Contents

Chapter 1- About Your Appliance...........................................................................................................................................1
  Sophos Web Appliance Features...................................................................................................................................1
  Sophos Management Appliance Features..........................................................................................................................2
  Common Features..................................................................................................................................................................2
Chapter 2- Getting Started......................................................................................................................................................3
  Appliance Hardware..............................................................................................................................................................3
  Virtual Appliances.................................................................................................................................................................15
  Network Deployment..............................................................................................................................................................16
  Understanding Mode and Model Differences..........................................................................................................................42
  Platforms and User Interface..................................................................................................................................................44
  Policy.....................................................................................................................................................................................47
  Updates..................................................................................................................................................................................52
  Getting Support....................................................................................................................................................................53
  Product Documentation...........................................................................................................................................................54
Chapter 3- Dashboard...............................................................................................................................................................55
Chapter 4- Configuration..........................................................................................................................................................59
  Accounts..................................................................................................................................................................................60
  Group Policy...........................................................................................................................................................................72
  Global Policy........................................................................................................................................................................100
  System................................................................................................................................................................................112
  Network...............................................................................................................................................................................146
Chapter 5- Reports.................................................................................................................................................................158
  Available Reports.................................................................................................................................................................158
  Modifying Reports.................................................................................................................................................................169
  Printing Reports...................................................................................................................................................................170
  Exporting Reports.................................................................................................................................................................171
  Options..................................................................................................................................................................................171
Chapter 6- Search.................................................................................................................................................................181
  Searching Recent Activity......................................................................................................................................................181
  Searching Sandstorm............................................................................................................................................................183
  Searching User Submissions................................................................................................................................................184
Chapter 7- System Status.........................................................................................................................................................188
  System Status on the Management Appliance..........................................................................................................................191
Chapter 8- Using Help............................................................................................................................................................192
  Searching the Documentation..............................................................................................................................................192
  Using the Table of Contents................................................................................................................................................192
  Sophos Support..................................................................................................................................................................192
  About................................................................................................................................................................................193
Appendix A- Configuring Ports................................................................................................................................................195
Appendix B- Configuring Your Browser................................................................................................................................197
  Adding the Sophos Root Certificate................................................................................................................................197
  Configuring Proxy Settings...............................................................................................................................................198
  Other Internet Explorer Settings.......................................................................................................................................200
  Other Firefox Settings........................................................................................................................................................201
Appendix C- Appliance Behavior and Troubleshooting..........................................................................................................202
  Network Deployment Troubleshooting.................................................................................................................................202
  Active Directory Troubleshooting...................................................................................................................................203
  eDirectory Troubleshooting..............................................................................................................................................206
  Grouped Appliance Troubleshooting................................................................................................................................208
  HTTPS Compatibility............................................................................................................................................................211
  Images Display as Gray.........................................................................................................................................................215

(2019/01/08)
<table>
<thead>
<tr>
<th>Appendix D- Interpreting Log Files</th>
<th>216</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appendix E- Copyrights and Trademarks</td>
<td>222</td>
</tr>
<tr>
<td>OpenLDAP Public License</td>
<td>224</td>
</tr>
<tr>
<td>Appendix F- Contacting Sophos</td>
<td>225</td>
</tr>
<tr>
<td>Appendix G- Glossary</td>
<td>226</td>
</tr>
</tbody>
</table>
Chapter 1

1 About Your Appliance

The Sophos Web Appliance and Sophos Management Appliance include a powerful, highly effective, and easy-to-use administrative web interface that provides configuration and reporting tools, automated software updates, and self-monitoring to minimize the administrator’s day-to-day involvement in web security and control maintenance. You can customize the appliances’ default URL-handling policy and message pages, and accept or reject end user requests for changes to the handling of blocked URLs submitted via an end user feedback system.

Organizations typically expend considerable resources and effort preventing virus, worm, and Trojan infections from entering their networks via email. These threats, as well as spyware, adware, and phishing scams are increasingly infiltrating organizations’ networks via web browsing.

Inappropriate web browsing by employees is also a significant legal liability and productivity concern for many organizations. The Sophos Web Appliance provides extensive URL categorization data that allows you to set acceptable web access policies for your organization that are highly customizable and enforceable. These policies can allow user access, warn users that they will be violating policy if they continue to a requested site, or block user access based on over fifty categories of URLs. In addition to your default acceptable web access policy, group-based exceptions are available as differentiated “Special Hours” policies. There is also the potential to create numerous additional policies that can be used as per-user or per-group exceptions to the default and Special Hours web access policies.

The web appliances use the proven Sophos Anti-Virus engine, regularly updated with the latest internet threats every 5 to 30 minutes by SophosLabs™, our global threat detection network. SophosLabs has more than 20 years’ experience in protecting businesses from known and emerging threats. URL categorization data is similarly updated every 5 to 30 minutes, and the enhanced categorization data is updated hourly.

The web appliance is easy to install, configure, and maintain.

1.1 Sophos Web Appliance Features

The web appliance is an enterprise solution for organizations of various sizes.

Fast, full-spectrum protection and control

The web appliance provides protection against all web-based threats, while controlling access to undesirable content. The web appliance:
• is a highly efficient unified scanner that guarantees accurate detection with low system impact and negligible latency.
• inspects and secures web traffic against spyware, viruses, adware, potentially unwanted applications, and other malicious threats.
• prevents access to known malicious websites, hidden malicious code, phishing sites, and undesirable content.
• provides extensive, regularly updated URL categorization data upon which customizable web access policies can be based.

1.2 Sophos Management Appliance Features

The management appliance works with multiple web appliances to provide:
• centralized management of up to 50 web appliances
• centralized policy configuration
• centralized reporting and activity searches
• a centralized dashboard that provides a status overview for any joined web appliances
• storage for as many as 2,000 users (on the SM2000) or 10,000 users (on the SM5000). Three years of reporting data is available.

1.3 Common Features

Easy to use
The appliances reduce administrative effort by providing quick access to relevant information. The appliances offer:
• an intuitive management console that enables optimal control with minimal time and effort.
• a unified security policy that eliminates the complexity of administering effective web security.
• powerful reports that deliver unprecedented insight on inbound and outbound web traffic.

Dependable
The appliances offer a complete infrastructure built to replace customers’ concerns about security with the assurance of protection. The appliances provide:
• dynamic threat response with instant protection against new web-based threats every 5 minutes.
• remote "heartbeat" monitoring that proactively ensures up-to-date protection and optimal hardware and software performance.
• industry-leading 24/7/365 live support directly from Sophos.
• on-demand remote assistance that provides easy, direct access to Sophos Technical Support.
• a robust hardware platform designed specifically to Sophos specifications.
• a hardened Linux operating system optimized for Sophos software.
2 Getting Started

The Sophos Web Appliance is designed to function as a web proxy that provides HTTP security at the gateway. Potentially risky content is scanned for various forms of malware. URL requests are compared to the Sophos site list, in which sites are assigned a risk class and a site category. Access to sites can be blocked on the basis of degree of risk or by site category.

Instead of blocking access to URLs that violate your organization’s acceptable browsing policy, you can, as the administrator, allow access or allow access after a warning is displayed to users, which they can acknowledge and continue or cancel the request to view. User access to such URLs is recorded. Also, as the administrator, you can extend or override the Sophos site list by adding URLs to a local site list. In the case of sites already in the Sophos site list, you can override the default handling by changing the risk class or site category.

Only approved and scanned content is passed to users. It may be cached to increase performance. If users attempt to access blocked URLs or download blocked content, message pages are displayed, informing users of the problem and optionally providing a user-feedback form that allows them to request changes to the handling of the blocked URL or file type. Similarly, requests for large files can cause the web appliance to display a patience page (if you have chosen to enable this option), advising the user that downloading and scanning is in progress and will take some time.

This section introduces the role of the Sophos Web Appliance and the Sophos Management Appliance in your network. It describes the compatible platforms and the administrative web interface. It provides an overview of the appliance’s major capabilities and configurable behavior and a general description of the appliances’ software and security data updating features. Finally, this section provides information on contacting Sophos Technical Support.

2.1 Appliance Hardware

There are certain hardware differences between the various appliance models, which are summarized in the following table or discussed in the sections below.

<table>
<thead>
<tr>
<th>Feature</th>
<th>WS100</th>
<th>WS500</th>
<th>WS1000</th>
<th>WS1100</th>
<th>WS5000</th>
<th>SM2000</th>
<th>SM5000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processors</td>
<td>dual-core, light capacity</td>
<td>dual-core, medium-capacity</td>
<td>dual-core, high-capacity</td>
<td>quad-core, high-capacity</td>
<td>quad-core, high-capacity</td>
<td>quad-core, high-capacity</td>
<td>quad-core, high-capacity</td>
</tr>
<tr>
<td>Memory (RAM)</td>
<td>2 GB</td>
<td>2 GB</td>
<td>4 GB</td>
<td>8 GB</td>
<td>16 GB</td>
<td>8 GB</td>
<td>8 GB</td>
</tr>
<tr>
<td>Bridge card</td>
<td>No</td>
<td>Optional</td>
<td>Yes</td>
<td>Optional</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Replaceable Power Supply</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Replaceable Hard Drives</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>4</td>
<td>No</td>
<td>4</td>
</tr>
</tbody>
</table>

Note
Operating in bridged mode is only possible on a web appliance with a bridge card installed.
The Sophos Web Appliance is a high-performance appliance designed to handle web proxy access for organizations of various sizes. The web appliance is scalable to much larger numbers of users by grouping multiple web appliances by joining them to a single Sophos Management Appliance. The appliances raise alerts via the administrative web interface and via email if any hardware components are not functioning optimally.

This section describes the front and back panel LEDs, powering the appliances down gracefully, and hardware-related alerts. The management appliance provides centralized policy configuration and centralized reporting for grouped appliances, thus minimizing system administration work while providing organization-wide information without sacrificing security or customizable web use control.

The appliances have a number of ways to alert you if there is a problem with one of their hardware components. In addition to status indicators in the administrative web interface and alerts sent via email, the appliances have LED indicators and audible alarms.

Front Panel LEDs

Indicators on the front of each appliance provide status information and warnings. The arrangement of the front panel LEDs are the same for the WS100, WS500, WS1000, WS1100, and the SM2000. The indicators on the front of the SM5000 are slightly different, and the indicators on the front of the WS5000 are also slightly different. Each variant is shown in the following diagrams.

<table>
<thead>
<tr>
<th>WS100</th>
<th>WS500, WS1000, WS1100, &amp; SM2000</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Front Panel LEDs for WS100" /></td>
<td><img src="image2" alt="Front Panel LEDs for WS500, WS1000, WS1100, &amp; SM2000" /></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SM5000</th>
<th>WS500</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image3" alt="Front Panel LEDs for SM5000" /></td>
<td><img src="image4" alt="Front Panel LEDs for WS5000" /></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Key</th>
<th>LED</th>
<th>Color</th>
<th>State</th>
<th>Indicates</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Temp. Sensor</td>
<td>Red</td>
<td>On</td>
<td>System Overheated</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Off</td>
<td>System Normal</td>
</tr>
<tr>
<td>3</td>
<td>Unit ID LED (SM5000 only)</td>
<td>Blue</td>
<td>Off</td>
<td>Shows rack location front and back</td>
</tr>
<tr>
<td>4</td>
<td>NIC1 (config)</td>
<td>Green</td>
<td>On</td>
<td>Linked</td>
</tr>
</tbody>
</table>
### Front Panel LEDs

The front panel LEDs are on the upper-right corner of the front panel, to the left of the reset and power buttons (and to the right of the Unit ID button on the SM5000).

**Important** Sophos strongly suggests that you use the software shutdown and restart options as documented on the System Status page. Although a quick press and release of the appliance’s power button will perform an elegant shutdown, if the power button is held down for four seconds or more, an inelegant, immediate shutdown is performed. Also, the reset button on the appliance always triggers an inelegant, immediate restart, so again the software option is preferred. *Using the appliance’s power and reset buttons may lead to file corruption and data loss.*

### Rear Panel LEDs

Indicators on the rear of each appliance provide status information and warnings. The arrangement of the rear panel LEDs depend upon whether the appliance is configured with a bridge card. There is always a bridge card in a WS1000. Bridge cards are optional for the WS500 and WS1100. There is never a bridge card in a WS100, SM2000, or SM5000.

**For appliances with no bridge card:**

<table>
<thead>
<tr>
<th>Key</th>
<th>LED</th>
<th>Color</th>
<th>State</th>
<th>Indicates</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Key</td>
<td>LED</td>
<td>Color</td>
<td>State</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Blink</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Off</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>NIC2 (non-bridged only)</td>
<td>Green</td>
<td>On</td>
<td>Linked</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Blink</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Off</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>HDD LED</td>
<td>Amber</td>
<td>Blink</td>
<td>HDD Activity</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Off</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Power LED</td>
<td>Green</td>
<td>On</td>
<td>System On</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Off</td>
<td></td>
</tr>
</tbody>
</table>
There are two RJ45 network ports along the bottom of the appliance to the right of the middle:

- The **Config** port
  
  This is the port to which you connect your laptop or PC to run the setup wizard.

- The **Network** port
  
  This is the port to which you make your LAN connection after the setup wizard has been completed.

The two LEDs at the top of these ports indicate the following:

<table>
<thead>
<tr>
<th>LED Position</th>
<th>Color</th>
<th>Indicates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Left</td>
<td>Green</td>
<td>100 Mbps</td>
</tr>
<tr>
<td>Left</td>
<td>Amber</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>Right</td>
<td>Blinking Yellow</td>
<td>Port active</td>
</tr>
</tbody>
</table>

For appliances with a bridge card:

There is one RJ45 network port along the bottom of the appliance to the right of the middle, the **Configuration** port

This is the port to which you connect your laptop or PC to run the setup wizard.

The two LEDs at the top of this port indicate the following:

<table>
<thead>
<tr>
<th>LED Position</th>
<th>Color</th>
<th>Indicates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Left</td>
<td>Green</td>
<td>100 Mbps</td>
</tr>
<tr>
<td>Left</td>
<td>Amber</td>
<td>1 Gbps</td>
</tr>
</tbody>
</table>
There is also a group of six LEDs to the left of the **WAN** and **LAN** ports on the bridge card, which is located in the upper right corner on the back of the appliance. The LEDs are arranged in two columns of three lights, with the left and right columns being indicators for the LAN and WAN connections, respectively. The rows of LEDs are interpreted as follows:

- **Bypass**: If all of the top four indicator lights are on, the appliance is in bypass mode.
  - **1000 (top)**: On indicates a 1000Mbps connection is established; blinking shows traffic; off indicates no connection.
  - **100 (middle)**: On indicates a 100Mbps connection is established; blinking shows traffic; off indicates no connection.
- **Act/Link (bottom)**: On indicates a connection at any speed is established; blinking shows traffic; off indicates no connection.

### Hardware Alerts

Depending on the severity of the issue, the appliances will raise an alert in the administrative web interface or via email, or both. Alerts advise that devices are not working normally or draw attention to potential problems. In most cases, the alert will instruct you to contact Sophos Technical Support.

### Powering Down the Appliances Gracefully

Power down the appliance gracefully by either pressing the power button briefly, or by clicking **Shutdown** on the **System Status** page. The appliance will safely shut down its software, and the fans will stop. Remove the power cord before servicing the unit.

**Note**

You can also power down by holding the power button for four or more seconds, which will force an immediate shutdown of the appliance; however, this may cause a corruption of the file system. Avoid immediate shutdown except in cases when graceful shutdown is not possible.

### 2.1.1 Replacing an SM5000 or WS5000 Hard Drive

The SM5000 and WS5000 have four hot-swappable redundant SCSI hard disk drives in a RAID 10 configuration. If a single hard drive fails, the other disk in the RAID mirror takes over, and the appliance continues to function normally. The failed drive can be removed and a replacement drive installed without removing these appliances from the rack, powering down or even exiting the administrative web interface. The appliance automatically detects the removal of a failed or defective drive and the installation of its replacement. After replacement, the RAID controller automatically begins rebuilding the new drive.
SM5000, front view showing the four hard disk drive bays

Hardware Configuration

On the SM5000 and WS5000, the disks are mirrored using RAID 10, so only one disk can be replaced or not be working at a time.

Failure Identification

Remove the front bezel to expose the disk drives. On a failed disk drive, the red LED on the front of the drive is illuminated (the bottom LED of the two drive-specific LEDs) and the appliance’s audible alarm is sounding.

Static-Sensitive Devices

**CAUTION**

Electrostatic discharge (ESD) can damage electronic components. To prevent damage to any printed circuit boards, it is important to handle them very carefully. The following measures are generally sufficient to protect your equipment from ESD damage.

- Be sure that the appliance chassis is properly grounded through the AC power cord or enclosure frame.
- Touch a grounded metal object before removing the drive from the antistatic bag.
- Put on the grounding wrist strap, handle the drive by its edges only, and do not touch components on the bottom.
Single Hard Drive Replacement Procedure

As the disks are mirrored using RAID 10, only one disk can be replaced or not be working at a time.

**CAUTION**
Disk drives are static-sensitive devices. Please make proper use of the wrist strap included in the disk field-replaceable unit (FRU) ship kit.

**CAUTION**
Removal of the other drive during this procedure or during the rebuild of the RAID 10 mirror will result in system failure.

1. Press the colored release button beside the drive’s LEDs on the failed drive to unlatch the handle.

2. Swing the handle fully out to disengage the drive.

3. Slide the drive halfway out of the drive bay and wait for it to spin down. Allow 10-20 seconds before removing the drive from the drive bay.

4. While the system is running, insert the replacement disk in the empty slot. Insert the replacement drive into the disk bay and slide the disk straight to the back of the bay.
5. Swing the handle in toward the appliance. Continue pushing the handle in until you feel it lock in place.

6. Press firmly on the both the left and right edges of the drive with both thumbs. Applying this pressure ensures that the drive is fully engaged, even if no movement of the drive is felt.

7. After the failed disk is replaced, the green and red LEDs on the new disk start to blink and the audible alarm is silenced, indicating that the mirror is rebuilding. Once the rebuild is complete, the red LED goes off. The front bezel can then be replaced.

2.1.2 Replacing an SM5000 Power Supply

The SM5000 has two hot-swappable redundant power supplies. If a single power supply fails, the redundant feature allows the other module to take over the full load, and the system runs without interruption. The failed power supply can be removed and a replacement power supply installed without removing the SM5000 from the rack, powering down, or even exiting the SM5000’s administrative web interface.

Hardware Configuration

On the SM5000, the two power supplies are located on the left side of the rear of the appliance.

In normal operation, the "Power Indicator" LED on the front panel is green.
as are the "Power Supply Status" LEDs on the back of the SM5000 for each power supply, which are shown in the graphics below.

Failure Identification

Case 1: If either of the two power supplies completely fails, the "Power Indicator" LED on the front panel turns yellow, and an alarm sounds until the power supply is replaced. On the back of the unit, the "Power Supply Status" LED for the unit that has failed is either off or yellow. This is the power supply to replace.

Case 2: If either of the two power supplies partially fails, the "Power Indicator" LED on the front panel is green and no alarm sounds. On the back of the unit, the "Power Supply Status" LED for the unit that has partially failed is yellow. This is the power supply to replace.

Static-Sensitive Devices

CAUTION
Electrostatic discharge (ESD) can damage electronic components. To prevent damage to any printed circuit boards, it is important to handle them very carefully. The following measures are generally sufficient to protect your equipment from ESD damage.

• Be sure that the appliance chassis is properly grounded through the AC power cord or enclosure frame.
• Touch a grounded metal object before removing the power supply from the anti-static bag.
• Put on the grounding wrist strap, handle the power supply by its edges only, and do not touch components on the bottom.

Single Power Supply Replacement

1. Ensure that the power cord is unplugged from the failed power supply module. Then, while holding onto the handle, press the green locking tab on the bottom right of the power supply in toward the handle. This will disengage the power supply.
2. Pull the power supply module straight out. Check to make sure that the replacement power supply module is the same type as the one previously removed.

3. Carefully push the replacement power supply module straight into the appliance until you hear the release tab click into place.

4. Plug the AC power cord back into the new power supply module. The "Power Supply Status" LED on the new module should now be green.

2.1.3 Replacing a WS5000 Power Supply

The WS5000 has two hot-swappable redundant power supplies. If a single power supply fails, the redundant feature allows the other module to take over the full load, and the system runs without interruption. The failed power supply can be removed and a replacement power supply installed without removing the WS5000 from the rack, powering down, or exiting the WS5000’s administrative web interface.
Hardware Configuration

On the WS5000, the two power supplies are located on the left side of the rear of the appliance. In normal operation, the "Power Indicator" LED on the front panel is green,
as are the "Power Supply Status" LEDs on the back of the WS5000 for each power supply, which are shown in the graphics below.

![LEDs Diagram](image)

Failure Identification

**Case 1**: If either of the two power supplies completely fails, the "Power Indicator" LED on the front panel turns yellow, and an alarm sounds until the power supply is replaced. On the back of the unit, the "Power Supply Status" LED for the unit that has failed is either off or yellow. This is the power supply to replace.

**Case 2**: If either of the two power supplies partially fails, the "Power Indicator" LED on the front panel is green and no alarm sounds. On the back of the unit, the "Power Supply Status" LED for the unit that has partially failed is yellow. This is the power supply to replace.

Static-Sensitive Devices

**CAUTION**
Electrostatic discharge (ESD) can damage electronic components. To prevent damage to any printed circuit boards, it is important to handle them very carefully. The following measures are generally sufficient to protect your equipment from ESD damage.

- Be sure that the appliance chassis is properly grounded through the AC power cord or enclosure frame.
- Touch a grounded metal object before removing the power supply from the anti-static bag.
- Put on the grounding wrist strap, handle the power supply by its edges only, and do not touch components on the bottom.
Single Power Supply Replacement

1. Ensure that the power cord is unplugged from the failed power supply module. Then, while holding onto the handle, press the red locking tab on the bottom right of the power supply in toward the handle. This will disengage the power supply.

2. Pull the power supply module straight out. Check to make sure that the replacement power supply module is the same type as the one previously removed.

3. Carefully push the replacement power supply module straight into the appliance until you hear the release tab click into place.

4. Plug the AC power cord back into the new power supply module. The "Power Supply Status" LED on the new module should now be green.
2.2 Virtual Appliances

As an alternative to the hardware-based version of the Sophos Web Appliance, you can deploy appliances as virtual machines using VMware. These appliances can be grouped with other virtual appliances or with hardware-based appliances. Once deployed, they operate in the same way as a hardware-based appliance.

Sophos virtual appliances provide a cost-effective web-filtering solution that is easy to set up. Virtual appliances occupy less rack space, are energy-efficient, and require less hardware.

To learn more about configuring a virtual web appliance, see the Sophos Virtual Web Appliance Setup Guide or the Sophos Virtual Management Appliance Setup Guide.

Note
Virtual appliances do not support Bridged Deployment, which requires a bridge card.

Related concepts
Understanding Mode and Model Differences (page 42)
Grouping Web Appliances (page 37)

2.2.1 Replacing Hardware Appliances with Virtual Appliances

At some point, you may decide to replace one or more of your hardware-based appliances. Replacing either a web appliance or management appliance with a virtual appliance should be done by following the steps in the order described below.

Note
These procedures only cover the replacement of existing hardware-based appliances with virtual appliances. If, instead, you want to add virtual appliances to use in conjunction with your existing hardware-based appliances, see the instructions in “Grouping Web Appliances” and “Central Management”. Virtual appliances integrate seamlessly with hardware-based appliances as well as other virtual appliances.

Replacing a Stand-Alone Web Appliance

If you have a single hardware-based Sophos Web Appliance that you want to replace with a virtual web appliance:

1. Configure the virtual appliance according to the instructions in the Virtual Web Appliance Setup Guide. Take care when configuring the network settings to assign a network address that is different from the hardware-based appliance it is replacing.

2. If your hardware appliance is not configured to perform automated backups, on the Configuration > System > Backup page, click Download Now. Or, if automated backups are configured, transfer the backed up archive file from the FTP site to the system on which you will be performing the restoration.

3. On the virtual appliance, select Configuration > System > Restore. Follow the instructions in Restoring a Backup.
Note
If your hardware-based appliance was configured to use Web Cache Communication Protocol, you must reconfigure those settings manually on the virtual appliance. WCCP settings cannot be restored from a backup.

4. When restoration is complete, power off and decommission the hardware-based appliance.

Replacing a Management Appliance

If you have a hardware-based Sophos Management Appliance that you want to replace with a virtual management appliance:

1. Configure the virtual appliance according to the instructions in the Virtual Management Appliance Setup Guide. Take care when configuring the network settings to assign a network address that is different from the hardware-based appliance it is replacing.

2. Join the newly configured management appliance to a functioning web appliance in your deployment (not the hardware-based management appliance) and copy its configuration data to the virtual management appliance. On the management appliance, ensure that these check boxes are selected: Allow Web Appliances to join this Management Appliance and Copy configuration and policy data from the first web appliance to join. For complete instructions, see On a Stand-Alone Web Appliance: Joining a Management Appliance.

3. When the join is complete, power off and decommission the hardware-based management appliance.

Related concepts
Central Management (page 140)

Related tasks
Backup (page 119)
Restore (page 122)
Configuring WCCP (page 152)

2.3 Network Deployment

You can deploy the Sophos Web Appliance in a variety of configurations, depending on the requirements of your organization and your existing network architecture.

Basic Deployment Options

Three basic network deployments are possible for the Sophos Web Appliance:

- **Explicit Deployment**: All client web browsers are explicitly configured to use the appliance, although this can be done centrally by using distributed Active Directory Group Policy Objects (GPO). Explicit Deployment also supports FTP over HTTP.

- **Transparent Deployment**: The firewall or router is configured to redirect port 80 and port 443 traffic through the web appliance. In this mode, web traffic filtering is transparent to users, who only see evidence of the web appliance if they attempt to connect to certain URLs and are presented with a notification page.
**Bridged Deployment:** All outbound network traffic is routed through the web appliance’s bridge card, but only port 80 and port 443 traffic is examined. This deployment requires the optional bridge card included with some appliance models. With a Bridged Deployment, network traffic continues to flow in the event of an appliance failure.

**Alternative Deployment Options**

There are three additional deployments that allow the web appliance to work with some common network topologies. You may want to use one of the following, depending on the structure of your existing network.

- **Bypass for Internal Servers:** Allows clients to access specific internal servers directly. This is recommended for use with Explicit Deployment.
- **Use with an Existing Cache:** Allows the web appliance to work in conjunction with a pre-existing investment in a web-caching server in any one of the three basic network deployments (Explicit, Transparent, or Bridged).
- **Use with an ISA/TMG Server:** Allows the web appliance to work with a downstream or upstream Microsoft Internet Security and Acceleration (ISA) or Microsoft Forefront Threat Management Gateway (TMG) Server in any one of the three basic network deployments (Explicit, Transparent, or Bridged).

**Network Deployment Recommendations**

It may be necessary to make additional adjustments to accommodate the requirements of your network.

**Important**

If Active Directory integration is not enabled, the web appliance allows connections from any user or computer that can access it. This means that it could allow people from outside of your organization to use your web appliance as a proxy, consuming your bandwidth and creating traffic that appears to come from your organization. Sophos strongly advises that you take the following steps to prevent this:

1. Configure your firewall to prevent inbound connections to the web appliance from outside your network. The web appliance does not require that any inbound ports be open for external traffic.
2. Configure the web appliance to accept requests only from your own network. To do this:
   a) Select **Configuration > Group Policy > Default Groups**.
   b) Create a custom user group consisting of all your internal subnets and add this group to the **Selected groups** list.
   c) Select the **Only the users/groups selected below** option, and click **Apply**.

Configure your firewall to allow email with attachments from the web appliance to wsasupport@sophos.com. This is necessary information for Sophos, which uses system status snapshots that you submit as email attachments to ensure that your web appliance is operating within acceptable thresholds.
Network Deployments Comparison Table

The following table presents the key characteristics of each basic supported deployment scenario. For details of each, see the sections that follow.

<table>
<thead>
<tr>
<th></th>
<th>Explicit Deployment</th>
<th>Transparent Deployment</th>
<th>Bridged Deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCCP Integration</td>
<td>No</td>
<td>Yes</td>
<td>n/a</td>
</tr>
<tr>
<td>web appliance Traffic Performance</td>
<td>Only carries web traffic</td>
<td>Only carries web traffic</td>
<td>Carries all outbound traffic</td>
</tr>
<tr>
<td>Network Configuration</td>
<td>Configure all clients</td>
<td>Configure firewall or router</td>
<td>Configure only web appliance</td>
</tr>
<tr>
<td>Post-Failure Reconfiguration</td>
<td>Configure all clients</td>
<td>Configure the firewall or router</td>
<td>Power down web appliance</td>
</tr>
</tbody>
</table>

**Note**

If you use the Transparent or Bridged deployment, see Switching from Transparent Mode to Explicit Mode or Switching from Bridged Mode to Explicit Mode to learn about making the transition to Explicit Deployment.

**Related tasks**

- Configuring Authentication (page 132)
- Hostname and Other Network Settings (page 150)
- Configuring the Network Interface (page 146)
- Load Balancing with the Management Appliance (page 155)

### 2.3.1 Explicit Deployment

This deployment involves explicitly configuring all client web browsers to use the web appliance, although you can also do this centrally by using distributed Active Directory Group Policy Objects (GPO).

- Inspects HTTP, HTTPS, and FTP over HTTP traffic.
- All clients require configuration (may be done centrally; see the “Configuration” section below).
- If the deployment fails, all clients must be reconfigured (may be done centrally; see the “Configuration” section below).

**Operation**
• Users’
  HTTP, HTTPS, and FTP over HTTP requests are passed to the web appliance.

• The web appliance
  assesses URLs, blocks disallowed requests, checks if allowed URL requests are currently cached, and passes URL requests that are not cached through the firewall to retrieve them from the internet.

Note
Port 80, port 443, port 20, and port 21 requests from users are blocked at the firewall. URLs are only accepted by the firewall if they are from the web appliance.
Sophos Web Appliance

- The web appliance receives any new pages or files and caches them; it passes the pages or files of allowed requests back to the users.

- The users receive only safe and allowed pages and files or a notification page.

Configuration

1. Connect your organization’s LAN to the web appliance’s LAN port.
2. Configure each user’s web browser to use the web appliance via port 8080 as their web proxy for HTTP, HTTPS, and FTP. (Ports 3128 and 8081 are also supported, but their use is only suggested if the web appliance is replacing a previous proxy configuration that used one of these ports.)

Note
For information about adding support for HTTPS applications that use non-standard ports, see “Using the Local Site List Editor” in the Group Policy section of the documentation.

Note
Configuring all users’ browsers to use the web appliance as a web proxy can be done centrally in Windows networks by using any of the methods described in the Sophos Web Appliance: Configuring your network for Explicit Deployment Knowledgebase article, which also includes links to the following:

- Creating, Testing, and Deploying a proxy.pac File
- Publishing Proxy Information as a wpad.dat File
- Creating a GPO
3. In the web appliance’s administrative web interface, on the Configuration > Network > Network Interface page, set the Deployment Mode to Explicit proxy.

Related concepts
Configuring Your Browser (page 197)
This section contains instructions for configuring your browser to use the web appliance web proxy server.

Related tasks
Using the Local Site List Editor (page 97)
Specifying an Upstream Proxy (page 151)
Bypassing for Internal Servers (page 30)
Upstream ISA/TMG Server Deployment (page 33)

Related information
Windows Server Group Policy

Downstream ISA/TMG Server Deployment

This option, which uses either a Microsoft Internet Security and Acceleration (ISA) server or a Microsoft Forefront Threat Management Gateway (TMG) server, is based on the Explicit
Deployment. This deployment is different in that it includes an ISA/TMG server (and optionally an Active Directory server) between users and the web appliance.

- Allows the web appliance to work with an ISA/TMG Server.
- If the Sophos ISA/TMG plug-in is installed, and an Active Directory server is on the network side of the ISA or TMG server, then clients (users) can be seen as usernames.
- Allows you to use multiple web appliances in a simple load-balancing deployment.
- If the Sophos ISA/TMG plug-in is not installed, all traffic will be identified as coming from one user: the ISA/TMG server.
- If the Sophos ISA/TMG plug-in is not installed or an Active Directory server is not on the network side of the ISA/TMG server, then clients (users) will appear as IP addresses only.
- Does not support individual user opt-out, although with the ISA/TMG plug-in installed custom policy can be applied to an individual user or group.

**Operation**

- Users’ HTTP and HTTPS requests are passed through an ISA/TMG server that uses NTLM or IWA Authentication.
- The ISA/TMG server
Sophos Web Appliance

• The web appliance assesses the URL.
• The web appliance blocks disallowed requests, checks if allowed URL requests are currently cached, and passes URL requests that are not cached through to the firewall.

Note
Port 80 and 443 requests from users are blocked at the firewall, which retrieves the URL’s material from the internet; URLs are only accepted by the firewall if they are from the web appliance.

• The web appliance receives new pages or files, caches them, and passes the page or file on to the users.
• The users receive only safe and allowed pages and files or a notification page.

Note
If the Sophos ISA/TMG plug-in is installed, clients (users) are identified individually; otherwise, all traffic is identified as coming from one user: the ISA/TMG server.
If the Sophos ISA/TMG plug-in is installed, and an Active Directory server is on the network side of the ISA/TMG server, then clients (users) can be seen as usernames; if the Active Directory server is not appropriately located, clients (users) appear only as IP addresses in reports and user activity logs.

The ISA/TMG plug-in can be downloaded from the Configuration > Network > Hostname page. The ISA/TMG plug-in is compatible with Microsoft ISA Server 2004 and 2006, and Microsoft Forefront TMG 2010.

**Configuration**

**Important**
The web appliance may not catch malware stored in the ISA/TMG server’s cache. To avoid this risk, be sure to clear the ISA/TMG cache prior to enabling this network deployment.

Follow the configuration instructions for the Explicit Deployment scenario, but with the following differences:

- Ensure that your ISA/TMG server is between the clients and your web appliance.
- Ensure that your ISA/TMG server is configured to pass traffic through the web appliance if it is configured in an Explicit Deployment.
- Ensure that your Active Directory server, if you are using one, is located on the network side, between your clients (users) and your ISA/TMG server. The ISA/TMG server must also be configured to allow communications between your web appliance and your Active Directory server.

**Note**
web appliance policy will be applied to users authenticated by the Active Directory server using the pre-Windows 2000 format `DOMAIN\username` only.

- If the ISA/TMG plug-in is installed, enter the IP address of the downstream ISA/TMG server in the Accept authentication from downstream ISA/TMG servers section on the Configuration > Network > Hostname page.
A simple way to set up load balancing amongst multiple web appliances is to set up a DNS round robin scheme. If you do this, you should disable DNS caching because Windows DNS caching can mask the round robin effect. To disable Windows DNS caching, see the Microsoft Support article [http://support.microsoft.com/kb/318803](http://support.microsoft.com/kb/318803). You must ensure that you have a firewall with network address translation (NAT), but not an ISA or TMG server in firewall mode, between the web appliances and the internet. This firewall must be configured to present a single IP for the web appliances to the sites on the internet. The NAT, or IP masquerading, prevents sites that check and record the IP address of visitors in cookies from encountering multiple IP addresses.

Explaining how to configure an ISA/TMG Server is beyond the scope of this documentation. For details on ISA/TMG Server configuration, see the [Microsoft ISA Server Deployment](http://support.microsoft.com/kb/318803) page or the [Microsoft Forefront TMG Deployment](http://support.microsoft.com/kb/318803) page.

**Related tasks**
- [Existing Cache Deployment](http://support.microsoft.com/kb/318803) (page 32)

**Related information**
- Disabling Client-Side DNS Caching
- Microsoft ISA Server Deployment
- Microsoft Forefront TMG Deployment

### 2.3.2 Transparent Deployment

This deployment involves configuring the firewall or router to route all port 80 and port 443 traffic to the web appliance. In this mode, web traffic filtering is transparent to users. Unlike Explicit Deployment, you are not required to configure end user browsers.

- Inspects HTTP and HTTPS traffic.
- Only the firewall and/or the router requires configuration.
- If it fails, only the firewall and/or the router must be reconfigured.

**Operation**
• Users
  make HTTP/HTTPS requests from their clients that are sent out to the LAN.

• The router
  receives all network traffic and bounces all HTTP/HTTPS requests to the web appliance.

• The web appliance
  assesses URLs, blocks disallowed requests, checks if allowed URL requests are currently cached, and passes URL requests that are not cached out to the LAN.

• The router
  passes all HTTP/HTTPS requests from the web appliance out through the firewall
to retrieve the URLs from the internet.
receives the new pages or files and caches them; it passes the pages or files of allowed requests back to the users.

- The users receive only safe and allowed pages and files or a notification page.

Configuration
1. Connect the web appliance’s LAN port to your organization’s LAN.
2. In the web appliance’s administrative web interface, on the Configuration > Network > Network Interface page, set the Deployment mode to Transparent.
3. Configure your router so that it redirects all port 80 traffic to port 80 and port 443 traffic to port 443 on the web appliance. In this case, the destination of each packet remains unaltered, but the packets are sent by the router to the web appliance. Traffic on port 80 and 443 from the web appliance should be passed to the firewall. All other port traffic is passed as usual.

Note
With Active Directory enabled in Transparent mode, a Windows issue causes Internet Explorer to be repeatedly prompted for authentication. When deploying in Transparent mode, all workstations must be able to resolve the hostname of the web appliance into a FQDN (for instance http://ws1000 must resolve to http://ws1000.example.com). For more information, please see http://support.microsoft.com/kb/303650. Firefox users may need to type their password repeatedly unless browser settings are reconfigured.

Related tasks
Configuring Firefox for Active Directory in Transparent mode or Bridged mode (page 201)
Configuring WCCP (page 152)

Switching from Transparent Mode to Explicit Mode

This page describes the steps required to make the transition from a Transparent Deployment to an Explicit Deployment.

To transition from a Transparent to an Explicit deployment:
1. Ensure the web appliance’s LAN port is connected to an area of your network that is accessible to your client systems. Also ensure that your router or firewall does not redirect any traffic to your web appliance.
2. On the Configuration > Network > Network Interface page, change the Deployment mode from Transparent to Explicit proxy.
3. Configure each user’s web browser to use the web appliance via port 8080 as their web proxy for HTTP, HTTPS, and FTP. (Ports 3128 and 8081 are also supported, but their use is only suggested if the web appliance is replacing a previous proxy configuration that used one of these ports.)

Note
To add support for HTTPS applications that use non-standard ports, see Add Local Classification.
Note
Configuring all users’ browsers to use the web appliance as a web proxy can be done centrally in Windows networks by using one of several methods. See the Sophos Knowledgebase pages for instructions on how to do this by:

- Creating, Testing, and Deploying a proxy.pac File
- Publishing Proxy Info as a wpad.dat File
- Creating a GPO

2.3.3 Bridged Deployment

This deployment is similar to Transparent Deployment in that all outbound network traffic flows through the web appliance. Bridged Deployment, however, requires the optional bridge card included with some appliance models.

- Inspects HTTP and HTTPS traffic.
- Only the web appliance requires configuration.
- If it fails, you must power down the web appliance, but network traffic will continue to flow.

Operation

This deployment uses the web appliance’s bridge card, with the Network Interface page’s Deployment mode set to Bridged. In this configuration, the Configuration port to which you connect your laptop or PC to run the setup wizard still appears along the bottom of the appliance, as illustrated in the diagram below (to the right of the middle on the back of the appliance), but this is the only RJ45 port at that location.

There are two ports on the bridge card in the upper-right corner of the back of the appliance. Immediately to the left of these is a small group of six LEDs that indicate LAN connection status, as described in the "Appliance Hardware" page. Of the two RJ45 ports on this card, the one to the left is the WAN port, which you connect to your firewall for WAN or internet access; the port to the right is the LAN port, which you connect to your LAN.

All outbound and inbound traffic passes through the web appliance, which filters all port 80 and 443 traffic, allowing only secure and permissible web content to be accessed by your users, while non-web network traffic is passed through.
If the web appliance shuts down, the bridge card will be shut down with the LAN circuit closed, meaning that all LAN traffic will pass through.

- All outbound network traffic passes through the web appliance
- Users’ URL requests are intercepted by the web appliance on their way to the firewall
- All other traffic passes through.
Sophos Web Appliance

- The web appliance assesses all URL requests, blocks disallowed requests, checks if allowed URL requests are currently cached and passes uncached URL requests through the firewall and retrieves them from the internet.

- The web appliance receives any new pages or files and caches them; it passes the pages or files of allowed requests back to the users.

- The users receive only safe and allowed pages and files or a notification page.

**Configuration**

1. Connect the web appliance’s LAN port to your organization’s LAN.
2. Connect the web appliance’s WAN port to your organization’s firewall.
3. In the web appliance’s administrative web interface, on the **Configuration > Network > Network Interface** page, set the **Deployment mode** to **Bridged**, and click **Configure** to create a list of IP addresses or IP ranges for internal web servers that are exempted from handling by the web appliance.

   **Note**
   You are not required to configure users’ web browsers.

**Switching from Bridged Mode to Explicit Mode**

This page describes the steps required to convert your web appliance from a Bridged Deployment to an Explicit Deployment.

To transition from a Bridged to an Explicit deployment:

1. Leave the web appliance’s LAN port connection to your organization’s LAN unchanged.
2. Remove the connection between the web appliance’s WAN port and your organization’s firewall.
3. On the **Configuration > Network > Network Interface** page, change the **Deployment mode** from **Bridged** to **Explicit**.
4. Configure each user’s web browser to use the web appliance via port 8080 as their web proxy for HTTP, HTTPS, and FTP. (Ports 3128 and 8081 are also supported, but their use is only suggested if the web appliance is replacing a previous proxy configuration that used one of these ports.)

   **Note**
   To add support for HTTPS applications that use non-standard ports, see **Add Local Classification**.
Note
Configuring all user’s browsers to use the web appliance as a web proxy can be done centrally in Windows networks by using one of several methods. See the Sophos Knowledgebase pages for instructions on how to do this by:

- Creating, Testing, and Deploying a \texttt{proxy.pac} File
- Publishing Proxy Info as a \texttt{wpad.dat} File
- Creating a GPO

2.3.4 Bypassing for Internal Servers

This option allows clients to access specific internal servers directly. You might choose this setup if you want to let users access internal web pages without routing requests through the appliance. When based on the Explicit Deployment, this option does the following:

- Inspects HTTP, HTTPS, and FTP over HTTP traffic.
- Supports individual user opt-outs.
- Requires configuration for all clients.
- If it fails, all clients must be reconfigured, although clients can be configured to bypass the web appliance should it fail.

Operation
• Users’
HTTP, HTTPS, and FTP requests are examined by the PAC script
or similar configuration and forwarded to the appropriate server: the web appliance
or another server

• When requests are forwarded to the web appliance, it
assesses the URLs, blocks disallowed requests, checks if allowed URL requests are
currently cached, and passes URL requests that are not cached through the firewall
to retrieve them from the internet

Note
Port 80, port 443, and port 21 requests from users
are blocked at the firewall
URLs are only accepted by the firewall
if they are from the web appliance

• The web appliance
receives any new pages or files and caches them; it passes
the pages or files of allowed requests back to the users

• The users
receive only safe and allowed pages and files or a notification page.

