SOPHOS

Cybersecurity made simple.

# Sophos Enterprise Console

## policy setup guide

product version: 5.5

# Contents

# 1 About this guide

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

**Note**
Some features will be unavailable if your license does not include them.

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

See the Sophos Enterprise Console quick startup guide prior to reviewing this guide.

All Sophos Enterprise Console documents are available at http://www.sophos.com/en-us/support/documentation/enterprise-console.aspx.

# 2 General policy recommendations

When you install Sophos 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 network access control, patch, application control, data control, device control, or tamper protection, 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 Sophos Enterprise Console for all central policy settings, and set options in Sophos 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 will only work if both roaming laptops and fixed endpoints are managed by the same Sophos Enterprise Console instance and use the same software subscription. Any third-party firewalls must be configured to allow update location queries and responses. The port used by default is 51235, but it can be changed.

  For more information, see the Sophos Enterprise Console help. For frequently asked questions about location roaming, see Sophos support knowledgebase article 112830 (http://www.sophos.com/en-us/support/knowledgebase/112830.aspx).
- 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.
- To take full advantage of Sophos Live Protection, which is enabled by default, we recommend also selecting the **Automatically send sample files to Sophos** option.
- Enable Malicious Traffic Detection, which detects communications between endpoint computers and command and control servers involved in botnet or other malware attacks. The **Detect malicious traffic** option is enabled by default for new installations of Sophos Enterprise Console 5.3 or later. If have upgraded from an earlier version of Sophos Enterprise Console, you need to enable this option to benefit from the feature.

  **Note**
  Malicious traffic detection is currently supported only on Windows 7 and later non-server operating systems. It requires Sophos Live Protection.

- 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.

For more information, see Sophos support knowledgebase article 114345 (http://www.sophos.com/en-us/support/knowledgebase/114345.aspx).

## 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 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. Sophos Live Protection is required by the Malicious Traffic Detection and Download Reputation features.
   - Make sure that the **Enable Live Protection for on-access scanning** and **Enable Live Protection for on-demand scanning** options are selected. 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.

- Select the **Automatically send sample files to Sophos** option. 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. When Live Protection is enabled, 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/en-us/support/knowledgebase/62637.aspx). 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.

3. 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 29) or Using scheduled scans (page 30).
   b) Select cleanup options for viruses/spyware.
4. 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** option in the scanning settings.
   c) Select cleanup options for suspicious files.
   d) As appropriate, authorize any files that are allowed to run.
5. Detect malicious and suspicious behavior, buffer overflows, and malicious traffic (behavior monitoring).
   These options monitor running processes continuously to determine if a program exhibits malicious or suspicious behavior. They are useful for stopping security flaws.
   a) Ensure that behavior monitoring for on-access scanning is enabled. It is enabled by default.
   b) Ensure that the **Detect malicious traffic** option is selected.
   c) Use the **Alert only** option to only detect suspicious behavior and buffer overflows. This option is enabled by default.
   d) Authorize any programs or files you want to continue to run in the future.
   e) 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/en-us/support/knowledgebase/50160.aspx).
6. 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/en-us/support/knowledgebase/13815.aspx).

7. Detect threats in web pages.

This option blocks sites that are known to host malicious content and scans downloads for malicious content.

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 **Content 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.

d) Ensure that file reputation checking is enabled.

**Note**
In addition, you can use the web control policy to control user web surfing by filtering the websites in the top 14 most inappropriate site categories. For information on how to set up a web control policy, see Recommended settings (page 24).

For more information about setting up anti-virus and HIPS policies, see the Sophos Enterprise Console help.

# 5 Setting up firewall policies

## 5.1 About the firewall policy

The firewall policy specifies how the firewall protects computers. Only named applications, or classes of applications are allowed to access the company network or internet.

**Note**
Sophos Client Firewall is not supported on server operating systems. For hardware and operating system requirements, see the system requirements page of the Sophos website (http://www.sophos.com/en-us/products/all-system-requirements).

