode is set to Report Only. This policy performs remediation actions on the computer if the policy mode is set to Remediate or Enforce.
- **Managed:** This policy can be used for computers that are managed with Enterprise Console and have the Compliance Agent installed. By default, the policy mode is set to Report Only. This policy performs remediation actions on the computer if the policy mode is set to Remediate or Enforce.
- **Unmanaged:** This policy can be used for computers from outside of the company. This policy does not perform remediation actions on the computer. The Compliance Dissolvable Agent uses the Unmanaged policy.

For more information on updating pre-defined policies, see the Sophos NAC Manager Help.

10.2 How to roll out NAC policy

Initially, the "Default" NAC policy is applied to all computers. If you want to change policy settings or use a different policy, you can use Sophos NAC Manager to edit a policy and Enterprise Console to apply that policy to computers. We recommend that you introduce NAC policy as follows:

1. In Enterprise Console, create or import groups and deploy the Sophos Compliance Agent to computers using the Protect computers wizard.
2. In the NAC Manager, ensure that the NAC policies contain the settings, profiles, and access templates you want to use.
3. Use Enterprise Console to apply the Managed NAC policy to all groups managed in Enterprise Console.

The Agents will begin assessing compliance in Report Only policy mode.

4. Use the reports in the NAC Manager to determine the current compliance state of users.

The reports provide a realistic view of how compliant users are with the NAC policy.

5. Use the NAC Manager to update the Managed NAC policy. Change the policy mode from Report Only to Remediate.
6. Use the reports in the NAC Manager to determine the current compliance state of users.
Over time, computers that are non-compliant and partially compliant should be corrected automatically to improve the overall compliance state.
7. Use the NAC Manager to update the Managed NAC policy. Change the policy mode from Remediate to Enforce.
8. Use the reports in the NAC Manager to determine the current compliance state of users.
Computers that are non-compliant must remediate or those users are denied access to network resources.

For more information on NAC configuration, see the Sophos NAC Manager Help.

11 Scanning recommendations

The scanning options in the following sections are set within the anti-virus and HIPS policy; although, some scanning options, such as extensions and exclusions, also apply to the application control policy. When setting scanning options, consider the following:

- Use default settings when possible.
- Set scanning in Enterprise Console versus on the computer itself when possible.
- Consider the role of the computer (e.g. desktop or server).
- The **Scan all files** option is generally not needed or recommended. Instead, select the **Scan only executable and other vulnerable files** option to scan for threats found by SophosLabs. Only scan all files on the advice of technical support.
- The **Scan inside archive files** option makes scanning slower and is generally not required. When you attempt to access the contents of an archive file, the file is scanned automatically. Therefore, we do not recommend also selecting this option unless you use archive files extensively.
- We recommend scanning a computer's system memory for threats. System memory is used by the operating system. You can scan system memory periodically in the background while on-access scanning is enabled. You can also include system memory scanning as part of a scheduled scan. The **Scan system memory** option is enabled by default for new software installations and new policies only. For software upgrades, you must enable this option.

12 Using on-access scans

When using on-access scans, consider the following:

- Use default settings when possible.
- Use the **Read** on-access scanning option. The **Write** and **Rename** on-access scanning options are generally not needed, but are provided as options for maximum security. These options may be useful during malware outbreaks.
- On-access scanning may not detect viruses if certain encryption software is installed. Change the startup processes to ensure that files are decrypted when on-access scanning begins. For more information on how to use anti-virus and HIPS policy with encryption software, see Sophos support knowledgebase article 12790 (<http://www.sophos.com/support/knowledgebase/article/12790.html>).
- When you do not select on-access scanning, ensure that computers use scheduled scans. For more information, see [Using scheduled scans](#) (page 26).



Caution: Be aware that disabling on-access scanning increases security risk.