Configuration
1. Connect your organization’s LAN to the web appliance’s LAN port.
2. Configure each client with either a PAC file (the more flexible method) or by distributing the
configuration to users via Active Directory Group Policy (the easier method).

Note
When using .pac files with Internet Explorer, we highly recommend disabling automatic
proxy caching. Specific instructions can be found in this Microsoft Support article: http://
support.microsoft.com/kb/271361.
3. In the web appliance’s administrative web interface, on the **Configuration > Network > Network Interface** page, set the **Deployment mode** to **Explicit proxy**.

**Related tasks**
- Explicit Deployment (page 18)

**Related information**
- Disabling Automatic Proxy Caching

### 2.3.5 Existing Cache Deployment

This option allows the web appliance to work in conjunction with an existing web-caching server.

**Operation**

The operation will vary according to the deployment scenario that you choose. As an example, the deployment shown in the diagram above and described in the points below is based on a Bridged Deployment.

- **Users’ URL requests** are passed to the web appliance.
- **The web appliance**
passes allowed requests to the cache server

• If the cache server

do not have the pages or files cached, it passes the request through the firewall

if it has the requested pages or files cached or when the request is returned through the firewall, the cache server

passes the requested pages or files back to the web appliance

Note
Even with the presence of a cache server, the web appliance will cache static content.

Note
This configuration is not intended to work with Microsoft Internet Security and Acceleration (ISA) servers or Microsoft Forefront Threat Management Gateway (TMG) servers. If you want a network deployment that will work effectively with ISA/TMG servers, try either the Downstream ISA/TMG Server Deployment or the Upstream ISA/TMG Server Deployment.

• The web appliance

scans the pages or files and passes allowed requests back to the users

• The users

receive only safe and allowed pages and file or a notification page.

Configuration

Follow the configuration instructions for the basic network deployment scenario that you want to use (Explicit Deployment, Transparent Deployment, or Bridged Deployment), but with the following differences:

• Ensure that your existing cache server is between your web appliance and your firewall.
• Ensure that your cache server is configured to be transparent to the web appliance.

Related tasks
Downstream ISA/TMG Server Deployment (page 20)
Upstream ISA/TMG Server Deployment (page 33)

2.3.6 Upstream ISA/TMG Server Deployment

This option is similar to the Downstream ISA/TMG Server Deployment. It can be used with any of the basic deployment options. It allows the web appliance to work with an ISA/TMG server, although in this case, one that is upstream in the network from the web appliance (see diagram below).
Sophos Web Appliance

- Allows the web appliance to work with an ISA/TMG server.
- Allows you to use multiple web appliances in a simple load-balancing deployment.
- Does not support individual user opt-out.

**Operation**

The operation varies according to the basic deployment scenario that you choose. As an example, this option is shown in the diagram above and described in the points below as a Bridged Deployment.

- **Users’**
  1. HTTP and HTTPS requests are passed through the web appliance
  2. The web appliance
  3. assesses URLs.

- **The web appliance**
  2. blocks disallowed requests, checks if allowed URL requests are currently cached, and passes URL requests that are not cached through to the ISA/TMG server

- **The ISA/TMG server**
Sophos Web Appliance

retrieves new pages or files from the internet
and passes them back to the web appliance.

- The web appliance receives the allowed pages or files, caches them, and passes them on to the users.

- The users receive only safe and allowed pages and files or a notification page.

Configuration

Follow the configuration instructions for the basic network deployment scenario that you want to use—Explicit Deployment, Transparent Deployment, or Bridged Deployment—but locate your web appliance between the ISA/TMG server and your users.

Note

Even if you have an upstream proxy (a proxy between the web appliance and the internet) configured, you still need to configure the web appliance with access to your organization’s DNS server, which is set on the Configuration > Network > Network Interface page.

Note

A simple way to set up load balancing amongst multiple web appliances is to set up a DNS round robin scheme. If you do this, you should disable DNS caching because Windows DNS caching can mask the round robin effect. Also, you must ensure that you have a firewall with network address translation (NAT), but not an ISA/TMG server in firewall mode, between the web appliances and the internet. This firewall must be configured to present a single IP for the web appliances to external sites. The NAT, or IP masquerading, prevents sites that check and record the IP address of visitors in cookies from encountering multiple IP addresses. To disable Windows DNS caching, see the Microsoft support article http://support.microsoft.com/kb/318803.

Note

Explaining how to configure an ISA/TMG server is beyond the scope of this documentation. For details on ISA/TMG server configuration, see Microsoft’s ISA Server Deployment page or the Microsoft Forefront TMG Deployment page.

Related tasks

Existing Cache Deployment (page 32)
Explicit Deployment (page 18)

Related information

Disabling Client-Side DNS Caching
Microsoft ISA Server Deployment
Microsoft Forefront TMG Deployment
2.3.7 Integrating with Sophos Email Products

The appliance can be configured to work with Sophos email products, such as the Sophos Email Appliance or Sophos PureMessage. The instructions for doing so are listed below.

- To configure your Sophos Web Appliance or Sophos Management Appliance to route email via your Sophos Email Appliance:
  a) On your web or management appliance, on the Configuration > Network > Hostname page, enter the IP address of your email appliance in the Outgoing SMTP mail server text box.
  b) On your email appliance, on the Configuration > Routing > Internal Mail Hosts page, enter the IP address of your web or management appliance in the Internal hosts and networks text box, and click Add.

- To configure your Sophos Web Appliance or Sophos Management Appliance to route email via your Sophos PureMessage server:
  a) On your web or management appliance, on the Configuration > Network > Hostname page, enter the IP address of your Sophos PureMessage server in the Outgoing SMTP mail server text box.
  b) On your Sophos PureMessage server, on the Policy > Internal Hosts page, enter the IP address of your web or management appliance.

- To configure your Sophos Email Appliance to access the internet via your Sophos Web Appliance:
  If you are using Active Directory, you must exclude your Email Appliance from authentication.
  a) On your web appliance, on the Configuration > System > Connection Profiles page, create a connection profile that includes the IP address of your email appliance.
  b) On your web appliance, on the Configuration > System > Authentication page, use the Profiles tab to create an authentication profile that applies to the connection profile for the email appliance that you created in the previous step.
     For more information on creating authentication profiles, see “Authentication” in the web appliance’s main documentation.
  c) On your email appliance, on the Configuration > Network > Hostname and Proxy page, enter the following information in the Proxy server configuration section:
      — Server address: enter the IP address of your web appliance
      — Port: 8080
      — Username and Password: leave these blank
  d) Click Apply.

- To configure your Sophos PureMessage server to access the internet via your Sophos Web Appliance:
  If you are using Active Directory, you must exclude your Sophos PureMessage server from authentication.
  a) On your web appliance, on the Configuration > System > Connection Profiles page, create a connection profile that includes the IP address of your Sophos PureMessage server.
  b) On your web appliance, on the Configuration > System > Authentication page, use the Profiles tab to create an authentication profile that applies to the connection profile for the Sophos PureMessage server that you created in the previous step.
     For more information on creating authentication profiles, see “Authentication” in the web appliance’s main documentation.
c) On your Sophos PureMessage server, configure the IP address of your web appliance using the `HTTP_proxy` environment variable. Specify port 8080. Do not specify a username or password.

Related information
Sophos Email Security and Control site

2.3.8 Grouping Web Appliances

The Sophos Web Appliance is available in a variety of models, each capable of providing web browsing security and control features for different numbers of end users. As indicated in the table below, appliances differ in their processing capacity and memory.

Larger organizations and those with multiple locations can use multiple web appliances grouped together by a common management appliance to provide web security and control for their various locales and a large number of end users. Management appliances centralize control of policy and configuration data and consolidate reports. In order to group two or more appliances together, you must purchase a Sophos Management Appliance.

Web appliances and management appliances can also be purchased as virtual machines that run on VMware. Their capacity depends on how much CPU, memory, and disk space you allocate. For more information, see “Virtual Appliances” in the product documentation.

For detailed instructions on joining and disconnecting appliances, see “Central Management” in the System section of the product documentation.

<table>
<thead>
<tr>
<th>Model</th>
<th>Processors</th>
<th>Memory (RAM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>WS100</td>
<td>dual-core, light-capacity</td>
<td>2 GB</td>
</tr>
<tr>
<td>WS500</td>
<td>dual-core, medium-capacity</td>
<td>2 GB</td>
</tr>
<tr>
<td>WS1000</td>
<td>dual-core, high-capacity</td>
<td>4 GB</td>
</tr>
<tr>
<td>WS1100</td>
<td>quad-core, high-capacity</td>
<td>8 GB</td>
</tr>
<tr>
<td>SM2000</td>
<td>quad-core, high-capacity</td>
<td>8 GB</td>
</tr>
<tr>
<td>SM5000</td>
<td>quad-core, high-capacity</td>
<td>8 GB</td>
</tr>
<tr>
<td>WS5000</td>
<td>quad-core, high-capacity</td>
<td>16 GB</td>
</tr>
</tbody>
</table>

Note
The number of end users that an appliance can handle is determined by the frequency at which your organization’s users browse the web throughout the day and the volume and nature of the files that they download and access. The number of users that a grouped deployment supports depends on the number of joined appliances.

Scaling and Deployment

Your organization can either grow to require more than one appliance, or—if your organization is a new web appliance user that is a large, multi-site organization—you can begin by using multiple, grouped appliances. In a grouped web appliance deployment, configuration and policy data is distributed from the management appliance. If you have an existing standalone appliance, there is also the option of the management appliance extracting configuration and policy data from the first web appliance to join.
Scenario 1: Your growing organization now requires more than one appliance

If your organization begins with a single standalone web appliance and then grows to require a multiple web appliances, the deployment of the additional appliances would be as follows:

Preparing to Join a Management Appliance

Before you join an existing web appliance to a management appliance, take the following steps to ensure that building your group is a smooth and successful process.

1. Be sure that you perform a backup that includes system configuration data and system logs.

2. If you want to use the policy and configuration data from an established web appliance that you plan to join to a management appliance, on the Configuration > System > Central Management page on the management appliance, be sure to select the Copy configuration and policy data from the first web appliance to join before joining the established web appliance. Ensure that the established web appliance is the first web appliance that you join to the management appliance.

Joining a Management Appliance and Other Appliances

1. Join your organization’s original, already-configured web appliance

The original web appliance’s configuration and policy data are copied to the management appliance (shown with blue dotted line).
2. Join the new web appliances to the management appliance

   This can be done in any order, whether the new web appliances are in the same location or in remote locations. The new web appliances that are joined then receive their configuration and policy data from the management appliance.

Scenario 2: Your large or multi-site organization’s deployment starts with multiple appliances

If your organization begins with multiple appliances that are deployed at the same time, the setup is as follows:
1. Unconfigured web appliances, whether they are in the same location and or in remote locations and are joined (in any order) to the management appliance (joins must be performed from each new web appliance).

2. The configuration is done on the management appliance, which then distributes this configuration data to the joined web appliances (shown with blue dotted lines).

**Note**
Follow the steps in Scenario 1 if you prefer to configure one of your new web appliances for testing purposes first, join it to the management appliance, and then distribute the configuration data to the other web appliances.

**Joined Appliances (Scenarios 1 and 2)**

In both scenarios, once all of the appliances are joined, ongoing configuration changes are done on the management appliance and distributed to the web appliances thus providing centralized configuration (blue dashed lines). Also, report data is sent from the web appliances to the management appliance, providing centralized reporting (red smooth lines).

**Appliance Mode and Model Differences**

Web appliances can operate in standalone or joined mode. You can also join a management appliance to one or more web appliances for centralized management.

There are differences in the administrative user interface, depending on which mode the appliance is in or if it is a management appliance. For a detailed breakdown of these variations, see “Mode and Model Differences.”

**Related concepts**
- Central Management (page 140)
- Understanding Mode and Model Differences (page 42)
- Grouped Appliance Troubleshooting (page 208)
2.3.9 Network Deployment Troubleshooting

The following is a list of known web appliance network deployment issues and their solutions.

"Blocked" Notification Page Lacks Graphics and a Stylesheet

**Problem**: If the "Blocked" notification page is displayed without any graphics and as raw HTML without the formatting of a stylesheet, the problem can result from the following combination of conditions in your network deployment:

- Your browser is configured to bypass use of the web appliance for your internal sites (for example, the domain name of your web appliance would normally be bypassed).
- Your browser is configured with the web appliance’s IP address instead of its fully qualified hostname.
- Your DNS server cannot resolve the web appliance’s IP address.

**Solution**: The best solution is to add the web appliance to your DNS server.

Firewall reports attachments stripped from web appliance-generated email

**Background**: The web appliance provides a managed appliance experience that is enabled in part by sending system status snapshots as email attachments to Sophos to ensure that your web appliance is operating within acceptable thresholds.

**Problem**: Firewalls can strip attachments from web appliance-generated email.

**Solution**: To enable the Sophos managed appliance experience, configure your firewall to allow email with attachments from the web appliance to wsasupport@sophos.com.

Long delays when loading web pages

**Problem**: If latency is significantly increased when browsing through the appliance, the problem may be due to an inappropriate Speed and duplex setting forced by enabling the auto-detect option.

**Solution**: To test if this is the case, set one of the manual options in the Speed and duplex option on the Configuration > Network > Network Interface page. If this change does not remedy the high latency problem, reinstate the automatic option and contact Sophos Technical Support.

RealPlayer Content Appears to be Blocked

**Problem**: RealPlayer content fails to play. This is typically a firewall configuration issue and not a web appliance problem. RealPlayer uses port 554, which is typically blocked in default firewall configurations.
Note
The remote site can force the use of a non-HTTP port, which will result in users not being able to view the content if the firewall is blocking the port being used.

Solution: To enable access to RealPlayer content, open port 554 on your firewall.

2.4 Understanding Mode and Model Differences

The Sophos Web Appliance is available in a variety of models, each capable of providing web browsing security and control features for different numbers of end users.

Larger and multi-location organizations can use multiple web appliances grouped together by a common management appliance to provide web security and control support for their various locales and a large number of end users. Management appliances centralize control of policy and configuration data and consolidate reports. In order to group two or more appliances together, you must purchase a Sophos Management Appliance.

Sophos web appliances can operate in standalone or joined mode. The management appliance (purchased separately) can be joined to one or more web appliances for centralized management. The user interface options differ, depending on whether it is a standalone web appliance, a joined web appliance, or a management appliance.

- **Standalone Web Appliance**: The default mode for a web appliance. It can be joined to a Sophos Management Appliance with Central Management options.
- **Joined Web Appliance**: A standalone web appliance that has been joined to a Sophos Management Appliance with Central Management options.
- **Sophos Management Appliance**: An appliance with the dedicated purpose of central management. When joined to other appliances, it is used for centralized reporting as well as centralization of configuration and policy data.

### Modes and Models in the Documentation

The administrative user interface varies slightly, depending on the mode or if you are managing grouped appliances from a management appliance.

Many administrative interface pages described in this documentation are not available on a joined web appliance; the functionality is shifted to the management appliance so that you can configure settings for multiple appliances from a single location.

The **Reports** and **Search** tabs are grayed out, and most of the **Configuration** tab’s options seen on the sidebar of a management appliance or standalone appliance do not appear on a joined web appliance. The documentation notes all instances where options are available but differ from one appliance mode to another.

Throughout the documentation, you will see notes containing this “grouped appliance” icon. These notes describe which user interface options are available for which modes and models.

The availability of pages of the administrative web interface are outlined in the table below.
<table>
<thead>
<tr>
<th>Administrative web interface page(s)</th>
<th>Standalone Web Appliance</th>
<th>Joined Web Appliance</th>
<th>Sophos Management Appliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboard</td>
<td>Yes</td>
<td>Yes, but no report links</td>
<td>Yes; additional <strong>Select View</strong> option to see only information for a specific appliance; for <strong>All appliances</strong> option, numbers are totals or averages</td>
</tr>
<tr>
<td>Configuration Landing Page</td>
<td>Yes</td>
<td>no post-installation tasks; the only quick task is <strong>Configure Central Management</strong></td>
<td>Yes</td>
</tr>
<tr>
<td>Accounts &gt; Administrators</td>
<td>Yes</td>
<td>Yes, but accounts are for the local system only</td>
<td>Yes</td>
</tr>
<tr>
<td>Accounts &gt; Notification Pages</td>
<td>Yes</td>
<td>None</td>
<td>Yes</td>
</tr>
<tr>
<td>Group Policy</td>
<td>Yes</td>
<td>Policy Test only</td>
<td>Yes</td>
</tr>
<tr>
<td>Global Policy</td>
<td>Yes</td>
<td>Only <strong>General Options</strong> page, which has only &quot;Cache settings&quot;</td>
<td>Yes; the <strong>General Options</strong> page has no &quot;Cache settings&quot;</td>
</tr>
<tr>
<td>System &gt; Updates</td>
<td>Yes</td>
<td>Status info &amp; <strong>Update</strong> button only</td>
<td>Yes</td>
</tr>
<tr>
<td>System &gt; Backup</td>
<td>Yes</td>
<td>None</td>
<td>Yes; added Report data backup option</td>
</tr>
<tr>
<td>System &gt; Restore</td>
<td>Yes</td>
<td>None</td>
<td>Yes</td>
</tr>
<tr>
<td>System &gt; Alerts &amp; Monitoring</td>
<td>Yes</td>
<td>Syslog only</td>
<td>Yes</td>
</tr>
<tr>
<td>System &gt; Active Directory</td>
<td>Yes</td>
<td>Yes; no LDAP access options (LDAP data is downloaded from the management appliance)</td>
<td>Yes</td>
</tr>
<tr>
<td>System &gt; Time Zone</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>System &gt; Central Management (each unique)</td>
<td>Join management appliance</td>
<td>Revert to standalone management appliance</td>
<td>Set &quot;Join&quot; options</td>
</tr>
<tr>
<td>Network &gt; Network Interface</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes; no <strong>Deployment mode</strong> menu, no <strong>Configure</strong> button</td>
</tr>
<tr>
<td>Network &gt; Hostname</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes; no <strong>DNS search suffixes</strong> or <strong>Accept authentication from downstream ISA/TMG servers</strong> options</td>
</tr>
<tr>
<td>Network &gt; Network Connectivity</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Network &gt; Diagnostic Tools</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### 2.5 Platforms and User Interface

#### Supported Platforms

<table>
<thead>
<tr>
<th>End-User Browser</th>
<th>Internet Explorer 8.0 and newer, recent versions of Chrome and Firefox</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator Browser</td>
<td>Internet Explorer 8.0 and newer, recent versions of Firefox</td>
</tr>
<tr>
<td>eDirectory</td>
<td>eDirectory 8.73 and 8.8 on Netware 6.5 SP3</td>
</tr>
<tr>
<td></td>
<td>eDirectory 8.8 on SUSE</td>
</tr>
<tr>
<td></td>
<td>eDirectory 8.8 on Windows Server 2003</td>
</tr>
</tbody>
</table>

**Related concepts**
- Grouped Appliance Troubleshooting (page 208)
- Grouping Web Appliances (page 37)
- Central Management (page 140)
- Virtual Appliances (page 15)
Appliance Administrative Web Interface

The appliances’ administrative web interface includes the following components:
The System Information bar shows the following (from left to right):

- **Remote Assistance session established** is displayed while an outbound SSH connection to Sophos Technical Support is open.
- **Sophos proactive monitoring is off** is displayed when the Activate appliance support alerts are turned off on the **System: Alerts** page.
- **v#.#.##** shows the version number of the current appliance software. Click the version number to open the release notes in a new window.
- **Logged in as <username>** is displayed, indicating the username of the current user. To change the current user’s password, click on this.
- **Log out** can be clicked to exit from the appliances’ administrative web interface.
- The current time in 12-hour format.

Click the items on the Navigation bar to view:

- The **Dashboard** tab
- The **Configuration** tab
- The **Reports** tab (not available on a joined web appliance)
- The **Search** tab (not available on a joined web appliance)
- The Appliance **Help** window
- The **System Status** tab

Most of these tabs contain multiple pages, which can be accessed from the Navigation sidebar.

The Content pane displays the pages of the appliance’s administrative web interface.

Near the top of the Content pane on the **Configuration** and **Search** pages is a short explanation of the purpose of the page, which is marked with an information icon, as shown to the left.

The Navigation sidebar only appears on the **Configuration**, **Reports**, and **Search** tabs. Click the links on this sidebar to view the various **Configuration**, **Reports**, and **Search** options in the Content pane.

The Content pane displays the pages of the administrative web interface.

**Note**

At the bottom edge of the Content pane on each of the **Configuration**, **Reports** and **Search** pages is a status bar that displays the response to actions performed in the administrative web interface.
The Quick Tasks sidebar only appears on the Configuration tab. Click any of these links to perform common configuration tasks.

The Parameters sidebar (not shown) appears on the Reports tab and the Search tab. Use this area to set date and display options.

2.6 Policy

The Sophos Web Appliance provides security and control for your users’ web browsing by preventing the loading of viruses, Trojans, worms, other malware, and potentially unwanted applications (PUAs).

The web appliance does this by using site lists. Sophos provides a basic and an enhanced list of URLs—the Sophos Basic Categorization Data and the Sophos Enhanced Categorization Data—each of which assigns a risk classification (high, medium, low, or trusted) and a site category (business, education, sports, gambling, illegal drugs, weapons, etc) to the listed URLs.

You can extend these Sophos lists, or override the risk classification or the site category of the URLs by adding custom entries. In addition to URLs, you can set whether requests for various downloadable file types are allowed, warned, or blocked. "Block" or "warn" pages are displayed in response to inappropriate user requests, and you can give users the ability to ask for a reclassification or re-categorization of the site. The message that users see on these pages can also be modified.

Default actions are as follows:

• Content from sites classified as being high-risk is always blocked
• Content from low-risk sites is always scanned
• Content from trusted sites is always allowed

Additionally, you can set whether content from medium-risk sites is blocked or scanned and whether content from unclassified sites is handled in the same way as content from low, medium, or high-risk sites.

HTTPS

This security protection can be extended to HTTPS (encrypted) sites, which can also contain security threats. You configure your web appliance to handle certificate validation, thus deciding for your users about which HTTPS sites to trust.

HTTPS Scanning

To provide secure sessions between your users and commercial or banking sites, HTTPS can encrypt web content between the website server and the user’s browser. To scan encrypted content for malware, it must first be decrypted, then scanned, then re-encrypted for delivery to the requesting end user’s browser. Doing this maintains the privacy of the encrypted content, as the process takes place automatically without human eyes viewing the content.
Active Directory

The web appliance allows you to view lists of user groups imported from your organization’s Active Directory server and define custom groups. On this page, you either apply the default policy to a select list of groups, or you apply the default policy to all groups except those in the select list.

Acceptable Use Policies

The web appliance protects your organization and your users from visiting sites that violate your organization’s browsing policy, including sites that violate inappropriate browsing legislation. Site categories can also be used to provide productivity control by disallowing access to entertainment sites and other diversions.

Custom Policies

You can define a Special Hours policy, consisting of modified access settings that will apply to the same set of users as the default policy, but that provides, for example, a more relaxed web browsing policy during the lunch hour and after business hours.

You can also create as many as 80 Additional Policies, overriding the default policy and the Special Hours policy. These can be applied to select users or groups and can also be set to take effect only during a scheduled period. Additional policies can be turned on and off as required, and they can be set to automatically deactivate at a specified date and time.

Applying tags lets you set policy rules more simply and flexibly than is possible by using other policy features. You can use the Local Site List to apply one or more tags to a URL. With Additional Policies, you can set what action is taken in response to a tag.

Dynamic Categorization

Sophos provides the ability to block attempts by your users to evade policy controls through anonymizing proxies and caching websites by automatically detecting such sites with the Dynamic Categorization feature.

Data Leakage Prevention

You can secure your users against leaking vital data through web use by using the Data Leakage Prevention features to selectively block them from sending webmail messages and posting on blogs.

Related concepts

- Group Policy (page 72)
- Global Policy (page 100)

2.7 Endpoint Web Control

Sophos web appliances can perform filtering for URLs and file types at the network gateway. Sophos Enterprise Console allows you to extend some of this same capability via Sophos Endpoint Security and Control, filtering 14 essential site categories on endpoint machines.
By combining a web appliance with Sophos Enterprise Console, however, your organization can take advantage of features that both products have to offer. Once you have configured them to work together, you can apply a full web control policy with more than 50 site categories to each user machine by way of Endpoint Security and Control.

Endpoint machines then communicate with the designated Sophos Web Appliance or Sophos Management Appliance, receiving policy updates and sending back web activity reports to the appliance and web events to Enterprise Console. Optionally, you can grant users the ability to receive policy updates and send web activity reports through a cloud service during periods when users are disconnected from your corporate network.

As illustrated below, Enterprise Console can enable endpoint web control using three different methods.

Method 1: Enterprise Console (standalone mode)

![Diagram of Enterprise Console (standalone mode)]

Even without a web appliance or management appliance, Enterprise Console offers basic web filtering. When a web control policy is configured and enabled solely through Enterprise Console, rules for 14 essential categories are applied for each user through Sophos Endpoint Security and Control. The policy, defined on Enterprise Console as “Potentially Unwanted Website Control,” is published to users. Users’ web activity data is sent back to Enterprise Console, where they are displayed as “web events.”

If necessary, the endpoint software performs URL classifications via SXL queries to Sophos. SXL is the infrastructure that Sophos uses to submit real-time, DNS-based queries to SophosLabs regarding IP addresses, URLs within messages, and image fingerprints.
Method 2: Enterprise Console and Appliance

When a full web control policy is applied using either a web appliance or management appliance, Enterprise Console supplies the hostname of the corresponding appliance so that endpoints can communicate with it. The users’ endpoint software connects to that appliance and obtains a complete web-filtering policy. Users’ web activity data is sent back to the designated appliance, while web event data (websites scanned and assessed by the live URL-filtering feature) is sent to Enterprise Console.

If necessary, the endpoint software performs URL classifications via SXL queries to Sophos. SXL is the infrastructure that Sophos uses to submit real-time, DNS-based queries to SophosLabs regarding IP addresses, URLs within messages, and image fingerprints.
Method 3: Enterprise Console and Appliance with LiveConnect

Optionally, you can deploy full web control with LiveConnect enabled. Data is exchanged exactly as it is in Method 2, except that users have access to a cloud service that allows roaming endpoints to connect with the designated web appliance without you having to grant special access through your organization’s firewall or reconfigure any externally facing network services.

It does so by providing a bridge between outbound HTTP connections made by the endpoint and its managing appliance (as shown above). This allows the endpoint to apply the same web-filtering rules for roaming users as they would get when protected by a gateway appliance.

Benefits of Endpoint Web Control

While the Sophos Web Appliance provides security and productivity protection for systems browsing the web from within your corporate network, Endpoint Web Control extends this protection to users’ machines. This provides protection, control, and reporting for endpoint machines that are located, or roam, outside your corporate network.

Enterprise Console can deliver Web Control policies to your endpoint machines that provide malware protection and productivity rules based on common site categorizations. With the combination of Sophos Enterprise Console and a Sophos Web Appliance it is possible to extend your Full Web Policy to endpoint machines, providing more than 50 site categories, highly flexible policy configuration, and detailed reporting on threats and usage.

Related concepts
- eDirectory (page 127)

Related tasks
- Endpoint Web Control (page 144)
- Viewing Connected Endpoints (page 145)
2.7.1 Appliance Features Not Supported by Endpoint Web Control

While there are many benefits to extending full Web Control to the endpoint, some features are only available from behind a web appliance. The following features are supported on the web appliance but not Endpoint Web Control:

- Dynamic categorization
- Data leakage prevention (webmail and blogs)
- HTTPS scanning
- Certificate validation
- Download options
- Google feature controls
- Sandstorm
- Download-type controls for Windows system files, Windows scripts, and Windows HTML App files

Related tasks
Configuring Dynamic Categorization (page 102)
Configuring Data Leakage Prevention (page 103)
Configuring HTTPS Scanning (page 104)
Configuring Certificate Validation (page 106)
Setting Download Options (page 108)

2.8 Updates

New threats are constantly evolving on the internet: viruses, spyware, and other security attacks. To ensure that your appliance is able to deal with these changes, it automatically downloads and installs updated information from SophosLabs. Website URL categorization data is also updated: every 5 to 30 minutes for the standard categorization data and every hour for the enhanced categorization data.

SophosLabs is a global network of highly skilled analysts with more than 20 years’ experience in protecting businesses from known and emerging threats. SophosLabs sites around the world provide rapid response to evolving threats like viruses, spam, phishing, spyware, and other malware, 24 hours a day, seven days a week.

The appliance constantly updates anti-virus definitions and Sophos website categorization data throughout the day. It also downloads "Critical" and "Maintenance" software updates. Critical updates are security-related and protect against anything that can compromise the appliance. Maintenance updates contain the latest non-critical software updates and bug-fixes. Maintenance updates can be installed on a configurable schedule to avoid slowdowns at peak periods.

Related concepts
About Appliance Versions (page 113)
2.9 Getting Support

Sophos Appliances are equipped with advanced monitoring and assistance technologies that deliver a superior customer support experience. Every installed appliance is kept up to date and at its operational peak with minimal administrative involvement. Sophos appliances communicate with Sophos Technical Support every five minutes, automatically receiving anti-virus and URL classification updates and reporting on hardware health and protection status.

You can send a support request directly from the appliance help system. Click the Sophos Support icon in the online help’s titlebar to access this feature.

Sophos appliances also feature optional Remote Assistance via a secure reverse-tunnel SSH connection. This lets you grant Sophos Technical Support direct remote access to your appliance for faster problem resolution. Contact Sophos Technical Support before enabling Remote Assistance.

Active Monitoring also delivers automatic alerts on the protection status and license validity.

Sophos Appliances with Active Monitoring deliver a new height of gateway protection, offering the control and efficiency of an appliance and the simplicity of a managed service.

To contact your local Sophos office, see: http://sophos.com/companyinfo/contacting/

Product Warranty

Each unit comes with a three-year advanced replacement warranty to help keep networks up and running even in the event of hardware failure. If a hardware component or entire appliance requires replacement at any time during the first three years, Sophos will cover the costs of the new appliance and delivery. The customer is responsible for returned unit delivery charges.

Hardware Support

All appliances carry a standard Advanced Replacement Warranty. Sophos will initiate the replacement within two hours of a confirmed failure. Next-day delivery (not including delays from international Customs clearing, if required) will occur according to the following cut-offs, Monday through Friday:

<table>
<thead>
<tr>
<th>Customer Region</th>
<th>Local Cut-off Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States, Canada</td>
<td>12:00 (Boston, USA)</td>
</tr>
<tr>
<td>United Kingdom, EMEA</td>
<td>12:00 (London, UK)</td>
</tr>
<tr>
<td>France and Spain</td>
<td>13:00 (Paris, FR)</td>
</tr>
<tr>
<td>Germany, Switzerland and Austria</td>
<td>13:00 (Frankfurt, DE)</td>
</tr>
<tr>
<td>Italy</td>
<td>13:00 (Milan, IT)</td>
</tr>
<tr>
<td>Asia Pacific</td>
<td>16:00 (Sydney, AU)</td>
</tr>
<tr>
<td>Japan</td>
<td>14:00 (Yokohama, JP)</td>
</tr>
<tr>
<td>Australia, New Zealand</td>
<td>16:00 (Sydney, AU)</td>
</tr>
</tbody>
</table>
Hardware replacement requests received after the times shown above will be fulfilled on the second subsequent business day.

2.10 Product Documentation

In addition to the online help, the following product documentation and support resources are available from the Web Appliance Documentation page:

- Release notes
- Setup guides
- Configuration guides

The Knowledge Base is a collection of articles that address the following issues:

- Common questions received by Sophos Support about the appliance.
- Technical issues that are not commonly encountered by appliance administrators.
- Technical issues that involve third-party hardware or software products that affect web appliance and management appliance deployment or operations.
### 3 Dashboard

The Dashboard tab provides a quick overview of web appliance activity and status in several panels: Select View, Summary Statistics Today, URL Test, Virus Updates, Web Traffic, Blocked Sites, Viruses and Malware, and Traffic Patterns.

**Select View**

This panel allows you to select from which appliances the Dashboard draws its information. You can select any joined web appliance, or you can select **All appliances**.

**Note**

When viewing the information for **All appliances**, the time period covered is based on the management appliance’s time zone. When viewing the information for a specific web appliance, the time period covered is based on the viewed appliance’s time zone.

**Summary Statistics Today**

The **Summary Statistics Today** panel displays the following information:

- **Unique users (since 12AM)**: The total number of users that have used the web appliance’s services since midnight.
- **Concurrent users**: The number of concurrent users in the last minute.
- **Concurrent users peak**: The peak number of concurrent users during the busiest minute today.
- **Connected endpoints**: The total number of active Sophos Endpoint Security and Control users whose web activity is currently filtered by an appliance-based policy. You must use Sophos Enterprise Console together with an appliance to deploy web filtering by way of Endpoint Security and Control. Click to view details of any connected endpoints. If you are not filtering at the endpoints, the number shown is always zero.
- **Page latency**: The average time in milliseconds per page that was added to page loads by the web appliance in the last minute.
- **Page latency peak**: The peak time in milliseconds that has been added to page loads by the web appliance during the busiest minute today. This peak value may be due to a large or complex download and should not be interpreted as average page latency, which is shown in the preceding **Page latency** value.
- **Bytes downloaded**: The total number of bytes (expressed in kB, MB, or GB) of content downloaded through the web appliance today since midnight. This is a comprehensive measure of the bytes downloaded.

---

The **Select View** section of this page is only available on a management appliance. When **All appliances** is selected in the **Select View** section, the numbers displayed are totals or averages of all managed web appliances. Also, the links to reports in the **Blocked Sites, Viruses and Malware** panel are not available on joined web appliances.
Note
If the domain name or the time zone of the web appliance is changed, the count for the number of Concurrent Users is set to zero, potentially causing an inaccurately low number to be displayed for the rest of the day on which the change was made.

The lower part of the Summary Statistics Today panel displays the following information:

- **Bandwidth consumption**: The bandwidth usage today, both in terms of bytes (expressed in KB, MB, or GB) and as a percentage of today’s total bandwidth use for:
  - **Page views**: The bandwidth consumed by loading all pages that show HTML content, including graphics, style sheets, and JavaScript.
  - **Downloads**: The bandwidth consumed by loading all other (non-HTML page) content.
- **Download requests**: The file download requests today, both in terms of the number of requests and as a percentage of the total for:
  - **Allowed** (download requests)
  - **Denied** (download requests)
- **Page requests**: The web page view requests today, both in terms of the number of requests and as a percentage of the total for:
  - **Allowed** (web page requests)
  - **Denied** (web page requests)
- **Throughput**: The number of kilobits or megabits per second of data passed to users throughout the current day (in white), and the same information over the preceding day (in red).

**Test URL/Submit to Sandstorm**

To test the category and security risk of a URL, click the Test URL tab, type a URL or IP address, and click Test.

To send a file to Sandstorm for analysis, click the Submit to Sandstorm tab, select a file or type the URL of a file, and click Submit. To view the progress of the test, click Search and go to Sandstorm > Sandbox Activity.

Note
This option is available only to licensed users of Sophos Sandstorm.

**Advanced Threat Protection**

Information on the number of machines on your network that are potentially infected. If no threats have been detected for a given time interval, a green checkmark will be displayed. If any potentially infected machines have been detected, a red circle with an X will be displayed. Click the infected hosts count to show the Advanced Threat Protection report with details for the indicated time interval.

**Web Traffic**

The Web Traffic panel displays two gauges:
• **Throughput (kbps/Mbps):** The total kilobits or megabits per second of data passed to users.

• **Added latency (ms):** The time in milliseconds that is added to page loads by the web appliance.

### Blocked Web Traffic

The **Blocked Web Traffic** panel displays the following information:

• **Viruses:** The total number of viruses blocked. Click to view the full Users: Virus Downloaders report.

• **PUAs:** The total number of PUAs blocked. Click to view the full Users: PUA Downloaders report.

• **High risk sites:** The number of blocked URL requests for high-risk sites. Click to view the full Users: High Risk Site Visitors report.

• **Policy violations:** The total number of policy violations. Click to view the full Users: Policy Violators report.

• **App Control Violations:** The total number of web application violations. Click to view the full Users: Top Web Application Users report.

*Note*

These are not available on a joined web appliance. All numbers reset at midnight.

### Sophos Sandstorm

Sophos Sandstorm is a cloud-based service that provides enhanced protection against new and targeted attacks. You can configure the appliance to send suspicious files to Sandstorm for analysis or submit suspicious files on an individual basis. Sandstorm detonates the file to check for malware and sends the results to you. Because the analysis takes place in the cloud, your system is never exposed to potential threats.

The **Sophos Sandstorm** panel displays the following information:

• **Suspicious Downloads:** The total number of downloads that have been flagged as suspicious. Depending on how you have configured Sandstorm, some of these may not be sent to the Sophos Active Sandbox for analysis.

• **Sent for Analysis:** The total number of downloaded items sent to the Sophos Active Sandbox today.

• **Awaiting result:** The number of downloaded items that were sent to the Sophos Active Sandbox, and that are currently waiting to be analyzed.

• **Malicious:** The total number of suspicious items users attempted to download that exhibited unwanted or risky behavior when executed.

• **Clean:** The total number of suspicious items users downloaded that did not pose a threat.

• **Average Analysis Time:** The average amount of time it takes to process an item submitted for analysis.

*Note*

If you have a trial license, this will display the number of days left in your trial.
• **Malicious/Suspicious gauge**: displays information about the number of downloaded items that were categorized as malicious (red), and the total number of items flagged as suspicious (blue) during the last seven days.

*Note*
This information is available only to licensed users of Sophos Sandstorm.
4 Configuration

The Configuration tab provides an interface for setting web security, browsing policy options, and performing appliance network configuration and administrative tasks.

Note

The post-installation tasks do not appear on a web appliance that is joined to a management appliance, and the only item on the Quick Tasks sidebar is Configure Central Management.

The Configuration tab sidebar lists all of the available configuration pages. They are as follows:

- Use the Accounts pages to create and manage appliance administrator accounts and to set user notification page preferences.
- Use the Group Policy pages to set specialized URL filtering for groups and individuals, including setting modified URL web access policy during specific times or additional policies for specific purposes.
- Use the Global Policy pages to change the web appliance URL filtering behavior.
- Use the System pages to update, back up, and restore the appliance’s system and to change its configuration.
- Use the Network pages to change the configuration of the appliance’s connection to, and identity within, your organization’s network and to check network connectivity.

After installation or a major upgrade, the Configuration Homepage displays a list of post-installation tasks that you should perform to ensure that the appliance performs optimally in your environment. The title of each task links to the configuration page where these configuration tasks should be performed. The post-installation tasks are:

- Set up Default Policy: Use this page to configure how URL requests to sites categorized by content type and download types are handled by the appliance.
- Set up Default Groups: Use this page to choose whether the default policy is applied to everyone or to selected groups of users.
- Create Additional Policies: Use this page to set additional policies that can be used as exceptions to the Default Policy and the Special Hours Policy and which are executed as part of the web appliance’s application of acceptable browsing policy.
- Set up Active Directory: Use this page to configure the appliance’s access to your Active Directory server.
- Set up eDirectory: Use this page to configure the appliance’s access to your eDirectory server.
- Certificate Validation: Use this page to configure the web appliance to examine HTTPS certificates and automatically accept valid, known certificates.
- User Notification Options: Use this page to modify the appearance of the notification pages that the web appliance displays to users when they try to access virus-infected files, malware, blocked sites, when they download large files that take a long time to scan, or warning pages that are displayed when users attempt to access a URL that violates policy.

When the above changes are made, or if no changes are desired, these items can be removed by clicking the Remove button to the right of each link.

A Quick Tasks sidebar on the right of the Configuration Homepage provides easy access to the following main administrative tasks and commonly adjusted settings:
4.1 Accounts

Use the **Accounts** pages to create and manage appliance administrator accounts, set end user notification page preferences, modify notification page messages, or add logos.

- Use the **Administrators** page to create, modify, and delete appliance administrator accounts.
- Use the **Notification Page Options** page to configure the look, text, and behavior of the various notification pages that the web appliance shows to end users.

**Note:** The **Notification Page Options** page is not available on a joined web appliance, as this functionality has been shifted to the management appliance. The **Administrators** page is renamed **Local Administrators** on a joined web appliance, as accounts created on a joined system are available only on that system.

4.1.1 Administrators

On a joined web appliance this page is named **Local Administrators**, as accounts created on a joined system are available only on the local system. An account created on a management appliance, including **Limited Access Administrator** accounts, is referred to as a “global account”. Global accounts can access the same features on any web appliance for which their role or roles grant them permission.

The **Configuration > Accounts > Administrators** page allows you to create, modify, and delete appliance administrator accounts. New appliance **Administrators** can be either **Full Access Administrators**, who have access to all system management tasks or **Limited Access Administrators**, who can only access the system management tasks for which they have been granted permission.

The default administrator account cannot be deleted and only its password can be changed. If you need to reset a forgotten password for the default administrator, you can do so by following the instructions provided when you click the **Reset password for default administrator** link on the main login page.

**Note**

To reset the default administrator’s password, you will need the product activation code that you received when you purchased your appliance. This allows you to enable Sophos Remote Assistance, after which Sophos Technical Support is able to reset the password.

**Related concepts**

*Reporting Groups* (page 171)
Creating a New Administrator Account

In the Administrators table, click the Add button to open the Administrator Accounts Wizard.

Use the Previous and Next buttons to move between pages of the wizard or the Cancel button to close the wizard and discard the entry.

To add a new administrator:

1. On the Details page of the wizard, enter the Full name, Username and Password, and then Confirm password for that user.

2. On the Roles page of the wizard, select whether the user should be a Full Access Administrator, or a Limited Access Administrator.

   For a Limited Access Administrator, select one or more of the following roles:
   - Helpdesk: Approves user submissions, tests the policies, and verifies network connectivity
   - Policy: Configures and tests global and group web browsing policies.
   - Reporting: Views or schedules reports.
   - User Activity: Has access to detailed web activity data.

   **Note**
   The comment section of new entries in the Local Site List will include which Helpdesk administrator approved a user submission.

3. The Reporting Groups page is enabled when a Limited Access Administrator is being created with one or both of the Reporting or User Activity roles.
   - Select Include all reporting groups if you want the new administrator to have access to all existing groups.
   - Select Include only selected reporting groups if you want to restrict the administrator’s access to specific groups. Then, in the Reporting Groups table, select the specific groups to which the administrator should have access.

4. On the Description page of the wizard, enter a description for the administrator.

5. Click Save.

   The Administrator Accounts Wizard is closed, and the new administrator account appears in the Administrators list.

Administrator Access Rights

Access rights for Full Access and Limited Access Administrators

Administrators may have different access rights, depending on what Roles they have been granted. The following table provides a summary of what each role is able to access.