**CAUTION**
You must configure the firewall policy before use. Deploying an unmodified default policy to a group via Sophos Enterprise Console will cause problems with network communications.

The default firewall policy is not intended to be deployed "as is" and is not adequate for normal use. This is a base for you to build up your own policy.

By default, the firewall is enabled and blocks all non-essential network traffic. Anything more than basic networking, for example, your email software, web browser and any network database access, will probably not function correctly with the default policy which blocks all non-essential connections. 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.

## 5.2 Planning firewall policies

Plan your firewall policies and what you want them to do before creating or editing firewall rules (global, application, or other).

When planning your firewall policies, you should take into account:

- Which computers should have Sophos Client Firewall.
- Whether a computer is a desktop or a laptop. You may want to set up dual location for laptops.
- Which location detection method you want to use, that is, DNS lookup or gateway MAC address detection.
- Network-wide systems and protocols.
- Remote connections.

Based on applications and network access rights required by different groups of users, decide how many firewall policies you will need to create. The policies would cover different applications, and vary in restrictiveness. Remember that multiple policies require multiple groups in Sophos Enterprise Console.

- You should not use just one Sophos Client Firewall policy. You would be forced to add rules for only one or two computers (for example, the administrator's workstation), but these rules would be present over the whole network. This is a security risk.

- Conversely, using large numbers of configurations will mean extra time spent on monitoring and maintenance.

### Network-wide systems and protocols

Take into account the services that your network relies upon. For example:

- DHCP
- DNS
- RIP
- NTP
- GRE

Rules exist in the default firewall configuration to govern most of these services. However, be aware of those that you should allow, and those that you don't need.

### Remote access to computers

If you use remote access software to monitor and fix computers, you must build rules into your configuration to enable you to work this way.

Identify the technologies that you use to access the computers on your network. For example:

- RDP
- VPN client/server
- SSH/SCP
- Terminal services
- Citrix

Check what sort of access is needed, and create your rules accordingly.

## 5.3 Recommended settings

When setting up your firewall policy, consider the following:

- When Sophos Client Firewall is installed, Windows Firewall 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 **Events > Firewall Events**.
- Review the rules created via the Event Viewer. An application may trigger multiple firewall events (different events for different actions performed by the application) but an application rule must cover all application actions. For example, an email client may trigger two different events when sending email and receiving email, but an application rule for that client must deal with both these actions.

- 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 whenever possible.
- Do not use the **Interactive** mode in a policy in which dual location is set up.
- Do not use the **Interactive** mode on large or medium-sized networks and in domain environments. The **Interactive** mode may be used to create firewall rules on very small networks (for example, up to 10 computers) in workgroup environments and on standalone computers.

# 5.4 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, on the **General** tab, under **Applied location**, 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.

# 5.5 How to roll out a firewall policy

Roll out a policy which allows you to monitor all traffic that is passing throughout your network. You will receive traffic reports in the Firewall Event Viewer. Use this information to set up a basic policy.

You should run a phased rollout of the Sophos Client Firewall across your network, that is, roll out Sophos Client Firewall to one group at a time. This will avoid flooding your network with traffic in the initial stages.