13 Using scheduled scans

When using scheduled scans, consider the following:

- Use default settings when possible.
- Use scheduled scans as a way of assessing threats or estimating the prevalence of unwanted or controlled applications.
- Use scheduled scans on server directories where performance will be affected by using on-access scanning. For example, you could have a group for Exchange servers that uses scheduled scans on particular directories. For more information, see Sophos support knowledgebase article 12421 (<http://www.sophos.com/support/knowledgebase/article/12421.html>).
- When you do not select on-access scanning, ensure that computers use scheduled scans. Put these computers in a group and define a scheduled scan.
- Be aware of performance issues when scheduling scans. For example, if you are scanning a server that reads and writes constantly to databases, consider when its performance will be the least affected.
- For servers, consider the tasks that are running. If there is a backup task, do not run a scheduled scan at the same time the backup task is running.
- Scan at set times. Ensure that a scheduled scan is performed daily on each computer, such as at 9 PM. At a minimum, scheduled scans should be performed weekly on all computers.
- The **Run scan at lower priority** option allows a scheduled scan on Windows Vista and later operating systems to run at a lower priority so that it has minimal impact on user applications. This option is recommended; however, the scan will take longer to run than scans without this option.

14 Using on-demand scans

When using on-demand scans, consider the following:

- Use on-demand scans when manual assessment or cleanup is required.

15 Excluding items from scanning

Exclude items from scanning as follows:

- Use extensions to exclude specific file types from scanning.
- Use exclusions to exclude specific items, such as files or drives, from scanning. You can create drive-level exclusions (X:), directory-level exclusions (X:\Program Files\Exchsrvr\), or file-level exclusions (X:\Program Files\SomeApp\SomeApp.exe).
- Consider excluding media drives from on-access scanning for specific users who use them a considerable amount of time. Media drives read and write temporary files, and each file is intercepted and scanned each time it is used, making scanning slower.
- Use the **Exclude remote files** option when you do not want remotely located files (on network resources) to be scanned. We recommend that all computers scan remote files when accessing them; however, you may want to select this option on file servers or in specific cases where large or constantly changing files are accessed remotely.



Caution: Be aware that excluding items from scanning increases security risk.

16 Technical support

You can find technical support for Sophos products in any of these ways:

- Visit the SophosTalk community at <http://community.sophos.com/> and search for other users who are experiencing the same problem.
- Visit the Sophos support knowledgebase at <http://www.sophos.com/support/>.
- Download the product documentation at <http://www.sophos.com/support/docs/>.
- Send an email to support@sophos.com, including your Sophos software version number(s), operating system(s) and patch level(s), and the text of any error messages.

17 Legal notices

Copyright © 2011 Sophos Limited. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the license terms or you otherwise have the prior permission in writing of the copyright owner.

Sophos and Sophos Anti-Virus are registered trademarks of Sophos Limited. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

Common Public License

The Sophos software that is referenced in this document includes or may include some software programs that are licensed (or sublicensed) to the user under the Common Public License (CPL), which, among other rights, permits the user to have access to the source code. The CPL requires for any software licensed under the terms of the CPL, which is distributed in object code form, that the source code for such software also be made available to the users of the object code form. For any such software covered under the CPL, the source code is available via mail order by submitting a request to Sophos; via email to support@sophos.com or via the web at <http://www.sophos.com/support/queries/enterprise.html>. A copy of the license agreement for any such included software can be found at <http://opensource.org/licenses/cpl1.0.php>

ConvertUTF

Copyright 2001–2004 Unicode, Inc.

This source code is provided as is by Unicode, Inc. No claims are made as to fitness for any particular purpose. No warranties of any kind are expressed or implied. The recipient agrees to determine applicability of information provided. If this file has been purchased on magnetic or optical media from Unicode, Inc., the sole remedy for any claim will be exchange of defective media within 90 days of receipt.

Unicode, Inc. hereby grants the right to freely use the information supplied in this file in the creation of products supporting the Unicode Standard, and to make copies of this file in any form for internal or external distribution as long as this notice remains attached.