<table>
<thead>
<tr>
<th>Page</th>
<th>Full Access Admin</th>
<th>Helpdesk</th>
<th>Policy</th>
<th>Reporting</th>
<th>User Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboard &gt; Endpoints</td>
<td>Yes (read-only)</td>
<td>Yes (read-only)</td>
<td>Yes (read-only)</td>
<td>Yes (read-only)</td>
<td>Yes (read-only)</td>
</tr>
<tr>
<td>Dashboard &gt; Block counts</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Config &gt; Landing</td>
<td>Yes</td>
<td>Yes (read-only)</td>
<td>Yes (read-only)</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Config &gt; Quicktasks</td>
<td>Yes</td>
<td>Yes (read-only)</td>
<td>Yes (read-only)</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Config &gt; Group Policy</td>
<td>Yes</td>
<td>Yes (read-only)</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Page</td>
<td>Full Access</td>
<td>Helpdesk</td>
<td>Policy</td>
<td>Reporting</td>
<td>User Activity</td>
</tr>
<tr>
<td>----------------------------------------------------</td>
<td>-------------</td>
<td>------------------------</td>
<td>-------------------</td>
<td>-----------</td>
<td>---------------</td>
</tr>
<tr>
<td><strong>Config &gt; Global Policy</strong></td>
<td>Yes</td>
<td>Yes (read-only)</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td><strong>Config &gt; System</strong></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td><strong>Config &gt; Network, except Network connectivity and diagnostic tools</strong></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td><strong>Config &gt; Network &gt; Network connectivity and diagnostic tools</strong></td>
<td>Yes</td>
<td>Yes (read-only)</td>
<td>Yes (read-only)</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td><strong>Reports &gt; All, except Options</strong></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td><strong>Reports &gt; Options &gt; Reporting Groups</strong></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td><strong>Reports &gt; Options &gt; Report Scheduler</strong></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes (limited)</td>
<td>No</td>
</tr>
<tr>
<td><strong>Reports &gt; Options &gt; Report Exemptions</strong></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td><strong>Reports &gt; Options &gt; Search Terms</strong></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes (read-only)</td>
<td>No</td>
</tr>
<tr>
<td><strong>Search &gt; Recent Activity Search</strong></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Search &gt; User Submissions &gt; Sites</strong></td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td><strong>Search &gt; User Submissions &gt; PUAs</strong></td>
<td>Yes</td>
<td>Yes (delete only)</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td><strong>Search &gt; User Submissions &gt; File Types</strong></td>
<td>Yes (delete only)</td>
<td>Yes (delete only)</td>
<td>Yes (delete only)</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td><strong>Help &gt; Sophos Support Link</strong></td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td><strong>System Status</strong></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Modifying an Administrator Account**

In the **Administrators** table, click the username of the account that you want to modify. The **Administrator Accounts Wizard** is displayed with the information for the existing account shown.

Use the **Previous** and **Next** buttons to move between pages of the wizard, the **Save** button to close the wizard and save any changes you have made to the account, or the **Cancel** button to close the wizard and discard any changes you have made to the account.

In the **Administrator Accounts Wizard** make any required changes:
- On the **Details** page of the wizard, you can modify the **Full name** and **Password** for that user.
Note
You can only change the password of the initial, default administrator account; you cannot change the **Full name** or the **Username** of the account. For added accounts, only the **Username** cannot be modified.

- On the **Roles** page of the wizard, you can modify whether the user should be a **Full Access Administrator** or a **Limited Access Administrator**, or you can select different roles for a **Limited Access Administrator**.

Note
If there are scheduled reports that have been created by a **Limited Access Administrator** account, that role cannot be removed from that account until any associated reports have first been deleted.

- The **Reporting Groups** page is enabled only for **Limited Access Administrators** with one or both of the **Reporting** or **User Activity** roles selected.

Note
You cannot remove a reporting group from a report user if that reporting group is used by a scheduled report belonging to that report user.

- On the **Description** page of the wizard, you can modify the description of the administrator.
- Click **Save** when you have finished making changes. The **Administrator Accounts Wizard** is closed, and changes to the modified account appear in the **Administrators** list.

### Removing an Administrator Account

- In the **Administrators** table, select the check box beside the account (or multiple accounts) that you want to delete.

  Note
  — The initial, default administrator account cannot be selected or deleted.
  — You cannot delete an account if you are logged in to that account.
  — If there are scheduled reports that have been created by an account, that account cannot be deleted until its associated reports have first been deleted.

- At the bottom of the table, click **Delete**. The selected account is removed from the table.

### 4.1.2 Notification Page Options

The **Configuration > Accounts > Notification Page Options** page allows you to modify the appearance of the notification pages that the web appliance shows to users when they try to access:

- virus-infected files
• malware
• blocked sites
• sites or applications that violate policy
• sites which will use or exceed their quota time
• restricted sites
• large, downloadable files that take a long time to scan
• unapproved secure sites

The Global options panel allows you to set options that apply to every notification page. The Notification page text panel allows you to edit the text of specific notification pages.

Related concepts
About Authentication (page 131)

Setting Global Notification Options
The Global options panel allows you to set options that apply to every notification page.

1. On the Global options panel, select the check box to the left of any of the options that you want enabled.
2. If you want to display your own graphic on the notification pages, select the Display logo on notification pages option. Select the graphic file on your local (browsing) system by clicking Browse to find the graphic on your local system, and then copy it to the appliance by clicking Upload. If you do not upload your own graphic, the default Sophos logo will be used.

Note
It is suggested that you use .jpeg files because the appliance assigns the graphic a default name of image.jpg. Using .gif or .png files may work because your users' browsers will likely detect the proper file type, but this might not work with all browsers. The logo graphic must be no larger than 512 Kb.

3. Click Apply.

Modifying Notification Page Text

1. On the Notification page text panel, from the Page drop-down list, select the notification page that you want to modify.
2. From the Choose language drop-down list, select the language in which you want the notification page to be displayed.

Note
For your users to view non-English notification pages properly, their browsers must be configured to use UTF-8 character encoding. Also, for you to view previews of non-English notification pages, you must have your browser configured to use UTF-8 character encoding.

3. Optionally, in the Page title text box, type the page title that is displayed on the notification page and in the browser title bar.
4. Optionally, in the Text explanation text box, type the explanation that is displayed in the body of the notification page.
5. Optionally, click **Preview** to see how the notification page will look.
   If you decide to change your selected options, you must clear the currently selected options first by clicking **Cancel**.

6. Repeat steps 1 through 5 for each of the notification pages that you want to modify.

7. Click **Apply**.

**Advanced Notification Page Options**

Use the **Advanced** tab to download, edit, and upload notification page templates that allow you to extensively customize the notification pages displayed to your users. There are three different notification page templates:

- **Block page template**: This template is used by all policy-related notification pages displayed to users when they try to access:
  - virus-infected files
  - malware
  - blocked sites
  - sites or applications that violate policy
  - sites which will use or exceed their quota time
  - restricted sites
  - or when they try to access unapproved secure sites

- **Patience page template**: This template is used by the page displayed when users request a large file download.

- **Error page template**: This template is used by the server error pages that display HTTP error messages. For example, the 404 File not Found or the 500 Internal Server Error.

To upload a modified notification page template to the appliance:

a) Click **Browse** in the **Templates** section of the **Advanced** tab.
   The **File Upload** dialog box is displayed.

b) Navigate to the directory in which you saved the modifications to the uploaded template files, select one of the modified notification template files, and click **Open**.
   The file is uploaded to the appliance.

c) Click **Apply**.

To download a modified notification page template from the appliance:

a) Click **Using custom template** beside the modified template that you want to download and save the file using your browser’s save file capabilities.
   The selected template is saved to the hard disk on your local system.

b) Edit and save the template using a text editor.

c) Click **Apply**.

To revert to using the default notification pages:

a) Select the check box to the right of the template that you no longer want to use.

b) Click **Delete** in the **Templates** section of the **Advanced** tab.
   The selected notification page template is deleted from the appliance and the appliance reverts to using the relevant default notification pages.

c) Click **Apply**.
• To upload an image for use in a template:
  a) Click **Browse** in the **Images** section of the **Advanced** tab.
     The **File Upload** dialog box is displayed.
  b) Navigate to the directory in which you saved the modifications to the uploaded template files,
     select one of the modified notification template files, and click **Open**.
     The file is uploaded to the appliance.
  c) Click **Apply**.
• To delete an uploaded image:
  a) Select the check box to the right of the graphic that you want to delete.
  b) Click **Delete** in the **Images** section of the **Advanced** tab.
     The selected image is deleted from the appliance.
  c) Click **Apply**.

**Block Page Template**

The block page template allows you to modify the appearance of the various notification pages that
the web appliance displays to users when they try to access:

- virus-infected files
- malware
- blocked sites
- sites or applications that violate policy
- sites which will use or exceed their quota time
- restricted sites
- unapproved secure sites

This template affects neither the appearance of the patience page (the page displayed when users
request a large file download), nor the server error pages (HTTP error messages), for example, 404 File not Found or 500 Internal Server Error.

This template has very few required elements, and it provides a set of optional page element keys.
Apart from HTML requirements and the page element keys that are required for the appliance’s
administrative web interface, you are free to use or remove any of the optional page element keys
provided by the template and to modify the template as much as you like.

Right-click this link and select “Save Link As” or “Save Target As” to download the Block Page Template.

**Important**

If you plan to use a custom template, it is strongly recommended that you download the Sophos
template, available from the preceding link rather than using a template from another source.
Sophos cannot be held responsible for any malicious or problematic code included in other
templates or introduced in added code. Realize that such malicious or problematic code could be
distributed to many of your users if included in a custom template and, therefore, exercise caution.

**Required Elements**

The following elements are required:
• **DOCTYPE Declaration**: The provided HTML DOCTYPE declaration of XHTML 1.0, Strict, is required. You should not change this.

• `<div id="main" class="[full|mini]"> ... </div>`: This `<div>` tag can be used with the class attribute set to `full`. It will be automatically set to `mini` when the page is shown in an iframe. By default, the `full` option displays any graphics within these tags and contains no iframe layout settings. By default, the `mini` option hides any graphics within this tag and includes iframe layout settings, making this section full page width. The CSS settings controlling these options can, however, be modified.

This tag must wrap the visible content of the notification page, with the exception that banner or background images may be placed before this `<div>` tag.

• `%%sophos_blockpage_content%%`: This page element key must appear within the `<div id="main" class="[full|mini]"> ... </div>` tags. This content includes text entered in the Text explanation text box.

• `%%sophos_warn_proceed_content%%`: This page element key must appear within the `<div id="main" class="[full|mini]"> ... </div>` tags if you wish to use the Warn option in any of the policy pages.

• `%%sophos_feedback_content%%`: This page element key must appear within the `<div id="main" class="[full|mini]"> ... </div>` tags if you wish to enable the Allow user feedback option in any of the policy pages.

• `%%sophos_quota_proceed_content%%`: This page element key must appear within the `<div id="main" class="[full|mini]"> ... </div>` tags if you wish to use the Quota time option in any of the policy pages.

Note
Server-side scripting is not supported within this block page template.

Optional Elements

The following page element keys are available:

• **Client-side scripting**: You may add client-side scripting, such as JavaScript.

• `%%title%%`: It is suggested that you use this in the `<head>` section of the template. It provides the appropriate `<title>` for the block pages. Also, this page element key can also be used within the `<div id="main" class="[full|mini]"> ... </div>` tags of the template. In this location, it provides the appropriate in-page heading for the block pages. As this key is replaced with plain text, you may choose to wrap it in a div or heading tag; for example:

```
<h1>%%title%%</h1>
```

This content is drawn from text entered in the Page title text box.

• `%%server_address%%`: This page element key provides the fully qualified domain name (FQDN) of the web appliance. It is an essential initial part of the URL for any of the Sophos-supplied graphics, but the use of these is optional. If you continue to use any of these graphics, you must retain this page element key, as well as the rest of the URL for the graphic, `/resources/images/[filename.ext]`. For example:

```
%%server_address%%/resources/images/SophosImageFile.jpg
```

• `%%image_asset%%`: This page element key is used as the base URL for any graphic that you have uploaded in the Images section of the Advanced tab in the Configuration > Accounts >
**Notification Page Options** page. You must complete this URL by adding a slash (/) and the full filename of the uploaded graphic, for example:

```
%%image_asset%%/MyImageFile.jpg
```

- **%%user_name%%**: This page element key provides the name of the user who has made the request for the blocked page, as provided by Active Directory. If Active Directory is not available, the IP address from which the request was made will be displayed instead.

- **%%user_ip%%**: This page element key provides the IP address from which the request for the blocked page has been made.

- **%%user_workstation%%**: This page element key provides the hostname from which the request for the blocked page has been made. If this cannot be determined, the IP address will be displayed instead.

- **%%sophos_block_text%%**: This page element key provides the reason that a requested page has been blocked.

- **%%logo%%**: This page element key calls the logo set in the **Global Options** tab of the **Configuration > Accounts > Notification Page Options** page. This page element key is replaced with a string for the logo image like `<img src="path_to_logo/logo_filename" />`. Note that the **Display logo on notification pages** option must be enabled on the **Global Options** tab for this page element key to work.

- **%%alert_icon_class%%**: This page element key may be used as the value for the class attribute of the div to specify the display of an alert icon.

**Patience Page Template**

The patience page template allows you to modify the appearance of the patience page (the page displayed when users request a large file download).

This template affects neither the appearance of the server error pages (HTTP error messages), for example, 404 File not Found or 500 Internal Server Error, nor the various notification pages that the web appliance displays to users when they try to access:

- virus-infected files
- malware
- blocked sites
- sites or applications that violate policy
- restricted sites
- unapproved secure sites

This template has very few required elements, and it provides a set of optional page element keys. Apart from HTML requirements and the page element keys that are required for the appliance’s administrative web interface, you are free to use or remove any of the optional page element keys provided by the template and to modify the template as much as you like.

Right-click this link and select “Save Link As” or “Save Target As” to download the Patience Page Template.
Important
If you plan to use a custom template, it is strongly recommended that you download the Sophos template, available from the preceding link, rather than using a template from another source. It is required that the patience page use CSS that includes all of the elements from the sample patience template CSS for the page to be rendered properly. Sophos cannot be held responsible for any malicious or problematic code included in other templates or introduced in added code. Realize that such malicious or problematic code could be distributed to many of your users if included in a custom template and, therefore, exercise caution.

Required Elements

The following elements are required:

• **DOCTYPE Declaration**: The provided HTML DOCTYPE declaration of XHTML 1.0, Strict, is required. You should not change this.

• `<div class="alertTitle" id="heading">`: It is required that you have a div with id='heading'. It is recommended that you set its initial value as `%title%%`, for example:

```html
<div class="alertTitle" id="heading">
  %title%
</div>
```

The contents of the id=heading div will change as the patience page downloads and scans the file. It will also change appropriately if a virus/error is found.

• `%sophos_patience_content%`: This page element key must appear somewhere in the template. This content includes text entered in the Text explanation text box.

Note
Server-side scripting is not supported within this patience page template.

Note
There must not be a closing </body> or </html> tag in the patience template.

Optional Elements

The following page element keys are available, or can be used, depending upon your preference:

• **Client-side scripting**: You may add client-side scripting, such as JavaScript.

• `%title%`: It is suggested that you use this in the <head> section of the template. It provides the appropriate <title> for the patience page. Also, this page element key can also be used within the <div id="main" class="[full|mini]"> ... </div> tags of the template. In this location, it provides the appropriate in-page heading for the patience page. As this key is replaced with plain text, you may choose to wrap it in a div or heading tag; for example:

```html
<h1>%title%</h1>
```

This content is drawn from text entered in the Page title text box.
Sophos Web Appliance

- **%%server_address%%**: This page element key provides the fully qualified domain name (FQDN) of the web appliance. It is an essential initial part of the URL for any of the Sophos-supplied graphics, but the use of these is optional. If you continue to use any of these graphics, you must retain this page element key, as well as the rest of the URL for the graphic, /resources/images/[filename.ext]. For example:

  %%server_address%%/resources/images/SophosImageFile.jpg

- **%%image_asset%%**: This page element key is used as the base URL for any graphic that you have uploaded in the Images section of the Advanced tab in the Configuration > Accounts > Notification Page Options page. You must complete this URL by adding a slash (/) and the full filename of the uploaded graphic, for example:

  %%image_asset%%/MyImageFile.jpg

- **%%logo%%**: This page element key calls the logo set in the Global Options tab of the Configuration > Accounts > Notification Page Options page. Note that the Display logo on notification pages option must be enabled on the Global Options tab for this page element key to work.

**Error Page Template**

The error page template allows you to modify the appearance of the server error pages (HTTP error messages), for example, 404 File not Found or 500 Internal Server Error.

This template affects neither the appearance of the patience page (the page displayed when users request a large file download), nor the various notification pages that the web appliance displays to users when they try to access:

- virus-infected files
- malware
- blocked sites
- sites or applications that violate policy
- restricted sites
- unapproved secure sites

This template has very few required elements, and it provides a set of optional page element keys. Apart from HTML requirements and the page element keys that are required for the appliance’s administrative web interface, you are free to use or remove any of the optional page element keys provided by the template and to modify the template as much as you like.

Right-click this link and select “Save Link As” or “Save Target As” to download the Error Page Template.

**Important**

If you plan to use a custom template, it is strongly recommended that you download the Sophos template, available from the preceding link, rather than using a template from another source. Sophos cannot be held responsible for any malicious or problematic code included in other templates or introduced in added code. Realize that such malicious or problematic code could be distributed to many of your users if included in a custom template and, therefore, exercise caution.

**Required Elements**

The following elements are required:
• **DOCTYPE Declaration**: The provided HTML DOCTYPE declaration of XHTML 1.0, Strict, is required. You should not change this.

• `<div id="main" class="[full|mini]"> ... </div>`: This `<div>` tag can be used with the class attribute set to `full`. It will be automatically set to `mini` when the page is shown in an iframe. By default, the `full` option displays any graphics within these tags and contains no iframe layout settings. By default, the `mini` option hides any graphics within this tag and includes iframe layout settings, making this section full page width. The CSS settings controlling these options can, however, be modified.

This tag must wrap the visible content of the notification page, with the exception that banner or background images may be placed before this `<div>` tag.

• `%%sophos_error_content%%`: This page element key must appear after the `<div id="main" class="[full|mini]"> ... </div>` tags and immediately before the closing `</body>` tag. This content includes text entered in the Text explanation text box.

**Note**
Server-side scripting is not supported within this error page template.

### Optional Elements

The following page element keys are available, or can be used, depending upon your preference:

• **Client-side scripting**: You may add client-side scripting, such as JavaScript.

• `%%title%%`: It is suggested that you use this in the `<head>` section of the template. It provides the appropriate `<title>` for the error pages. Also, this page element key can also be used within the `<div id="main" class="[full|mini]"> ... </div>` tags of the template. In this location, it provides the appropriate in-page heading for the error pages. As this key is replaced with plain text, you may choose to wrap it in a div or heading tag; for example:

```html
<h1>%%title%%</h1>
```

This content is drawn from text entered in the Page title text box.

• `%%server_address%%`: This page element key provides the fully qualified domain name (FQDN) of the web appliance. It is an essential initial part of the URL for any of the Sophos-supplied graphics, but the use of these is optional. If you continue to use any of these graphics, you must retain this page element key, as well as the rest of the URL for the graphic, `/resources/images/[filename.ext]`. For example:

`%%server_address%%/resources/images/SophosImageFile.jpg`

• `%%image_asset%%`: This page element key is used as the base URL for any graphic that you have uploaded in the Images section of the Advanced tab in the Configuration > Accounts > Notification Page Options page. You must complete this URL by adding a slash (/) and the full filename of the uploaded graphic, for example:

`%%image_asset%%/MyImageFile.jpg`

• `%%logo%%`: This page element key calls the logo set in the Global Options tab of the Configuration > Accounts > Notification Page Options page. Note that the Display logo on notification pages option must be enabled on the Global Options tab for this page element key to work.
4.2 Group Policy

Use the Group Policy pages to configure how the web appliance policies are applied to specified user groups or are applied at specified times.

- Use the Default Policy page to configure how URL requests to sites categorized by content type and download types are handled by the web appliance, and to manage access to popular Web Applications.
- Use the Default Groups page to select the groups of users to which the default policy rules set on the Default Policy page are applied.
- Use the Special Hours page to configure a second set of rules about how URL requests to sites classified by content type and download types are handled by the web appliance that can be used during scheduled time periods.
- Use the Additional Policies page to create additional policies that can override the Default policy and the Special hours policy.
- Use the Local Site List page to view all of the URLs that have been added to the list and to manage that list. URLs are added to the list to extend the filtering provided by the web appliance to URLs not included in the Sophos site list or to override the default filtering specified in the Sophos site list.
- Use the Policy Test page to test the policy applied to a specified site with a specified user and, optionally, at a specified time.

Related concepts
Policy (page 47)

4.2.1 Default Policy

Use the Configuration > Default Policy pages to configure the default policies that are applied to all users and groups, and to manage access to popular Web Applications. Select either the Categories & Download Types or Web Applications tab to configure the related default policies.

Related tasks
Controlling Web Applications (page 91)
Categories & Download Types

The Configuration > Group Policy > Default Policy > Categories & Download Types page allows you to configure how URL requests to sites categorized by content type and files categorized by download type are handled by the web appliance.

1. Set the behavior that you want the web appliance to apply to each category listed in the Site categories section:
   - **Allow**: Lets users view sites of this classification.
   - **Warn**: Presents a warning to users that they are at risk of violating their organization’s web use policy, but allows them to proceed. Once a user has chosen to proceed, no warning page for that site will be displayed to that user for 30 minutes. If the site is in the Streaming Media category, proceeding will enable all streaming media for 30 minutes.
   - **Block**: Prevents users from viewing sites of this classification.

   **Important**
   Blocking Advertisements and Pop-ups also blocks content that appears behind interstitial pages, pages of advertising that appear prior to the loading of a requested content URL. In blocking these pages, the content that is behind them is also blocked.

2. **Allow user feedback** from the notification pages by selecting this check box or remove this option by clearing it.

   This option applies to only low risk sites and to medium risk sites if they have been configured to be scanned.

   **Note**
   If this option is enabled, users’ requests from notification pages for site recategorizations or to allow downloading of file types or PUAs can be viewed in the Search > User Submissions pages.

3. Select the download type controls that you want to apply.

   **Note**
   Download-type controls for Windows system files, Windows scripts, and Windows HTML App files are not supported in Endpoint Web Control.

   - **Allow**: Lets users download files of this type.
   - **Warn**: Presents a warning to users that they are at risk of violating their organization’s download policy, but allows them to proceed. A log entry is created when a user proceeds in possible contravention of the organization’s web use policy.
   - **Block**: Prevents users from downloading files of this type.

   **Note**
   The display of web appliance warning pages disrupts the playback of streaming media players, such as Windows Media Player, RealPlayer, and the QuickTime player. If you want to allow your users to play streaming media using any of these players, ensure that the Warn option is not selected.
Important
To enable access to Quicktime video with a warning displayed to users, set the Site category, "Streaming Media", with Warn enabled. Then set the Download type of "QuickTime Video (mov)" to Allow with Warn cleared. When users request a streaming QuickTime video URL, a warning page will be displayed, and when they click Proceed, the media stream will begin.

4. Select the Sandstorm profile that you want to apply.
   - Send any suspicious files for analysis: all suspicious downloaded items will be sent for analysis in the Sophos Active Sandbox component of Sophos Sandstorm.
   - Exclude suspicious PDFs and documents: send all suspicious downloads for analysis in the Sophos Active Sandbox, except PDFs and other documents.
   - Do not send suspicious files for analysis: do not send any downloaded items for analysis, even if they are suspicious.

Note
The Sandstorm option is not available if you do not have a Sophos Sandstorm license.

5. Block PUA Downloads from being downloaded by users by selecting this check box, or allow PUA downloads by clearing it.

Note
Specific PUAs can be allowed with this feature enabled by setting the exception on the Configuration > Global Policy > Download Options page.

6. Click Apply.

Related tasks
Web Applications (page 81)
Additional Policies (page 87)

Site Categories
The pages in this section describe the SophosLabs site categories.

Adult Sexually Explicit
This category includes sites for adult products including sex toys, CD-ROMs, and videos; child pornography and pedophilia (including the IWF list); adult services including video-conferencing, escort services, and strip clubs; erotic stories and textual descriptions of sexual acts; explicit cartoons and animation; online groups, including newsgroups and forums that are sexually explicit in nature; sexually-oriented or erotic sites with full or partial nudity; depictions or images of sexual acts, including with animals or inanimate objects used in a sexual manner; sexually exploitive or sexually violent text or graphics; bondage, fetishes, genital piercing; naturist sites that feature nudity; and erotic or fetish photography, which depicts nudity.

Note
We do not include sites regarding sexual health, breast cancer, or sexually transmitted diseases (except those with graphic examples).
Advertisements and Pop-ups
This category includes sites of banner ad servers, sites with pop-up advertisements, and sites with known adware.

Important
Blocking Advertisement and Pop-ups also blocks content that appears behind interstitial pages, pages of advertising that appear prior to the loading of a requested content URL. In blocking these pages, the content that is behind them is also blocked.

Note
Sophos’s advanced categorization data uses the most current technical definition for Adware, and thus recognizes the difference between non-malicious adware, such as “cookies” and more serious Spyware.

Alcohol and Tobacco
This category includes sites that promote or distribute alcohol or tobacco products for free or for a charge.

Arts
This category includes sites for museums, galleries, artist sites (sculpture, photography, etc.), performing arts (theater, vaudeville, opera, symphonies, etc.), dance companies, studios, and training; book reviews and promotions; and variety magazines and poetry.

Blogs and Forums
This category includes sites of weblogs (blogs), newsgroups, and opinion or discussion forums.

Business
This category includes general business corporate web sites, international and multi-national large general business corporate sites, business associations, and basic business sites, such as FedEx, that enable organizations to manage their necessary daily business tasks.

Note
Business sites that fit more appropriately into another related category, such as Finance or Travel, will be categorized in those categories.

Chat
This category includes sites of web-based chat and instant message servers.

Note
This category filters HTTP traffic only.

Computing and Internet
This category includes sites of reviews, information, buyer’s guides of computers, computer parts and accessories, computer software and internet companies, industry news and magazines, and pay-to-surf sites.

Criminal Activity
This category includes sites for advocating, instructing, or giving advice on performing illegal acts; tips on evading law enforcement; and lock-picking and burglary techniques.
**Custom**

This category is available for you to define a custom policy for whichever sites you assign to it. For example, you could set sites that you want to be always approved by adding them to your local classifications list, and setting their **Risk class** to **Trusted** and their **Site category** to **Custom**.

**Downloads**

This category includes sites for downloadable (non-streaming) movie, video or sound clips; downloadable PDA software, including themes and graphics; freeware and shareware sites; personal storage or backup sites; and clip art, fonts and animated .gif pages.

**Note**

This category does not include update sites such as those for operating systems, anti-virus agents, or other business-critical programs.

**Education**

This category includes sites for educational institutions, including pre-schools, elementary, secondary, and high schools and universities; educational sites at the pre-school, elementary, secondary, and high school and university levels; distance education and trade schools, including online courses; and online teacher resources (lesson plans, etc.).

**Entertainment**

This category includes sites about television, movies, music and video programming guides; online magazines and reviews of the entertainment industry; celebrity fan sites; broadcasting firms and technologies (satellite, cable, etc.); horoscopes; jokes, comics, comic books, comedians, or any site designed to be funny or satirical; online greeting cards; and amusement and theme park sites.

**Fashion and Beauty**

This category includes sites of fashion or glamor magazines, online beauty products, and cosmetics.

**Finance and Investment**

This category includes sites for stock quotes, stock tickers, and fund rates; online stock or equity trading; online banking and bill-pay services; investing advice or contacts for trading securities; money management or investment services or firms; general finances and companies that advise about finances; and accountancy, actuaries, banks, mortgages, and general insurance companies.

**Food and Dining**

This category includes sites for recipes, cooking instruction and tips, food products, and wine advisors; restaurants, cafes, eateries, pubs, and bars; and food and drink magazines and reviews.

**Gambling**

This category includes sites of online gambling or lottery web sites that invite the use of real or virtual money; information or advice for placing wagers, participating in lotteries, gambling, or running numbers; virtual casinos and offshore gambling ventures; sports picks and betting pools; and virtual sports and fantasy leagues that offer large rewards or request significant wagers.

**Note**

Casino, hotel, and resort sites that do not feature online gambling or provide gaming tips are categorized under Travel.
Games
This category includes sites for game playing or downloading, game hosting or contest hosting, tips and advice on games or obtaining cheat codes ("cheatz"), and journals and magazines dedicated to online game playing.

Government
This category includes sites for local, state, federal and international government sites, and government services, such as taxation, armed forces, customs bureaus, and emergency services.

Hacking
This category includes sites for the promotion, instruction, or advice on the questionable or illegal use of equipment and software for purpose of hacking passwords, creating viruses, gaining access to other computers and computerized communication systems; sites that provide instruction or workarounds for filtering software; cracked software and information sites; warez; pirated software and multimedia download sites; and computer crime sites.

Health and Medicine
This category includes sites for prescription medicines; medical information and reference about ailments, conditions, and drugs; general health, such as fitness and well-being; medical procedures, including elective and cosmetic surgery; dentistry, optometry, and other medical-related sites; general psychiatry and mental well-being sites; psychology, self-help books, and organizations; promoting self-healing of physical and mental abuses, ailments, and addictions; alternative and complementary therapies, including yoga, chiropractic, and cranio-sacral; and hospital and medical insurance sites.

Hobbies and Recreation
This category includes sites for recreational pastimes, such as collecting, gardening, and kit airplanes; outdoor recreational activities, such as hiking, camping, and rock climbing; tips or trends focused on a specific art, craft, or technique; online publications on a specific pastime or recreational activity; online clubs, associations, or forums dedicated to a hobby; traditional games, such as board games and card games, and their enthusiasts; and animal and pet related sites, including breed-specific sites, training, shows, and humane societies sites.

Hosting Sites
This category includes web sites that host business and individuals’ web pages, for example GeoCities, earthlink.net, and AOL.

Illegal Drugs
This category includes sites for recipes, instructions or kits for manufacturing or growing illicit substances for purposes other than industrial usage; glamorizing, encouraging, or instructing on the use of or masking the use of alcohol, tobacco, illegal drugs, or other substances that are illegal to minors; information on "legal highs", including glue sniffing, misuse of prescription drugs, or abuse of other legal substances; distributing illegal drugs free or for a charge; and displaying, selling, or detailing the use of drug paraphernalia.

Infrastructure
This category includes sites for content delivery networks, XML reference schemas, web analytics and statistics services, transaction servers, and corporate image servers.

Note
Sophos recommends that this category of its enhanced categorization data be used for monitoring and reporting purposes only.
Intimate Apparel and Swimwear

This category includes sites for lingerie, negligee, and other intimate apparel modeling; swimwear modeling; models' fan pages; modeling information and agencies; and fitness models and sports celebrities sites.

Intolerance and Hate

This category includes sites that advocate or incite degradation or attack of specified populations or institutions based on associations such as religion, race, nationality, gender, age, disability, or sexual orientation; sites that promote a political or social agenda that is supremacist in nature and exclusionary of others based on their race, religion, nationality, gender, age, disability, or sexual orientation; holocaust revisionist or denial sites and other revisionist sites that encourage hate; coercion or recruitment for membership in a gang\(^1\) or cult\(^2\); militancy and extremist sites; and flagrantly insensitive or offensive material, including those with a lack of recognition or respect for opposing opinions and beliefs.

Note
We do not include news, historical, or press incidents that may include the above criteria (except in graphic examples).

\(^1\) A gang is defined as: a group whose primary activities are the commission of felonious criminal acts, which has a common name or identifying sign or symbol, and whose members individually or collectively engage in criminal activity in the name of the group.

\(^2\) A cult is defined as: a group whose followers have been deceptively and manipulatively recruited and retained through undue influence such that followers' personalities and behavior are altered; a group in which leadership is all-powerful, ideology is totalistic, and the will of the individual is subordinate to the group; and a group that sets itself outside of society.

Job Search and Career Development

This category includes sites of employment agencies, contractors, job listings, career information, career searches, and career-networking groups.

Kids Sites

This category includes child-oriented sites and sites published by children.

Motor Vehicles

This category includes sites for car reviews, vehicle purchasing or sales tips, and parts catalogs; auto trading, photos, and discussion of vehicles including motorcycles, boats, cars, trucks, and RVs; journals and magazines on vehicle modification, repair, and customization; and online automotive enthusiast club sites.

News

This category includes online newspapers, headline news sites, newswire services, personalized news services, and weather sites.

Peer-to-Peer

This category includes peer-to-peer file sharing clients and peer-to-peer file sharing servers.

Personals and Dating

This category includes singles listings, matchmaking and dating services, advice for dating or relationships, and romance tips and suggestions sites.
Philanthropic and Professional Organizations
This category includes sites of philanthropic and charity organizations, environmental organizations, professional associations, labor unions, and social organizations.

Phishing and Fraud
This category includes sites involved in phishing and telephone scams, service theft advice sites, and plagiarism and cheating sites, including the sale of research papers.

Photo Searches
This category includes sites that provide resources for photography, image searches, online photo albums, digital photo exchanges, and image hosting.

Politics
This category includes sites for political parties; political debate, canvassing, election information, and results; and conspiracy theory and alternative government view sites that are not hate-based.

Proxies and Translators
This category includes sites for remote proxies or anonymous surfing, search engine caches that circumvent filtering, and web-based translation sites that circumvent filtering.

Real Estate
This category includes sites for home, apartment, and land listings; rental or relocation services; tips on buying or selling a home; real estate agents; and home improvement sites.

Reference
This category includes sites for personal, professional, or educational reference; online dictionaries, maps, and language translation sites; census, almanacs, and library catalogs; and topic-specific search engines.

Religion
This category includes sites of churches, synagogues, and other houses of worship; any faith or religious belief sites, including non-traditional religions such as Wicca and witchcraft.

Ringtones and Mobile Phone Downloads
This category includes sites of providers of mobile phone downloads, including ringtones, logos, backgrounds, screensavers, and games.

Search Engines
This category includes general search engines, such as Yahoo, AltaVista, and Google.

Sex Education
This category includes sites with pictures or text advocating the proper use of contraceptives; sites relating to discussion about the use of the pill, IUDs, and other types of contraceptives; and discussion sites on how to talk to your partner about diseases, pregnancy, and respecting boundaries.

Note
Not included in the category are commercial sites that sell sexual paraphernalia. These sites are typically found in the Adult category.

Shopping
This category includes sites for department stores, retail stores, company catalogs, and other sites that allow online consumer shopping, sites for online auctions, online downloadable product warehouses, specialty items for sale, and freebies or merchandise giveaways.
Society and Culture

This category includes sites on home life and family-related topics, including weddings, births and funerals; parenting tips and family planning; non-pornographic gay, lesbian, and bisexual issues; foreign cultures and socio-cultural information; and non-explicit tattoo and piercing parlors.

Spam URLs

This category includes URLs found in spam, particularly on these topics: computing, finance and stocks, entertainment, games, health and medicine, humor and novelties, personal and dating, products and services, shopping, and travel.

Sports

This category includes sites for team or conference web sites; national, international, college, professional scores and schedules; sports-related online magazines or newsletters; and fantasy sports and virtual sports leagues that are free or low-cost.

Spyware

This category includes sites that provide or promote information gathering or tracking that is unknown to, or done without the explicit consent of, the end user or the organization, including sites that carry malicious executables or viruses, third party monitoring, and other unsolicited commercial software, spyware, and malware "phone home" destinations.

Note

The technical definition of Spyware used for this category may not exactly match the definition used elsewhere by Sophos. This category focuses on filtering malicious and tracking content, not simply adware and cookies. For non-malicious adware filtering, please block the Advertisements and Pop-ups category.

Streaming Media

This category includes sites for streaming media files or events (any live or archived audio or video file), Internet TV and radio, non-explicit personal webcam sites, telephony sites that allow users to make calls via the internet, and VoIP services.

Tasteless and Offensive

This category includes sites that feature offensive or violent language, including through jokes, comics, or satire, and excessive use of profanity or obscene gesticulation.

Travel

This category includes sites of airlines and flight booking agencies, accommodation information, travel package listings, city guides and tourist information, and car rentals.

Uncategorized

This category includes all sites that have not been categorized. This means that these sites have not come to the attention of Sophos Labs.

Violence

This category includes sites portraying, describing or advocating physical assault against humans, animals, or institutions; depicting torture, mutilation, gore, or horrific death; advocating, encouraging, or depicting self-endangerment, or suicide, including through eating disorders or addictions; instructions, recipes, or kits for making bombs or other harmful or destructive devices; sites promoting terrorism; and excessively violent sports or games, including videos and online games.
Note
We do not block news, historical, or press incidents that may include the above criteria, except those that include graphic examples.

**Weapons**

This category includes sites with online purchasing or ordering information, including lists of prices and dealer locations; any page or site predominantly containing, or providing links to, content related to the sale of guns, weapons, ammunition or poisonous substances; displaying or detailing the use of guns, weapons, ammunition or poisonous substances; and clubs which offer training on machine guns, automatics, other assault weapons, and sniper training.

Note
Weapons are defined as something (as a club, knife, or gun) used to injure, defeat, or destroy.

**Web-Based Email**

This category includes sites for web-based e-mail accounts and messaging sites.

**Web Applications**

The **Configuration > Group Policy > Default Policy > Web Applications** page allows you to configure the default policy for popular Web Applications, such as Facebook, or Linkedin. Settings configured on this page take precedent over policy configured for categories or tags.

Note
If you do not have HTTPS scanning enabled on the **Configuration > Global Policy > HTTPS Scanning** page, detection and control of web applications will not work for sites that use HTTPS.

1. Next to the related web application click the **Action** drop down menu.
2. Select a policy for an application by selecting an option from the related **Action** drop down menu:
   - Choose **Allow** to allow access to the web application.
   - Choose **Block** to block access to the web application.
   - Choose **Follow Category** to allow the site category to control access to the web application.
3. For web applications that are set to **Allow** you can also configure **Enabled features**:
   a) Click on the row for an application.
   b) Ensure that only the features you want enabled are selected. For instance, if only **Status Update** is not selected under **Enabled features** for Facebook only status updates will be disabled. Access to the rest of the site will be allowed.
4. Click **Apply**

**Related tasks**

**Categories & Download Types** (page 73)
**Configuring Sandstorm** (page 101)

Sophos Sandstorm is a cloud-based service that provides enhanced protection against new and targeted attacks. You can configure the appliance to send suspicious files to Sandstorm for analysis or submit suspicious files on an individual basis. Sandstorm detonates the file to check for malware and
sends the results to you. Because the analysis takes place in the cloud, your system is never exposed to potential threats.

4.2.2 Default Groups

The Configuration > Group Policy > Default Groups page allows you to set the user groups to which the default policy is applied. If Active Directory or eDirectory access has been properly configured, the Available groups list is populated with your organization’s Active Directory or eDirectory groups.

If your appliance is configured to access a single-domain Active Directory server, Active Directory group names are displayed in the form "groupname"; if the appliance is configured to access the global catalog of a multidomain Active Directory forest, Active Directory group names are displayed in the form "domain\groupname". If the appliance is configured to integrate with eDirectory, then group names are displayed in eDirectory format (group.context).

Alternatively and additionally, you can create, edit, and delete custom groups. Once the Available groups list is populated to meet your requirements, you can select which groups are denied or allowed access to the internet, depending upon which policy association option you have selected.

Creating a Custom User Group

1. In the Available Groups list, click Create.

The Group Editor dialog box is displayed.

Note
The groups that are added in this window are also added to the Reports > Options > Reporting Groups page.

2. In the top text box, enter a name for the group.

3. Use at least one of the following methods to select the members of the new custom group:

   a) Click the Groups tab, highlight the groups that you want to include in your custom group, and click the double-right arrow (>>) to move the selected groups into the Selected Entries list.

   b) Click the Users tab, highlight the users that you want to include in your custom group, and click the double-right arrow (>>) to move the selected users into the Selected Entries list.

   c) Optionally, to remove a group or user from the Selected Entries list, highlight the item(s) that you want to remove from the custom group, and click the double-left arrow (<<).

   d) To add manual entries that are not listed in the Groups or Users lists, do the following:

      i) In the text box in the Manual Entries section, enter a username, IP address, or an IP address range, and click Add.

      Usernames must be in the form DOMAIN\username for Active Directory and user.context for eDirectory. IP address ranges must be in CIDR format.
Important

The web appliance will interpret any dotted quad followed by a slash and a number less than 33 as a CIDR range. This creates the possibility that a URL entered as an IP address followed by a numbered directory from 0 to 32 would be improperly treated as a CIDR range. To avoid this possibility, always enter URLs to numbered directories using fully qualified domain names rather than IP addresses.

After clicking Add, the entry is displayed in the Manual Entries list.

II) Optionally, to delete an item from the list, select the check box to the right of the entry that you want to delete, and click Delete.

The selected item is removed from the Entries list.

4. Once you have the list of group members that you want in the Selected Entries and Manual Entries lists, click Save.

The Group Editor dialog box closes and you are returned to the Configuration > Group Policy > Default Groups page with the newly created custom group shown in the Available Groups list.

5. Click Apply.

Editing a Custom User Group

1. Click the name of the custom group that you want to edit.

Note

Custom groups, which can be edited, are indicated by a Sophos icon ( ); Active Directory and eDirectory groups, which cannot be edited, are indicated by a directory icon ( ).

The Group Editor dialog box is displayed with the selected list properties displayed.

Note

The group changes that you make in this window are also displayed on the Reports > Options > Reporting Groups page.

2. Optionally, in the top text box, enter a new name for the group.

3. Optionally, use any of the following methods to change the members for the selected custom group:

   a) Click the Groups tab, highlight the groups that you want to add to your custom group, and click the double-right arrow (>>) to move the selected groups into the Selected Entries list.

   b) Click the Users tab, highlight the users that you want to add to your custom group, and click the double-right arrow (>>) to move the selected users into the Selected Entries list.

   c) To remove a group or user from the Selected Entries list, highlight the item(s) that you want to remove from the custom group, and click the double-left arrow (<<).

   d) To add manual entries that are not listed in the Groups or Users lists, do the following:
I) In the text box in the **Manual Entries** section, enter a username, IP address, or an IP address range, and click **Add**.

Usernames must be in the form `DOMAIN\username` for Active Directory and `user.context` for eDirectory. IP address ranges must be in CIDR format.

**Important**
The web appliance will interpret any dotted quad followed by a slash and a number less than 33 as a CIDR range. This creates the possibility that a URL entered as an IP address followed by a numbered directory from 0 to 32 would be improperly treated as a CIDR range. To avoid this possibility, always enter URLs to numbered directories using fully qualified domain names rather than IP addresses.

After clicking **Add**, the entry is displayed in the **Manual Entries** list.

II) Optionally, to delete an item from the list, select the check box to the right of the entry that you want to delete, and click **Delete**.

The selected item is removed from the **Manual Entries** list.

4. Once you have modified the name, or the list of group members that you want in the **Selected Entries** and **Manual Entries** lists, click **Save**.

The **Group Editor** dialog box closes and you are returned to the **Configuration > Group Policy > Default Groups** page with the modified custom group listed in the **Available groups** list.

5. Click **Apply**.

### Deleting a Custom User Group

1. In the **Available groups** list, select the check box to the right of the custom group(s) that you want to delete.

The custom group that you want to delete must not be in the **Selected Entries** list.

**Note**
Custom groups, which can be deleted, are indicated by a Sophos icon ();$;
Active Directory and eDirectory groups, which cannot be deleted, are indicated by a directory icon ();$.