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

1. Deploy Sophos Client Firewall to a test group of computers, which is representative of the various roles in your network.
2. Configure a firewall policy to use the **Allow by default** mode to detect but not block common traffic, applications and processes, and assign the policy to the test group.
   a) Create a new firewall policy. In Sophos Enterprise Console, in the **Policies** pane, right-click **Firewall** and select **Create Policy**. Give this policy a name, and then double-click it.
   The **Firewall Policy** wizard appears.
   b) Choose either to use the wizard, by clicking **Next**, or to configure the policy manually, by clicking **Advanced firewall policy**.
      - Using the wizard: Click **Next**. Select **Single location** and click **Next**. Select **Monitor**, click **Next**, and then **Next** again, and then **Finish**.
      - Using the **Advanced firewall policy** option: In the **Firewall Policy** dialog box, next to **Primary location**, click **Configure**. On the **General** tab, set the working mode to **Allow by default**. Click **OK**, and then **OK** again.
   c) Assign the new firewall policy to the test group.
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 **Events > Firewall Events**.
4. Monitor firewall events and build up your policy for some time, for example, over a couple of weeks.
   a) Create rules from the Event Viewer. Right-click on an event to create a rule for it. For more information about creating firewall rules, see the Sophos Enterprise Console help.
   b) Check for any weaknesses in the policy (for example, giving too much access to some users).
   c) Where needs differ, subdivide the group and create extra policies and rules as needed.
5. Review the rules created via the Event Viewer. An application may trigger multiple firewall events (different events for different actions performed by the application) but an application rule must cover all application actions. For example, an email client may trigger two different events when sending email and receiving email, but an application rule for that client must deal with both these actions.
6. Split the rest of your network into manageable groups, representative of the various roles in your network, for example, sales workstations, IT administrator workstations, and so on.
7. Once you are satisfied that you have covered everything, for example, when you are no longer getting many new firewall events for which there are no rules, create policies from your rules

and assign them as required. If you have a significant number of computers on your network, we recommend that you deploy Sophos Client Firewall to one group at a time.

8. Once you've tested the rules, change the policy mode to **Block by default**; otherwise, computers will remain insecure.

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

**Note**
As an alternative to monitoring network traffic and creating rules using the Firewall Event Viewer, on a very small network or on single standalone computers running Windows 7 or earlier, you can install Sophos Client Firewall on a test computer and configure it in **Interactive** mode. Run as many applications used on your network as possible, including web browsers. Then import and edit the firewall configuration containing rules established by that process. For more information, see the Sophos Endpoint Security and Control 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 **Events > 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 an 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 **Events** > **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.

**Note**
Application Control can be configured to block CScript.exe that is used by Patch. If you use both Application Control and Patch, ensure that you do not block **Microsoft WSH CScript** in the **Programming/Scripting tool** category. By default, programming and scripting tools are allowed.

# 7 Setting up data control policies

## 7.1 Defining a 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.

## 7.2 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 Sophos Enterprise Console. You can access the Event Viewer by clicking **Events** > **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.

# 7.3 How to roll out a 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 16).

  **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 **Events > 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.

# 7.4 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/en-us/support/knowledgebase/63016.aspx).

| Applications | Data Control Scanning Actions |
|---|---|
| Web browsers | **Scanned:**<br>• File uploads<br>• Webmail attachments<br>• Microsoft SharePoint uploads<br>**Not scanned**<br>• Webmail message content<br>• Blog entries<br>• File downloads<br>**Note**<br>In a small number of cases, files may be scanned when downloaded. |
| Email clients | **Scanned**<br>• Email attachments<br>**Not scanned**<br>• Email message content<br>• Forwarded attachments<br>• Attachments made using the "Send" email option within applications (e.g. Windows Explorer and Microsoft Office)<br>• Attachments using the "E-mail this file" option within Windows Explorer<br>• Attachments copied from one email to another email<br>• Saved attachments<br>**Note**<br>In a small number of cases, files may be scanned when saved. |

| Applications | Data Control Scanning Actions |
| --- | --- |
| Instant messaging (IM) clients | **Scanned**<br>• File transfers<br><br>**Note**<br>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.<br><br>**Not scanned**<br>• IM message content<br>• Sent files |

# 8 Setting up device control policies

## 8.1 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 **Events** > **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/en-us/support/knowledgebase/63102.aspx).
- 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 Sophos Enterprise Console server to the computer through the network; therefore, once the network is blocked, it cannot be unblocked from Sophos Enterprise Console since the computer cannot accept additional configuration from the server.

## 8.2 How to roll out a 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 **Events > 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.

# 9 Setting up tamper protection policies

## 9.1 About the tamper protection policy

Tamper protection enables you to prevent users (local administrators with limited technical knowledge) from reconfiguring, disabling, or uninstalling Sophos security software. Users who do not know the tamper protection password cannot perform these operations.