**Note**
The groups that are deleted in this window are also removed from the **Reports > Options > Reporting Groups** page.

2. Click **Delete**.

The selected custom group(s) is removed from the **Available Groups** list.

3. Click **Apply**.

### Applying the Default Policy to Groups

1. Select the desired **Default Policy association** option button.
You can choose between:

- **All users/groups except those selected below** This will block internet access for users in the selected groups and apply the default policy for internet access to all others.

- **Only the users/groups selected below** This will apply the default policy for internet access for users in the selected groups and block access to all others.

2. In the **Available Groups** list, select the groups that will be blocked (if you chose the first option in step 1) or that will have the default policy applied to their browsing (if you chose the second option in step 2).

   You can **Shift-click** to select a range of groups, or **Ctrl-click** to select several groups individually.

3. Click the right arrow button, (>), to move the selected groups into the **Selected groups** list.

4. Click **Apply**.

### 4.2.3 Special Hours

The **Configuration > Group Policy > Special Hours** page allows you to set a second policy to override the rules of the default policy controlling how URL requests to sites (categorized by content type) and to files (categorized by download type) are handled. You then define the hours during which these rule overrides are used instead of the **Default Policy** page rules.

For example, if you want to apply a default policy that restricts users from accessing sites that reduce productivity during regular working hours, but you want to allow users to access those sites outside of regular working hours, you can configure the special hours policy to apply from the end of regular work hours to the beginning of regular work hours and during the lunch hour too.

**Related tasks**

**Configuring Sandstorm** (page 101)

Sophos Sandstorm is a cloud-based service that provides enhanced protection against new and targeted attacks. You can configure the appliance to send suspicious files to Sandstorm for analysis or submit suspicious files on an individual basis. Sandstorm detonates the file to check for malware and sends the results to you. Because the analysis takes place in the cloud, your system is never exposed to potential threats.

**Setting a Special Hours Policy**

1. Set the schedule during which the special hours policy will apply:

   a) Set the main block of time during which the special hours policy will apply by selecting **Daily from** and setting the beginning and end times by using the adjacent time selector controls.

      You can set the times by clicking beside either the hour, minute, or meridian (AM or PM) setting and scrolling with your mouse wheel until you get the time that you want.

   b) Optionally, set a second block of time during which the special hours policy will apply by selecting **And from** and setting the beginning and end times by using the adjacent time selector controls.

      You can set the times by clicking beside either the hour, minute, or meridian (AM or PM) setting and scrolling with your mouse wheel until you get the time that you want.

   c) Optionally, select the check box **and all day on weekends** to apply the special hours policy settings 24 hours per day throughout the weekends as well, which overrides the time blocks set in the **Daily from** and **And from** time settings.
Note
You can also set which days of the week are treated as the weekend by clicking *weekends* and selecting only those days that you want treated as weekend days.

2. Set the policy rules for the **Site categories** and **Download types**, as well as for the **Sandboxing Profile**, **Allow user feedback**, and **Block potentially unwanted applications** options in the same way as you did on the **Default Policy** page:

a) Set the behavior that you want the web appliance to apply to each category listed in the **Site categories** section.
   - **Allow**: Lets users view sites of this classification.
   - **Warn**: Presents a warning to users that they are at risk of violating their organization’s web use policy, but allows them to proceed. Once a user has chosen to proceed, no warning page for that site will be displayed to that user for 30 minutes.
   - **Block**: Prevents users from viewing sites of this classification.

   **Important**
   Blocking **Advertisements and Pop-ups** also blocks content that appears behind interstitial pages, pages of advertising that appear prior to the loading of a requested content URL. In blocking these pages, the content that is behind them is also blocked.

b) Select the **Sandstorm** profile that you want to apply.
   - **Send any suspicious files for analysis**: all suspicious downloaded items will be sent for analysis in the **Sophos Active Sandbox** component of **Sophos Sandstorm**.
   - **Exclude suspicious PDFs and documents**: send all suspicious downloads for analysis in the **Sophos Active Sandbox**, except PDFs and other documents.
   - **Do not send suspicious files for analysis**: do not send any downloaded items for analysis, even if they are suspicious.

   **Note**
   The **Sandstorm** option is not available if you do not have a **Sophos Sandstorm** license.

c) **Allow user feedback** from the notification pages by selecting this check box or remove this option by clearing it.

   **Note**
   If this option is enabled, users’ requests from notification pages for site recategorizations or to allow downloading of restricted file types or PUAs can be viewed on the **Search > User Submissions** pages.

d) Select the controls that you want to apply to the web appliance’s handling of each of the file **Download types**.
   - **Allow**: Lets users download files of this type.
   - **Warn**: Presents a warning to users that they are at risk of violating their organization’s download policy, but allows them to proceed.
   - **Block**: Prevents users from downloading files of this type.
e) **Block potentially unwanted applications** from being downloaded by users by selecting this check box or allow PUA downloads by clearing it.

Note
Specific PUAs can be allowed with this feature enabled by setting the exception on the **Configuration > Global Policy > Download Options** page.

3. Click **Apply**.

**Related tasks**
- Configuring Tags (page 92)
- Configuring Sandstorm (page 101)

Sophos Sandstorm is a cloud-based service that provides enhanced protection against new and targeted attacks. You can configure the appliance to send suspicious files to Sandstorm for analysis or submit suspicious files on an individual basis. Sandstorm detonates the file to check for malware and sends the results to you. Because the analysis takes place in the cloud, your system is never exposed to potential threats.

**Disabling a Special Hours Policy**

1. Ensure that the **Daily from**, **And from**, and **And all day on weekends** check boxes are all cleared.
2. Click **Apply**.

**4.2.4 Additional Policies**

The **Configuration > Group Policy > Additional Policies** page allows you to set additional policies that can be used as exceptions to the Default Policy and the Special Hours policy and which are executed as part of the web appliance’s policy filtering process.

Additional policies are added or modified in the **Additional Policy** editor. The additional policies that have been added are arranged by execution priority (enabled or disabled) and deleted on the **Additional Policies** page.

Note
The **Quarantined Machines** policy is a default policy that cannot be deleted, turned off, or have its priority changed. This policy manages machines which have been blocked because they have been detected attempting to contact malware command and control services. This policy applies only to machines connecting from inside your network.

- To add a policy:
  a) Click **Add**.
  
The **Additional Policy** editor is displayed.
  
  b) Configure the new special policy on the seven tabs of the **Additional Policy** editor:
  
  — **Selecting Users** (page 89): specify the groups or users to which the additional policy will apply.
  
  — **Configuring Site Categories** (page 90): set overrides to both the Default and Special Hours policy’s handling of site categories.
— **Configuring Download Types** (page 91): set overrides to the Default and Special Hours policy’s handling of download types.

— **Controlling Web Applications** (page 91): configure how the additional policy differs from the default policy for specific web applications.

— **Configuring Tags** (page 92): set what actions will be applied to tags.

— **Additional Options** (page 94): set additional options, including sandboxing, quota minutes, and whether to disable logging for the new addditional policy.

— **Name and Schedule** (page 95): set the name of the new additional policy, schedule when it will apply, set whether it is enabled, and if it will be deactivated at a predefined date and time.

Once created, the new policies appear in the **Additional Policies** list in the order they were created.

- **To edit an additional policy**, click the name of the additional policy that you want to modify in the **Policy Name** column and make the required changes on the pages of the **Additional Policy editor**.

- **To set the order in which the special policies will be applied**, click the up or down arrows in the **Priority** column beside the special policy for which you want to change the priority to move that policy up or down in the list, and click **Save Order** to save the priority order.

  Optionally, click **Reset Order** to return to the last saved priority order.

- **To set the operational status for a policy**, either click **Turn On** in the row of the policy that you want to enable, or click **Turn Off** in the row of the policy that you want to disable.

  **Note**

  A warning icon will appear in the **Active** column if the time period for the policy is set to **Special Hours** and the special hours policy has been deactivated. This only happens if the Special Hours policy is deactivated after an Additional Policy was created based on the previous Special Hours policy. You cannot define a policy based on a Special Hours if Special Hours is not activated.

- **To remove a special policy**, select the check box to the right of the additional policy that you want to remove, and click **Delete**.

**Related concepts**

- Using Tags (page 93)
- About Authentication (page 131)
- Policy & Content: Advanced Threat Protection (page 167)

**Related tasks**

- Web Applications (page 81)
- Categories & Download Types (page 73)
- Configuring the Local Site List (page 96)
- Using the Local Site List Editor (page 97)

**Quota Time**

Policies created under **Configuration > Group Policy > Additional Policies** can be configured using the quota time feature. Quota time allows you to create a policy that allows access to certain sites for a limited amount of time in a day. For instance, you may want to limit access to social media sites without blocking them completely. Using the quota time feature, you can create policies for
different users and groups to limit access based on categories and tags to a specified amount of browsing time.

When creating a policy in the **Additional Policy Wizard**, you can choose **Quota** from the **Action** drop-down on both the **Site Categories** and **Tags** page, and then set the allowed minutes for that policy on the **Name and Schedule** page. All categories and tags set to **Quota** for an additional policy will count towards the allowed minutes for that quota, which can be configured on the **Name and Schedule** page of the **Additional Policy Wizard**.

**Note**

Sophos Endpoint Web Control cannot enforce quota time. If you use Endpoint Web control you can configure an alternate action on the **Configuration > System > Endpoint Web Control** page. By default, Endpoint Web Control will warn a user when browsing to a site associated with a quota time policy.

**Related tasks**

[Controlling Web Applications](page 91)
[Endpoint Web Control](page 144)

**Selecting Users**

On the **Select Users** page of the **Additional Policy** wizard:

- Set the users or groups to which you want the additional policy to apply:
  - In the **Groups** list, select the groups that you want, and click the right arrow button to move them to the **Selected groups** list.
    
    This list will be populated with Active Directory or eDirectory groups (if Active Directory or eDirectory has been properly configured) as well as any custom groups added on the **Default Groups** or **Reporting Groups** pages.

    - On the **Users** tab, select the users that you want, and click the right arrow button to move them to the **Selected Entries** list.

    This list will be populated with Active Directory or eDirectory users (if Active Directory or eDirectory integration has been properly configured).

- In the text box in the **Manual Entries** section, enter a username, IP address, or an IP address range, and click **Add**.

  Usernames must be in the form **DOMAIN\username** for Active Directory and **user.context** for eDirectory. IP address ranges must be in **CIDR** format, using full dotted quad notation (**X.X.X.X/X**).

  The entry is displayed in the **Manual Entries** list.

- To delete an entry from the **Manual Entries** list, select the check box beside the entry that you want to remove, and click **Delete**.

**Note**

If there are long lists of entries in the **Groups**, **Users**, or **Selected Entries** lists, you can use the paging controls at the top of these lists to navigate through the lists, or use the filtering controls at the bottom to reduce the number of items that are displayed.

The individuals or groups (or their IP addresses or range of IP addresses) listed in both the **Selected Entries**, and the **Manual Entries** lists are affected by the new policy that you are creating.
Note
Additional policies are applied as exceptions to, or extensions of, the default policy, so if you add a user to an additional policy who is exempt from the default policy, they will become subject to the default policy with the additional policy differences.

• Once the users to which this additional policy will apply are set, move to the next page of the wizard by clicking either the Site Categories icon or the Next button.

Configuring Site Categories

On the Site Categories page of the Additional Policy wizard, you can modify any of the default policy settings or leave them unchanged to accept the default.

Note
The current option, whether it is Allow, Warn, or Block, is shown as Use default, indicating the state as set in the default or special hours policy at the time that the additional policy is first created.

• Modify the settings or accept the default settings for any of the Site Categories that you want to change by selecting:
  — Allow (green): If selected, lets users view sites of this category; if cleared, denies users the ability to view them.
  — Warn (yellow): If selected, presents a warning to users that they are at risk of violating their organization’s web use policy, but allows them to proceed to their requested page. Once a user has chosen to proceed, no warning page for that site will be displayed to that user for 30 minutes. A log entry is created when a user does proceed in possible contravention of the organization’s web use policy. If cleared, no warning is given.
  — Block (red): If selected, prevents users from viewing sites of this category, and displays a warning page explaining the reason why access is blocked.
  — Quota (blue): If selected, presents a page to users that allows them to select how much quota time they wish to consume. Once a user has chosen to proceed, no warning page for that site will be displayed to that user until they have used their current selection of quota time. After they have consumed all of their available quota time, they will be presented with a block page that informs them they have no quota time remaining.
  — Use default (gray): This is the current setting, to which you can restore any changed category.

Note
Rules that have been overridden are displayed with the background color associated with that setting: Allow is green, Warn is yellow, and Block is red. This does not necessarily mean that the override setting is different from the default or special hours policy setting. It only indicates that this option is no longer drawn from the default or special hours policies settings.

Important
Blocking Advertisements and Pop-ups also blocks content that appears behind interstitial pages (pages of advertising that appear prior to the loading of a requested content URL). In blocking these pages, you are also blocking access to the content that is behind them.
• Modify the settings or accept the default settings for the **Allow user feedback** option.

**Note**
If the **Allow user feedback** option is set to **Yes**, users’ requests for site reclassifications can be viewed on the **Search > User Submissions** pages.

• Once the category handling for this additional policy is set, move to the next page of the wizard by clicking either the **Download Types** icon or the **Next** button.

**Related tasks**
[Controlling Web Applications](#) (page 91)
[Configuring the Local Site List](#) (page 96)

### Configuring Download Types
On the **Download Types** page of the **Additional Policy** wizard, you can modify any of the default policy settings or leave them unchanged to accept the default.

• Modify the settings or accept the default settings for any of the **Download Types** that you want to change by selecting:

  — **Allow** (green): If selected, lets users download content of this type; if cleared, denies users the ability to download them.

  — **Warn** (yellow): If selected, presents a warning to users that they are at risk of violating their organization’s web use policy, but allows them to proceed with their requested downloads of this type. A log entry is created when a user does proceed in possible contravention of the organization’s web use policy.

  — **Block** (red): If selected, prevents users from downloading content of this type and displays a warning page explaining the reason why access is blocked.

  — **Use default** (gray): This is the current setting, to which you can restore any changed type.

**Note**
Rules that have been overridden are displayed with the background color associated with that setting: Allow is green, Warn is yellow, and Block is red. This does not necessarily mean that the override setting is different from the default or special hours policy setting, it only indicates that this option is no longer drawn from the default or special hours policies settings.

• Modify the settings or accept the default settings for the **Block potentially unwanted applications** option.

• Once the category handling for this additional policy is set, move to the next page of the wizard by clicking either the **Tags** icon or the **Next** button.

### Controlling Web Applications
On the **Web Applications** page of the **Additional Policy** wizard you can configure how your additional policy differs from the default policy for each web application. The default behavior is to **Use default**.

1. Click the drop-down menu under **Action**.

   • **Use default** will use the Default Policy.
Sophos Web Appliance

- Choose **Allow** to allow access to the web application.
- Choose **Block** to block access to the web application.
- Choose **Quota** to allow access to the web application, but have it count towards your Quota Time.
- Choose **Follow Category** to allow the site category to control access to the web application.

2. For web applications that are set to **Allow** or **Quota**, you can also configure **Enabled features**:
   a) Click on the row for an application.
   b) Ensure that only the features you want enabled are selected.
      For instance, if only **Status Update** is not selected under **Enabled features** for Facebook only status updates will be disabled. Access to the rest of the site will be allowed.

3. Click **Next** or **Save**.

**Related concepts**
- Quota Time (page 88)
- Default Policy (page 72)

**Related tasks**
- Configuring Site Categories (page 90)
- Configuring Tags (page 92)
- Configuring the Local Site List (page 96)

### Configuring Tags

Adding tags to your additional policy is optional. Tags allow you to set policy rules more simply and flexibly than is possible by using other policy features.

Tags can be created in two places: this wizard and the **Local Site List Editor** dialog box, which is accessed on the **Configuration > Group Policy > Local Site List** page. In the **Local Site List Editor** dialog box, you can apply one or more tags to a URL. In the **Additional Policy** wizard, you can set what action is taken in response to a tag. For tags to work, you must perform the configuration steps in both places.

1. In the **Tag** editable drop-down list, either enter the name of a new tag that you want to create in the text box, or click the adjacent down arrow icon to choose an existing tag from the drop-down list.

   **Note**
   There is no need to delete tags. Any tags that are not applied to URLs in the Local Site List and that do not have an additional policy set are automatically removed every Sunday night at midnight.

2. From the **Action** drop-down list, select the action that you want taken in response to the tag. The available actions are:
   - **Allow**: If selected, allows access to the sites to which this tag has been applied.
   - **Warn**: If selected, presents a warning to users that they are at risk of violating their organization’s web use policy, but allows them to access the sites to which this tag has been applied.
   - **Block**: If selected, prevents users from accessing the sites to which this tag has been applied.
   - **Quota**: If selected, allows users to select a portion of their allotted quota time and continue browsing. Once all of a user’s quota time has been consumed, prevents them from accessing the sites to which this tag has been applied.
3. Once you have set the action that you want taken to the selected tag, click Add. A line is added to the list that shows the Tag name and the Action that will be taken.

4. Optionally, you can remove a tag from the list by selecting the check box to the right of the tag that you want to remove and clicking Delete.

5. Repeat the preceding steps as often as required to set as many tags and actions as are required for your additional policy.

6. Move to the next page of the wizard by clicking either the Name and Schedule icon or the Next button.

Related concepts
Using Tags (page 93)
Quota Time (page 88)

Related tasks
Controlling Web Applications (page 91)
Configuring the Local Site List (page 96)
Using the Local Site List Editor (page 97)
Configuring Sandstorm (page 101)

Sophos Sandstorm is a cloud-based service that provides enhanced protection against new and targeted attacks. You can configure the appliance to send suspicious files to Sandstorm for analysis or submit suspicious files on an individual basis. Sandstorm detonates the file to check for malware and sends the results to you. Because the analysis takes place in the cloud, your system is never exposed to potential threats.

Categories & Download Types (page 73)
Setting a Special Hours Policy (page 85)

Using Tags
Tags allow you to set properties to individual websites, so that set policy rules may enforce an action on these individual sites, regardless of the policy applied to the category in which the sites belong. This is implemented more simply and flexibly than is possible by using other policy features.

Using tags, you can fine tune a policy to the point of applying default policy overrides for individual users. For example, in your organization, you may wish to create a policy that allows the CEO to visit a number of news websites, even though the News category is blocked by default for the entire organization.

This can be done in two simple steps:

1. Tags are created and applied to a URL on the Configuration > Group Policy > Local Site List page’s Local Site List Editor dialog box. In the Local Site List Editor dialog box, you can create and apply one or more tags to a URL.

2. Once tags are applied to one or more URLs, you can set the policy for a tag on the fourth tab of the Configuration > Group Policy > Additional Policy page’s Additional Policy wizard. On the Tags tab of the Additional Policy wizard, you select the tag for which you want to set policy from a drop-down list of all the available tags. or enter the name for a new tag. Then you select the action that you want applied to URLs marked with this tag. Because additional policies are applied to only those users that you select on the first tab of the Additional Policy wizard, this tag-based policy can be applied to as few or as many individuals or groups as you want.

For tags to work, you must perform these configuration steps in both the Local Site List Editor and the Additional Policy wizard. If you start by creating a new tag in the Additional Policy wizard and applying policy to that tag, you must reverse the steps listed above and subsequently add this new tag to the URLs of your choice in the Local Site List Editor.

There are, however, three system tags, Globally allowed sites, Globally blocked sites, and Never send to Sandstorm. These tags only appear in the Local Site List Editor dialog box’s tag drop-
down list. Their actions are predefined and match what their name indicates. The **Globally allowed sites** tag will not override the behavior expected as a result of a site’s risk class.

**Note**
There is no need to delete tags. Any tags that are not applied to URLs in the Local Site List and that do not have an additional policy set are automatically removed every Sunday night at midnight.

**Related tasks**
Configuring the Local Site List (page 96)
Using the Local Site List Editor (page 97)
Additional Policies (page 87)
Configuring Tags (page 92)

**Additional Options**

On the **Additional Options** page of the **Additional Policy** wizard:

1. Select the **Sandstorm** profile that you want to apply.
   - **Use default**: use the default Sandstorm profile.
   - **Send any suspicious files for analysis**: all suspicious downloaded items will be sent for analysis in the **Sophos Active Sandbox** component of **Sophos Sandstorm**.
   - **Exclude suspicious PDFs and documents**: send all suspicious downloads for analysis in the **Sophos Active Sandbox**, except PDFs and other documents.
   - **Do not send suspicious files for analysis**: do not send any downloaded items for analysis, even if they are suspicious.

   **Note**
The **Sandstorm** option is not available if you do not have a **Sophos Sandstorm** license.

2. Under **Quotas** select the number of quota minutes allowed for this policy.
   The browse time for all categories and tags that have been set to **quota** will count toward the browse time selected here.

   **Note**
   If you update the allowed browse time, the new setting will not take effect until the next day. If you need the new browse time to take effect immediately, you can manually reset users’ quota times on the **Configuration > Group Policy > Quota Status** page.

3. Optionally, select **Don’t log traffic for this policy** if you do not wish to record logging information for users and actions associated with this policy.

4. Click **Next** or **Save**.

**Related concepts**

*Quota Time* (page 88)
Name and Schedule

On the Name and Schedule page of the Additional Policy wizard:

1. In the Policy name text box, enter the name for the added policy.
2. In the Effective time panel, set the time during which you want the policy to apply.
   a) Select either:
      • All the time: The policy will always apply.
      • Specified times: If you select this option, you must select one of the following options from the drop-down list:
        — Regular hours: The policy will apply during regular hours (not during Special Hours).
        — Special Hours: The policy will apply during special hours (as defined on the Special hours page).
        — Custom times: If you select this option, you must set at least one custom time by doing the following:
          I) Set the start and end times by using the From and to time-selector controls.
             You can set the times by clicking beside either the hour, minute, or meridian (AM or PM) setting and scrolling with your mouse wheel until you get the time that you want.
          II) Select the days of the week check boxes for the days on which you want the additional policy to apply.
          III) Click Add to add the date and time setting to the list of custom times.
             You can select multiple date and time settings, but the times that you select must be chronological: the From time cannot follow the to time. For example, you cannot set a time range ending at 12:00 AM, as this is treated as the beginning of the day, not the end of the day, which is 11:59 PM. You can set up to 25 custom times. All of the custom times that you set will be used.

   Note
   If you select Specified times, and Special hours is not available, this is because you have not defined a special hours policy, or you have configured a special hours policy and enabled it, but then disabled it.

3. Select the Turn on this policy for machines connecting from: check box and choose anywhere, outside your network or inside your network. If you do not select this check box, the policy will not be immediately enabled.
   For more information on how users can connect from outside your network, see Endpoint Web Control (page 144).
4. Optionally, select the Automatically deactivate policy on check box, and set the Date and Time on which you want the exception turned off.
   You can set the times by clicking beside either the hour, minute, or meridian (AM or PM) setting and scrolling with your mouse wheel until you get the time that you want.
5. Click Save to close the Additional Policy wizard and return to the Additional Policies page.
4.2.5 Configuring the Local Site List

The Configuration > Group Policy > Local Site List page allows you to view all of the URLs that have been added to the list and to manage that list. URLs are added to the list to extend the filtering provided by the web appliance to URLs not included in the Sophos site list or to override the default filtering specified in the Sophos site list. The URLs listed in the Local Site List can be edited to change their Tags, Risk class, or Site category, or they can be deleted from the list.

For information on adding sites using the Local Site List Editor and on the use of tags, see Using the Local Site List Editor (page 97).

The default display of the list, if you accessed it by clicking Local Site List on the Configuration tab's sidebar, is to show all Local Site List entries. If you accessed this page from the Security Filter page, the list is limited to showing only entries that match the Risk class option from which you accessed this page.

- To add a local classification entry, click Add Site. The Local Site List editor dialog box is displayed. See "Using the Local Site List Editor" for instructions on the use of this pop-up dialog box.
- To edit a local classification entry, click on the URL of the entry that you want to edit. The Local Site List editor dialog box is displayed. See "Using the Local Site List Editor" for instructions on the use of this pop-up dialog box.
- To filter the list of local sites that is displayed, click Show Filters and use the newly displayed Filters toolbar to narrow the list of displayed entries.
  - Site: Enter a search pattern in the text box below and click the icon to apply the filter. Click the icon to clear the text box.
  - Tagged as: Enter a search pattern in the text box below and click the icon to apply the filter. Click the icon to clear the text box.
  - Category: Select the category of the URLs that you want to view.
  - Risk: Select the security risk level of the URLs that you want to view.

Only those URLs currently in the Local Site List that match your selected criteria are displayed. Click Hide Filters to close the Filters toolbar, which will reset all of the filters to display the full list of site in the local site list.

- To delete a local classification URL entry, click on the check box to the right of that entry in the Current local site list, and click Delete. The selected URL is deleted from the Local Site List list.
- To change the sort order of the filtered results, click the up/down arrow icon that appears to the right of each column name (Site, Tagged as, Category, and Risk). To reverse the order of the entries, click on the same up/down arrow icon a second time.

Related concepts
Using Tags (page 93)
Related tasks

Configuring Sandstorm (page 101)
Sophos Sandstorm is a cloud-based service that provides enhanced protection against new and targeted attacks. You can configure the appliance to send suspicious files to Sandstorm for analysis or submit suspicious files on an individual basis. Sandstorm detonates the file to check for malware and sends the results to you. Because the analysis takes place in the cloud, your system is never exposed to potential threats.

Using the Local Site List Editor

1. On the Configuration > Group Policy > Local Site List page, click Add Site.
2. In the Specify the site to add text box, enter the URL, domain, top-level domain (TLD), IP address, or CIDR range that you want to add.

To add multiple entries by entering one per line, click Enter multiple sites to expand the Specify the site to add text box. Click Enter single site to reduce it to single line size. When URLs are added, the protocol is stripped from the URL. So, to the web appliance, http://example.com is the same as ftp://example.com. Note that:

- A TLD entry should begin with a '.' (for example '.edu').
- If you enter a domain or top-level domain (TLD) with a single subdomain level, any additional subdomain levels will also be filtered. For example, an entry such as example.com will also filter subdomain.example.com and sub.subdomain.example.com.
- If your entry includes a path (query) and the website is blocked for any reason, the appliance may need to decrypt HTTPS traffic even if HTTPS scanning is turned off in order to apply the correct policy. For example, if HTTPS scanning is off and https://example.com is blocked by a category, and you add a local site list entry that allows https://example.com/ads, the appliance decrypts the traffic in order to see the query and apply the correct policy. Once the appliance determines that the traffic is allowed, no further scanning is applied.
- If your entry includes a domain and at least one level of subdomains, no additional subdomains will be filtered. For example, an entry such as subdomain.example.com will not result in the filtering of other subdomains of example.com, including other.example.com or sub.subdomain.example.com.

Note
Some TLDs are known as second-level domains. These are similar to a subdomain and TLD. For instance, .co.uk is a second-level TLD that is distinct from .uk. In the above, if .example.com was a second-level TLD, the other entries would be filtered.

- You can simultaneously create different rules for TLDs and subdomains. For instance, if a country had a TLD of .zz, you could block all sites by blocking the .zz top level domain and then selectively allow specific sites such as example.zz.
• You can add the URL of an HTTPS service that uses a non-standard port (other than port 443), which extends web appliance filtering support to that URL. We suggest that you set such sites as **Low Risk**.

**Important**
The web appliance will interpret any dotted quad followed by a slash and a number less than 33 as a CIDR range. This creates the possibility that a URL entered as an IP address followed by a numbered directory from 0 to 32 would be improperly treated as a CIDR range. For example, `http://192.168.3.4/6`, where ‘/6’ is a directory, would be interpreted as a CIDR range. To avoid this possibility, always enter URLs to numbered directories using fully qualified domain names rather than IP addresses.

3. On the **Modify the site properties** panel, do one or more of the following:

**Important**
You must choose at least one of the following three options to create a new local site list entry.

• From the **Tag** editable drop-down list, either enter the name of a new tag that you want to create in the text box, or click the adjacent down arrow icon to choose an existing tag from the drop-down list.

  Tags allow you to set policy rules more simply and flexibly than is possible by using other policy features. Tags can be created in two places, this **Local Site List Editor** and the **Configuration > Group Policy > Additional Policy** page. In the **Additional Policy** wizard, you can set what action is taken in response to a tag. In this, the **Local Site List Editor** wizard you can apply one or more tags to a URL. For tags to work, you must perform the configuration steps in both places.

  There are, however, three system tags: **Globally allowed sites**, **Globally blocked sites**, and **Never send to Sandstorm**. These tags only appear in the **Local Site List Editor** dialog box’s tag drop-down list. Their actions are predefined and match what their name indicates. The **Globally allowed sites** tag will not override the behavior expected as a result of a site’s risk class.

  **Note**
  There is no need to delete tags. Any tags that are not applied to URLs in the Local Site List and that do not have an additional policy set are automatically removed every Sunday night at midnight.

• Select **Override the risk class**, and select the risk class that you want to use from the drop-down list.

• Select **Override the category**, and select the category that you want to use from the drop-down list.

4. Optionally, add a comment explaining why you are treating the URL this way.

  This is useful for future reference and for other administrators.

5. Click **Save**.

  The **Local Site List** editor closes, and the new local site list entry that you configured is viewable in the **Local Site List**.

**Related concepts**
**Using Tags** (page 93)
Related tasks
Explicit Deployment (page 18)
Configuring Sandstorm (page 101)

Sophos Sandstorm is a cloud-based service that provides enhanced protection against new and targeted attacks. You can configure the appliance to send suspicious files to Sandstorm for analysis or submit suspicious files on an individual basis. Sandstorm detonates the file to check for malware and sends the results to you. Because the analysis takes place in the cloud, your system is never exposed to potential threats.

Configuring Security Filtering (page 100)
Configuring Tags (page 92)
Additional Policies (page 87)

4.2.6 Testing Policy Applied to a URL

The Configuration > Group Policy > Policy Test page allows you to test what policy is applied to a specified URL for a specified user.

1. Enter the URL or IP address that you want to test in the URL or IP address text box.
2. Enter the name of the user or IP address that you want to test in the Username or IP address text box.
   You must enter either the Active Directory username in the Down-Level Logon Name format (for example, DOMAIN\username), or the eDirectory username (for example, user.context).
3. Optionally, select the Test for a page request at check box and select the time and day from the adjacent controls.
   You can set the times by clicking beside either the hour, minute, or meridian (AM or PM) setting and scrolling with your mouse wheel until you get the time that you want.
   This option allows you to check the time periods that a time-specific Additional Policy will affect the specified site for the specified user.
4. Click Test.
   The security risk level, category, and the policy rules for the default, special hours, and additional policies that are applied to that URL or user, as well as any tags that are applied to it, are displayed in the Results section.

4.2.7 Quota Status

The Configuration > Group Policy > Quota Status page allows you to view quota usage by users for each quota policy, and reset a user’s quota for a given policy. This starts their quota time over for that period. You can filter entries based on User, Policy Name, or Time Remaining to help find a particular user or policy.

1. Find users in the Quota Status text box.
   You can sort by User, Policy Name, or Time Remaining. Optionally, click Show Filters and enter a User or Policy Name to find the users or policies. The search boxes provide substring matching to display all matching results.
2. Select entries.
   Click the check box next to entries you would like to reset. To select all items listed, select the check box at the top.
3. Click Reset to start the user and policy quota for the current time period.
4.3 Global Policy

Use the Global Policy pages to change the web appliance’s default processing of user web requests.

- Use the Security Filter page to configure how user requests for Medium Risk and Unclassified sites are handled by the web appliance.
- Use the Dynamic Categorization page to enable or disable the automatic detection of anonymizers and web caching sites, which knowledgeable users can access to view sites that would otherwise be blocked.
- Use the Data Leakage Prevention page to disallow users from sending web mail or posting to web logs (blogs).
- Use the HTTPS Scanning page to enable or disable malware scanning of HTTPS (SSL) sessions.
- Use the Certificate Validation page to set whether HTTPS certificates are automatically validated, and to add certificates not in the Sophos certificate list to the Custom certificate list for automatic validation.
- Use the Download Options page to allow or block access to specific types of downloads.
- Use the General Options page to set a variety of appliance options.

4.3.1 Configuring Security Filtering

Sophos supplies the web appliance with lists of URLs compiled by SophosLabs. These URLs are classified according to their level of risk.

The Configuration > Global Policy > Security Filter page allows you configure how the web appliance treats websites, based on the level of risk associated with the site. Although a specific action applies to most classifications by default, you can choose to block or scan user requests for Medium risk sites. You can also configure how the appliance treats user requests for Unclassified sites.

To set the actions for Medium risk sites, and set the risk level for Unclassified sites:

1. Configure the action for Medium risk sites (all other classifications have a default action and are non-configurable):
   - High risk: These sites have been analyzed by SophosLabs and are know to host malicious content that may compromise network security. These sites are always blocked.
2. Configure a risk level for **Unclassified** sites. These sites have yet to be analyzed or reviewed by SophosLabs and may compromise network security. The options are:

- **Low risk**: (Recommended) This is the default setting. Files that Sophos considers unsafe are scanned. SophosLabs maintains an up-to-date list of file types that are deemed unsafe.

- **Medium risk**: All files on medium risk sites are scanned. Selecting this option will apply the setting selected for medium risk sites as described above. If medium risk sites are set to **Scan**, all files on unclassified sites are scanned, regardless of file type. Sophos recommends setting unclassified sites to **Low risk** to ensure an optimal balance between scanning and user experience.

- **High risk**: All files on the site are blocked, regardless of file type.

3. Click **Apply**.

*To view a list of local sites*, click the **Sites** button next to the risk classification that you want to view. The **Local Site List** page is displayed, and any local sites specified for that classification are shown. You can also enter new sites by clicking **Add Site**. For more information, see “Configuring the Local Site List” and “Using the Local Site List Editor”.

**Related tasks**

- Configuring the Local Site List (page 96)
- Using the Local Site List Editor (page 97)

### 4.3.2 Configuring Sandstorm

Sophos Sandstorm is a cloud-based service that provides enhanced protection against new and targeted attacks. You can configure the appliance to send suspicious files to Sandstorm for analysis or submit suspicious files on an individual basis. Sandstorm detonates the file to check for malware and sends the results to you. Because the analysis takes place in the cloud, your system is never exposed to potential threats.

*This page of the administrative web interface is not available on a joined web appliance as this functionality has been shifted to the management appliance.*

The **Configuration > Global Policy > Sandstorm** page allows licensed users to enable Sophos Sandstorm, a cloud service that executes and analyzes suspicious downloads. If you do not have a license, you can obtain a 30-day trial license on this page.
Once enabled, you can set default Sandstorm profiles on the Configuration > Group Policy > Default Policy and Configuration > Group Policy > Special Hours pages. You can also select a custom Sandstorm profile for any additional policies you add or edit.

To turn Sandstorm on or off, click the On/Off switch.

You can view the current license status in the License status text box.

Files to be analyzed by Sandstorm are transmitted using a secure SSL connection to a data center in the cloud. Data centers are located in the United States and Europe. Sandstorm selects the closer data center according to the location of the appliance.

You can override the default behavior by selecting a data center in the Sandstorm data center list.

Note
Changing data centers may affect any analysis that is currently in progress.

**Related concepts**
- Default Policy (page 72)
- Special Hours (page 85)

**Related tasks**
- Configuring the Local Site List (page 96)
- Using the Local Site List Editor (page 97)
- Configuring Tags (page 92)
- Categories & Download Types (page 73)
- Web Applications (page 81)
- Searching Sandstorm (page 183)
- Setting a Special Hours Policy (page 85)

### 4.3.3 Configuring Dynamic Categorization

**Note**
Dynamic Categorization is not supported for Endpoint Web Control.

The Configuration > Global Policy > Dynamic Categorization page allows you to enable or disable the automatic detection of anonymizing proxies and caching sites. Such sites can allow users to access websites that would otherwise be blocked. For example, the URL to a cached Google page contains the encoded URL of the original page wrapped in the URL of the Google caching server.

While many of the anonymizers and similar sites are known, new ones are created on an ongoing basis. Web appliance detection of such sites is based on both lists of identified anonymizing proxies and caching sites, as well as URL characteristic analysis. This helps catch previously unidentified sites, thus greatly increasing our success in blocking users’ access to objectionable content through such sites.

Enable this option if preventing access to such sites is important for policy enforcement in your organization.

**Note**
Enabling this option may have a performance impact.
**Important**

If you enable this option, you should also enable the SophosLabs sharing option to maximize the benefit of this feature. The SophosLabs sharing option is set on the **Configuration > Global Policy > General Options** page.

To enable or disable dynamic categorization of anonymizers:

- Click **On** to the right of **Anonymizers** to enable automatic detection of anonymizing proxies.
- Click **Off** to the right of **Anonymizers** to disable automatic detection of anonymizing proxies.

**Related concepts**

*Appliance Features Not Supported by Endpoint Web Control* (page 52)

### 4.3.4 Configuring Data Leakage Prevention

**Note**

Data Leakage Prevention is not supported for Endpoint Web Control.

The **Configuration > Global Policy > Data Leakage Prevention** page allows appliance administrators to enable or disable posting capabilities for their users on select webmail sites, and on sites categorized as **Blogs & Forums**.

When your users attempt to send a webmail message or post a message to a blog, and you have data leakage prevention enabled, they could very likely see an error message generated by the webmail or blogging site rather than a notification page from the web appliance itself.

- **To manage Webmail control:**
  
  a) **Click On** to the right of **Webmail control** to prevent your users from sending webmail on the listed sites.

  This feature applies to the following webmail sites: Google Mail (Gmail), Yahoo! Mail, Windows Live Hotmail, and AOL Mail.

  **Note**

  Google Mail (Gmail) uses HTTPS for all connections. Therefore, **Webmail control** for Gmail will function only with HTTPS scanning turned on. (See also: **Configuring HTTPS Scanning** and **Default HTTPS access for Gmail**)

  b) **Click Off** to the right of **Webmail control** to allow your users to send webmail on the listed sites.

- **To manage Blog control:**
  
  a) **Click On** to the right of **Blog control** to prevent your users from posting on sites categorized as **Blogs & Forums**.

  b) **Click Off** to the right of **Blog control** to allow your users to post on sites categorized as **Blogs & Forums**.

**Related concepts**

*Appliance Features Not Supported by Endpoint Web Control* (page 52)
4.3.5 Configuring HTTPS Scanning

Note
HTTPS scanning is not supported for Endpoint Web Control.

To provide secure sessions between your users and commercial or banking sites, HTTPS encrypts web content between the website server and the user’s browser. While the traffic between the two is encrypted during an HTTPS session, the content that is delivered is just as likely to be infected with viruses or other malware as content from non-encrypted sites. To scan encrypted content, it must first be decrypted, then scanned, then re-encrypted for delivery to the requesting end user’s browser. Doing this maintains the privacy of the encrypted content, as the process is done automatically without human eyes viewing the content. However, because the traffic has been decrypted, the original site certificate cannot be used by the browser to authenticate the connection, so the original certificate is replaced by one generated automatically on the appliance using a Sophos-generated certificate authority. This replaces the original certificate, which requires that you download and install the Sophos-generated certificate authority into your users’ browsers, which can be done as a centralized system administration operation using Active Directory Group Policy Objects.

Just as there is a slight performance impact on the processing of encrypted traffic with any SSL transaction, so there will be if you enable HTTPS scanning. Consider this impact on the traffic throughput and capacity for your network and the appliance when deciding whether to use this feature.

The Configuration > Global Policy > HTTPS Scanning page allows you to enable or disable HTTPS (SSL) scanning and set logging options for HTTPS transactions.

- **To enable or disable HTTPS scanning**, either click On beside HTTPS scanning to enable it, or click Off to disable it, and then click Apply.

  **Important** When you enable HTTPS scanning, certificate validation is automatically enabled. Certificate validation ensures that sites with invalid certificates (often phishing sites) are not accessed. If you do want certificate validation disabled while HTTPS scanning is enabled, you must disable it on the Configuration > Global Policy > Certificate Validation page after enabling HTTPS scanning.

- **To set the HTTPS logging options**, select either Log hostname only for HTTPS transactions or Log complete URLs for HTTPS transactions to enable that logging option for HTTPS transactions, and then click Apply.
- **To create and manage a list of sites exempted from scanning**, see the "Managing HTTPS Scanning Exemptions" page.
- **To download a copy of the Sophos certificate authority**, see the "Downloading the Certificate Authority" page.

**Related concepts**
HTTPS Compatibility (page 211)
Appliance Features Not Supported by Endpoint Web Control (page 52)
Managing HTTPS Scanning Exemptions

The **Configuration > Global Policy > HTTPS Scanning** page allows appliance administrators to create and manage a list of sites that are exempted from scanning. Certain sites do not function properly if HTTPS scanning is enabled. To ensure that these sites work properly, add these problematic sites to this list of sites exempt from HTTPS scanning.

- To exempt sites from HTTPS scanning:
  a) In the text box to the left of the **Add** button, enter the domain or site (for example, example.com or host.example.com) that you want exempted from scanning. The entry must be in one of the following forms:
     - a top-level domain, such as example.com
     - a fully qualified domain name, such as host.example.com
     - a fully qualified domain name including a subdomain, such as host.subdomain.example.com
   The entry must not be in either of the following forms:
     - a domain name including a sub-domain, but without the hostname, such as subdomain.example.com
     - a specific URL, such as host.example.com/page.html
   Optionally, you can append a port number (for example, example.com:443). If a port number is not appended, a port number of 443 is assumed.

**Note**

The sites that typically require exemption are software activation and update sites, software that validates the site certificate (such as some instant messaging clients and banking software), and any specific HTTPS sites you do not want scanned.

The following table lists the applications and domains of sites that you should add to the **Sites exempt from HTTPS scanning** list in order to make those applications to work properly for your users.

<table>
<thead>
<tr>
<th>Incompatible Application</th>
<th>Domain that must be exempted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firefox updates</td>
<td>mozilla.org</td>
</tr>
<tr>
<td>LogMeIn (used for remote assistance)</td>
<td>logmeinrescue-enterprise.com and logmein.com</td>
</tr>
<tr>
<td>Sophos appliance administrative web interface</td>
<td>&lt;SWAorSMA_hostname&gt;.&lt;your_domain&gt;.&lt;toplevel_domain&gt;</td>
</tr>
<tr>
<td>Surgient web site</td>
<td>surgient.com</td>
</tr>
<tr>
<td>WebEx Communications Inc.</td>
<td>webex.com</td>
</tr>
<tr>
<td>Windows Vista activation</td>
<td>sls.microsoft.com</td>
</tr>
<tr>
<td>Windows Live Messenger (No exemption is required for Windows Live Messenger 2009.)</td>
<td>loginnet.passport.com and login.live.com and msn.com</td>
</tr>
<tr>
<td>Yahoo! Messenger</td>
<td>login.yahoo.com</td>
</tr>
</tbody>
</table>
Note
The appliance automatically exempts two sites from HTTPS scanning: webex.com, which is not compatible with proxies that scan HTTPS content, and the Windows Vista activation’s site sls.microsoft.com, whose certificate is required by Windows Vista to complete its activation.

b) Click Add.

The domain or site appears in the Sites exempt from HTTPS scanning list.

c) Click Apply.

- To remove a site from the exempt sites list, select the check box to the right of that site or domain, click Delete to remove it from the list, and click Apply.
- To exempt financial and investment sites from HTTPS scanning, select the Exempt Finance & Investment sites from HTTPS scanning option, and click Apply.

Important
Many financial sites check that the user’s browser has their certificate authority installed, so exempting such sites from HTTPS scanning is required.

Downloading the Certificate Authority

Once the HTTPS content has been decrypted, the original site certificate cannot be used by the browser to authenticate the connection, so the original certificate is replaced by one generated automatically on the appliance using a Sophos-generated certificate authority. This replaces the original certificate, which requires that you download and install the Sophos-generated certificate authority into your users’ browsers, which can be done as a centralized system administration operation using Active Directory Group Policy Objects.

To download the Sophos-generated certificate authority and distribute it to your users’ browsers:

1. Click Download a copy of the certificate authority.

   If you are prompted for the purpose of the authority, select "to identify web sites".

2. Save the authority.

3. Distribute the authority to your users using a Group Policy Object in Active Directory.

   See the Installing the Sophos-Generated Certificate Authority in your Users’ Browsers Knowledgebase article for instructions on how to do this.

4.3.6 Configuring Certificate Validation

Often, end users have little knowledge about the reliability of a certificate authority, so they will often accept certificate authorities without knowing if they are from trusted sources. To overcome this problem, the web appliance includes most of the reliable certificate authorities, and it can automatically validate certificate authorities from the Sophos certificate authority list. There is also the ability to add custom certificate authorities. This allows you to deny users the ability to accept certificate authorities.

The Configuration > Global Policy > Certificate Validation page allows you to control the HTTPS (SSL) certificate validation process. Sophos provides a list of certificates from recognized third-party certificate authorities that are automatically accepted. Also, you can add certificates from other
sources that you want to be accepted. If Certificate Validation is enabled, your users will only be able to access HTTPS sites that use a certificate listed in the Sophos certificate list or the Custom certificate list. If your users attempt to access HTTPS sites that use certificates from sources that are not in these lists, the Invalid certificate page is displayed and access to the requested site is blocked.

- **To enable or disable automatic certificate validation**, beside Certificate Validation, either click On to enable it, or click Off to disable it, and click Apply.

  Automatic certificate validation is based on both the Sophos and Custom lists.

  **Important**
  When HTTPS scanning is enabled, certificate validation is also automatically enabled. If you want certificate validation disabled while HTTPS scanning is enabled, you must disable it on this page, but be aware of the risks of doing so. Having certificate validation enabled is advised as HTTPS scanning replaces the actual certificate from the site, so it may be harder for users to identify phishing sites in their browser. Certificate validation ensures that such sites are not accessed.

- **To add a certificate from a website to the custom certificate list**, see "Adding a Certificate from a Web Site".

- **To add a certificate authority to the custom certificate list**, see "Adding a Root Authority Certificate".

- **To remove a certificate from the custom certificate list**, select the check box to the right of the certificate in the custom certificate list that you want to remove, click Delete, and then click Apply.

- **To view Sophos root authorities**, at the bottom of the custom certificates list, click View Sophos root authorities, and browse the list of the root certificate authorities supplied by Sophos in the Root Authorities pop-up dialog box.

**Related concepts**
HTTPS Compatibility (page 211)
Appliance Features Not Supported by Endpoint Web Control (page 52)

**Related tasks**
Adding a Certificate from a Web Site (page 107)
Adding a Root Authority Certificate (page 108)

### Adding a Certificate from a Web Site

**Important**
Retrieving certificates from HTTPS sites can be difficult when HTTPS scanning is enabled, as the web appliance will provide its own certificate in place of the remote one. Turn HTTPS scanning off on the **Configuration > Global Policy > HTTPS Scanning** page to be able to download any certificate other than the Sophos-generated certificate. Be sure to turn HTTPS scanning back on once you are done.

1. Enter the URL to the site from which you want to get the certificate, and click Get Certificate.
   
   You must enter a site URL, not a file or directory-specific URL.
   
   The Add Certificate dialog box is displayed, and it shows the certificate information.

2. Click Add.
   
   The site certificate is added to the certificate list.
Related concepts
HTTPS Compatibility (page 211)

Related tasks
Configuring Certificate Validation (page 106)

Adding a Root Authority Certificate

Important
Retrieving certificates from HTTPS sites can be difficult when HTTPS scanning is enabled, as the web appliance will provide its own certificate in place of the remote one. Turn HTTPS scanning off on the Configuration > Global Policy > HTTPS Scanning page to be able to download any certificate other than the Sophos-generated certificate. Be sure to turn HTTPS scanning back on once you are done.

1. Click Browse, and navigate to the certificate file that you want to add.
   Only PEM format certificates are accepted by the web appliance.
   To download the certificate needed:
   a) Open the website’s certificate information in your browser and look for the Issuer field.
      This field lists the URL of the authority that signed the certificate.
   b) Go to the website of that authority. Find and download the authority’s certificate that signed
      the website’s certificate.
   c) If intermediate certificates are involved, these must also be downloaded and added.
2. Once the path and filename are shown in the text box, click Add.
   The selected certificate is added to the certificate list.

Related concepts
HTTPS Compatibility (page 211)

Related tasks
Configuring Certificate Validation (page 106)

4.3.7 Setting Download Options

Note
Advanced download options are not available for Endpoint Web Control.

The Configuration > Global Policy > Download Options page allows you to set whether the appliance will allow or block downloading of large files and whether the appliance will allow or block downloading of unscannable files. Unscannable files are downloaded files that cannot be scanned for viruses because of corruption or encryption. You can also remove the authorization for users to download PUAs that had been previously allowed on the Search > User Submissions > PUAs page.

• To set whether the appliance will allow or block downloading of files larger than 800 MB:
  — To allow downloading, select the Allow large files (>800M) that are not scanned check box, and click Apply.
— To block downloading, clear the **Allow large files (>800M) that are not scanned** check box, and click **Apply**.

**Note**  
The web appliance determines the file size from the HTTP content-length header, so the option that you set will be applied based on that indication, not the actual file size.

- **To set whether the appliance will allow or block downloading of unscannable files**, select the **Allow unscannable files** check box, and click **Apply**.
  - To allow downloading, select the **Allow unscannable files** check box, and click **Apply**.
  - To block downloading, clear the **Allow unscannable files** check box, and click **Apply**.

- **To remove access to a previously authorized PUA**, select the check box to the right of the PUA to which you want to remove access, click **Delete** to remove the PUA, and click **Apply**.

  The selected PUA is removed from the **Authorized PUAs** list.

**Related concepts**  
Appliance Features Not Supported by Endpoint Web Control (page 52)

### 4.3.8 Setting General Options

<table>
<thead>
<tr>
<th><strong>On this page, the available features are:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• On a standalone web appliance: all options.</td>
</tr>
<tr>
<td>• On a joined web appliance: cache settings only.</td>
</tr>
<tr>
<td>• On a management appliance: all options except for cache settings.</td>
</tr>
</tbody>
</table>

Use the **Configuration > Global Policy > General Options** page to set web appliance policy-related filtering options.

**Cache Settings**

- **To enable caching**, click **On** on the **Cache settings** panel.

  **Note**  
  Caching is off by default. With the exception of large file downloads, setting Caching to **Off** results in higher performance.

- **To disable caching**, click **Off** on the **Cache settings** panel.

- **To change the cache settings**, on the **Cache settings** panel, enter the size in bytes of the **Maximum cacheable object size** and the **Minimum cacheable object size** in the appropriate text boxes, and click **Apply**.
Note
The default cache settings (maximum 100,000,000 bytes, minimum 100,000 bytes) are usually optimal. Lowering the setting for **Minimum cacheable object size** will decrease the performance of your web appliance.

SophosLabs

To enable sharing of data, including sample files, with Sophos that will help improve the protection provided by your web appliance, select the **SophosLabs** check box, and click **Apply**.

Note
Sample files will be sent to Sophos for additional threat analysis. Learn more about [sample submission](#).

Logging Mode

To exclude user name and IP information (if, for example, gathering this information is illegal in your jurisdiction), in the appliance logs and reports, clear the **Logging mode** check box, and click **Apply**.

Note
Please ensure that it is legal to record user-identifiable data in your jurisdiction before enabling this feature, as recording such data is illegal in certain jurisdictions.

Note
If the **Logging mode** check box is cleared, several reports will always show "No Data": Reports > Policy & Content > Suspect Machines and reports in the Reports > Users section. All searches will show "No Data" as well.

Report data retention

In the **Report data retention** text box, set the number of months for which you want to retain data. If the new retention time is shorter than the previously configured time, you will lose any data that is older than the new retention time.

Google feature controls

Configure settings that limit access to certain Google services.

- To limit YouTube content when viewing videos, select the **YouTube content restrictions** check box. Access to restricted content can be controlled with YouTube settings in Google Apps.

- With **Control Google Apps access**, you can prevent users from signing in to Google services using any accounts other than the accounts you provided them with. For example, you may not want them to use their personal Gmail account from another domain. To limit access to Google accounts and services to only the domains you specify, select the **Control Google Apps access** check box and type one or more domains.
Additional options

• To allow users to access external sites by entering IP addresses, select the **Allow public IP access** check box, and click **Apply**.

**Important**
If this option is not enabled, users will be unable to access any URL that uses an IP address from any web page, flash script, or other content. For example, **youtube.com** flash videos commonly contain URLs encoded as IP addresses.

• To enforce search engine filtering (SafeSearch), select the **Enforce Search Engine Filtering (SafeSearch)** check box, and click **Apply**.

Some search engines provide a “SafeSearch” option that excludes inappropriate content from search results. The appliance can enforce this option for search engines that support it. Check the product documentation for your search engine to see if SafeSearch is supported and for details about this feature.

**Note**
The effectiveness of this option depends on the implementation of SafeSearch by your search engine.

When this option is enabled, users cannot override SafeSearch by changing settings in their search engines.

**Note**
In order to support SafeSearch, some search engines require HTTPS scanning to be turned on.

• Select **Restrict image results to openly licensed content** to limit image results to those that have been labeled as being free to share, modify and reuse.

### Submitting Samples to Sophos

If you have enabled automatic submission of sample files to Sophos, and a file is deemed potentially malicious but cannot be positively identified as malicious based on its characteristics alone, Sample Submission allows Sophos servers to request a copy (sample) of the file. If Sophos does not already hold a sample of the file, the file is submitted to Sophos automatically.

Submission of such sample files helps Sophos to enhance detection of malware continuously and reduce the risk of false positives. Because Sample Submission increases the protection that our software provides, we strongly recommend that this feature be enabled to provide a more secure experience.
Note
The maximum sample size is 10 MB. The timeout for sample upload is 30 seconds.

Privacy Information
Because enabling Sample Submission will send a copy of the potentially malicious file(s) to Sophos for scanning, you should consider any data protection obligations that you may be subject to before deciding to allow Sample Submission to be enabled. You are solely responsible for your compliance with any applicable data protection obligations. Sophos understands that our users' files can contain sensitive information. Sophos will only use your files for the purposes of providing you with threat assessment and analysis services, and improving our threat detection and management capabilities and technology. Samples that are detected as malicious are retained by Sophos so that we can protect you and other users from that threat in the future, and to improve detection of similar threats. Depending on where you are geographically located, samples may be sent for processing in Sophos data centres outside of the European Union, but Sophos takes all appropriate and legally obliged measures to ensure that such data is secured and protected to European data protection standards, including the General Data Protection Regulation (GDPR). Learn more about how we process samples and view the Sophos Group Privacy Policy.

We strongly recommend that you enable Sample Submission as it will provide you with a more secure experience, better protection for your sensitive data, and also help us to improve our collective efforts to mitigate cybersecurity threats in the global community.

4.4 System
Use the System pages to change the configuration of the appliance’s system software.

**Note:** Only the Updates, Active Directory, Time Zone, and Central Management pages are also available on a joined web appliance. There are also considerable differences between some of these pages, depending on the operating mode of the system on which they are running.

- Use the **Updates** page to view the current versions of the threat definitions and software engine, and to see if newer versions are available. If a software engine update is available, there are also details about the nature of the update, the time and date of the next scheduled automatic update, and the option to perform the update manually prior to the scheduled automatic installation.
- Use the **Alerts** page to configure who should receive email alerts regarding appliance operations, potential virus infections, and user policy violation attempts, as well as related procedures.
- Use the **Backup** page to configure the appliance to automatically upload system configuration and log data to an FTP site at regular intervals as backup or to manually download configuration data to your current system.
- Use the **Restore** page to restore a previous appliance configuration backup file in the event of an undesirable configuration change.
- Use the **Active Directory** page to configure access to your organization’s Active Directory server so that the appliance can use existing user data.
- Use the **eDirectory** page to configure access to your organization’s eDirectory server so that the appliance can use existing user data.
- Use the **Time Zone** page to set the local time that is used to indicate the time in appliance transaction log files, and reports.
• Use the **Central Management** page to join this web appliance to a Sophos Management Appliance for centralized configuration, centralized policy control, and for consolidated reporting.

### 4.4.1 Updates

**Note**: On this page on a joined web appliance, the capability for “Scheduling Automatic Updates” is not available as this functionality has been shifted to the management appliance.

Use the **Configuration > System > Updates** page to check the software update status, manually initiate queued software updates, and to set the schedule for automatic software updates.

New threat definitions from SophosLabs (including anti-virus, anti-malware, and IP classification data) are automatically downloaded and installed without delay.

The **Software engine** section of the **Updates** page lists the current software version and available software updates. You can manually initiate a pending software update any time prior to the scheduled automatic software update time specified in the **Software engine update schedule** section. If there are multiple versions of the software available, selecting the most recent will apply previous updates, one at a time, until the appliance is at the latest software revision.

If **Enable automatic updates** is selected under **Software engine update schedule**, you can configure what time period and day(s) that software updates will be applied. If you do not perform the pending update manually before this scheduled operation, then any pending software maintenance updates will be performed during the time period and on the days indicated, so that no update is ever missed. Critical software updates are applied on the day they are received, even if that day is not selected in the schedule, and they are performed during the time window specified for all updates.

**Important**

Sophos recommends you select **Enable automatic updates**. If you choose to only update manually, you should still apply updates in a timely manner. If **Enable automatic updates** is not selected:

- Critical updates, which can include very important security enhancements, will not be automatically installed.
- Updating to the latest revision can be a lengthy process, as each available update will be applied one at a time until the system is at the current revision, including reboots for those that require it.
- When contacting support, you will need to update to the latest revision to properly troubleshoot any issue you.

**Related concepts**

- [Grouped Appliance Troubleshooting](#) (page 208)

**About Appliance Versions**

The installed and latest available software engine version numbers are displayed. The version number is divided by decimal points into four parts, for example 3.2.2.1. Reading from left to right, the parts signify:

<table>
<thead>
<tr>
<th>Version Type</th>
<th>Version Element</th>
</tr>
</thead>
<tbody>
<tr>
<td>major release</td>
<td>3.2.2.1</td>
</tr>
</tbody>
</table>
Sophos Web Appliance

<table>
<thead>
<tr>
<th>Version Type</th>
<th>Version Element</th>
</tr>
</thead>
<tbody>
<tr>
<td>minor release</td>
<td>3.2.2.1</td>
</tr>
<tr>
<td>maintenance release</td>
<td>3.2.2.1</td>
</tr>
<tr>
<td>hotfix release</td>
<td>3.2.2.1</td>
</tr>
</tbody>
</table>

Hotfix releases are rare. For this reason, you will usually see a version number consisting of three parts. For example, 3.2.2.

**Related concepts**
Updates (page 52)

**Related tasks**
Restore (page 122)

**Checking Update Status**
- Read the information in the **Threat definitions** and the **Software engine** tables.
  - The **Last updated** column shows the date and time of the most recent update.

  **Note**
  The version number in the **Installed** column of the **Software engine** section is linked to the version Release Notes.

**Scheduling Automatic Updates**

**Note**: You cannot schedule automatic updates on a web appliance joined to a management appliance. You must perform this operation on the management appliance.

1. On the **Software engine update schedule** panel, use the **From** and **To** drop-down lists to set the time period during which you want automatic software updates performed.

   **Note**
   All updates will interrupt the proxy service. Any updates that require a reboot may interrupt service for up to five minutes.

2. Select or clear the days of the week check boxes to set the day(s) on which you want automatic software updates performed.

3. Click **Apply**.

**Performing a Manual Update**
If there is a pending software update available, you can manually install it at a time when network activity is low so that the installation is done when it is least disruptive.

1. Check that there is a pending software update available.

   Pending software updates appear in the **Available** column of the **Software engine** panel and, when they are available, the **Update** button is enabled.
2. If there is a pending software update available, click **Update**.
   The pending software update is performed.

### 4.4.2 Alerts & Monitoring

Use the **Configuration > System > Alerts & Monitoring** page to:

- Specify which people in your organization will be notified by email when a system alert is raised.
- Specify who in your organization will be notified by email whenever a user’s web query contains a term that has been specified in the Search Terms list.
- Turn off/on the support alerts that are sent to Sophos.
- Set the appliance to transfer web traffic logs to a Syslog server.
- Set the contact information for the person in your organization who administers the appliance. This information is added to any system status alerts that are submitted to Sophos as part of the managed web appliance and management appliance support program.
- Send email notifications whenever users submit requests.

System alerts are described in greater detail in the System Status documentation.

**Related concepts**

**System Status** (page 188)

The icons on the System Status tab indicate the system’s alert level by their color. If it is a joined appliance, the System Status button on the navigation bar becomes animated if the appliance is synchronizing with other appliances. The status indicated by these icons is shown in the following table. Differently shaped icons are used for the web appliances (disks) and the management appliance (network icons).

**Related tasks**

**Searching Sandstorm** (page 183)

### Adding an Alert Recipient

You can specify which people in your organization will be notified by email when a system alert is raised.

1. On the **Configuration > System > Alerts & Monitoring** page, select the **System Alerts** tab.
2. In the **Alert Recipients** text box, enter the full email address of the intended recipient, and click **Add**.
   The email address that you entered is added to the list.
3. To include or exclude alerts when users submit requests, select **On** or **Off** under **Send email alerts when users submit sites, filetypes, and PUAs for review**.
4. Click **Apply**.

**Related tasks**

**Removing an Alert Recipient** (page 116)
Removing an Alert Recipient

The Alert recipients list contains the addresses of people in your organization who will be notified by email when a system alert is raised.

2. Select the check box to the right of the email address that you want to remove from the list.
3. Click Delete.
   The selected email address is deleted from the list of Alert recipients.
4. Click Apply.

Related tasks
Adding an Alert Recipient (page 115)

Adding a Search Term Alerts Recipient

You can create a list of recipients who receive an email notification any time that a user query contains a term that has been specified in the Search Terms list.

These notifications are only sent if you have created one or more search terms for reporting. For more information, see “Search Terms” in the Reports documentation.

Note
An alert is only issued if the user’s query was sent using Google, Bing, or Yahoo!

1. On the Configuration > System > Alerts & Monitoring page, select the Search Terms Alerts tab.
2. Select Enable search term alerts.
3. In the Alert Recipients text box, enter the full email address of the intended recipient, and click Add.
   The email address that you entered is added to the list.
4. Click Apply.

Note
Consider the following before adding one or more recipients:

• Email notifications are sent in clear text, so the contents of the messages are not secure.
• Sending these notifications may have an impact on performance, especially if numerous search terms have been defined and there are many matches for the terms.

Related concepts
Search Terms (page 178)
Users: Users By Search Queries (page 165)

Related tasks
Removing a Search Term Alerts Recipient (page 117)
Removing a Search Term Alerts Recipient

The Search Terms Alerts list contains the email addresses of those in your organization who are notified about users who have sent a web query that contains words or phrases that are specified in the Search Terms list.

1. On the Configuration > System > Alerts & Monitoring page, select the Search Terms Alerts tab.
2. In the Alert Recipients text box, select the check box next to the address of the recipient that you want to remove.
3. Click Delete.
   - The email address is removed from the list
4. Click Apply.

Related concepts
- Search Terms (page 178)
- Users: Users By Search Queries (page 165)

Related tasks
- Adding a Search Term Alerts Recipient (page 116)

Turning Off/On Sophos Support Alerts

You can turn the alerts that are sent to Sophos Technical Support off or back on. This option is disabled by default, although the current setting is preserved during upgrades. Turning Sophos support alerts off is typically done during testing to avoid unnecessary contact from Sophos Technical Support.

1. On the Configuration > System > Alerts & Monitoring page, on the Support tab, clear the Activate appliance support alerts check box to suspend the emailing of alerts to Sophos, or select this check box, and fill in all required fields, to turn the emailing of support alerts back on. For more about filling in the required fields, see “Setting a Support Contact”.
2. Click Apply.
   - When the check box is disabled, the status information bar at the top of the window displays the notice, “Sophos proactive monitoring is off”.

Note
- Be sure that you have turned support alerts back on when you are ready to return the appliance back to normal operation.

Related tasks
- Setting a Support Contact (page 118)

Configuring Syslog

The appliance Syslog capability can send transaction logs to a Syslog server for auditing, storage, and analysis.

1. On the Configuration > System > Alerts & Monitoring page, select the Syslog tab.
2. Select the Enable syslog transfer of web traffic check box.
3. In the **Hostname/IP** text box, enter the address of the Syslog server to which the appliance will send logs.

**Note**
If the Syslog server becomes unavailable to the appliance, it is possible that some log information may be dropped before the server becomes available again. The amount of information dropped depends on the duration that the server is unavailable.

4. In the **Port** text box, enter the port number that your Syslog server uses.
5. Select a **Protocol** option button to select whether the appliance will send Syslog data using UDP, unencrypted TCP, or encrypted TCP. While UDP is faster than TCP, delivery is not guaranteed, and TCP provides more reliable delivery.

   If you select **TCP - encrypted**, you will need to add the valid signing certificate associated with your syslog server:

   a) Click **Choose File** and navigate to the signing certificate that you want to add.
   b) Once the path and filename are shown in the text box, click **Upload** to add the signing certificate.

**Note**
Standard UDP and TCP do not provide secure transmission of Syslog data.

6. Click **Apply**.

### Setting a Support Contact

You can set the contact information for the person Sophos should contact, if your appliance experiences a problem. This information is added to any system status alerts that are submitted to Sophos as part of the managed web appliance and management appliance support program.

1. On the **Configuration > System > Alerts & Monitoring** page, select the **Support** tab.
2. Select the **Activate appliance support alerts** check box.
3. For **Critical alerts**, provide the **Name** and **Email** of the person Sophos should contact.
4. **Note**
   A non-critical alert indicates a transient error that Sophos would like to investigate. These alerts do not indicate a problem with web filtering.

5. Click **Apply**.

### Related tasks

**Turning Off/On Sophos Support Alerts** (page 117)

### Phone Number Format

Follow these guidelines when you enter phone numbers:

- Enter only the country code, the area code and the phone number into the **Phone** field.
- Do not enter spaces or any of the following characters:
  - + (plus)
Example Phone Numbers

<table>
<thead>
<tr>
<th>Country</th>
<th>Country Code</th>
<th>Example Phone Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td>61</td>
<td>61294099111</td>
</tr>
<tr>
<td>France</td>
<td>33</td>
<td>33969322717</td>
</tr>
<tr>
<td>Germany</td>
<td>49</td>
<td>491805767467</td>
</tr>
<tr>
<td>Italy</td>
<td>39</td>
<td>390291180860</td>
</tr>
<tr>
<td>Singapore</td>
<td>65</td>
<td>6567767467</td>
</tr>
<tr>
<td>South Africa</td>
<td>27</td>
<td>27114444000</td>
</tr>
<tr>
<td>United Arab Emirates</td>
<td>971</td>
<td>97143754332</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>44</td>
<td>441235465818</td>
</tr>
<tr>
<td>United States and Canada</td>
<td>1</td>
<td>17814945800</td>
</tr>
</tbody>
</table>

For other countries’ phone number formats, see International Telecommunication Union - Dialing Procedures.

4.4.3 Backup

On the **Configuration > System > Backup** page, you can set the appliance to automatically upload system configuration data and log data to an FTP site at regular intervals as backup. Alternatively, you can manually download the appliance’s configuration data at any time.

- To configure automated backups via FTP, see "Automating Backups."
- To manually download configuration data, click **Download Now**, and save the archived backup file using your web browser’s save file features.

**Note**

When you manually download configuration data, an archive file is created with all of the configuration data so that it can be downloaded via your browser to a selected location on your local system. Be patient when using this feature because there is a slight delay while the configuration data is copied and archived into the file for download.

- [Management Appliance Only] To manually perform an immediate reports data backup, click **Start backup**.

Reports data is backed up to the FTP server and directory location specified in the Automated upload section. The progress of the manual reports data backup is displayed in the **Reports backup status** panel. After completion, this panel on the Management Appliance shows the date and time of the last reports data backup.

Please observe the following backup and restore considerations:

- Appliance backups do not include network settings.
• Report data for the management appliance should be backed up regularly to protect against the possibility of an appliance failure. Report data is restored through optional steps in the setup wizard for configuring a new management appliance. When selected, you can retrieve the data from an FTP location, and download it to the new appliance.

• When setting up a replacement management appliance, all web appliances that were previously joined to it must first be reverted to standalone mode, then joined to the new management appliance.

• The configuration backups do not include FTP, Active Directory, or eDirectory passwords. To ensure that these connections are properly configured, they are disabled after a restore operation, so you must re-enter your usernames and passwords for these connections and re-enable FTP and directory services synchronization on the System: Backup, System: Active Directory, and System: eDirectory pages.

• You cannot restore system configuration data made from a management appliance to a web appliance and vice versa.

• You can only restore from a backup that was made under the same major.minor release. For instance, you could restore a version 3.2.2.1 appliance from a backup made under version 3.2.1. But you could not restore that same appliance from a backup made under version 3.1.3.

Related concepts
Grouping Web Appliances (page 37)
Replacing Hardware Appliances with Virtual Appliances (page 15)

Related tasks
Restore (page 122)
Automating Backups (page 120)

Automating Backups

Configure the appliance to automatically upload system configuration data, log data, and reports data (only available on a management appliance) to an FTP site at regular intervals as a backup.

1. In the Upload options section, select what data will be backed up:

   Note
   You must select at least one of the Upload options to enable the FTP server configuration text boxes.

• Select System configuration data if you want all configurable settings and appliance resources, including your local classifications, to be backed up.

   If you enable this option, you must also select how frequently the system configuration data is backed up. The options are: Daily at midnight, Weekly on Friday at midnight, or Monthly on the 1st at midnight.

   Note
   Appliance backups do not include network settings.

• Select Transaction log files at least once daily at midnight if you want your transaction log files backed up daily.

   If you enable this option, you must also select the format in which the logs are backed up: Sophos format or Squid format.
Note

The Squid log format includes the following information to help administrators to review system activity: System time, Duration of transaction in milliseconds, Requesting IP address, Result Code and Status Code, Size of data delivered in bytes, Request Method, URL, Username (if available), Hierarchy Code explaining how the request was handled, and the Object Type that was requested. The Sophos log format lists additional details of the transaction such as the Hostname, Connection Status, Referrer, and User-agent to help Sophos Technical Support troubleshoot potential issues.

Sophos format logs may be viewed using a text editor. Squid format logs may be viewed using third party Squid log analysis tools, such as Kraken Reports. Sophos makes no guarantees, no warranties, accepts no responsibility, and offers no technical support for such third party programs.

• [Management Appliance Only] Select Reports data backed up each day at midnight if you want that data backed up regularly.

If you select this option, you can also save the data to a different location on your FTP server by selecting Use alternative FTP path and, in the adjacent text box, entering the path to the directory where you want the report data to be backed up. This path should be entered using Unix style directory separators (slashes), as this is required by the FTP protocol. For example: /home/admin/swadata/reportdata/.

Note

Report data should be backed up regularly to protect against the possibility of an appliance failure. Report data is restored from the setup wizard used to configure a management appliance, making your data available on the new appliance.

2. Fill in the text boxes to configure FTP access to the backup host that you want to use to receive and store the backup data:

• FTP location: [Required] Enter the hostname or IP address for the FTP site.

  Optionally, you can specify a custom port, other than the standard port 21. This must be entered in the form <server>:<port>, for example, ftp.example.com:3621. If you do not specify a port, the default of 21 is used.

• FTP path (optional): Enter the directory location on the FTP site. This path should be entered using Unix style directory separators (slashes), as is required by the ftp protocol. For example: /home/admin/swadata/.

• Username: [Required] Enter the user account name that will be used to access the FTP site.

• Password: Enter the user account password that will be used to access the FTP site.

3. Click Verify & Save Settings to ensure that the values entered in the preceding text boxes are valid.

Note

Ensure that the appliance has access to the FTP location before applying the backup settings.

Click Close to exit the Verify Settings dialog box once the verification process is complete.

Related concepts

Interpreting Log Files (page 216)
This page provides the information required to interpret a web appliance log file.

Related tasks
Backup (page 119)
Restore (page 122)

4.4.4 Restore

Use the Configuration > System > Restore page to restore a configuration and local classifications backup in the event of an undesirable configuration change, an appliance failure, or an appliance replacement.

1. Access the appliance’s administrative web interface from the system that contains the backup data. Whether it is data that has been saved manually using the Download Now option, or data that has been automatically backed up to an FTP location, it must be accessible from the workstation you are using to restore this backup.

2. On the Configuration > System > Restore page, click Browse. On your system, navigate to the manually downloaded configuration archive file, or the configuration archive file that you have downloaded from your automatic upload FTP server.

The path and filename of the backup file are displayed in the Location text box.

3. Click Restore.

The progress of the restore operation is displayed in the Status panel.

Please observe the following backup and restore considerations:

• Appliance backups do not include network settings.

• Report data for the management appliance should be backed up regularly to protect against the possibility of an appliance failure. Report data is restored through optional steps in the setup wizard for configuring a new management appliance. When selected, you can retrieve the data from an FTP location, and download it to the new appliance.

• When setting up a replacement management appliance, all web appliances that were previously joined to it must first be reverted to standalone mode, then joined to the new management appliance.

• The configuration backups do not include FTP, Active Directory, or eDirectory passwords. To ensure that these connections are properly configured, they are disabled after a restore operation, so you must re-enter your usernames and passwords for these connections and re-enable FTP and directory services synchronization on the System: Backup, System: Active Directory, and System: eDirectory pages.

• You cannot restore system configuration data made from a management appliance to a web appliance and vice versa.

• You can only restore from a backup that was made under the same major.minor release. For instance, you could restore a version 3.2.2.1 appliance from a backup made under version 3.2.1. But you could not restore that same appliance from a backup made under version 3.1.3.

Related concepts
Replacing Hardware Appliances with Virtual Appliances (page 15)
About Appliance Versions (page 113)
Active Directory (page 123)
eDirectory (page 127)

Related tasks
Backup (page 119)
4.4.5 Active Directory

Use the Configuration > System > Active Directory page to configure access to your Active Directory server, which allows the appliance to use Active Directory user and group information.

**Important**

It is essential that the time on your Active Directory server is synchronized with the time on your appliance. We suggest that you use the network time protocol on your Active Directory server with 0.sophos.pool.ntp.org as the NTP server, which is the NTP server pool used by the appliance. If you use a different NTP server for your Active Directory server, you must configure the appliance to use the same NTP server, which is configured on the Configuration > System > Time Zone page.

Active Directory authentication options are configured on the System: Authentication page. You can authenticate users with a single sign on, through a captive portal, or use a combination of the two. By creating authentication profiles and connection profiles, you can specify different authentication methods for different connections. For more information, see “Authentication”.

**Related concepts**

Authentication (page 131)

**Related tasks**

Configuring Firefox for Active Directory in Transparent mode or Bridged mode (page 201)

Restore (page 122)

**Configuring Active Directory Access**

On this page of a joined web appliance, most of the options are unavailable because they are controlled from the management appliance. The main exception is Configure Active Directory settings locally, which is described below.
Important

**Firewall Configuration:** If you have a firewall between the appliance and your Active Directory server, you need to ensure that ports 88 and 389 are open for both TCP and UDP, and that ports 445 (raw SMB) and 139 (NetBIOS over TCP/IP) are open for TCP on that firewall in order to perform Active Directory authentication.

**Requirements for an Active Directory Forest:** Sophos supports the integration of an Active Directory forest with the appliance only if the following conditions apply:

- Integrate with only a single Active Directory forest containing a single Active Directory tree.
- The Active Directory server to which you configure access must be the root domain controller of the Active Directory forest.
- The root domain of your Active Directory forest must have an explicit trust relationship with all subdomains within the forest. If this condition does not exist, users will be able to authenticate, but the appliance will not be able to synchronize Active Directory groups membership information, which will result in all affected users having only the default web appliance policy applied to them.
- The Active Directory administrator account that you use to access the Active Directory forest must have valid credentials on all subdomains for authenticating users and accessing LDAP information.
- In addition to the firewall configuration described above, you must ensure that port 3268 is open for both TCP and UDP between your appliance and your Active Directory server, that use of the global catalog is properly configured on your Active Directory server, that TCP access from the appliance to your Active Directory server, and that bi-directional UDP traffic between the two is allowed. Also, port 389 must be open between the appliance and all domain controllers within the Active Directory forest.
- Ensure that the domain controllers have the global catalog enabled, including on any backup domain controllers. If you do not, problems may occur when the appliance attempts to synchronize: your users may complain about authentication pop-ups that repeatedly fail, and the subdomain groups may disappear from the Configuration > Group Policy > Default Groups page. Although this situation may resolve itself automatically in certain circumstances, it will likely recur. Enabling the global catalog on all domain controllers, including those configured as backup domain controllers on your Active Directory server, is the only complete solution for this problem.

1. Near the top of the page, next to **User authentication via Active Directory**, click **On**.
   
The three **Active Directory Settings** text boxes in the leftmost column become available.

   **Note:** On a joined web appliance, the On/Off button is not functional. It only shows the status as set on the management appliance.

2. [Optional] On a joined web appliance, you can change some of the Active Directory settings to access a different domain controller by selecting the **Configure Active Directory settings locally** check box.
## Joined Appliance Considerations

The setting to **Configure Active Directory settings locally** is only available on a joined web appliance. It is typically used to access a local Primary Domain Controller in a branch location instead of the main Domain Controller in the central office. The settings are similar to those required on an appliance that is not joined and are documented in steps 3 and 4. Read the remainder of this section for information about configuration differences. Once these steps are complete, you must verify and apply the settings on the joined appliance, as described in steps 5 and 6.

When **Configure Active Directory settings locally** is selected, only the **Username** and **Password** text boxes are functional, allowing you to set a different Active Directory account for accessing Active Directory authentication. LDAP user data is not synchronized on a joined web appliance; this data is synchronized on the management appliance only and downloaded to the joined web appliances.

Active Directory access from a joined web appliance is for authentication only, LDAP synchronization is only performed by the management appliance.

On a joined web appliance with the **Configure Active Directory settings locally** check box selected and the **Auto-detect advanced settings** check box cleared, only the **Primary Domain Controller** and **Active Directory Kerberos server** text boxes are functional, allowing you to select a different Active Directory server. The server that you select must not be a child domain of the **Active Directory domain**, although it can be a secondary Domain Controller.

### 3. Enter the Active Directory Settings required to access the server:

- **Active Directory domain**: Enter the domain name of your organization’s Active Directory server.
- **Username**: Enter the username to access the Active Directory server.

**Important**
To connect the appliance to an Active Directory domain, you must use a pre-existing account on the Active Directory server with permissions to join a computer to the Active Directory domain and to authenticate users. Also, if you intend to access the global catalog of an Active Directory forest with a single Active Directory tree, the user account must have permissions to authenticate users in multiple subdomains. Be sure to use an Active Directory account with only the privileges that are required.

- **Password**: Enter that user’s password.

### 4. Enter the Active Directory settings by doing one of the following:

- Select the **Auto-detect advanced settings** check box (the associated text boxes are automatically filled).

  **Or**

- Ensure that the **Auto-detect advanced settings** check box is not selected and fill in the remaining text boxes. The six additional text boxes are:
  - **Primary Domain Controller**: The fully qualified domain name (FQDN) of the desired Primary Domain Controller.
  - **Secondary Domain Controller (Optional)**: A secondary domain controller in case there are problems connecting to the **Primary Domain Controller**. If an appliance cannot reach the primary controller it will fail over to the secondary controller. If an appliance has joined
to the **Secondary Controller**, the **Configuration > System > Active Directory** page will display a **Revert to Primary** button. Use this to reconnect to the primary.

- **Active Directory Kerberos server:** The FQDN of the desired Kerberos server. If uncertain, use the same hostname as the Domain Controller. Should be a fully qualified domain name.

  **Note**

  If you have configured a **Secondary Domain Controller**, your Active Directory Kerberos server **must** be the same as your **Primary Domain Controller**.

- **Active Directory LDAP server:** The FQDN of the desired LDAP server, with the port number. If uncertain, use the same hostname as the Domain Controller, with the port number. The port number for a single Active Directory server is usually 389. For an Active Directory server designated as a global catalog server, it is 3268. If you enter an incorrect FQDN, the appliance will attempt to auto-detect the FQDN. If you cannot successfully connect to your Active Directory forest, disable **Auto-detect advanced settings** and manually change the port number for the Active Directory LDAP server to 389 to force the appliance to access the AD server as a single domain.

- **LDAP authentication DN (optional):** The LDAP "Distinguished Name" that corresponds to the **Username** text box. If left blank, the appliance will attempt to discover the correct DN. If you are uncertain, leave this blank.

- **LDAP base DN (optional):** The LDAP "folder" under which users can be found. Defaults to the whole domain. If you are uncertain, leave this blank.

- **LDAP account attribute (optional):** The LDAP object attribute that contains the "login name" of a user. Defaults to 'sAMAccountName', which is the only correct value for Active Directory LDAP servers. If you are uncertain, leave this blank.

5. Click **Verify Settings**.

   If you chose the **Auto-detect advanced settings** option, the remaining fields of the **Active Directory settings** are automatically filled. The appliance will first look for an Active Directory global catalog at port 3268. If it can't find that, it defaults to a single-domain Active Directory configuration using port 389.

  **Note**

  With **Auto-detect advanced settings** selected, the appliance will choose a domain controller based on the lowest ping time.

The **Detect Settings** dialog box is displayed, showing the results of the connection attempt. Successful operations are indicated with a green check mark icon; failed operations are indicated with a red "x" icon. The **Detecting subdomains** step can also show an orange exclamation mark, which indicates that one or more trusted (child) domains could not be synchronized. To the right of the **Detecting subdomains** verification item is a **Show details** button, which you can click to view the results of attempts to connect to the subdomains of your Active Directory forest. The subdomains are listed in one of two groupings: **Authentication Successful** or **Authentication Failed**.

If there are failed operations in the **Detect Settings** process, a troubleshooting message is displayed below the list of verification checks. This message links to explanatory text that will assist you in correcting the problem. If you encounter failed operations, read the troubleshooting message, then **Close** the **Detect Settings** dialog box, correct the **Active Directory Settings** in the left column, and click **Verify Settings** again.

When all **Verify Settings** operations are successful, all of the required Active Directory text boxes are filled.
Important
If the verification of a connection to an Active Directory subdomain fails because that server is down at the time that you run the verification, bringing the server back up will not enable Active Directory synchronization with the appliance. You must have a successful Verify Settings operation for any connection to a subdomain server to enable communications between it and the appliance.

6. Click Apply.
7. [Optional] Click Synchronize Now to have the appliance immediately synchronize user and group information with the configured Active Directory server. This can only be done after steps 4, 5 and 6 have been completed successfully.

Related concepts
Grouped Appliance Troubleshooting (page 208)
Authentication (page 131)
About Authentication (page 131)

Related tasks
Configuring Authentication (page 132)
Configuring Active Directory to support Kerberos for Mac OS X (page 133)
Configuring an Authentication Profile (page 134)

Trusted Domains and Subdomains
The web appliance supports trusted domains and trusted subdomains in Active Directory. For example, the root parent domain example.local could have both dev.example.local and sales.example.local as trusted subdomains. This same parent domain could have a trust relationship with another domain, another.local. On Configuration > System > Active Directory, enter the following:

- Active Directory domain: Enter the FQDN and not the NetBIOS domain name of the root parent domain.
- Username: Enter the username without any domain information.
  You should use a Domain Admins user account, or a user account as described in the Requirements for the AD user account knowledgebase article.
- To enable Active Directory integration for trusted domains not under the root parent domain tree (another.local in the above example), create an Active Directory user account with the same username and password in the trusted domain.

4.4.6 eDirectory
Use the Configuration > System > eDirectory page to configure access to your eDirectory server, which allows the appliance to access eDirectory user and group information.

Note
eDirectory is not supported with Full Endpoint Web Control.

Related concepts
Endpoint Web Control (page 48)
Configuring eDirectory Access

On this page on a joined web appliance, the Off | On button is disabled.

Important
Network Configuration: All of the eDirectory servers that you want to work with must be reachable from your web appliance or management appliance. If they are not, you must configure static routes to them in the Advanced Settings of the Configuration > Network > Network Interface page.

Important
Firewall Configuration: If you have a firewall between the appliance and your eDirectory server, you need to ensure that port 636 (or another LDAPS port configured on the eDirectory server) is open for both TCP and UDP in order to perform eDirectory identification.

1. Beside eDirectory integration, near the top of the page, click On.

   The four Configure eDirectory text boxes are enabled.

   Your appliance cannot have the same hostname as the eDirectory LDAP server.

   On a joined web appliance, the On/Off button is not functional. It only shows the status as set on the management appliance.

2. Fill in the Configure eDirectory information required to access the server:

   On a joined web appliance, you must select the Configure eDirectory settings locally to make these text boxes editable. If you do not, your joined web appliance LDAP information is synchronized from your management appliance.

   • LDAP server and port: Enter the domain name or IP address, and the port, of your organization’s eDirectory server.

   • Authentication DN:

     Enter the username to access the eDirectory server. For example:

     \texttt{cn=admin,o=company}

     To enable eDirectory integration, you must use a pre-existing account on the eDirectory server with permissions to query the eDirectory database. Be sure to specify an eDirectory user who is a trustee of the root of the tree, with explicitly set read permissions for the entire tree.

     • Password: Enter the password of the user specified in the Authentication DN: field.

     • LDAP base DN: Optionally, enter the base DN of the LDAP tree that you want to use.

3. [Standalone and Joined Appliances only] You can optionally configure replicas. Under the Configure Replicas (optional) section:
a) In the **LDAP server** text box, enter the IP address and port.
b) In the **Replica** text box, enter the Replica designation.

**Note**
Misconfiguring replicas can result in poor performance. For recommendations, see **Configuring Connections to eDirectory Replicas**.

4. Click **Verify Settings**.

The **Detect Settings** dialog box is displayed, showing the results of the connection attempt. Successful operations are indicated with a green check mark icon, warnings are indicated with a yellow exclamation mark, and failed operations are indicated with a red "x" icon.

If there are failed operations in the **Detect Settings** process, a troubleshooting message is displayed below the list of verification checks. If you encounter failed operations, read the troubleshooting message, then **Close** the **Detect Settings** dialog box, correct the **Configure eDirectory** settings, and click **Verify Settings** again.

The **Verify Settings** button is available on a joined web appliance if you have selected the **Configure eDirectory settings locally** option.