**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 Recommended settings (page 4).

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 (such as Sophos Anti-Virus, Sophos Client Firewall, Sophos AutoUpdate, or Sophos Remote Management System) 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 **Events > Tamper Protection Events**.

## 9.2 About Enhanced Tamper Protection

Enhanced Tamper Protection builds on the functionality of Tamper Protection. If Enhanced Tamper Protection is enabled, the following actions are blocked for Sophos Anti-Virus, Sophos AutoUpdate, Sophos Management Communication System, Sophos Remote Management System and Sophos Endpoint Defense:

- Stopping services from the Services UI
- Killing services from the Task Manager UI
- Changing service configuration from the Services UI
- Stopping services/editing service configuration from the command line
- Uninstalling
- Reinstalling
- Killing processes from the Task Manager UI
- Deleting or modifying protected files or folders
- Deleting or modifying protected registry keys

**Important**
To enable Enhanced Tamper Protection, Tamper Protection must be enabled.

## 9.3 How to roll out a tamper protection policy

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

**Note**
If you enabled enhanced tamper protection during the installation, tamper protection will already be enabled.

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.

   **Important**
   If tamper protection is disabled, enhanced tamper protection will automatically be disabled.

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

# 10 Setting up patch policies

## 10.1 About the patch policy

The patch policy allows you to check that your computers have the most up-to-date security patches installed.

When setting up your patch policy, consider using the patch assessment Event Viewer to audit missing patches on your company's computers. It contains information about security patches and results of patch assessments. You can view patch status by computer, group, or threat after you have enabled patch assessment in the patch policy. You can access the Event Viewer by clicking **Events > Patch Assessment Events**.

**Note**
Patch uses CScript.exe which can be blocked using Application Control. If you use both Application Control and Patch, ensure that you do not block **Microsoft WSH CScript** in the **Programming/Scripting tool** category in the **Application control** policy. By default, programming and scripting tools are allowed by Application control.

## 10.2 How to roll out a patch policy

Initially, the "Default" patch policy is applied to all computers. Patch assessment is disabled in the default policy.

Once patch assessment is enabled, computers begin an assessment. This can take several minutes. Subsequent assessments occur at the interval set in policy, which is daily by default.

**Note**
If computers run an assessment before Enterprise Console has downloaded patch data from Sophos for the first time, the Patch Event viewer displays no results. The download can take several hours. To check if this has completed, see the **Patch updates** field in the **Patch Assessment - Event Viewer**.

We recommend that you introduce patch policy as follows:

1. Deploy the patch agent to computers using the Protect Computers Wizard. (On the **Select features** page of the wizard, select **Patch**.)

   **Note**
   You must reprotect computers by running the Protect Computers Wizard if they are already running Endpoint Security and Control but do not have the patch agent installed.

2. Enable patch assessments in your default patch policy.

   At this time, you have one patch policy for your entire network.
3. Use the patch assessment Event Viewer to view which computers are missing patches and which are up-to-date. You can access the Event Viewer by clicking **Events** > **Patch Assessment Events**.

**Note**
You must install missing patches on computers manually.

4. If you require the ability to enable or disable patch policy or assign different patch assessment intervals for various groups, create different policies for different groups.

For more information on setting up patch policy, see the Sophos Enterprise Console help.

# 11 Setting up web control policies

## 11.1 Recommended settings

There are two polices to choose from when configuring web control: Inappropriate Website Control and Full Web Control. The recommendations differ, depending on which policy you select. When setting up your web control policy, consider the following:

### Inappropriate Website Control

- Review the action for each website category, and make adjustments to suit your organization or group. To grant web access differently for various computer groups, create different policies for different groups. For example, there may be websites, such as Facebook, that you want to make available only to the human resources department.
- Plan a list of website exemptions prior to rolling out a policy. You can manually enter websites that you want to exclude from the policy using the **Website Exceptions** tab. For example, you may have a series of local web addresses that do not require filtering, or you may want to block websites within a category that is otherwise allowed.
- Use the web control Event Viewer to quickly filter events for investigation. You can access the Event Viewer by clicking **Events > Web Events**. You may want to adjust the website category settings, based on the actions displayed.