5. Click **Apply**.

6. Optionally, click **Synchronize Now** to have the appliance immediately synchronize user and group information with the configured eDirectory server. This can only be done after you have configured and applied the settings specified in the previous steps.

**Note**
The **Synchronize Now** button does not exist on a joined web appliance.

7. To set which IP addresses and CIDR ranges are available for unauthenticated browsing:

   a) In the **eDirectory Options** section, select **Do not associate eDirectory usernames with the following IP addresses**.

   b) Click **Add**.

   The **Exempt Authentication** dialog box is displayed.

   c) Enter an IP address or CIDR IP address range into the text box and select which address type it is (**IP Address** or **IP Range**) from the adjacent drop-down list, and then click **Add**.

**Important**
The web appliance will interpret any dotted quad followed by a slash and a number less than 33 as a CIDR range. This creates the possibility that a URL entered as an IP address, followed by a numbered directory from 0 to 32, would be improperly treated as a CIDR range. To avoid this possibility, always enter URLs to numbered directories using fully qualified domain names rather than IP addresses.

The IP address or range of IP addresses is added to the list below.

**Note**
If you exempt users by their IP address, any reports or searches that normally display a **User** name field will show their IP address instead. Other system functions will continue to operate as expected.
d) [Optional] To delete a listed IP address or IP range, select the check box beside the entry that you want to remove, and click **Delete**. The IP address or range of IP addresses is removed from the list.

e) Click **Save**.

### Boosting eDirectory Performance via Custom Indexes

The performance of the eDirectory server can improve significantly if two attributes, `objectClass` and `networkAddress`, are indexed. Results will vary, depending on the size and structure of your network, but it is recommended that all users make this change.

Although eDirectory has a number of default indexes, you can add custom indexes using either Novell iManager or Novell ConsoleOne.

**Note**

You must make the changes on all eDirectory servers.

When creating a custom index, you are prompted to select the index rule ("Value," "Presence," and "Substring"). For best results, it is recommended that you select "Presence." For more information, go to Micro Focus support.

### Configuring Connections to eDirectory Replicas

You can reduce network traffic and improve the accuracy of identifying users in eDirectory by properly configuring the correct replica for a specific group. Properly configured replicas will:

- reduce load on your root eDirectory server.
- reduce network traffic between your eDirectory servers.

### Reduce Root Server Load

Properly configured connections to local replicas can greatly reduce the load on your root server. The web appliance regularly pulls identification information. Communicating with a local replica for the given organizational unit will reduce the load of your root eDirectory server.

### Network Impact

Connecting to a local replica will also reduce network traffic between your eDirectory servers. If the web appliance is communicating with a server holding a local replica for the given organizational unit, that eDirectory server will not have to pull information from a different eDirectory server in your network before passing that information back to the web appliance.

### Identification Performance

The web appliance synchronizes identification data from eDirectory servers. Properly configuring your web appliance to connect to the correct replica for a given organizational unit, the web appliance will allow it to receive more timely information about who is logged in.
4.4.7 Authentication

Note
No matter which form of authentication you apply, Active Directory must first be configured and turned on. Authentication options are unavailable if Active Directory is turned off. For more information, see “Configuring Active Directory Access.”

Authentication allows the appliance to perform identification on the basis of an Active Directory username, providing improved policy control and logging. Without authentication users can only be identified by IP address. As a result, appliance policy decisions and logging are based solely on IP addresses.

Use the Configuration > System > Authentication page to configure default authentication settings and create authentication profiles.

Authentication profiles can be configured to apply different types of authentication for different connection types (for example, devices and client applications that cannot be authenticated with Active Directory). To specify connection types, you must also create a connection profile using the Connection Profile Editor on the Configuration > System > Connection Profiles page.

The connection profiles that you create are then available to be referenced in authentication profiles.

Authentication profiles can also apply different types of authentication to specific destinations. For example, you may want to create an exception to the main authentication settings so that internal sites do not require authentication.

Related concepts
Active Directory (page 123)
Connection Profiles (page 138)

Related tasks
Configuring Active Directory Access (page 123)
Configuring Active Directory to support Kerberos for Mac OS X (page 133)
Adding a Connection Profile (page 139)

About Authentication

When configuring authentication, you have two main choices: bypass authentication or authenticate using selected options.

If you choose to bypass authentication, web traffic is filtered by the appliance’s Default Policy rules, or Additional Policies that are based on IP addresses and IP ranges.

If instead you choose to turn on authentication, you can select one or both of the following options:

- **Single Sign On**: Automatically authenticates with the credentials of the currently logged on user. You can configure Single Sign On to process the credentials without user interaction.

- **Captive Portal**: Allows access through a special web page, where users can log in. When enabled, users are automatically redirected to this page if Single Sign On fails or if Single Sign On is turned off. You can configure the Captive Portal feature to authenticate users and devices that cannot authenticate through Single Sign On. If “Allow access” is also turned on, a guest login link is displayed on the portal page.

  The login page itself is customizable. For more information, see “Notification Page Options.”
You can also configure how to manage access if authentication fails for Single Sign On or Captive Portal. You can either block access, or allow access using the appliance’s IP-based policy rules. The results vary, depending on the combination of selected options.

At the very least, you must select either Single Sign On or Captive Portal. The appliance does not permit you to save the settings unless one or both of the options is selected. If both are enabled, the appliance will first attempt to authenticate with Single Sign On.

In many cases, it will be sufficient to accept the factory settings on the Default Settings tab of the System: Authentication page. On a newly installed appliance, both Single Sign On and Captive Portal are enabled. On authentication failure, the default is to Allow access.

The settings that you configure on the Default Settings tab will apply to all users, unless you specify authentication exceptions on the Profiles tab.

Authentication Profiles

“Authentication profiles” reference “connection profiles” that apply a different form of authentication to specified connection sources (IP addresses, devices, or client applications). For example, you may want to exempt certain connection sources from the main type of authentication you have configured on the Default Settings tab.

On the Profiles tab, you can create authentication profiles. Using the Authentication Profile Editor, you can configure each authentication profile to:

• apply to all connections, or only to selected connection profiles. (Connection profiles must be created using the Connection Profile Editor on the System: Connection Profiles page.)

• apply to all destination sites, or only to specified sites.

• bypass authentication and apply IP-based policy rules, or authenticate using Single Sign On and/or Captive Portal.

Related concepts
Notification Page Options (page 63)
Connection Profiles (page 138)

Related tasks
Configuring Active Directory Access (page 123)
Additional Policies (page 87)
Configuring Active Directory to support Kerberos for Mac OS X (page 133)
Adding a Connection Profile (page 139)

Configuring Authentication

Select Configuration > System > Authentication > Default Settings to configure authentication or to bypass authentication and filter web traffic with IP-based policy rules instead.

Single Sign On, which is enabled by default, authenticates on the basis of Active Directory credentials. A second default option, Captive Portal, can be used to authenticate devices, client applications, and users, and to grant alternative access to guest users.

Important
Features on the Default Settings tab are not available unless Active Directory is enabled. For more information, see “Configuring Active Directory Access.”

1. Choose an authentication method.
Select **Bypass authentication** (Web traffic is filtered according to IP-based policy rules.)
or
Select **Authenticate using** (Depending on the options selected, authentication can be performed for both Active Directory users and guest users.)

- **Single Sign On**: Users can authenticate with their stored Active Directory credentials. If the appliance is configured to allow access as a result of authentication failure (see step 2), users can still gain entry to the network as guests.
  - **Perform SSO for Mac**: When this option is selected, the appliance can perform single sign on for Mac OS X systems using Kerberos. In addition, you must first configure your Active Directory server to support Kerberos authentication. For instructions, see “Configuring Active Directory to Support Kerberos for Mac.” If this option is not turned on, Mac OS X computers are still prompted for login credentials, even though single sign on does not occur.
  - **Authenticate all requests**: Select this check box to authenticate all user and client application requests against Active Directory. This option only takes effect if the appliance is deployed in explicit mode.
    
    For more information about deployment modes, see “Network Deployment.”
    
    If this check box is cleared, the appliance authenticates requests from supported end user browsers against Active Directory and uses cached information to authenticate requests from client applications.

- **Captive Portal**: Select this option to allow access through a special web page. When selected, users are automatically redirected to this page if single sign on fails or single sign on is turned off. If the appliance is configured to allow access as a result of authentication failure (see the next step), users can gain entry to the network through a guest link on the portal page.
  - **Enforce a timeout**: Specify the number of hours and minutes for which the users will remain authenticated. The default is 1 hour, after which the session times out. Users must then re-authenticate.

2. Select an authentication failure result.

**On authentication failure**

- **Block access**: Do not permit unauthenticated access. If single sign on fails or it is turned off, a web browser pop-up is displayed, prompting for credentials.
- **Allow access**: If single sign on fails, allow access using IP-based policy rules. If the Captive Portal feature is turned on, the login page contains a link to gain access as a guest user.

3. Click **Apply**, or click the **Profiles** tab to create exceptions to these general authentication settings. For instructions on creating a profile, see “Configuring an Authentication Profile.”

**Related concepts**
- Network Deployment (page 16)

**Related tasks**
- Configuring Active Directory Access (page 123)
- Configuring an Authentication Profile (page 134)
- Configuring Active Directory to support Kerberos for Mac OS X (page 133)

Configuring Active Directory to support Kerberos for Mac OS X

If you want to support single sign on for Mac OS X clients, you must configure your Active Directory server to use Kerberos. Before selecting the **Perform SSO for Mac** check box on the **System: Authentication** page, complete the steps below.
1. Log in to your Active Directory domain controller.
2. Run the following commands, providing the Active Directory username in both.

Note
The “AD Username set on the appliance” must match the username set on the System: Active Directory page.

Be sure to provide the appliance’s fully qualified domain name for the first command, and the appliance’s hostname for the second command.

```
setspn -a HTTP/<MyAppliance.example.com> <AD username set on the appliance>
```

```
setspn -a HTTP/<MyAppliance> <AD username set on the appliance>
```

Related concepts
Authentication (page 131)
About Authentication (page 131)

Related tasks
Configuring Active Directory Access (page 123)
Configuring Authentication (page 132)
Configuring an Authentication Profile (page 134)

Configuring an Authentication Profile
Select Configuration > System > Authentication > Profiles to configure an authentication profile based on a connection profile that you have created. You can also create authentication profiles that apply to specific destination sites.

If you want to create an authentication profile that is based on a connection profile, you must also create a profile using the Connection Profile Editor. For more information, see “Adding a Connection Profile.”

Important
Features on the Profiles tab are not available unless Active Directory is enabled. For more information, see “Configuring Active Directory Access.”

If there are multiple authentication profiles configured, the first one in the list that matches is used. Consider an appliance that has two authentication profiles: one that causes an IP range to authenticate using SSO (SSOprofile), and another to exempt specific client applications from authentication (ExemptApps). If SSOprofile is listed before ExemptApps, then ExemptApps will never be used if a system is in that IP range. In this example, you would want to move ExemptApps up in precedence so that it is listed before SSOprofile.

1. Click Add.
   The Authentication Profile Editor is displayed.
2. Choose a connection type.
   Select Apply to all connections
   or
   Select Apply to only the following connection profiles
   a) Select a connection profile from the drop-down list, or type a portion of the profile name in the text box.
**Important**  
Connection profiles are used to define a set of connection sources that can be referenced in authentication profiles. You must configure a connection profile on the **System: Connection Profiles** page in order to select it here.

b) Click **Add**.
Repeat these steps to add multiple connection profiles.

3. Click **Next**.

4. Choose which destinations the profile will cover.

   Select **Apply to all destinations**
   
or
   Select **Apply to only the following destinations**

a) In the **Destination Sites** text box, enter the domain, hostname, or IP address of the site. This text box also accepts both path names and wildcards.

b) Click **Add Site**.
Repeat these steps to add multiple sites.

**Note**
There is an "and" relationship between selected connections and destinations.

5. Click **Next**.

6. Choose an authentication method.

   Select **Bypass authentication** (Web traffic is filtered according to IP-based policy rules.)
   
or
   Select **Authenticate using** (Depending on the options selected, authentication can be performed for both Active Directory users and guest users.)

   - **Single Sign On**: Users can authenticate with their stored Active Directory credentials. If the appliance is configured to allow access as a result of authentication failure (see step 7), users can still gain entry to the network as guests.

     — **Perform SSO for Mac**: When this option is selected, single sign on authentication is performed for Mac OS X systems using Kerberos. In addition, you must first configure your Active Directory server to support Kerberos authentication. For instructions, see “Configuring Active Directory to Support Kerberos for Mac OS X.”

     — **Authenticate all requests**: Select this option to authenticate all user and client application requests against Active Directory.

     This option only takes effect if the appliance is deployed in “Explicit” mode. For more information about deployment modes, see “Network Deployment.”

     If this check box is cleared, the appliance authenticates requests from supported end user browsers against Active Directory, and uses cached information to authenticate requests from client applications.

   - **Captive Portal**: Select this option to allow access through a special web page. If enabled, users are automatically redirected to this page if single sign on fails or single sign on is turned off. If the appliance is configured to allow access as a result of authentication failure (see the next step), users can gain entry to the network through a guest link on the portal page.
— **Enforce a timeout**: Specify the number of hours and minutes for which the users will remain authenticated. The default is 1 hour, after which the session times out.

7. Choose an authentication failure method.
   - **Block access**: Do not permit unauthenticated access. If single sign on fails or it is turned off, a web browser pop-up is displayed, prompting for credentials.
   - **Allow access**: If single sign on fails, allow access using IP-based policy rules. If the Captive Portal feature is turned on, the login page contains a link to gain access as a guest user.

8. In the **Authentication profile name** text box, enter a meaningful name for the profile (for example, "Mobile Devices").

9. Click **Save**.

   *To activate the profile*, click the **Turn On** button for that profile name.

   *To deactivate the profile*, click **Turn Off** beside the profile name.

   *To delete a profile*, select the check box next to the profile name, and click **Delete**.

   *To change the priority of a profile*, click the up or down arrow next to the profile name to increase or decrease its ranking. Click **Save Order** to preserve the re-arranged profile ranking, or click **Reset Order** to revert to the last saved order.

**Related concepts**

- Example: Configuring Connection and Authentication Profiles (page 136)

**Related tasks**

- Configuring Active Directory Access (page 123)
- Configuring Authentication (page 132)
- Configuring Active Directory to support Kerberos for Mac OS X (page 133)
- Adding a Connection Profile (page 139)

**Example: Configuring Connection and Authentication Profiles**

While you can configure authentication to apply to all users, the web appliance allows different types of authentication based on different connection sources.

The appliance uses two kinds of profiles (connection profiles and authentication profiles) to specify authentication for IP addresses, devices, or client applications. This example demonstrates how to create an authentication profile that controls the way in which mobile devices are authenticated.

First, you will create a connection profile that defines these mobile devices, and then you will create an authentication profile that references that connection profile.

**Creating a Connection Profile**

1. Select **Configuration > System > Connection Profiles**.

2. Click **Add**.

   The Connection Profile Editor is displayed.

3. In the **Connection profile name** text box, enter *Mobile Devices*.

4. On the **Devices** tab, select **Include only the selected devices in this profile**.

5. In the **Devices** list, select *Android devices, Blackberry devices, iOS devices, and Kindle devices*. 
6. Click **Save**.

   The “Mobile Devices” profile is displayed in the **Connection Profiles** list. The **In use** status is **No**.

### Creating an Authentication Profile

1. Select **Configuration > System > Authentication**.
2. Select the **Profiles** tab.
3. Click **Add**.

   The Authentication Profile Editor is displayed.
4. On the **Connection Profile** page, select **Apply to only the following connection profiles**.
5. Type or select **Mobile Devices**.
Optionally, an authentication profile can contain multiple connection profiles. For example, you could later decide to create a separate “Blackberry” profile, and add it to this authentication profile.

6. Click **Add**, and then click **Next**.
7. On the **Destination** page, accept the default setting, **Apply to all destinations**. Click **Next**.
8. On the **Authentication** page, accept the default setting, **Bypass authentication**. Click **Next**.
9. In the **Authentication profile name** text box, enter **Mobile**.
10. Click **Save**.

   The “Mobile” profile is displayed on the **Profiles** tab. Notice that there is “No Authentication Required” for this profile. If you return to the **Configuration > System > Connection Profiles** page, you'll see that the **In use** status of the “Mobile Devices” connection profile is now **Yes**.

11. Select **Configuration > System > Authentication > Profiles**.
12. Click **Turn On**. The authentication profile becomes active.

**Related tasks**
- Adding a Connection Profile (page 139)
- Configuring an Authentication Profile (page 134)

### 4.4.8 Connection Profiles

Use the **Configuration > System > Connection Profiles** page to configure profiles based on IP address, device type, client application, or any combination of these. Once you have created a connection profile, you can reference it on the **Configuration > System > Authentication** page. Authentication profiles determine how connection profiles are authenticated.

For instance, you could:

- Set up a connection profile for iOS devices, and then create an authentication profile that requires authentication for web browsing using the Captive Portal feature.
- Create a connection profile for client applications (not including web browsers) that access the internet (for example, iTunes), and then exempt them from authentication.
- Create a connection profile of the IP range provided on your "guest" wireless network, and exempt that IP range from authentication.
Adding a Connection Profile

Configure a connection profile based on connection sources, including IP addresses, device types, and client applications.

The Connection Profile Editor contains tabs for **IP Addresses**, **Devices**, and **Client Applications**. Often, you will configure options on just one of the tabs, but you can configure a combination of options on two or three tabs. For example, you could specify a certain form of authentication for all Windows computers in the 192.0.2.0/24 range. Windows computers outside of this range would be authenticated differently.

There is an “and” relationship between the settings on each tab. In other words, the combination of IP address, device, and client application settings always applies to each profile.

**Important**

Any connection profile that you create here does not take effect until you reference it as part of an authentication profile. For more about authentication and using the Authentication Profile Editor, see “Authentication.”

1. On the **Configuration > System > Connection Profiles** page, click **Add**.
2. In the **Connection profile name** text box, enter a meaningful name for the profile you are about to create.
3. Define the profile using one or more of the three tabs: **IP Addresses**, **Devices**, and **Client Applications**.

   - **IP Addresses**
     
     Select **Include all IPs in this profile**
     
     or
     
     Select **Include only the following IPs in this profile**
     
     a) In the **IP Addresses or IP ranges** text box, enter an address or range, and click **Add**.
     
     The new entry is displayed in the list below.
     
     To remove an address or range from the list, select the check box next to the entry you want to remove, and click **Delete**.
     
     To search for an address or range in the list, enter a search term in the text box below the list, and click **Filter**.
     
     To delete a search term from the text box, click **Clear**.

   - **Devices**
     
     Select **Include all devices in this profile**
     
     or
     
     Select **Include only the following devices in this profile**
     
     — In the **Devices** list, select the types of devices that you want to include. If the device type does not match any of the categories in the list, select **Unknown**.

   - **Client Applications**
Select **Include all client applications in this profile**

or

Select **Include only the selected applications in this profile**

a) In the **Client Applications** list, select the client application(s) that you want to include.

b) If the client application you wish to add is not listed, enter it in the **Application name** text box. Enter the product’s **User agent string** (The appliance performs prefix matching for this field. If you enter a prefix of the user agent string, all user agents that start with the same characters will match). Click **Add**.

4. When you have finished defining the profile, click **Apply**. The profile is displayed in the list of **Connection Profiles**. Once it is referenced in an authentication profile, the **In use** status changes to **Yes**. For more information, see “Authentication.”

**Related concepts**
- Example: Configuring Connection and Authentication Profiles (page 136)
- About Authentication (page 131)
- Authentication (page 131)

**Related tasks**
- Configuring an Authentication Profile (page 134)

### 4.4.9 Time Zone

The **Time Zone** page always sets the configuration for the local system time only, even on a management appliance. If you want to specify different time zones for the management appliance and joined appliances you must configure each one separately.

Use the **Configuration > System > Time Zone** page to set the local time that is used to indicate the time in quarantine information, logs, and reports.

By default, Sophos appliances use `0.sophos.pool.ntp.org`. If you need to use a different network time protocol (NTP) server to synchronize the appliance time with your Active Directory server, you can do so on this page.

- **To set the time zone**, select the zone that is most appropriate for your organization from the **Time zone** drop-down list, and click **Apply**.

- **To specify a network time protocol (NTP) server**, select the **Specify an NTP server to use instead of default** check box in the **Network Time Protocol server** section, enter the IP address or the fully qualified hostname of the NTP server that you want to use in the text box to the right, and click **Apply**.

### 4.4.10 Central Management

Scaling Sophos Web Appliances to handle large numbers of users is accomplished by using multiple web appliances that are centrally managed by a Sophos Management Appliance. The management appliance provides centralized configuration, centralized policy management, and consolidated reporting.

The **Configuration > System > Central Management** page serves three different functions, depending on the type of appliance, or the current operating mode. For more information see “Grouping Web Appliances”.

140 Copyright © 2019 Sophos Limited
On a Stand-Alone Web Appliance: Joining a Management Appliance

Use the **Configuration > System > Central Management** page on a stand-alone web appliance to join a Sophos Management Appliance.

**Important**

- Joining a web appliance to a management appliance will interrupt web browsing through that web appliance while LDAP user and group information is copied to the management appliance. You should plan to join during periods of low usage for your web appliance.

- In order to join a web appliance to a management appliance, both appliances must be running the same software engine versions. Check **Configuration > System > Updates**, and perform any necessary updates before joining.

- By default, management appliances are set to **Copy configuration and policy data from the first web appliance to join**. When setting up a new group of appliances, be sure that the first web appliance that you join to your management appliance is an established web appliance with existing configuration and policy data, otherwise a new web appliance will set your management appliance configuration to that of an unconfigured web appliance.

1. On the management appliance, select **Configuration > System > Central Management**. Ensure that these check boxes are selected: **Allow Web Appliances to join this Management Appliance** and **Copy configuration and policy data from the first web appliance to join**. Then ensure that the Web appliance it is joining to is the established appliance with existing configuration and policy data.

2. On the stand-alone appliance, select **Configuration > System > Central Management**.

3. In the **Hostname** text box, enter the hostname or IP address of the management appliance to which you want this Sophos web appliance joined.

4. In the **Join password** text box, enter the connection password for the management appliance to which you want this Sophos web appliance joined.

5. Optionally, if this web appliance has been in use for a significant period of time prior to joining to the management appliance, and you want to save and use report data, select **Upload historical report data from this appliance** to add this appliance’s report data to the management appliance.

   **Note**
   
   If you do not upload historical data, it will be deleted.

6. Click **Join Management Appliance**.

   As the join operation progresses, the icons in the **Join status** panel change to indicate the status of each stage of the operation.
Upon a successful join of your web appliance to your management appliance, the following changes occur to the administrative web interface:

- The options on the Configuration > System > Central Management page change to Revert to Standalone Mode
- The Reports and Search options are removed from the Navigation bar
- The Configuration pages are reduced in number and some are simplified in content.

To access any of these removed features, see the administrative web interface of the management appliance, which is where that functionality is now controlled.

On a Joined Web Appliance: Reverting to Standalone Mode

Use the Configuration > System > Central Management page on a joined web appliance to revert to standalone mode.

1. Click Revert to Standalone Mode.
   
   A verification dialog box is displayed, prompting you to confirm that you want to break the connection with the management appliance to resume in standalone mode.

2. Click OK.

Upon a successful separation of your web appliance from your management appliance, the following changes occur to the web appliance administrative web interface:

- The options on the Configuration > System > Central Management page change to Hostname and Password with a Join Management Appliance button.
- The Reports and Search options are restored to the Navigation bar.
- The Configuration pages are increased in number, and some have expanded content.

On a Management Appliance: Configuring Joining Options

Use the Configuration > System > Central Management page on a Sophos Management Appliance to configure central management options.

- To allow web appliances to join this management appliance, select Allow web appliances to join this Management Appliance, and click Apply.

Note

Once you have all of your web appliances joined to the management appliance, you can clear the Allow web appliances to join this Management Appliance option to increase the security of your appliance group.

- To set the "join" password, type the password into the text box in the Join password section, and click Apply.
- To use the configuration and policy data from the first web appliance to join this management appliance, see "Using web appliance Configuration Data".

On a Management Appliance: Using Web Appliance Configuration Data

This option allows you to download the configuration and policy data from your established web appliance, allowing you to avoid repeating configuration work on your new management appliance. The configuration that is downloaded to the management appliance is then downloaded to other web appliances that are subsequently joined.

1. Select Copy configuration and policy data from the first web appliance to join.
Do this before you join any web appliances.

2. On your original web appliance, join the management appliance.

**Important**
Be sure that the first web appliance that you join to your management appliance is the established web appliance with existing configuration and policy data, otherwise a new web appliance will set your management appliance configuration to that of an unconfigured web appliance.

This will cause the management appliance to download the configuration and policy data from this first web appliance.

These subsequently joined web appliances will download their configuration and policy data from the management appliance.

### 4.4.11 Certificates

Use the **Configuration > System > Certificates** page to manage the certificate used by the appliance. This certificate is used by the web appliance to create secure connections with browsers for HTTPS scanning as well as the Administrative User Interface.

**Note**
You can either provide your own certificate, or use the self-signed certificate provided with the web appliance.

On the **Certificate Authority** tab you can select from the following:

- **Original Sophos Certificate** The original self-signed certificate provided with the appliance will expire soon. When it expires, the appliance will automatically switch to the new certificate. To prevent end-user warnings, download the new Sophos certificate using the link provided and deploy it to all users. Then, select **New Sophos Certificate**.

- **Sophos Certificate** This option replaces the original Sophos certificate and is available only after you have switched to the new Sophos certificate.

- **Custom Certificate** Use your own private key and signing certificate.

**Note**
In the near future, Microsoft, Mozilla, and potentially other companies will begin to block or warn when using SHA-1 based certificates. You can use the new **Regenerate Certificates** button to switch the Sophos certificate to a more secure SHA-256 signature.

**Related reference**
Certificates and Certificate Authorities

**Custom Certificate**

When you select **Custom Certificate**, controls will be displayed that allow you to upload a private key and a custom certificate.

- To add a custom certificate:
• For the **Private key**, click the **Choose file** button, and select the file that contains the private key associated with the custom certificate that you want to use.

• For the **Signing certificate**, click the **Choose file** button, and select the file that contains the custom certificate that you want to use.

• Click **Upload** to add the private key and signing certificate pair that you want to use.

**Note**
The certificate must be in **PEM** or **PKCS#12** format. A certificate must be a self-signed certificate that has been deployed to endpoint browsers, or by one of the authorities already supported by the browser on the endpoint.

**Related reference**
Certificates and Certificate Authorities

### 4.4.12 Endpoint Web Control

If you want to use an appliance together with Sophos Enterprise Console, you must provide Enterprise Console with an appliance hostname and an authentication key. Once this is configured, a web control policy can be applied to the endpoint machines by the designated appliance.

The authentication key is generated on the appliance as described below. You must then enter the same key as part of the Web control policy on Enterprise Console. The hostname and authentication key are published to the endpoints, allowing the endpoints to exchange data with the appliance.

Optionally, you can also enable Sophos LiveConnect so that policy updates are published to user machines, even when users are not directly connected to the network. In addition, you can choose to allow roaming endpoints to upload web activity data.

**Note**
If you choose **not** to enable the LiveConnect options described in steps 4 and 5, endpoints that are disconnected from the network will:

- use the last web policy downloaded before the endpoint machine disconnected from the network.
- upload the most recent web activity data to the appliance when the endpoint machine reconnects with the network. The data is limited to the last two months of web activity.

1. Select the **Configuration > System > Endpoint Web Control** page.
2. Click **On** to enable **Endpoint Web Control**.
3. In the **Endpoint Authentication Key** text box, there is an alphanumeric key. Enter the same key in the Sophos Enterprise Console. See “Configuring the web control policy” in the Sophos Enterprise Console documentation for specific instructions. If, at any time, you need to change the key, click **Regenerate**, and a new key will be displayed. This new key must then be transferred to Enterprise Console, replacing the original key.
4. [Optional] Select **Use Sophos LiveConnect Service**. When this check box is enabled, policy updates are published to user machines, even when users are not directly connected to the network.
Neither web traffic nor user data passes through LiveConnect. It is only used to securely publish web policy updates to users and to securely submit web activity reports from the endpoint machines back to the appliance.

5. [Optional] Select **Allow roaming endpoints to submit web activity reports.** When this check box is enabled, web activity data is uploaded from roaming user machines and compiled for reports on the appliance. This option is only available when **Use Sophos LiveConnect Service** is enabled.

6. Choose an alternate action for enforcing quota time on the endpoint.

Sophos Endpoint Web Control cannot enforce time quotas. Here you can select to either **Allow**, **Block**, or **Warn** when an endpoint user visits a site that has an associated quota time policy.

7. Click **Apply**.

**Related concepts**

**Quota Time** (page 88)

**Viewing Connected Endpoints**

If you are using an appliance together with Sophos Enterprise Console, you can view details of all connected user machines, or specific user machines, that are running Sophos Endpoint Security and Control.

Since this list of endpoints can be very large, you can click **Show Filters**, and use the available search features to narrow the endpoints that are displayed.

- On the **Dashboard**, click **Connected endpoints**.

  The results of the endpoint search are displayed.

  Each entry shows whether the endpoint is **Active**, the **Machine Name**, its **IP Address**, its **Username**, and the time that the endpoint was **Last Connected**.

- Optionally, click the up/down arrow button that appears immediately to the right of any of the column headers to sort the list according to that header:

  — **Active**: Sorts the entries according to their activity. By default, active machines are shown first, followed by inactive machines. Regardless of the sort order, a maximum of 1000 endpoints can be displayed. Active endpoints are those that have contacted the appliance within the past hour. Active endpoints are indicated by a green status icon; inactive endpoints are indicated by a gray status icon.

  — **Machine Name**: Sorts the entries alphabetically by the name of the machine that is home to the endpoint software.

  — **IP Address**: Sorts the entries in numeric order from lowest to highest.

  — **Username**: Sorts the entries alphanumerically by the username. The username show is either the Active Directory username or the hostname of the connected machine.

  — **Last Connected**: Sorts the entries chronologically by date and time.

**Note**

If the text in any field is too long to view, place your mouse pointer over the text and the full text is displayed in a screen tip box.
To reverse the order of the entries, click on the same up/down arrow button that you clicked previously.

- To narrow the list of endpoints displayed, click **Show Filters**. Use the **Active** drop-down list, to show only **Active** or **Inactive** endpoints. You can also can also enter specific search terms for **Machine Name**, **IP Address**, and **Username**. Click **Hide Filters** if you do not want the advanced search options displayed.

- Click **Refresh** to force an update of the list of connected endpoints.

**Related concepts**
**Endpoint Web Control** (page 48)

**Related tasks**
**Endpoint Web Control** (page 144)

### 4.5 Network

Use the **Network** pages to change the configuration of the appliance’s connection to, and identity within, your organization’s network.

**Note:** All of the pages in this section are available in all three operating modes—stand-alone web appliance, joined web appliance, and management appliance—however, not all features on the **Network Interface** and **Hostname** pages are available in every operating mode. See the documentation for those pages for detailed information about what features are available in each operating mode.

- Use the **Network Interface** page to configure your appliance’s IP address and its access to DNS servers.
- Use the **Hostname** page to set your appliance’s hostname as well as an upstream or downstream proxy.
- Use the **WCCP** page to enable **Web Cache Communication Protocol (WCCP)** integration between your web appliance and WCCP-enabled routers.
- Use the **Network Connectivity** page to test your appliance’s connection to any upstream proxy, your ISA/TMG server, the internet, and to Sophos.
- Use the **Diagnostic Tools** page to troubleshoot connection problems between the appliance and other servers on the internet.

### 4.5.1 Configuring the Network Interface

Neither the **Deployment Mode** option nor the **Configure** button are available on the management appliance, as deployment modes are not relevant.

Use the **Configuration > Network > Network Interface** page to configure your appliance’s IP address and to configure access to your network’s DNS servers.
Note
The appliance uses 172.24.24.173 as the network address to access its initial configuration. This may cause routing conflicts if your local network also uses addresses in the range of 172.24.24.0-255. Contact Sophos Technical Support for a solution if this applies to your deployment.

Important
If WCCP is enabled (on the Configuration > Network > WCCP page), all network settings on the Network Interface page, except Specify the DNS servers, will be disabled until you turn off Web Cache Communication Protocol integration.

1. Select either DHCP or Static IP.

If you choose the DHCP option, the Obtain DNS servers automatically option button is selected by default. DHCP is not recommended for a production environment, as the IP address can unexpectedly change, disrupting your users.

If you choose the Static IP option, you must also fill in the following text boxes:

- Enter the IP Address for the appliance.
- Enter the Network Mask. The network mask is the range of addresses that the appliance can connect to directly. IP addresses outside of this range are reached via the Default Gateway.
- Enter the IP address of your network’s Default Gateway.
- [Optional] From the Deployment Mode drop-down list, select the mode that you want to use. The options are:
  - Explicit proxy: Select this option if you have elected to use the explicit network deployment.
  - Transparent: Select this option if you have elected to use the transparent network deployment.
  - Bridged (inline): Select this option if you have elected to use the bridged network deployment. This option is not available if no bridge card is installed in your appliance.

See "Network Deployment" for a description of each of these and other deployment types.

- If you chose the Bridged (inline) option in the previous step, you can click Configure beside the Deployment Mode option to create a list of IP addresses or IP ranges to exempt from appliance handling. These IP addresses will be exempt from all web appliance filtering, including virus scanning.

- In the Bridged Mode Configuration dialog box, enter the IP address or IP range in CIDR format in the text box, select IP Address or IP Range from the drop-down list as is appropriate for the entry, and click Add. Click OK when you have added all the IP addresses or ranges that you want in the list.

Important
The web appliance will interpret any dotted quad followed by a slash and a number less than 33 as a CIDR range. This creates the possibility that a URL entered as an IP address followed by a numbered directory from 0 to 32 would be improperly treated as a CIDR range. To avoid this possibility, always enter URLs to numbered directories using fully qualified domain names rather than IP addresses.
Sophos Web Appliance

• [Optional] To configure Additional IP routes, IP Address to hostname map, or TCP listening ports, click Advanced Settings (see Configuring Advanced Settings).

2. Auto is the default setting, but, in certain cases, the appliance may not be able to connect to your network if Auto is selected, which will require that you manually set these options from the Speed and duplex drop-down list.

This option is always available, whether you are using DHCP or static IP, or the Explicit, Bridged, or Transparent deployment modes.

3. Select Obtain DNS servers automatically or Specify the DNS servers to set which method the appliance will use to obtain your DNS servers' IP addresses.

If you selected the Specify the DNS servers option, enter the IP addresses of your network’s DNS servers in priority order (Primary through Tertiary). When you specify more than one DNS server then:

• If the primary DNS server becomes unresponsive, the appliance will continually attempt to send requests to the primary DNS server. If a timeout occurs before the primary DNS server becomes available again, the appliance will send queries to the secondary DNS server.

• If the primary DNS server rejects queries, the appliance will immediately send queries to the secondary DNS server.

Similar behavior will apply if your secondary DNS server also becomes unresponsive or rejects queries, and you have specified a tertiary DNS server.

Note
Even if you have an upstream proxy (a proxy between the web appliance and the internet) configured, you still need to configure the web appliance with access to your organization’s DNS server.

4. Click Apply.

If your appliance is a Virtual Web Appliance or a Virtual Management Appliance there is the option to Re-register a cloned virtual appliance. If you clone a virtual appliance, each cloned instance must be re-registered before you can use it in live production mode.

Related concepts
Network Deployment (page 16)

Configuring Advanced Settings

Additional IP routes enable the Sophos Web Appliance to process requests from client machines with IP addresses that reside outside of the appliance’s subnet by re-routing the requests from those IP ranges.

Note
The appliance uses 172.24.24.173 to run the Setup Wizard. If your local network also uses addresses in the range of 172.24.24.0-255, adding an additional route that includes this address will cause routing conflicts. Adding routes incorrectly can make the administrative web interface inaccessible. See Adding Routes for more information.

• To add a route:
  a) Enter a descriptive Route Name.
  b) Enter the requested Destination IP Range in CIDR format.
Important
This range must not include the static IP address of the appliance. It must also be outside of the appliance's subnet. Always enter URLs to numbered directories using fully qualified domain names rather than IP addresses. The web appliance interprets any dotted quad followed by a slash and a number less than 33 as a CIDR range. Thus, a URL entered as an IP address followed by a numbered directory from 0 to 32 is improperly treated as a CIDR range.

c) Enter the Gateway IP Address to which you want to route the IP addresses. This address should be on the same subnet as the appliance.
d) Click Add.
To modify a route, you must delete it and add it again with the modified route information.

Note
If a route makes the administrative web interface inaccessible, you must delete the incorrect routes. Connect a laptop to the configuration port of the appliance and access the appliance by connecting to 172.24.24.173.

• To delete a route:
  a) Select the check box beside the route that you want to delete.
  b) Click Delete.
The Hostname to IP Address map feature allows you to map a hostname to an IP address. This feature is used to resolve hostnames or sites (for example, Active Directory servers) that the configured DNS server is not aware of. This is the same as implementing a hosts file on a server or workstation.
• To map a hostname to an IP address:
  1. Enter an IP address in the IP Address text box.
  2. Enter a hostname in the Hostname text box.
  3. Click Add.

Note
For Active Directory to work properly when the DNS server is not aware of the Active Directory server, you may need to include the following entries for your Active Directory server. Behavior of the the Active Directory service may be affected by the order of these entries. In most cases, the FQDN should be added first.

```
<IP address> host.domain.tld.
<IP address> host.domain.tld
<IP address> domain.tld
```

• To remove mapping:
  1. Select the check box beside the mapping that you want to delete.
  2. Click Delete.
The **TCP listening ports** feature allows you to configure additional ports on which the appliance will listen for web connections.

- **To add a TCP listening port:**
  1. Enter comma-separated port numbers in the **TCP listening ports** text box.

     The port numbers must be between 1024 and 65535. Reserved ports that cannot be used include: 8080, 8443, 8445, 8777, 10000, 13128, and 18081. Port 8080 is always used by default. You can enter spaces after commas.
  2. Click **Add**.

- **To modify the list of TCP listening ports:**
  1. Edit the list of comma separated port numbers that the appliance will use to listen for web connections.

     The port numbers must be between 1024 and 65535. Spaces after the commas are allowed.
  2. Click **Add**. If no ports are listed, the default of 8080 port 8080 will be used.

Click **Close** to exit the **Advanced Settings** dialog box.

### 4.5.2 Hostname and Other Network Settings

| **On a management appliance, neither the DNS search suffixes, nor the Accept authentication from downstream ISA/TMG servers options are available.** |

Use the **Configuration > Network > Hostname** page to set your appliance’s hostname and to configure various network deployment options. Different optional settings are appropriate, depending on your network environment, and the appliance deployment you implemented during setup.

- **To set the hostname**, type in the fully qualified hostname that you want to use for your appliance in the **Fully-qualified domain name** field, and click **Apply**.

  The following limitations are enforced via entry validation:

  — The hostname must not exceed 15 characters *(required for Active Directory)*.
  — The entire fully qualified domain name must not exceed 64 characters *(required for certificate generation in the administrative web interface)*.

  **Note**

  This field is disabled on the management appliance after the first web appliance joins it, and on the first joined web appliance. Changing FQDNs of either appliance after a join would break the connection between them.

  Changing the hostname will trigger the generation of a new administrative web interface certificate, which you should install. The generation of the new certificate may take as long as a minute or two. The **Hostname** page will then reload, using the old URL, so your browser will display a certificate mismatch error if the hostname in the URL does not match the hostname in the administrative web interface certificate. If this occurs, choose to proceed with the mismatched certificate.

  After changing the hostname, it is advised that you log out to avoid potential problems.

- **To set the search domain**, type in your organization’s search domain in the **DNS search suffix** text box, and click **Apply**.
This is typically your organization’s domain, which enables browsers to complete the domain name if a user types only a machine name in the address field.

- To set the outgoing mail server, type the fully qualified domain name of your organization’s outgoing SMTP mail server in the Outgoing SMTP mail server field, and click Apply.

This is required if your organization’s firewall will not permit the appliance to send email, such as alert notifications or reports.

**Important**
Setting the outgoing SMTP mail server is essential if you want to receive emailed alerts or reports, or if you want the Sophos Managed Appliance Service. If you do not want these features or this service, do not configure the Outgoing SMTP mail server, and be sure to turn Sophos Technical Support alerts off on the Configuration > System > Alerts page.

**Related concepts**
Network Deployment (page 16)

**Specifying an Upstream Proxy**

1. In the Specify upstream proxy section’s IP or FQDN field, type the IP address or the fully qualified domain name of the upstream proxy.

**Note**
The currently supported upstream proxy configurations are:
- Squid without user authentication.
- Forefront TMG 2010 in firewall and proxy mode without user authentication.

HTTP (port 80) and HTTPS (port 443) traffic will be proxied through the upstream server. You may need to configure your firewall to allow other external connections. Refer to the Setup Guide to review specific ports that the appliance uses for external and internal connections.

2. In the Specify upstream proxy section’s Port field, type the port number by which you access your organization’s web proxy.

3. Optionally, to forward requests for specific hostnames to a particular upstream proxy, click the Advanced Settings button.

The Advanced Settings dialog box is displayed.

a) In the Hostname text box, enter the IP address or hostname for which you want to forward requests. Wildcard (“*”) hostnames can be used, such as *.example.com, if you want to match an entire domain.

b) In the Upstream proxy text box, enter the hostname or IP address and the colon-separated port number of the upstream proxy to which you want to forward requests.
In Transparent or Bridged mode, if a user requests an HTTPS page from a browser that does not support Server Name Identification (SNI), and you have specified a proxy by hostname or domain in Advanced Settings, that alternative proxy will not be used. Rather, the request will go through the default upstream proxy that you entered in steps 1 and 2. To ensure that the alternative proxy is used instead, enter an IP address in the Advanced Settings.

c) Click Add to add the new entry to the list.
d) To remove entries from the list, first select the check box next to each entry that you want to remove, then click Delete.

4. Click Apply.

4.5.3 Configuring WCCP

To enable integration between your Sophos Web Appliance and WCCP routers, use the Configuration > Network > WCCP page. Your deployment can be in either Transparent Mode or Bridged Mode.

1. Enable WCCP on your routers. The web appliance will only process HTTP traffic that is directed to port 80 of external sites.

   Note
   When using WCCP with a router that supports the fast timers feature (Cisco firmware from later than 2012 or WCCP v2 rev1), you must disable the fast timers feature. To disable this on a Cisco router, use the command no ip wccp variable-timers.

2. Toggle the WCCP integration button to the On position.
3. Under Forwarding method, select GRE or L2.
**Important**

You must turn WCCP off on all appliances for a minimum of 30 seconds when you switch between the GRE and L2 forwarding methods.

- For optimal performance, choose L2, if there are no routers between the WCCP router and the web appliance. (In this example, the IP address of interface 1 is the WCCP Router IP address.)

- You must choose GRE if your network has more than one router between the WCCP router and the web appliance, or if your network topology has specific hardware or firewall requirements. (In this example, the IP address of interface 2 is the WCCP Router IP address.)
4. Enter the IP addresses for your routers.
   - For routers using a multicast IP address, enter one IP address, and click Add.
   - For a router with unicast IP addresses, enter one IP address, and click Add. Do the same for each router.