### Full Web Control

**Important**
You must have a Sophos Web Appliance or Security Management Appliance to use the Full Web Control policy.

- The Sophos Web Appliance Configuration Guide and the Security Management Appliance Configuration Guide contain general guidelines for setting up your appliance. The appliance provides a setup wizard to assist you in choosing the settings that are best for your organization.
- You may want to configure different policies for different types of users. See the Sophos Web Appliance online product documentation for details.

  The Sophos Web Appliance documentation is available at http://wsa.sophos.com/docs/wsa/.
- Prior to rolling out a policy, plan for any exceptions to the web control policy. For example, you can use the "Special Hours" feature to grant some or all access to certain websites outside of regular working hours, such as during the lunch hour. You can also create "Additional Polices" that only apply to certain users, and are exceptions to the Default Policy and the Special Hours policy.
- Consider what action (if any) that you want the Web Appliance to take if information for a website cannot be categorized. The check box **Block browsing if the website category cannot be determined** is **not** selected by default. This means that users are allowed to continue browsing if the categorization service fails. When the check box is selected, URLs that cannot be categorized are blocked until the service is restored.

For more information, see the Sophos Enterprise Console and Sophos Web Appliance documentation.

# 11.2 How to roll out a web control policy

First, decide which mode of web filtering to use: Inappropriate Website Control or Full Web Control. You must have a Sophos Web Appliance or Security Management Appliance to deploy the Full Web Control policy.

For more information on setting up a web control policy, see the Sophos Enterprise Console help.

## 11.2.1 How to roll out an inappropriate website control policy

This basic web control option includes 14 essential website categories. It is designed to protect users from visiting inappropriate websites. Consider the following when implementing a web control policy. See the Sophos Enterprise Console documentation for specific instructions.

1. Ensure that the web control policy is enabled.
2. If your organization has an acceptable use policy, you should tailor the settings accordingly, thus preventing users from visiting any sites that could be deemed inappropriate.
3. To grant access to websites differently for various computer groups, create a different policy for each group.
4. Think about which computer groups will be subject to web control, and what type of policy is suitable for each group of machines.
5. View the default action for each website category. If you prefer to apply a different action, select it from the drop-down list. Consider which categories you want to block users from visiting, which categories will be accessible, and which categories you want to warn users about visiting.
6. Determine which websites you want to exempt from filtering, and add them to the **Websites to Allow** list or **Websites to Block** list.

   **Note**
   If there are conflicting or overlapping entries in the 'Block' and 'Allow' lists, the entries in the Block list will always take precedence. For example, if the same IP address is included in the Block list and the Allow list, the website is blocked. Furthermore, if a domain is included in the Block list, but a subdomain of that same domain is included in the Allow list, the Allow entry is ignored, and the domain and all of its subdomains are blocked.

7. Use the web control Event Viewer to examine filtering results. You can access the Event Viewer by clicking **Events > Web Events**. Use the Event Viewer to see web events. You may want to make adjustments, based on these results.

For more information, see the Sophos Enterprise Console documentation.

## 11.2.2 How to roll out a Full Web Control policy

This mode uses a complete web policy. It enforces a comprehensive, full-featured web control policy, and provides complete reporting on web traffic. A Sophos Web Appliance or Security Management Appliance is required for this option.

1. Configure your Sophos Web Appliance or Security Management Appliance as described in the appliance documentation, ensuring that **Endpoint Web Control** is turned on.

2. Ensure that web control is enabled on the Sophos Enterprise Console.
3. If your organization has an acceptable use policy, you should tailor the settings accordingly, thus preventing users from visiting any sites that could be deemed inappropriate.
4. To grant access to websites differently for various groups of users, create a different policy for each set of users.
5. Consider which websites you want to control. Which categories do you want to prevent users from visiting? Which categories will be accessible? Which categories you want to warn users about visiting?
6. Determine which websites you want to exempt, and add them to the appliance's Local Site List.
7. With Full Web Control, you have the option of using Sophos LiveConnect. You can configure the appliance to use LiveConnect so that policy updates are distributed to users, and reporting data from user machines is uploaded, even when users are not connected from within the network.

For more information, see the Sophos Enterprise Console and Sophos Web Appliance documentation.

# 12 Setting up exploit prevention policies

## 12.1 Recommended settings

The exploit prevention policy specifies how the security software protects against ransomware and other forms of malware exploitation.

**Note**
By default all exploit prevention options are turned on.

We recommend that you use the default settings.

## 12.2 How to roll out an exploit prevention policy

Vulnerable applications are protected by default. You should be careful when excluding applications from exploit prevention. They will still be protected by CryptoGuard and Safe Browsing.

We recommend that you roll out an exploit prevention policy as follows:

1. All exploit prevention options are turned on by default. We recommend that you use the default settings. You should monitor any exploit prevention events for a period of time before altering the settings.
2. Use the Exploit Prevention Event Viewer to monitor any exploit prevention events. You can access the Event Viewer by clicking **Events > Exploit Prevention Events**.
3. Amend the exploit prevention policy based on your monitoring. For example you may want to exclude some applications or exploit events from exploit mitigation. For more information see the Sophos Enterprise Console help.

   **Important**
   For increased security, we recommend that you base the exclusion on the thumbprint of the exploit event rather than excluding the whole application.

   a) Create a new policy or amend the default policy.

   b) Check for any weaknesses in the policy.

   c) Where needs differ, subdivide the group and create extra policies as needed.
4. Assign your policies as required.

# 13 Scanning recommendations

The scanning options in the following sections are set within the anti-virus and HIPS policy. When setting scanning options, consider the following:

- Use default settings when possible.
- Set scanning in Sophos Enterprise Console versus on the computer itself when possible.
- Consider the role of the computer (e.g. desktop or server).

## Extensions

To access the extension options for on-access scanning, in the **Anti-Virus and HIPS Policy** dialog box, click **Configure** next to **Enable on-access scanning** and then go to the **Extensions** tab.

For scheduled scans, in the **Anti-Virus and HIPS Policy** dialog box, under **Scheduled scanning**, click **Extensions and Exclusions**.

- The **Scan all files** option is generally not needed nor 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.

## Other scanning options

To access other scanning options for on-access scanning, in the **Anti-Virus and HIPS Policy** dialog box, click **Configure** next to **Enable on-access scanning**.

For scheduled scans, in the **Anti-Virus and HIPS Policy** dialog box, under **Scheduled scanning**, select a scan and click **Edit**. In the **Scheduled scan settings** dialog box, click **Configure**.

- 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.

# 14 Using on-access scans

When using on-access scans, consider the following:

- Use default settings when possible.
- On-access scanning for **Read**, **Write** and **Rename** options are enabled by default for new software installations only. For software upgrades, you must enable them.
- 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/en-us/support/knowledgebase/12790.aspx).
- When you do not select on-access scanning, ensure that computers use scheduled scans. For more information, see Using scheduled scans (page 30).

**CAUTION**
Be aware that disabling on-access scanning increases security risk.

# 15 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.
- 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.

# 16 Using on-demand scans

When using on-demand scans, consider the following:

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

# 17 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.

# 18 Technical support

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

- Visit the Sophos Community at community.sophos.com/ and search for other users who are experiencing the same problem.
- Visit the Sophos support knowledge base at www.sophos.com/en-us/support.aspx.
- Download the product documentation at www.sophos.com/en-us/support/documentation.aspx.
- Open a ticket with our support team at https://secure2.sophos.com/support/contact-support/support-query.aspx.

# 19 Legal notices