   **Important**
   You should specify the IP address of the interface with the least number of hops to the web appliance.

5. [Optional] Select **Accept HTTPS redirection from WCCP router** to allow HTTPS traffic to be forwarded.

   **Note**
   This option requires that there be two WCCP service groups on the selected router. The required groups are group 0 for HTTP, and group 70 for HTTPS.

6. [Optional] Enter a password under **Service group password** to ensure the web appliance only accepts requests from authorized WCCP routers.

7. Click **Apply**.

   If the initial setup is successful, traffic will begin to flow through the web appliance. However, if the initial setup fails, the **System Status** will display a critical error after three minutes.
When a web appliance with an incompatible forwarding method attempts to join a WCCP service group, Cisco routers correctly detect that an unusable proxy has joined, but may not update the router’s record. To correct this, you must disable WCCP on the router, and then re-enable it, clearing the list of known routers.

**Related concepts**
Replacing Hardware Appliances with Virtual Appliances (page 15)

**Related tasks**
Transparent Deployment (page 24)

**Related information**
Integrating the Appliance with WCCP

### 4.5.4 Load Balancing with the Management Appliance

The features described in this section are only available on the management appliance.

Optionally, you can use the Configuration > Network > Load Balancing page to configure a Management Appliance as a load balancer. This lets the management appliance distribute load between any web appliances that are joined to it.

**Note**
You cannot configure load balancing when using DHCP.

To configure load balancing:
1. Click the **On** button to enable load balancing.
2. In the **Load balancing configuration** table, select the appliances to which you want to apply load balancing.
3. In the **Virtual IP** text box, enter the virtual IP that you want to assign to this management appliance.
4. Click **Apply**.

**Related concepts**
Network Deployment (page 16)

### 4.5.5 Testing Network Connectivity

Use the Configuration > Network > Network Connectivity page to test the appliance’s ability to access the Sophos site via the internet, which is required to receive regular security data and software updates, as well as to provide users with filtered access to the internet.

To test your appliance’s connection:

Click **Test**.

The test results are shown as the test proceeds. As each test is performed, one of three icons is displayed to the left of the line describing the test:
A green check mark icon indicates that the test is successful.

A yellow exclamation mark icon indicates that the test produced a warning.

A red "x" icon indicates that the test failed.

The icon that is displayed beside the "Test complete" message summarizes the outcome of the tests:

A green check mark icon indicates that all network configuration settings are valid.

A yellow exclamation mark icon indicates that one or more non-essential configuration settings were in error, but the appliance will function.

A red "x" icon indicates that one or more essential configuration settings failed, which means that the appliance is unusable with the current network configuration.

4.5.6 Running the Diagnostic Tools

The appliance offers a set of diagnostic tools that you can use to diagnose problems connecting to remote websites. Before trying these tools, you should ensure that you have checked the connection, using the Configuration > Group Policy > Policy Test page to confirm that access to the site is allowed by the policy.

1. Enter the hostname, URL, or IP address of the site to which you want to check the connection.

   If you are using Send HTTP request, you can specify the protocol (for example, HTTPS). You can also specify a particular file.

   Note
   Send HTTP request will not retrieve the actual file, just the headers.

2. Select the diagnostic tool that you want to use from the drop-down list.

   The options are Ping, Traceroute, DNS lookup, and Send HTTP request. The common uses of these tools are:

   • Ping: Tests connectivity to a server or site. You can either use ping to check if the appliance has the network access to contact a particular server, or—if you are confident that the appliance has no access problems—you can use it to check whether a particular server is actually up and running.

   • Traceroute: Identifies the "hops" the appliance has to go through to access a particular destination. If the appliance is having trouble accessing a destination, traceroute would show where the request is being routed and possibly identify the source of the problem (for example, you might find that a request is being routed to an unexpected router that is unable to handle the request).

   • DNS lookup: Checks which IP(s) a particular hostname resolves to. A site can be blocked by its hostname or by its IP address. If a site is being blocked, but its hostname is set to "Allow" in
the Policy Tester, it may be blocked according to its IP address. Alternatively, there may be a problem accessing a site because old or invalid DNS entries resolve to a non-existent or invalid IP address.

- **Send HTTP request**: Downloads the headers in response to an HTTP request. You can use this option to determine if the destination site is responding incorrectly to the appliance (the request would return an invalid HTTP header). This can help you troubleshoot a site that is not working.

3. Click **Run Test**.

The results of the selected test are displayed in the **Test results** panel.
5 Reports

The Reports tab provides graphical and textual data on a variety of aspects of web appliance activity and performance.

On the left side of the tab is a navigation sidebar with links to the individual reports pages.

From the Options section of the sidebar, you can configure the Reporting Groups (the groups upon which group-based reporting is based), and use the Report Scheduler (in which you set up the automated emailing of sets of reports sent as PDFs to selected individuals on a configurable schedule).

The reports, and the Options pages, are displayed on the middle part of the tab.

The Report Parameters sidebar on the right side of the tab allows you to modify the time period covered by the report, and, for some reports, allows you to change the type of data that is reported on as well.

You can modify, print, and export any of the reports from within the individual reports pages.

You can get related information by clicking on items in the report results. For instance, if you click on a specific category in the results of the Browse Time By User report, the report will switch to the Top Users By Category report with the relevant report parameters set. If you click on a username in the High Risk Site Visitors report, the appliance will run a search on that username filtered by Blocked (High Risk) and the relevant username.

Note

Search > Recent Activity Search results only include page views and file downloads, while Reports may include various other data, and may not match the results of Recent Activity Search queries. Similarly, reports may list no hits while still reporting a byte count.

5.1 Available Reports

On the Reports tab, the navigation sidebar lists the available reports. Click a report category (Traffic & Performance, Users, Policy & Content) on the side to access the reports within that category.

The full list of available reports is as follows:

5.1.1 Traffic & Performance: Volume

By default, a stacked-bar graph and data table of the total number of user requests by request type, hourly for the current day since midnight. You can sort the results according to site visits or bytes consumed. The available search parameters vary from one report to another. See “Modifying Reports” for a description of each parameter.

Note

This report displays the total of allowed traffic between clients and the proxy. This report does not display the total bandwidth usage for the appliance.
5.1.2 Traffic & Performance: Latency

By default, a bar graph and data table of the peak delay in seconds added to page views and downloads by the web appliance, hourly for the current day since midnight. If you view this report for multiple web appliances, the values shown are averages of all active web appliances (averages do not include web appliances without data).

The available search parameters vary from one report to another. See “Modifying Reports” for a description of each parameter.

5.1.3 Traffic & Performance: Throughput

By default, a bar graph and data table of the volume of data, in the form of megabits per second, that the web appliance has handled hourly for the current day since midnight. If you view this report for multiple web appliances, the values shown are totals of all web appliances.

The available search parameters vary from one report to another. See “Modifying Reports” for a description of each parameter.

5.1.4 Users: Virus Downloaders

By default, a pie chart of the top five virus downloaders, plus all others, each shown as a percentage of the total number of viruses downloaded today since midnight. The data table shows the following:

- full list of users who downloaded viruses during the reporting period. If your web appliance is configured to access a single-domain Active Directory server, only the username of each user is displayed; if the web appliance is configured to access the global catalog of a multidomain Active Directory forest, users are displayed in the form "domain\username". Usernames for eDirectory are specified in the form user.context.
- IP addresses to which the viruses were downloaded.
- Count of the viruses downloaded.
- The top five viruses downloaded (maximum) for each user.

Click on a username to view a Search > By User of all URLs blocked due to viruses.

The available search parameters vary from one report to another. See “Modifying Reports” for a description of each parameter.

5.1.5 Users: Sandstorm Users

By default, a pie chart of the top five users who have had the most files referred to Sophos Sandstorm, plus all others, each shown as a percentage of the total number of files flagged as suspicious today since midnight. The data table shows the following:

- **Username**: Full list of users with files referred to Sandstorm during the reporting period. If your web appliance is configured to access a single-domain Active Directory server, only the username of each user is displayed; if the web appliance is configured to access the global catalog of a multidomain Active Directory forest, users are displayed in the form "domain\username". Usernames for eDirectory are specified in the form user.context.
- **Originating IP**: The originating IP of the user.
• **Clean**: files that have been analyzed and that exhibit no malicious behavior.
• **Malicious**: files that Sandstorm has determined are malicious.
• **Unsuccessful**: files that could not be analyzed.
• **Excluded**: files that were not sent for analysis due to policy settings.
• **Total**: the total number of files that were flagged as suspicious.

Click on a username or IP address to view a **Search > By User** of all URLs blocked by the policy.

The available search parameters vary from one report to another. See “Modifying Reports” for a description of each parameter.

### 5.1.6 Users: PUA Downloaders

By default, a pie chart of the top five PUA downloaders, plus all others, each shown as a percentage of the total number of PUAs downloaded today since midnight. The data table shows the following:

• Full list of users who downloaded PUAs during the reporting period. If your web appliance is configured to access a single-domain Active Directory server, only the username of each user is displayed; if the web appliance is configured to access the global catalog of a multidomain Active Directory forest, users are displayed in the form "domain\username". Usernames for eDirectory are specified in the form `user.context`.
• IP addresses to which they downloaded PUAs.
• Count of PUAs downloaded.
• Top five PUAs (maximum) downloaded by each user.

Click on a username or IP address to view a **Search > By User** of all URLs blocked due to PUAs.

The available search parameters vary from one report to another. See “Modifying Reports” for a description of each parameter.

### 5.1.7 Users: High Risk Site Visitors

By default, a pie chart of the top five high risk site visitors, plus all others, each shown as a percentage of the total number of high risk sites visited today since midnight. The data table shows the following:

• Full list of users who visited high risk sites during the reporting period. If your web appliance is configured to access a single-domain Active Directory server, only the username of each user is displayed; if the web appliance is configured to access the global catalog of a multidomain Active Directory forest, users are displayed in the form "domain\username". Usernames for eDirectory are specified in the form `user.context`.
• IP addresses from which they browsed high risk sites.
• Count of the high risk sites visited.

Click on a username or originating IP address to view a **Search > By User** of all URLs blocked because they are high risk sites.

The available search parameters vary from one report to another. See “Modifying Reports” for a description of each parameter.
5.1.8 Users: Policy Violators

By default, a pie chart of the top five policy violators, plus all others, each shown as a percentage of the total number of policy violations today since midnight. The data table shows the following:

- full list of users who violated policy during the reporting period. If your web appliance is configured to access a single-domain Active Directory server, only the username of each user is displayed; if the web appliance is configured to access the global catalog of a multidomain Active Directory forest, users are displayed in the form "domain\username". Usernames for eDirectory are specified in the form `user.context`.
- The count of their policy violations.
- Top five (maximum) policy rules violated for each user.

Click on a username to view a Search > By User of all URLs blocked by the policy.

The available search parameters vary from one report to another. See “Modifying Reports” for a description of each parameter.

5.1.9 Users: Top Users By Quota

A data table is displayed showing top users of quota time.

By default, queries are ranked according quota time consumed, starting with the largest. You can also sort the results according to hits or bytes. The data table contains these columns:

- **Username**: The user who has consumed quota time. Click the username to open a recent activity report for that user. As with other reports, if your web appliance is configured to access a single-domain Active Directory server, only the username of each user is displayed; if the web appliance is configured to access the global catalog of a multidomain Active Directory forest, users are displayed in the form "domain\username".
- **Quota used**: The number of minutes a user has consumed of their current quota allocation.
- **Top 5 categories**: The top five categories in which the specified user browsed sites.
- **Hits**: The number of site accesses in each of the top five categories. The first row displays the total number of accesses in the top five categories.
- **Bytes**: The number of bytes downloaded each of the top five categories. The first row displays the total number of bytes downloaded in the top five categories.

The available search parameters vary from one report to another. See “Modifying Reports” for a description of each parameter.

5.1.10 Users: Top Bandwidth Users

By default, a pie chart is displayed of the top five bandwidth users and all others. These are shown as a percentage of the total bandwidth used today since midnight, counting both allowed and blocked traffic. The text output shows the following:

- Top 25 bandwidth users during the reporting period. If the appliance is configured to access a single-domain Active Directory server, only the username of each user is displayed. If the appliance is configured to access the global catalog of a multidomain Active Directory forest, users are displayed in the form "domain\username".
- Top five destinations of each user.
• Total bytes for each user, or bytes for the specified direction.
• Total bytes for each of the top 5 destinations for each user listed.

**Note**
The Top Bandwidth Users report may not match Browse Summary By User reports, as the former includes all data, while the latter include only data from initial page hits, and do not include any content, such as images or CSS.

Click on a username to view a Search > By User of all URLs viewed or downloaded.

The available search parameters vary from one report to another. See “Modifying Reports” for a description of each parameter.

### 5.1.11 Users: Top Users By Browse Time

By default, a pie chart is displayed of the top five users by browse time, plus all others. Each user section of the chart is shown as a percentage of the total time that all users spent browsing within the specified time period. The text output shows the following:

• A list of the top 25 users by time spent browsing web pages. If your web appliance is configured to access a single-domain Active Directory server, only the username of each user is displayed; if the web appliance is configured to access the global catalog of a multidomain Active Directory forest, users are displayed in the form "domain\username". Usernames for eDirectory are specified in the form user.context.

• The total amount of time that users spent browsing during the specified time period.

• The top five categories of sites that they visited and the time that they spent browsing in each of these top five site categories.

Click on a username link to view a more detailed browse time report for that user. Clicking a username generates the Report > Browse Time By User report filtered for the username that you clicked on and the time period that you are currently viewing.

The Top Users By Browse Time report excludes some categories of URLs that are typically called in the background and not initiated by the user. For instance, many advertising, certification, and image repository websites are excluded that show up on other usage reports.

The available search parameters vary from one report to another. See “Modifying Reports” for a description of each parameter.

### 5.1.12 Users: Browse Time By User

By default, a pie chart is displayed of the top five site categories browsed by the selected user. Each category section of the chart is shown as a percentage of the total time that the user was browsing during the selected time period. The text output shows the following:

• A list of all of the categories in which the selected user browsed.

• The total amount of time that they spent browsing in each category.

• The total number of hits, or pages loaded, in each category.

• The top five domains that they visited in each category.

• The total time that they spent browsing in each of these top five domains.

• The total number of hits in each of these top five domains.
Note
Usernames are specified in the format `DOMAIN\User` in the text box to the right of the report. Alternatively, if Active Directory integration is not enabled, an IP address may be specified. Usernames for eDirectory are specified in the form `user.context`. This report may also be generated for a specified user by clicking the username in the Top Users By Browse Time report.

The available search parameters vary from one report to another. See “Modifying Reports” for a description of each parameter. Some URLs that you see in other reports are excluded from this report. The Browse Time By User report excludes some types of URLs that are typically called in the background and not initiated by the user. For instance, many advertising, certification, and image repository websites are excluded that show up on other usage reports.

5.1.13 Users: Browse Summary By User

Use the Browse Summary By User report to get detailed browsing information for a specific user. Enter a user, optionally select a time period under Report Parameters, and click Run Report. You can choose which data you the graph to display with the Display by drop down. Select Browse time, Site visits, or Bytes consumed.

Text output below the graph displays:

• **Date**: For searches that span multiple days this field will show the date for the related usage. If searching a single day, this will display the hour.
• **Visits**: The total number of visits to each site.
• **Bytes**: The total number of bytes downloaded from each site.
• **Browse time**: The total browse time for the date (or hour if searching a single day).

Note
Usernames are specified in the format `DOMAIN\User` in the text box to the right of the report. Alternatively, an IP address may be specified.

Note
The Top Bandwidth Users report may not match Browse Summary By User reports, as the former includes all data, while the latter include only data from initial page hits, and do not include any content, such as images or CSS.

5.1.14 Users: Top Users By Category

By default, a pie chart is displayed of the top five bandwidth users for the selected category. These are shown as a percentage of the total bandwidth used today since midnight. The text output shows the following:

• Top 25 bandwidth users for a particular category during the reporting period. As with all other reports, if your web appliance is configured to access a single-domain Active Directory server, only the username of each user is displayed; if the web appliance is configured to access the global catalog of a multidomain Active Directory forest, users are displayed in the form "domain \username".
• Top five destinations of each user.
• Total number of hits for each user.
• Total bytes viewed and downloaded for each user.
• Total number of hits for each of the top 5 destinations for each user listed.
• Total bytes for each of the top 5 destinations for each user listed.

Click on a username to drill down to an Activity Search By User to view all the URL requests, filtered for the user you clicked on and the time period that you are currently viewing.

Click on the destination to drill down to an Activity Search By Site, filtered for the site you clicked on and the time period that you are currently viewing.

You can sort the results according to the number of hits or number of bytes consumed. The available search parameters vary from one report to another. See “Modifying Reports” for a description of each parameter.

### 5.1.15 Users: Category Visits By User

By default, a pie chart is displayed of the top five categories browsed by the specified user, plus a segment for all the other categories, counting only allowed pages. Each category segment of the chart is shown as a percentage of the total categories or bytes consumed during the specified time period. The text output shows the following:

- **Category**: A list of all categories in which the specified user browsed sites.
- **Top 5 destinations**: The top 5 destinations (domains) visited in each category.
- **Visits**: The total number of visits in each category, counting only allowed pages.
- **Bytes**: The total number of bytes downloaded in each category, counting only allowed pages.

The list may be sorted by site visits or bytes consumed.

Usernames are specified in the format `DOMAIN\User` in the text box to the right of the report. Alternatively, if Active Directory integration is not enabled, an IP address may be specified. Usernames for eDirectory are specified in the form `user.context`.

The available search parameters vary from one report to another. See “Modifying Reports” for a description of each parameter.

### 5.1.16 Users: Site Visits By User

By default, a pie chart is displayed of the top five sites browsed by the specified user, plus a segment for all the other sites. Each site segment of the chart is shown as a percentage of the total number of visits or bytes that the user was browsing during the specified time period, counting only allowed pages. The data table shows the following:

- **Sites**: A list of the top 25 sites in which the specified user browsed.
- **Category**: The category under which the site is listed.
- **Visits**: The total number of visits to each site.
- **Bytes**: The total number of bytes downloaded from each site.

The list may be sorted by site visits or bytes consumed.
Note

Usernames are specified in the format `DOMAIN\User` in the text box to the right of the report. Alternatively, if Active Directory integration is not enabled, an IP address may be specified.

The available search parameters vary from one report to another. See “Modifying Reports” for a description of each parameter.

### 5.1.17 Users: Users By Search Queries

A data table is displayed showing user queries that match keywords and phrases you have specified in the Search Terms list. No data is shown in this report unless you have added one or more entries to a Search Terms list that is turned on.

By default, user web queries are ranked according the date and time of the query, starting with the most recent query. You can also sort the results according to the list name or the user. The data table contains these columns:

- **User:** The username and/or the IP address of the machine on which the query was submitted.
- **Search query:** The word(s) included in the user query.
- **List name:** The name in the search terms list containing the matching word(s) or phrase(s).
- **Date/Time:** The exact time at which the query was submitted.

The available search parameters vary from one report to another. See “Modifying Reports” for a description of each parameter.

**Related concepts**

- [Search Terms](#)

**Related tasks**

- [Removing a Search Term Alerts Recipient](#)
- [Adding a Search Term Alerts Recipient](#)

### 5.1.18 Users: Top Web Application Users

By default, a chart is displayed of the number of site visits for the top web application users. The results displayed vary according to the parameters selected. The text output shows the following:

- Top web application users during the reporting period.
- Top web applications for each user. Specific features are displayed as separate items. Items not associated with a specific feature are listed as **General**. Each feature has a color coding that relates to the Application listed in the graph.
- Total hits for each of the top web applications for each user listed.

The **Status** parameter allows you to filter results by **Allowed**, **Blocked** and **Blocked (Application)**. See “Modifying Reports” for a description of the other parameters. **Report on a group** will allow you to run a report on specific groups.
5.1.19 Policy & Content: Allowed Sites

By default, a pie chart is displayed of the top 5 sites accessed, plus all others, shown as a percentage of the sites visited today since midnight of the current calendar day. The data table shows the following:

- the 25 most accessed sites
- number of visits to each site
- unique number of users who visited each site
- bytes used by each site

Clicking on a site in the list performs a Recent Activity Search: By Site.

You can sort the results according to site visits, unique users, or the number of bytes consumed.

The available search parameters vary from one report to another. See “Modifying Reports” for a description of each parameter.

Related tasks
Searching Recent Activity (page 181)

5.1.20 Policy & Content: Warned Sites

By default, a pie chart and data table of user site requests that resulted in warnings—shown as a proportion of the total number of warnings (chart)—organized by the number of warnings issued in the current calendar day since midnight.

The data table shows the number of warnings that were issued, and how many times someone proceeded to each site, despite the warnings. The table also shows the number of unique users who received warnings during the reporting period. You can sort the results on any of these columns.

The available search parameters vary from one report to another. See “Modifying Reports” for a description of each parameter.

5.1.21 Policy & Content: Blocked Sites

By default, a pie chart and data table of the top blocked sites, shown as a proportion of the total number of blocked sites and organized by the number of visits today since midnight. The text output also shows the number of unique users accessing the top listed blocked sites during the reporting period.

Note

The Blocked Sites report may include accessible sites if file types that users attempted to download were blocked by the policy.

You can sort the results according to the number of site visits or the number of unique users. The available search parameters vary from one report to another. See “Modifying Reports” for a description of each parameter.
5.1.22 Policy & Content: Categories

By default, a pie chart and data table of the categories of URLs allowed—as a proportion of the total number of allowed visits—today since midnight. The data table also shows the total number of bytes viewed or downloaded for each category.

Visits displays a count of page loads or Download files, while Bytes displays the total bytes of any downloads, so it is possible to have a positive value for Bytes while the value for Visits is zero. For example, if you download just a graphic file, it doesn't count as a page load or a Download file, but the bytes downloaded are recorded and shown in this report.

You can sort the results according to site visits or the number of bytes consumed. The available search parameters vary from one report to another. See “Modifying Reports” for a description of each parameter.

5.1.23 Policy & Content: Downloads

By default, a pie chart and data table of the file types downloaded—as a proportion of the total number of bytes downloaded—today since midnight. The data table also shows the total number of requests for each of the file types downloaded.

Note
This is not a comprehensive measure of bytes downloaded. It records only the downloads that users have explicitly requested. It does not, for example, include the data downloaded as a result of JavaScript calls.

You can sort the results according to site visits or the number of bytes consumed. The available search parameters vary from one report to another. See “Modifying Reports” for a description of each parameter.

5.1.24 Policy & Content: Sandstorm Usage

By default, a stacked-bar graph and data table of the total number of user downloads referred to the Sandstorm cloud service, listed by analysis result. The results are broken down hourly for the current day since midnight, and show:

- **Clean**: files that have been analyzed and that exhibit no malicious behavior.
- **Malicious**: files that Sandstorm has determined are malicious.
- **Analysis unsuccessful**: files that could not be analyzed.
- **Excluded by policy**: files that were not sent for analysis due to policy settings.

Use the Graph by drop down to select whether the graph displays the number of files downloaded, the number of bytes downloaded, the number of files sent for analysis, or the number of bytes sent for analysis. See “Modifying Reports” for a description of the other search parameters.

5.1.25 Policy & Content: Advanced Threat Protection

The Advanced Threat Protection (ATP) report lists each unique IP address/user combination for which the SWA has detected attempts to contact malware command and control services. You can
block and unblock machines listed in this report. Blocking a machine adds it to the Configuration > Group Policy > Additional Policies page in the Quarantined Machines policy.

The columns in the report are:

- **Block**: For each each IP address/user combination, you can use the block/unblock button to add or remove the IP address to or from the Quarantined Machines policy.

  **Note**
  Blocking a machine will block all instances of that IP address, not just the specific IP/user combination you select.

- **Status**: A red circle with an “X” indicates a potential threat that is unblocked. A green checkmark indicates the machine is blocked.

- **IP**: The IP address of the detected machine. Clicking this will display a search for suspicious activity from this IP address.

- **Machine**: The name associated with the machine. Clicking this will display a search for suspicious activity from the IP address associated with this machine.

- **User**: The username associated with the machine when the threat was detected. Clicking this will display a search for suspicious activity by this machine/user combination.

- **Count**: The number of times this particular IP/username combination has been detected as a threat.

- **Details**: The name or names of any detected threats. Clicking the name of a threat will open the webpage with the corresponding Sophos threat analysis.

To block or unblock all listed machines, use the **Block All** or **Unblock All** buttons at the bottom of the page.

**Related tasks**

- Searching Recent Activity (page 181)
- Additional Policies (page 87)

### 5.1.26 Policy & Content: Web Application Usage

By default, a chart and data table of the top web applications allowed today since midnight. The data table columns include **Rank**, **Application & Feature**, **Hits** (which displays a count of site visits) and **Bytes** (which displays the total bytes of uploads and downloads).

You can sort the results according to hits or the number of bytes consumed. The **Chart** parameter allows you to sort either by **Top Applications** or **Top Features**:

- **Top Applications** shows a chart of the most used applications. The table below summarizes each application as well as showing a breakdown of each feature.

- **Top Features** shows a chart of the most used features. The table below lists each feature with no grouping for their application.

The **Status** parameter allows you to filter results by **Allowed**, **Blocked** and **Blocked (Application)**.

See Modifying Reports for a description of the other parameters.
5.2 Modifying Reports

The reports about individual web appliances are available on a management appliance only.

On the right side of each report page is a **Report Parameters** sidebar with options for specifying the time period covered by the report and, sometimes, the kind of data that is displayed in the report. The options vary according to the type of report.

1. Set the desired parameters:
   a) Select an option for the **Period** that the report will cover.
      - **Today**: Only activity recorded since midnight for the current day is searched.
      - **Yesterday**: Only activity recorded during the previous calendar day (midnight to midnight) is searched.
      - **Last**: From the drop-down list, select a time increment for the report. Then, in the text box, enter a number specifying the time period (for example, **7 days**). Partial minutes, hours, weeks, days, and months count toward the total number specified. Time frames are defined as follows:
         — **minutes**: Any complete minutes within the specified span, plus the elapsed portion of the current minute.
         — **hours**: Any complete hours within the specified span, plus the elapsed portion of the current hour.
         — **days**: Any complete days within the specified span, plus the elapsed portion of the current day.
         — **weeks**: This includes any complete weeks (starting on Sunday of the first week) that fall within the specified span, plus the current week, up to the current day.
         — **months**: This includes any complete months (starting on the first day of the first month) that fall within the specified span, plus the current month, up to the current day.
      - **Custom**: Select the **From** and **To** date and time. Set the date by clicking on the calendar icon and selecting the date from the calendar pop-up dialog box.
   b) If available, select the data that you want displayed. Certain options are available for specific reports only. The following is a complete list of **Display** options:
      - **Appliance**: [management appliance only] This drop-down list appears on the **Latency** and **Throughput** report pages. You can generate the report on an individual joined appliance or **All appliances**.
        Whether viewing the information for **All appliances** or for a specific web appliance, the time period covered is always based on the management appliance’s time zone.
      - **Category**: Select a category on which to filter your results (for example, “Search Engines” or “Downloads”). You must choose a category.
      - **Report on a group**: This drop-down list provides reports by department if you select a group or **All Users**. The groups displayed in the list are set on the **Reports > Options > Reporting Groups** page.
      - **Top n users**: The number of users to display at once. If this number exceeds the number of users in your network, a complete list of users is displayed. The default is 25.
• **Top n sites**: The number of sites to display at once. If this number exceeds the number of sites searched, a complete list of users is displayed. The default is 25.

• **Sort**: The availability of these option buttons varies from one report to another. Some reports have none. If available, select one of the following to further refine the report data.
  — **Site visits**: Ranks the results according to the number of visits to an individual website.
  — **Bytes consumed**: Ranks the results according to the number of bytes downloaded from an individual website.
  — **Hits**: Ranks the results according to the number of times a site was accessed, broken down by domain (for example, yahoo.com).
  — **Matched terms**: Ranks the results according to the number of times a string or substring is included in a user query. Only matches for keywords defined in the Search Terms List dialog box are displayed.
  — **Date/Time**: Ranks the results according to the day and time that the search was performed, beginning with the most recent.
  — **User**: Ranks the results according to the IP address or directory services username of the user in numeric order, from lowest to highest.
  — **Search engine**: Ranks the results according to the search engine used to retrieve the results, in alphabetical order.
  — **Unique users**: Ranks the results according to the number of unique users who have visited a particular site.
  — **Warns**: Ranks the results according to the number of times that users received a warning about a specific site.
  — **Proceeds**: Ranks the results according to the number of times users proceeded to a given site after receiving a warning.

• **User**: Generate user-specific reports by either entering a user’s name in the form "Domain \user" or the user’s IP address.

2. Optionally, select View Report as PDF for a PDF version of the report, or leave this option blank to view the report on the page (as HTML).

   If you are unable to access the PDF, and you are using Internet Explorer, see Enabling PDF Access in Internet Explorer (page 201).

3. Click Run Report.

### 5.3 Printing Reports

1. On the Reports sidebar, click the name of the report that you want to print.

   The report is displayed.

2. Optionally, on the Report Parameters sidebar, select any of the available options that you want in the report, and click Run Report.

   The modified report is displayed.

3. Click View printable version.

   The report is displayed in a new window of your browser in a print-friendly format.

4. Use your browser’s print options to print the report.
5.4 Exporting Reports

Report data is exported in comma separated value (CSV) format.

1. On the Reports sidebar, click the name of the report that you want to export.
   The report is displayed.
2. Optionally, on the Report Parameters sidebar, select any of the available options that you want in the report, and click Run Report.
   The modified report is displayed.
3. Click Export.
   A text file is generated that contains the report data in CSV format. This may take a little time. Your browser’s file download feature then prompts you to save the file or open it in the default associated program.
4. Save or view the exported .csv file.

Related tasks
Searching Recent Activity (page 181)

5.5 Options

Use the Options pages to create and manage groups on which reports can be based, schedule the mailing of reports as PDFs, create exemptions for reports, and list search terms for inclusion in reports.

5.5.1 Reporting Groups

The Reports > Options > Reporting Groups page allows you to set the user groups on which a report can be generated. If Active Directory or eDirectory access has been properly configured, the Available groups list is populated with your organization’s groups from that directory service.

If your web appliance is configured to access a single-domain Active Directory server, Active Directory group names are displayed in the form "groupName"; if the web appliance is configured to access the global catalog of a multidomain Active Directory forest, Active Directory group names are displayed in the form "domain\groupName". All eDirectory names are displayed in the group.context format.

Alternatively, or additionally, you can create, edit, and delete custom groups. Once the Available groups list is populated to meet your requirements, you can move groups into the Reporting groups list. The groups in the Reporting groups list are displayed on the Report on a group drop-down list on the Report Parameters sidebar of the following reports:

- Virus Downloaders
- PUA Downloaders
- High Risk Site Visitors
- Policy Violators
- Top Bandwidth Users
- Top Users By Browse Time
• Top Users By Category
• Users By Search Queries
• Allowed Sites
• Warned Sites
• Blocked Sites
• Categories
• Downloads

Note
Reporting data is restricted based on choices made when creating reporting groups. A full administrator has access to all information. However, when a limited administrator searches by IP, the results only include users that came from that IP address and that are in the dataset. If a reporting group has an IP address in it, all data will be given for that IP address, regardless of users. For more information, see "Administrators."

Related concepts
Administrators (page 60)

Creating a Custom Reporting Group

1. In the Available groups list, click Create.
   The Group Editor dialog box is displayed.

   Note
   The groups that are created in this window are also displayed as custom groups on the Configuration > Group Policy > Default Groups page.

2. In the top text box, enter a name for the group.
3. Use at least one of the following methods to select the members of the new custom group:
   • Click the Groups tab, highlight the groups that you want to include in your custom group, and click the double-right arrow (>>) to move the chosen groups into the Selected Entries list.
   • Click the Users tab to highlight the users that you want to include in your custom group, and click the double-right arrow (>>) to move the chosen users into the Selected Entries list.
   • Optionally, to remove a group or user from the Selected Entries list, highlight the item(s) that you want to remove from the custom group, and click the double-left arrow (<<).
   • To add manual entries that are not listed in the Groups or Users lists, do the following:
     a) In the text box in the Manual Entries section, enter a username, IP address, or an IP address range, and click Add.

     Active Directory usernames must be in the form DOMAIN\username, while eDirectory usernames must be in the form user.context. IP address ranges must be in CIDR format.

     The entry is displayed in the Manual Entries list.

     b) Optionally, to delete an item from the list, select the check box to the right of the entry that you want to delete, and click Delete.
The selected item is removed from the Entries list.

4. Click Save.

The Group Editor dialog box closes, and you are returned to the Options: Reporting Groups page, with the newly created custom group shown in the Available groups list.

5. Click Apply.

Editing a Custom Reporting Group

1. Click the name of the custom group that you want to edit.

   Note
   Custom groups, which can be edited, are indicated by a Sophos icon
   ( ),
   Active Directory and eDirectory groups, which cannot be edited, are indicated by a directory icon
   ( ).

   The Group Editor dialog box is displayed with the selected list’s members.

   Note
   The group changes that you make in this window are also displayed in the custom groups on the Configuration > Group Policy > Default Groups page.

2. Optionally, in the top text box, enter a new name for the group.

3. Optionally, use any of the following methods to change the members for the selected custom group:
   • Click the Groups tab, highlight the groups that you want to add to your custom group, and click the double-right arrow (>>) to move the chosen groups into the Selected Entries list.
   • Click the Users tab, highlight the users that you want to add to your custom group, and click the double-right arrow (>>) to move the chosen users into the Selected Entries list.
   • To remove a group or user from the Selected Entries list, highlight the item(s) that you want to remove from the custom group, and click the double-left arrow (<<).
   • To add manual entries that are not listed in the Groups or Users lists, do the following:
     a) In the text box in the Manual Entries section, enter a username, IP address, or an IP address range, and click Add.
        Usernames must be in the form DOMAIN\username. Usernames for eDirectory must be in the form user.context. IP address ranges must be in CIDR format.
        The entry is displayed in the Manual Entries list.
     b) Optionally, to delete an item from the list, select the check box to the right of the entry that you want to delete, and click Delete.
        The selected item is removed from the Manual Entries list.

4. Click Save.

The Group Editor dialog box closes and you are returned to the Options: Reporting Groups page with the modified custom group listed in the Available groups list.

5. Click Apply.
Setting Reporting Groups

Use this procedure to set which groups will appear in the **Report on a group** drop-down list on the **Report Parameters** sidebar of the **Reports** pages, as well as on the first page (the **Report Package** page) of the **Report Scheduler** wizard.

1. In the **Available Groups** list, select the groups on which you want to be able to generate reports.
   - You can **Click, Shift-click** to select a range of groups, or repeatedly **Ctrl-click** to select several groups individually.
2. Click the double-right arrow button, (>>), to move the selected groups into the **Reporting Groups** list.
3. Optionally, to remove a group or groups from the **Reporting Groups** list, highlight the group or groups that you want to remove, and click the double-left arrow button, (<<).
4. Click **Apply**.

The groups that appear in the **Reporting groups** list will be displayed in the **Report on a group** drop-down list on the **Report Parameters** sidebar on the various **Reports** pages, allowing you to choose one of these groups as the group on which the report will be generated.

Deleting a Custom Reporting Group

1. In the **Available groups** list, select the check box to the right of the custom group or groups that you want to delete.
   - The custom group or groups that you want to delete must not be in the **Reporting groups** list.

   **Note**

   Custom groups, which can be deleted, are indicated by a Sophos icon (✉); Active Directory and eDirectory groups, which cannot be deleted, are indicated by a directory icon (✉).

   **Important**

   The group or groups that are deleted in this window will also be removed from the **Configuration > Group Policy > Default Groups** page.

2. Click **Delete**.
   - The selected custom group or groups are removed from the **Available groups** list.
3. Click **Apply**.

5.5.2 Report Scheduler

Use the **Reports > Options > Report Scheduler** page to create, modify, enable or disable, and delete scheduled reports, which are pre-configured jobs that automate the generation and emailing of selected sets of reports to selected recipients on a preset schedule.
Creating a Scheduled Report


2. Select one or more Report packages that you want included in the PDF file that is mailed out on schedule. Descriptions of each selected package of reports are displayed in the Description box.

3. If you select the Policy compliance package, you can also choose to Include detailed policy compliance reports and set the number of the top users (1 to 5) on which the included detailed report is generated.

4. From the Group selection drop-down list, select the groups that the reports will cover. The default option is All Users. The groups shown in this drop-down list are created and set on the Reports > Options > Reporting Groups page.

5. Click Create Schedule at the top of the page, or Next at the bottom of the page, to proceed to the next page of the wizard.

6. In the Frequency of reports section, select the time period that you want the report to cover. The options are:
   - Report for the past 24 hours, sent daily after midnight: Note that "after midnight" is actually slightly after 1:30 AM.
   - Report for the past "n" days, sent weekly on "x": If you choose this option, from the drop-down lists you must select both the range of days (7, 14, 21, or 28) and the day of the week on which you want the report sent to the recipients. The report will cover the selected number of days prior to the selected reporting day.
   - Report for the past month, sent on the first of each month: If you select this option, the report will be sent out on the first day of the month, and it will cover the previous complete one-month period.

7. In the Report scheduler name text box, enter a meaningful name for the scheduled report.

8. Optionally, select Activate this schedule to enable this scheduled report. Leave this option unselected if you want to enable it later.

9. Click Specify Recipients at the top of the page, or Next at the bottom of the page, to proceed to the last page of the wizard.

10. Specify the recipients by creating a list.
    a) Add a recipient to the list by typing the recipient’s email address into the Specify recipients text box and then clicking Add.
    b) Remove a recipient from the list by selecting the check box to the right of the recipient in the list and then clicking Delete.

11. Optionally, click Preview Reports to immediately generate an example report. The example report may include only a fraction of the specified reporting period, depending on the day that you request the preview.

12. Click Save. Before saving, you can click Previous to return to the preceding pages of the wizard to review or change the settings in those pages. The options that you had set previously will be retained while you have the wizard open and until you change them, but they will not be saved for use until you click Save.
Modifying a Scheduled Report

1. In the Scheduled reports table on the Reports > Options > Report Scheduler page, click the name of the scheduled job that you want to change.

   The Report Package page of the Report Scheduler wizard is displayed with the settings of the selected scheduled report displayed.

2. Optionally, select or clear the check boxes for any of the Report packages that you want to add or remove from the PDF file that will be mailed out to the selected users on the selected schedule.

   Descriptions of the reports included in each selected package are displayed in the Description box.

3. If you selected the Policy compliance package, you can also choose to Include detailed policy compliance reports and set the number of the top users (1 to 5) on which the included detailed report is generated.

4. Optionally, change the groups that the reports will cover from the Group selection drop-down list.

   The default option is All Users.

   The groups shown in this drop-down list are created and set on the Reports > Options > Reporting Groups page.

5. Click Create Schedule at the top of the page, or Next at the bottom of the page, to proceed to the next page of the wizard.

6. Optionally, in the Frequency of reports section, you can change the time period that you want the report to cover. The options are:

   - **Report for the past 24 hours, sent daily after midnight:** Note that "after midnight" is actually slightly after 1:30 AM.

   - **Report for the past 7 days, sent weekly on "x"** — If you choose this option, from the drop-down list you must select the day of the week on which you want the report sent to the recipients. The report will cover the 7 days prior to the selected reporting day.

   - **Report for the past 14 days, sent bi-weekly on "x"** — If you choose this option, from the drop-down list you must select the day of the week on which you want the report sent to the recipients. The report will cover the 14 days prior to the selected reporting day.

   - **Report for the past month, sent on day "x" of each month** — If you choose this option, from the drop-down list you must select the day of the month on which you want the report sent to the recipients. The report will cover the one-month period prior to the selected reporting day.

7. Optionally, in the Report scheduler name text box, change the name for the scheduled report.

8. Optionally, select Activate this schedule to enable this scheduled report, or clear it if you want to enable it later.

9. Click Specify Recipients at the top of the page, or Next at the bottom of the page, to proceed to the last page of the wizard.

10. Optionally, modify the recipients list.

    a) Add a recipient to the list by typing the recipient’s email address into the Specify recipients text box and then clicking Add.

    b) Remove a recipient from the list by selecting the check box to the right of the recipient in the list and then clicking Delete.

11. Optionally, click Preview to immediately generate an example report.

    The example report may include only a fraction of the specified reporting period, depending on the day that you request the preview.

12. Click Save.
Before saving, you can click **Previous** to return to the preceding pages of the wizard to review or change the settings in those pages. The options that you set previously will be retained while you have the wizard open until you change them, but they will not be saved for use until you click **Save**.

### Enabling/Disabling a Scheduled Report

- To enable an inactive scheduled report:
  
  In the **Scheduled Reports** table, on the **Reports > Options > Report Scheduler** page, click **Turn On** to activate an inactive scheduled report.

  The **Active** button will turn green, and the **Action** button will change to **Turn Off**.

- To disable an active scheduled report:
  
  In the **Scheduled Reports** table, on the **Reports > Options > Report Scheduler** page, click **Turn Off** to deactivate an active scheduled report.

  The **Active** button will turn gray, and the **Action** button will change to **Turn On**.

### Removing a Scheduled Report

1. In the **Scheduled reports** table on the **Reports > Options > Report Scheduler** page, select the check box to the right of the scheduled report that you want to delete.

2. At the bottom of the table, click **Delete**.

   The selected scheduled report is removed from the table.

### 5.5.3 Report Exemptions

The **Reports > Options > Report Exemptions** page allows you to exempt selected report categories and specified domains from report data. If report exemptions are enabled, and they apply to the report you are running, this is indicated in both the Reports status bar and the bottom left corner of the report.

### Exempting a Report Category

You can exempt one or more categories from reports containing category data. These reports are:

- **Policy Violators**
- **Top Users By Browse Time**
- **Browse Time By User**
- **Category Visits By User**
- **Site Visits By User**
- **Categories**

Any category that you exempt will not be included in all of the reports listed above.

To exempt a category:

1. On the **Reports > Options > Report Exemptions** page, select **Exempt Categories**.

2. From the drop-down list, select a category to exempt, and click **Add**.
Repeat steps 1 and 2 to exempt additional categories. To delete a category, select the check box beside the listed category, and click **Delete**.

**Exempting a Report Domain**

You can exempt one or more domains from reports containing domain data. These reports are:

- Top Bandwidth Users
- Top Users By Browse Time
- Browse Time By User
- Top Users By Category
- Category Visits By User
- Site Visits By User
- Allowed Sites
- Warned Sites
- Blocked Sites

Any domain that you exempt will not be included in all of the reports listed above.

To exempt a domain:

1. On the Reports > Options > Report Exemptions page, select **Exempt Domains**.
2. Enter a single domain, and click **Add**. Or click **Enter multiple domains**, type each domain name on a new line, and click **Add**.

Repeat steps 1 and 2 to exempt additional domains. To delete a domain, select the check box beside the listed domain, and click **Delete**.

**5.5.4 Search Terms**

Use the Reports > Options > Search Terms page to specify keywords that are displayed in the Users By Search Queries report. The appliance logs statistics about web queries, and if you specify words and phrases, data on these search terms is shown in the report.

Optionally, you can search for substring matches, which not only returns matches for specified terms, but also for any words or phrases that have the specified string within it. For example, the term “gun” would also match keywords such as “handgun” and “shotgun” because they contain the “gun” substring.

For more about how search term data is displayed, see the documentation for the “Users By Search Queries” report.

In addition, you can enable search term alerts, so that any specified recipients are notified if user web queries contain one or more of the listed words or phrases. For more information, see “Adding a Search Term Alerts Recipient”.

**Related concepts**

*Users: Users By Search Queries* (page 165)

**Related tasks**

*Adding a Search Term Alerts Recipient* (page 116)
*Removing a Search Term Alerts Recipient* (page 117)
**Adding Search Terms**

You can enter words or phrases that you want displayed in the “Users By Search Queries” report. Once a term has been entered, all instances of that term are included in reports, even if the term was used in a web query that was submitted before you added the term to the list of search terms.

Whether you specify one term or a number of terms, they must be contained by a list. Optionally, you can enable substring matches, so that user queries containing a portion of any specified term will match.

To add search terms:

1. Click **Add**. The **Search Terms List** dialog box is displayed.
2. In the **List name** text box, enter a name for the list that will contain your term(s).
3. In the **Search terms** text box, enter a word or phrase that you want to trigger a report entry, and click **Add**. Or, click **Enter multiple search terms**, type each search term on a separate line, and click **Add**.
4. [Optional] Select **Include substring matches** if you want your listed terms to also match within words and phrases in search queries. For example, if you specify the term “drug,” and enable substring matches, the appliance will report on queries that include the word “drug,” along with variants such as “drugs” and “drugstore.” You can choose to enable/disable this option in each search term list.
5. Click **Save**. The newly created entry is displayed in the **Search terms list**.

**Modifying Lists of Search Terms**

You can add, change, and remove words or phrases that are displayed in the “Users By Search Queries” report. Whether you specify one term or multiple terms, they must be contained by a list. Optionally, you can enable substring matches so that user queries containing a portion of any term will match.

To modify search terms:

1. In the **Search terms list**, click the list name that you want to edit. The **Search Terms List** dialog box is displayed.
2. Edit the list as follows:
   - **To remove a search term from the list**, select the check box next to the term, and click **Delete**.
   - **To add a search term to the list**, in the **Search terms** text box, enter the word or phrase, and click **Add**.
   - **To enable/disable substring matching**, select or clear the **Include substring matches** check box. You can choose to enable/disable this option in each search term list.
3. Click **Save**.

**Enabling/Disabling Lists of Search Terms**

You can turn lists on and off. Turning a list off makes it inactive, but it does not permanently remove the list or its contents.

To enable/disable a list of search terms:

In the **Search terms list**, click the **Turn On** or **Turn Off** button next to the list name.
The list becomes inactive, but remains available, if you turn it off. For instructions on deleting a list of search terms, see “Removing Search Terms”.

**Related tasks**

Removing Search Terms (page 180)

**Removing Search Terms**

You can remove individual search term entries or a complete list of entries.

- **To remove a search term:**
  
  1. In the **Search terms list**, click the name of the list that contains the term you want to remove.
     
     The **Search Terms List** dialog box is displayed.
  
     2. Select the check box next to the term, and click **Delete**. To remove multiple terms at once, select the appropriate check boxes, and click **Delete**.
  
     3. Click **Save**.

- **To remove a list of search terms:**
  
     1. In the **Search terms list**, select the check box to the right of the list that you want to delete.
  
     2. Click **Delete**.

     The list and its contents are removed.

**Related tasks**

Enabling/Disabling Lists of Search Terms (page 179)
6 Search

Use the search functionality to search user activity, sandbox activity, and user requests.

The Search tab allows you to:

- Perform a Recent Activity Search (of users’ activity) By User (username or IP address), or By Site requested.
- If Sandboxing is enabled, search for instances where a user has attempted a download that required further analysis by Sophos Active Sandbox.
- View User Submissions (requests) to recategorize, or allow access to, Sites, PUAs or File Types.

6.1 Searching Recent Activity

The Recent Activity Search section of the Search tab allows you to search the user activity logs By User (username or IP address), or to view users’ activity By Site.

1. On the Search tab sidebar, click the type of Recent Activity Search that you want to perform.

   There are three ways to search recent activity:

   - **By User**: Search by username or by the user’s IP address.
   - **By Site**: Search by web address.
   - **By Suspicious Activity**: Search for attempts to contact malware command and control services
   - **By User Timeline**: Search usage by user for specific date ranges.

   **Note**
   Searches will only display users that the administrator has permission to see. However, if the administrator also has permission to search by IP address, then all users will be shown in the search results.

2. On the Search Parameters sidebar, enter the criteria for your search:

   a) Set the Period to search by selecting one of the following options:

      - **Today**: Only activity recorded since midnight for the current day is searched.
      - **Yesterday**: Only activity recorded during the previous calendar day (midnight to midnight) is searched.
      - **Last**: From the drop-down list, select a time increment for the report. Then, in the text box, enter a number specifying the time period (for example, 7 days). Partial minutes, hours, weeks, days, and months count toward the total number specified. Time frames are defined as follows:
        - **minutes**: Any complete minutes within the specified span, plus the elapsed portion of the current minute.
        - **hours**: Any complete hours within the specified span, plus the elapsed portion of the current hour.
— **days**: Any complete days within the specified span, plus the elapsed portion of the current day.

— **weeks**: This includes any complete weeks (starting on Sunday of the first week) that fall within the specified span, plus the current week, up to the current day.

— **months**: This includes any complete months (starting on the first day of the first month) that fall within the specified span, plus the current month, up to the current day.

- **Custom**: Select the **From** and **To** date and time. Set the date by clicking on the calendar icon and selecting the date from the calendar pop-up dialog box. Set the time by positioning the cursor beside the hour, minute, or AM/PM setting, and using the up and down arrow buttons to select a time.

b) Enter the **User** or **Site** for which you want to search.

- If you chose to search **By User**, enter the username or user’s IP address that you want information on, and select a **Filter**. If your web appliance is configured to access a stand-alone Active Directory server, enter the username that you want to search on; if the web appliance is configured to access the global catalog of a multidomain Active Directory forest, enter the username that you want to search on in the form "domain\username". Optionally, you can narrow the search results by selecting an individual status from the **Filter by status** drop-down list. You can also enter a specific web site in the **Filter by site** text box to view pages from that location that were viewed by the specified user.

- If you chose to search **By Site**, enter the site name that you want information on; for example, domain.com/page.htm.

  You can also search by domain alone (e.g., "example.com"), and then refine your search further after reviewing the results. Optionally, you can narrow the search results, by selecting an individual status from the **Filter by status** drop-down list.

- If you chose to search **By Suspicious Activity**, enter the username or user’s IP address for which you want information. If your web appliance is configured to access a stand-alone Active Directory server, enter the username that you want to search on; if the web appliance is configured to access the global catalog of a multidomain Active Directory forest, enter the username that you want to search on in the form "domain\username". Optionally, you can enter a specific web site in the **Filter by site** text box to view pages from that location that were viewed by the specified user. You can also enter a reason in the **Filter by Reason** text box to view results for a particular reason. Only exact matches are supported in the **Filter by Reason** text box.

- If you chose to search **By User Timeline**, results will group browsing within a domain for a continuous amount of time. This will display the top level domain under **Site**, The time range the user spent on the site under **Time Frame**, and the number of page requests under **Requests**. Clicking a site will open the **By User** search for the user, using that site for the **Filter by site** option.

c) **Click Search**.

The results are displayed in the content pane.

**Note**

To avoid redundant entries in the **Recent Activity Search: By User** list, the web appliance aggregates multiple instances of one user accessing the same URL within one minute.

3. **[Optional]** To change the sort order of the results, toggle the up/down arrow icon that appears immediately to the right of any of the following column headers at the top of the list of entries.
Search results can often contain more than 150 pages of information. Despite the quantity, this may be only a small portion of the total data available. To see the complete results of a search, click **Export**, and view the results in another application.

### Related concepts

- **Policy & Content: Advanced Threat Protection** (page 167)
- **Policy & Content: Allowed Sites** (page 166)
- **Images Display as Gray** (page 215)

### Related tasks

- **Categories & Download Types** (page 73)
- **Exporting Reports** (page 171)

#### 6.1.1 Exporting Search Results

- Click **Export**.

  A text file is generated that contains the search result data in comma separated values (CSV) format. Your browser’s file download dialog box is then displayed, prompting you to save the file or open it in the default associated program.

  The export to CSV function can create a file with over 2 million rows, which greatly exceeds the number of rows that can be imported into most spreadsheet applications. To avoid losing data, you should chunk the file in a text editor to a size that your spreadsheet can import before importing it, or open the exported CSV file in a database that doesn't impose such modest data size limitations.

#### 6.2 Searching Sandstorm

Use these settings to view and manage downloads that were sent to Sandstorm for analysis in the sandbox. You can, optionally, release the file before the analysis is complete.

1. On the **Search** tab sidebar, click **Sandbox Activity**.

   A list will be displayed of all downloads that were sent for further analysis in the sandbox.

2. Optionally, you can narrow the search results by clicking the **Show Filters** button and entering filtering parameters:
   
   a) Enter the user or IP address for which you want to filter in the **User/IP** text box, then click the filter icon to the right of the text box.
      Click the red “x” icon to clear this filter.
   
   b) Enter the download source site for which you want to filter in the **Site** text box, then click the filter icon to the right of the text box.
      Click the red “x” icon to clear this filter.
   
   c) Use the **File Type** filter to select downloads by their file type.
   
   d) Use the **Status** filter so select downloads using their Sophos Sandstorm analysis result.
   
   e) Use the **Released** filter to select whether you want to filter for released files, unreleased files, or all files.

The filtered results are displayed in the content pane.

3. [Optional] To change the sort order of the results, toggle the up/down arrow icon that appears immediately to the right of any of the following column headers at the top of the list of entries.

4. To view details about a specific downloaded item, click its status.
A detailed report will be displayed with download information, file information, and results of the analysis.

5. [Optional] To release an item that is currently being analyzed by Sandstorm (that is, with a status of “In Progress” or “Error”) so that users can downloaded it immediately, select the check box in the Released column and click Release.

Sandstorm continues to analyze the file even if you release it.

If you release a file before the analysis is finished and the file is later determined to be malicious, you will receive an email notification.

**CAUTION**
Releasing an item before the analysis is finished may result in the downloading of malicious content.

Related concepts
Alerts & Monitoring (page 115)

Related tasks
Configuring Sandstorm (page 101)

Sophos Sandstorm is a cloud-based service that provides enhanced protection against new and targeted attacks. You can configure the appliance to send suspicious files to Sandstorm for analysis or submit suspicious files on an individual basis. Sandstorm detonates the file to check for malware and sends the results to you. Because the analysis takes place in the cloud, your system is never exposed to potential threats.

Categories & Download Types (page 73)

### 6.3 Searching User Submissions

The User Submissions section of the Search tab allows you to view users’ requests to recategorize, or grant them access to, a Site, File Type or Application. You can also configure email alerts to be sent when users submit sites, filetypes, or applications for review on the Adding an Alert Recipient page.

### 6.3.1 Viewing a User Submission Search

There are three user submission searches available for you to view:

- **Sites**: Lists the user requests for unblocking or recategorizing sites.
- **PUAs**: Lists the user requests for unblocking or recategorizing potentially unwanted applications.
- **File Types**: Lists the user requests for unblocking or recategorizing file types.

As these lists of logged user requests can be very large, you can filter the logs to narrow the entries that are displayed.

1. On the Search tab sidebar, click the User Submission search that you want to view.

   The results of the user submission search that you selected are displayed.

   Each entry has an information line and a details section. The information line shows the URL, IP/User, and Date. The details section contains the user’s comments, as well as some information that differs for each of the User Submission searches:
• The **Sites** list shows the current category and the category to which they want the site
  changed.

• The **PUAs** list shows the application name of the concerned PUA.

• The **File Types** list shows the file type of the concerned download file.

2. Optionally, click the up/down arrow button that appears immediately to the right of any of the
   column headers to organize the list by that information:
   - **URL**: Orders the entries alphabetically by URL.
   - **IP/User**: Orders the entries alphabetically by the requester’s username or IP address. If your
     web appliance is configured to access a stand-alone Active Directory server, only the users’
     username is displayed; if the web appliance is configured to access the global catalog of a
     multidomain Active Directory forest, users are displayed in the form “domain\username”. For
     eDirectory, enter the username in the form `user.context`.
   - **Date**: Orders the entries chronologically by their date or date range.

3. To reverse the order of the entries, click on the same up/down arrow button that you clicked in the
   previous step a second time.

   **Note**
   If the text in any field is too long to view, place your mouse pointer over the text and the full
   text is displayed in a screen tip box.

### 6.3.2 Allowing a User’s Request

Slightly different behavior is required to allow a user’s request for access to each of the different user
submission types.

• To allow a user’s request for access to a **Site**:
  a) Click the URL of the **Site** that the user wants to access.
     The **User Submissions: Sites** dialog box is displayed.
  b) See the Managing User Site Submissions (page 186) page for instructions on the use of this
     dialog box.

• To allow a user’s request for access to a **PUA**:
  a) Click the URL of the **PUA** that the user wants to access.
     A confirmation dialog box appears.
  b) Click **OK** to allow access.
     If you allow access, that PUA submission will be removed from the list, and the PUA
     will appear in the **Potentially unwanted applications authorization** section of the
     **Configuration > Global Policy > Download Options** page. If you subsequently choose to
     deny access to that PUA, you must remove it from the list of allowed PUAs on that page.

• Allowing access to a **File Type**:
Note

It is not possible to allow access to a File Type request for a specific user. You can allow access to a file type in the Configuration > Global Policy > Download Options page by either removing the file type from the Selected list or clearing the Block potentially unwanted applications check box. This would either allow access to all files of that type, or allow access to all PUAs, respectively.

Managing User Site Submissions

To manage user submissions:

Open the first user submission that you want to respond to by clicking on the requested URL on the Search > User Submission > Sites page.

The User Submissions: Sites dialog box is displayed, with the information about the request displayed in the Request details section.

Use the User Submissions: Sites dialog box to add the submitted URL to the Local Site List or to reject the request.

1. Select the action that you want to perform on the displayed user submission request.

   The options are:
   
   • Add this URL to the Local Site List: Select this option to accept the user submission request.
   
   • Reject this request: Select this option to reject the request and have it removed from the User Submissions list.
   
   • Skip this request: Select this option if you do not want to respond to this user’s submission at this time.

2. If you chose the Add this URL to the Local Site List option, set one or more of the following by selecting the check box beside the option and taking the described action:

   • Apply a tag to this URL: Select an available tag from the drop-down list or enter a new tag.
   
   • Override the category for this URL: Select the category that you want the URL to be classified as from the drop-down list.

   Note

   You can edit the URL to something more generic or appropriate for inclusion in the Local Site List.

   • Comment: Optionally, you can retain or edit the user’s comment. If selected, the contents of this text box are saved as the comment in the Local Site List.

   Note

   The comment field for new entries in the Local Site List will include which administrator approved the submission.

3. Click Apply & Next to apply your selected option and view the next user submission in the list, or click Apply & Close to apply your selected option and exit the User Submissions dialog box.

Optionally, on the Adding an Alert Recipient page, configure email alerts that will be sent when users submit sites for review.
### 6.3.3 Deleting a User’s Request

1. Select the check box to the right of the row for the request that you want to delete.
2. Click **Delete**.

   The user’s request to recategorize, or allow access to, a **Site**, **File Type** or **Application** is removed from the list without change to the policy.
7 System Status

The icons on the System Status tab indicate the system’s alert level by their color. If it is a joined appliance, the System Status button on the navigation bar becomes animated if the appliance is synchronizing with other appliances. The status indicated by these icons is shown in the following table. Differently shaped icons are used for the web appliances (disks) and the management appliance (network icons).

<table>
<thead>
<tr>
<th>Icon type</th>
<th>OK</th>
<th>Warning</th>
<th>Critical</th>
<th>Unknown</th>
<th>Data Sync.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disc icon (web appliance)</td>
<td>green</td>
<td>yellow</td>
<td>red</td>
<td>gray</td>
<td>N.A.</td>
</tr>
<tr>
<td>Network icon (management appliance)</td>
<td>green</td>
<td>yellow</td>
<td>red</td>
<td>gray</td>
<td>animated</td>
</tr>
</tbody>
</table>

The System Status tab lets you monitor the health and performance of the appliance. By default, only exceptions (warnings or critical alerts) are displayed. If there are no exceptions, the System Status tab’s default page shows nothing. The buttons at the bottom of the System Status page provide the following functionality:

- Click Show All to view a complete list of status items. Some items, such as those associated with Active Directory and eDirectory, are only shown if the program is enabled in the appliance.
- Click Show Exceptions to return to the display of only the existing exceptions.
- Click Shutdown to restart or shut down the web appliance. A confirmation prompt is displayed. Click Shutdown or Restart to perform the operation of your choice.

**Note**

Sophos strongly suggests that you use these software shutdown and restart options, as using the appliance’s power button or reset button, as described on the Appliance Hardware (page 3) page, may lead to file corruption and data loss. Also, note that any pending software updates will be applied during the shutdown and restart process.

The software shutdown and restart options are also very convenient for appliances that are housed off site or in a collocation facility.

The tab is organized into five sections, each with a different category of information. Every monitored condition displayed on the System Status tab shows the following information. At the far left of the page is the status icon itself, the color of which indicates the alert status of the item as one of Normal (green), Warning (yellow), or Critical (red).

- **Monitor**: Names the condition that is being monitored.
- **Message**: Provides details of the latest alert.
- **Potential remedies**: Describes possible solutions for the latest alert. For most warning and critical alerts, you are advised to contact Sophos Technical Support.
• **Last exception at:** Shows the date in MM/DD/YYYY format and the time in 12-hour, AM/PM format for the latest unacknowledged alert.

• **Exception:** Shows the number of alerts, including information (normal) alerts for that item. Click the "note" icon to open the **System Alerts** dialog box, which contains a history of alerts for this item. Click **Clear History** at the bottom of the **System Alerts** dialog box to clear the alert(s).

Monitored information is grouped into four sections: **Traffic, Hardware, Software,** and **License.** The monitored information varies depending on whether it is system status information for a management appliance, a joined web appliance, or a stand-alone web appliance. The monitored conditions for each of these sections are:

• **Traffic:**
  
  — **Scan time:** [Not available on management appliance] A warning alert is triggered if the average scan time over the last 5 minutes exceeds 10 seconds.

  — **WCCP:** [Standalone and Joined Appliances Only] A critical alert is triggered if the appliance is unable to communicate with configured Web Cache Communication Protocol routers.

• **Hardware:**
  
  — **Hard Disk:** A critical alert is triggered if the hard disk fails. The number of hard disks listed will vary according to the hardware platform.

  — **System memory usage:** A critical alert is triggered when 98% of physical memory (RAM) is used. If this condition persists, the appliance configuration may need to be adjusted to enable greater throughput, or an additional appliance may need to be deployed to handle current volumes.

  — **System memory (missing):** A critical alert is triggered if any of the expected memory (RAM) is not present. The amount of memory expected varies according to the hardware platform.

  — **System temperature:** A critical alert is triggered when the appliance’s temperature exceeds its normal temperature range.

  — **System fans:** A critical alert is triggered if the appliance’s system fan fails.

  — **CPU:** A critical alert is triggered if there are problems with the appliance CPU that could affect the stability of your system.

• **Software:**
  
  — **Connection to management appliance:** [joined web appliance only] A critical alert is triggered after 10 minutes of a loss of connection.

  — **Connections from joined appliances:** [management appliance only] A critical alert is triggered after 10 minutes of a loss of connection.

  — **System load:** A warning alert is triggered if the load average is greater than 50%.

  — **Report data backup:** [management appliance only] A critical alert is triggered if a scheduled upload fails.

  — **Transaction log files archive:** [Not available on management appliance] A critical alert is triggered if a scheduled upload fails.

  — **Configuration backup:** [Not available on Joined web appliance] A critical alert is triggered if a scheduled upload fails.

  — **Connection to Sophos:** A warning alert is triggered after two hours if the appliance is unable to connect to the Sophos site to receive threat definitions or software updates. A critical alert is issued if the appliance is unable to connect to the Sophos site after six hours.

  — **System updates:** A critical alert is triggered when a system software update fails or if the software is out of date.
— **System reboot**: A warning alert is triggered if there are pending updates that will cause the web appliance to automatically reboot in the next available update window.

— **Syslog server availability**: A warning alert is triggered if the appliance is unable to connect to its configured Syslog server.

— **Active Directory integration**: A critical alert is triggered if the appliance gets disconnected from the Active Directory domain. If this occurs, click **Verify Settings** on the appliance’s **Configuration > System > Active Directory** configuration page to ensure that the domain controller is accepting connections. Ensure that the username and password supplied have the relevant rights to access the domain and that your network is configured correctly to allow the appliance to access the relevant ports on the domain controller. Contact Sophos Technical Support if additional help is required.

— **Active Directory synchronization**: [Not available on Joined web appliance] The web appliance synchronizes with the configured Active Directory server every 2 hours. If this synchronization fails, a critical alert is raised.

— **Active Directory Trusted Domains synchronization**: [Not available on Joined web appliance] If synchronization with a trusted (or child) domain fails, a warning alert is raised.

— **eDirectory synchronization**: [Not available on Joined web appliance] A critical alert is triggered if the appliance has problems synchronizing with the eDirectory server.

— **eDirectory user identification**: [Not available on management appliance] A warning is triggered if the appliance has encountered a problem obtaining user identification data from the eDirectory server(s). A critical alert is triggered if the appliance has encountered problems over an extended period of time when attempting to obtain user identification data from the eDirectory server(s).

— **Web categorization data update**: An alert is triggered if the web appliance has problems receiving web categorization data.

— **Email alert delivery**: A warning alert is triggered if the appliance has not been able to send email notifications (EDNs) for 4 hours. A critical alert is triggered if the appliance has not been able to send any EDNs for 72 hours. The appliance was either unable to connect to an email server when trying to send an alert notice, or was unable to deliver the email to a specified recipient. Correct operation of the appliance requires that it be able to send email alerts to Sophos Technical Support and specified recipients. Ensure that an **Outgoing SMTP mail server** has been correctly specified on the **Configuration > Network > Hostname** page, and a valid recipient email address is specified on the **Configuration > System > Alerts** page.

— **Configuration version**: [Only available on Joined web appliance] A critical alert is triggered if a configuration update fails. If the configuration version of the joined appliance does not match that of the management appliance, configuration changes on the management appliance will no longer be downloaded to the Joined Appliance.

**License**:

— **Sophos license**: A warning alert is triggered when there are less than 30 days left on a trial license, and it continues until 10 days after a trial license expires. A critical alert is triggered 10 days after a trial license expires, and the appliance stops categorizing sites. If you do not block uncategorized sites users will still be able to browse, but will not be protected from categories that should be blocked.

**Related concepts**

- **Central Management** (page 140)
- **Alerts & Monitoring** (page 115)
7.1 System Status on the Management Appliance

The features described in this section only apply to the management appliance.

The System Status tab is different on the management appliance. The list of monitored conditions is outlined in the "System Status" topic, but the management appliance also has the ability to show the system status for any joined web appliance, as well as its own system status. Also, there are a number of controls that differ from those on the web appliances.

The initial page of the System Status tab on the management appliance shows a table divided into two sections:

- The Management Appliance section contains two columns of information:
  - Appliances: The name of the management appliance. Click the hostname or IP address of the management appliance to view the system status of that system.
  - Appliance type: The model number of the appliance.

In the management appliance system status view, the following buttons are available:

- Shutdown: Performs a graceful shutdown of this appliance.
- Back: Returns you to the System Status main page.
- Show Exceptions: Shows only those monitored conditions that are in a state of alarm.
- Show All: Shows all monitored conditions.

- The web appliances section contains six columns of information:
  - web appliances: The name of the web appliance. Click the hostname or IP address of the web appliance to view the system status of that system.
  - Last contact: The time that has elapsed since the last contact with this appliance.
  - Appliance type: The model number of the appliance.
  - Version: The version of the software load on this appliance.
  - Concurrent users: The number of concurrent users in the last reported minute.
  - Throughput (Mbps): The total kilobits or megabits per second of data passed to users.

In the web appliance system status view, the following buttons are available:

- Remove: Removes this appliance from the list of joined appliances.
- Back: Returns you to the System Status main page.
- Show Exceptions: Shows only those monitored conditions that are in a state of alarm.
- Show All: Shows all monitored conditions.
8 Using Help

The user help provides several mechanisms to help you master the use of the appliance.

• **Search box**: Provides full text search of the appliance help.

• **Table of Contents**

• **Sophos Support**: Provides a form for quick submission of a Sophos Technical Support request, as well as a mechanism for establishing a remote assistance session for Sophos support engineers. Only System administrators have access to this feature.

• **About**: Lists license information and links to other legal information. Only System administrators have access to this feature.

8.1 Searching the Documentation

1. In the **Search** text box, type the query.

   The following search refinements are supported:
   - To match phrases, set the phrase in double quotation marks.
   - To use Boolean operators, type in "AND", "OR", or "AND NOT" in uppercase letters.
   - Prepend a plus sign (+) to a term to require the presence of that term.
   - Prepend a minus sign (-) to a term to require the absence of that term.

2. Press Enter or click the button to the right of the **Search** text box.

   The search results have the following features:
   - Results are sorted by relevance.
   - Excerpts of the search results are displayed to help you assess the relevance of each result, and the search terms are highlighted.

3. Click on the page title of any search result to display that page.

8.2 Using the Table of Contents

The **Table of Contents** is displayed on the appliance’s Help window sidebar.

- To refresh the display of the table of contents, or to clear search results and re-display the table of contents following a search, click on the title, **Contents**.

- To display a page of the help in the Content pane, click on the name of the section of the help in the table of contents that you want to view.

8.3 Sophos Support

The **Sophos Support** icon

192 Copyright © 2019 Sophos Limited
on the right side of the Help window titlebar provides two options for getting help from Sophos Support Services. You can either submit a support request via email, or you can enable remote assistance to your system via an outbound SSH (Secure SHell) connection to Sophos Support Services.

8.3.1 Filing a Support Request By Email

1. On the appliance Help window titlebar, click the Sophos Support icon.

   The Sophos Assistance form is displayed in the Content pane.

2. Fill in the Sophos Support request via email form.

   Fill in the following text boxes:
   - **To:** Enter "wsaph_enr_jsw_hw" if that does not already appear in the text box.
   - **Name:** Enter your name.
   - **Email address:** Enter the email address at which you can be contacted.
   - **Company:** Enter the name of the organization to which the appliance is registered.
   - **Subject:** Enter a short descriptive subject line for the issue.
   - **Additional info:** Add whatever information is significant to understanding the problem.

3. Once you have filled in all of the required and relevant information, click Submit to email the request.

8.3.2 Opening a Remote Assistance Session

**Important**
Prior to opening a remote assistance session, contact Sophos Technical Support to speak with an engineer who will guide you through the remote session.

1. On the appliance Help window titlebar, click the Sophos Support icon.

   The Sophos Assistance form is displayed in the Content pane.

2. In the Remote Assistance section, click Enable to establish the connection.

   A status message is displayed on the status bar (above the tabs bar) that states "Remote Assistance enabled". This is displayed while an outbound SSH connection to Sophos Support Services is open. This connection will be closed by the Sophos Support Services engineer that is working on your assistance request, or the session will be closed automatically within 72 hours.

   When the session is finished, click Disable in the Enable remote assistance section to close the SSH connection.

8.4 About

The About page displays the appliance license information.

To display the "About" page information:
On the Help window sidebar, click About.

The following information is displayed:

- number of users licensed to use the appliance
- license term
- license expiry date for the appliance
A Configuring Ports

To ensure the functionality of the Sophos Web Appliance, configure your network to allow access on the ports listed below. Some ports are required only for specific situation, such as when you enable FTP backups or central management.

Table 1: External Connections

<table>
<thead>
<tr>
<th>Port</th>
<th>Function</th>
<th>Service</th>
<th>Protocol</th>
<th>Connection</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>Remote assistance</td>
<td>SSH</td>
<td>TCP</td>
<td>Outbound from appliance to sophos.com</td>
</tr>
<tr>
<td>22</td>
<td>Central configuration, status and reporting</td>
<td>SSH</td>
<td>TCP</td>
<td>Outbound from web appliance to management appliance (if not collocated)</td>
</tr>
<tr>
<td>25</td>
<td>Remote assistance notification</td>
<td>SMTP</td>
<td>TCP</td>
<td>Outbound from appliance to sophos.com</td>
</tr>
<tr>
<td>80</td>
<td>Outbound network web traffic</td>
<td>HTTP</td>
<td>TCP</td>
<td>Outbound from appliance to internet</td>
</tr>
<tr>
<td>123</td>
<td>Network time synchronization</td>
<td>NTP</td>
<td>UDP</td>
<td>Outbound from appliance to internet</td>
</tr>
<tr>
<td>443</td>
<td>Outbound network web traffic</td>
<td>HTTPS</td>
<td>TCP</td>
<td>Outbound from appliance to internet</td>
</tr>
</tbody>
</table>

Note
Opening ports 80 and 443 is a standard best practice. However, certain web sites may also require other ports to be opened.

Table 2: Internal Connections

<table>
<thead>
<tr>
<th>Port</th>
<th>Function</th>
<th>Service</th>
<th>Protocol</th>
<th>Connection</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>Backups using passive FTP</td>
<td>FTP</td>
<td>TCP</td>
<td>Outbound from appliance to FTP server</td>
</tr>
<tr>
<td>22</td>
<td>Central configuration, status and reporting</td>
<td>SSH</td>
<td>TCP</td>
<td>Outbound from web appliance to management appliance (if collocated)</td>
</tr>
<tr>
<td>53</td>
<td>DNS queries</td>
<td>DNS</td>
<td>UDP</td>
<td>Outbound from appliance to LAN</td>
</tr>
<tr>
<td>80</td>
<td>Administrative web interface</td>
<td>HTTP</td>
<td>TCP</td>
<td>Inbound from LAN to appliance</td>
</tr>
<tr>
<td>Port</td>
<td>Function</td>
<td>Service</td>
<td>Protocol</td>
<td>Connection</td>
</tr>
<tr>
<td>-------</td>
<td>-----------------------------------------------</td>
<td>-------------</td>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>88</td>
<td>Kerberos authentication</td>
<td>KERBEROS</td>
<td>TCP/UDP</td>
<td>Inbound/outbound between appliance and AD server</td>
</tr>
<tr>
<td>139</td>
<td>MS NetBIOS session</td>
<td>NETBIOS-SSN</td>
<td>TCP/UDP</td>
<td>Inbound/outbound between appliance and AD server</td>
</tr>
<tr>
<td>389</td>
<td>Directory services synchronization</td>
<td>LDAP</td>
<td>TCP/UDP</td>
<td>Inbound/outbound between appliance and AD server</td>
</tr>
<tr>
<td>443</td>
<td>Administrative web interface</td>
<td>HTTPS</td>
<td>TCP</td>
<td>Inbound from LAN to appliance</td>
</tr>
<tr>
<td>445</td>
<td>MS server message block</td>
<td>SMB</td>
<td>TCP/UDP</td>
<td>Inbound/outbound between appliance and AD server</td>
</tr>
<tr>
<td>636</td>
<td>LDAP synchronization</td>
<td>LDAPS</td>
<td>TCP</td>
<td>Inbound/outbound between appliance and eDirectory server</td>
</tr>
<tr>
<td>1024–1300, 49152–65535</td>
<td>Dynamic RPC</td>
<td>RPC</td>
<td>TCP</td>
<td>Inbound/outbound between appliance and AD server</td>
</tr>
<tr>
<td>3268</td>
<td>MS AD Global Catalog synchronization</td>
<td>MSGC</td>
<td>TCP/UDP</td>
<td>Inbound/outbound between appliance and AD server</td>
</tr>
<tr>
<td>8080</td>
<td>Proxy (end user web browsing)</td>
<td>HTTP/HTTPS</td>
<td>TCP</td>
<td>Inbound/outbound between LAN and appliance</td>
</tr>
</tbody>
</table>
B Configuring Your Browser

This section contains instructions for configuring your browser to use the web appliance web proxy server.

Before you configure your browser, you need to know the domain name (DNS) of your web appliance, and for certain browsers, the IP address. Contact your IT department to obtain this information. The proxy port number is 8080, although you can also use 3128 and 8081 if your system administrator instructs you to do so.

Select and apply the configuration instructions for each web browser that you use.

Note

The Browser Configuration page is included for distribution to your users as instructions on how to configure their browsers to use the appliance, as is required for Explicit Deployment (page 18). These instructions should be emailed to your users, along with the domain name, IP address, and port of your organization's appliance.

Note

Configuring all user’s browsers to use the web appliance as a web proxy can be done centrally in Windows networks by using any of the following methods, an overview of these can be found at the end of the Sophos Web Appliance: Configuring your network for Explicit Deployment Knowledgebase article, which includes the following:

- Creating, Testing, and Deploying a proxy.pac File
- Publishing Proxy Info as a wpad.dat File
- Creating a GPO

Related tasks

Explicit Deployment (page 18)

B.1 Adding the Sophos Root Certificate

This section contains information on adding the Sophos root certificate in different web browsers.

B.1.1 Adding the Sophos Root Certificate in Internet Explorer

The Install Root Certificate page of the setup wizard prompts you to install the Sophos root certificate. This page provides instructions for adding that root certificate in Internet Explorer.

To install the Sophos root certificate in Internet Explorer:

   The Internet Explorer File Download - Security Warning dialog box is displayed.

2. Click Open.
The Certificate dialog box is displayed.

3. Click Install Certificate.

The first page of the Certificate Import Wizard is displayed.

4. Click Next.

The Certificate Store page of the Certificate Import Wizard is displayed.

5. Select Place all certificates in the following store, click Browse, select Trusted Root Certificate Authorities, click OK and then click Next.

The Completing the Certificate Import Wizard page of the Certificate Import Wizard is displayed.

6. Click Finish.

A Security Warning dialog box is displayed.

7. Click Yes.

The Security Warning dialog box closes, the Certificate Import Wizard closes, and a Certificate Import Wizard alert dialog box is displayed, informing you that "The import was successful".

8. Click OK.

The Certificate Import Wizard alert dialog box closes.

9. In the Certificate dialog box, click OK.

The Certificate dialog box closes and the new Sophos root certificate is installed in your browser.

Note
For more information, see Installing the Sophos-Generated Certificate Authority in your Users' Browsers

B.1.2 Adding the Sophos Root Certificate in Firefox

The Install Root Certificate page of the setup wizard prompts you to install the Sophos root certificate. This page provides instructions for adding that root certificate in Firefox.

To install the Sophos root certificate in Firefox:


   The Firefox Downloading Certificate dialog box is displayed.

2. Select Trust this CA to identify web sites, and click OK.

   The dialog box closes and the new Sophos root certificate is installed in your browser.

Note
For more information, see Installing the Sophos-Generated Certificate Authority in your Users' Browsers

B.2 Configuring Proxy Settings

This section contains information on configuring proxy settings in different web browsers.
B.2.1 Internet Explorer Proxy Configuration

1. Select **Tools > Internet Options**.
   
The **Internet Options** dialog box is displayed.
2. On the **Connections** tab, click **LAN Settings**.
   
The **Local Area Network (LAN) Settings** dialog box is displayed.
3. Select the **Use a proxy server for your LAN** check box, and enter the **Address** (the domain name or IP address provided by your IT department), and **Port** (the proxy port number is 8080, unless you have been instructed to use 3128 or 8081).

   **Note**
   
   If you want to configure Internet Explorer to use the web appliance for FTP and secure sites as well, you must also click **Advanced** and set the same server and port for the FTP and secure (SSL) options. Also on the **Advanced** tab, ensure that the **Enable folder view for FTP sites** option is **not checked**.

4. Ensure that the **Bypass proxy server for local address** check box is checked.
5. Click **OK**.
   
   Your settings are saved and the **Local Area Network (LAN) Settings** dialog box closes.
6. In the **Internet Options** dialog box, click **OK**.
   
   The **Internet Options** dialog box closes.
7. Exit and restart Internet Explorer for your changes to take effect.
8. Verify that you have successfully configured the web appliance as your proxy by visiting **http://www.google.com** and performing a search.
   
   Google.com should display and return search results as usual.
9. Verify that the virus scanning and blocking is working by going to **http://www.eicar.org/download/eicar.com**.
   
   You will see the web appliance "Blocked request" page if the virus scanning and blocking functionality is working properly. (**eicar.com** is a dummy virus used for testing purposes.)

If you encounter any problems with this configuration, contact your IT department.

B.2.2 Firefox Proxy Configuration

1. Select **Edit > Preferences** (on Unix/Linux) or select **Tools > Options** (on Windows).
   
   The **Firefox Preferences** or **Firefox Options** dialog box is displayed.
2. Click the **Advanced** icon, the **Network** tab, and then click **Settings**.
   
   The **Connection Settings** dialog box is displayed.
3. Select the **Manual proxy configuration** option button, and enter the following settings:
   
   - **HTTP Proxy**: (the domain name or IP address provided by your IT department)
   - **Port**: (the proxy port number is 8080, unless you have been instructed to use 3128 or 8081)
4. Select the **Use this proxy server for all protocols** check box.
5. In the **No Proxy for** text box, enter "localhost, 127.0.0.1".
6. Click **OK**.
Your settings are saved and the Connection Settings dialog box closes.

7. In the Firefox Preferences dialog box, click Close.

   The Firefox Preferences or Firefox Options dialog box closes.

8. Exit and restart Firefox for your changes to take effect.

9. Verify that you have successfully configured the web appliance as your proxy by visiting http://www.google.com and performing a search.

   Google.com should display and return search results as usual.

10. Verify that the virus scanning and blocking is working by going to http://www.eicar.org/download/eicar.com.

   You will see the web appliance "Blocked request" page if the virus scanning and blocking functionality is working properly. (eicar.com is a dummy virus used for testing purposes.)

If you encounter any problems with this configuration, contact your IT department.

B.2.3 Apple Safari Proxy Configuration

1. Select Safari > Choose Preferences.

   The Safari Preferences dialog box is displayed.

2. On the Advanced tab, click Change Settings.

   The Network pane of the System Preferences dialog box opens.

3. Select the Web Proxy check box, and enter the following settings: IP address: (the domain name or IP address provided by your IT department); Port Number: (the proxy port number is 8080, unless you have been instructed to use 3128 or 8081)

4. Click Apply Now.

   Your settings are saved and the Safari Preferences dialog box closes.

5. Exit and restart Safari for your changes to take effect.

6. Verify that you have successfully configured the web appliance as your proxy by visiting http://www.google.com and performing a search.

   Google.com should display and return search results as usual.

7. Verify that the virus scanning and blocking is working by going to http://www.eicar.org/download/eicar.com.

   You will see the web appliance "Blocked request" page if the virus scanning and blocking functionality is working properly. (eicar.com is a dummy virus used for testing purposes.)

If you encounter any problems with this configuration, contact your IT department.

B.3 Other Internet Explorer Settings

This section contains information on configuring scenario-specific settings in Internet Explorer.

B.3.1 Increasing the Number of Concurrent Connections in Internet Explorer

Internet Explorer (version 7 and earlier) limits the number of concurrent connections to a server to 2. This creates a performance bottleneck for the Sophos Web Appliance. In order to improve
performance, you will need to increase the number of concurrent connections on your users’ systems to 10. See How do I configure Internet Explorer to download more than two files at one time? for more information.

**B.3.2 Enabling PDF Access in Internet Explorer**

Internet Explorer security settings may block Adobe Acrobat PDFs from being downloaded. If you are unable to view reports as PDFs, you can change this Internet Explorer option to enable access to Sophos reports.

1. Select **Tools > Internet Options**.
   The **Internet Options** dialog box is displayed.
2. On the **Security** tab, click **Custom level**.
   The **Security Settings** dialog box is displayed.
3. In the **Downloads** section of the **Settings**, select the **Enable** option for the **Automatic prompting for file downloads** option, and click **OK** to close each dialog box.
   The next time that you request a report as a PDF, a **File Download** dialog box is displayed, prompting you to open or save the file.

**B.4 Other Firefox Settings**

This section contains information on configuring scenario-specific settings in Firefox.

**B.4.1 Configuring Firefox for Active Directory in Transparent mode or Bridged mode**

When the web appliance uses Active Directory authentication in Transparent mode, and Web Cache Communication Protocol provides load balancing between two or more appliances, Firefox users are prompted to enter a username and a password once per appliance. To avoid these prompts, configure Firefox to connect automatically.

1. In the Firefox address bar, type **about:config**.
2. In the **Filter** text box type **ntlm**.
3. Double click on **network.automatic-ntlm-auth.trusted-uris** to edit the field.
4. Enter the hostname(s) of the web appliance(s).

**Related concepts**

Active Directory (page 123)

**Related tasks**

Transparent Deployment (page 24)
C Appliance Behavior and Troubleshooting

This section contains information on the general behavior of Sophos appliance operations and specific information on troubleshooting various aspects of web appliance deployment and configuration.

C.1 Network Deployment Troubleshooting

The following is a list of known web appliance network deployment issues and their solutions.

"Blocked" Notification Page Lacks Graphics and a Stylesheet

**Problem:** If the "Blocked" notification page is displayed without any graphics and as raw HTML without the formatting of a stylesheet, the problem can result from the following combination of conditions in your network deployment:

- Your browser is configured to bypass use of the web appliance for your internal sites (for example, the domain name of your web appliance would normally be bypassed).
- Your browser is configured with the web appliance’s IP address instead of its fully qualified hostname.
- Your DNS server cannot resolve the web appliance’s IP address.

**Solution:** The best solution is to add the web appliance to your DNS server.

Firewall reports attachments stripped from web appliance-generated email

**Background:** The web appliance provides a managed appliance experience that is enabled in part by sending system status snapshots as email attachments to Sophos to ensure that your web appliance is operating within acceptable thresholds.

**Problem:** Firewalls can strip attachments from web appliance-generated email.

**Solution:** To enable the Sophos managed appliance experience, configure your firewall to allow email with attachments from the web appliance to wsasupport@sophos.com.

Long delays when loading web pages

**Problem:** If latency is significantly increased when browsing through the appliance, the problem may be due to an inappropriate Speed and duplex setting forced by enabling the auto-detect option.

**Solution:** To test if this is the case, set one of the manual options in the Speed and duplex option on the Configuration > Network > Network Interface page. If this change does not remedy the high latency problem, reinstate the automatic option and contact Sophos Technical Support.
RealPlayer Content Appears to be Blocked

**Problem:** RealPlayer content fails to play. This is typically a firewall configuration issue and not a web appliance problem. RealPlayer uses port 554, which is typically blocked in default firewall configurations.

**Note**
The remote site can force the use of a non-HTTP port, which will result in users not being able to view the content if the firewall is blocking the port being used.

**Solution:** To enable access to RealPlayer content, open port 554 on your firewall.

C.2 Active Directory Troubleshooting

The common error messages that you may encounter when configuring Active Directory access are described in this section, as are the corrective actions that you can take to respond to them. The following errors may be displayed at the bottom of the page when you click **Verify Settings** on the **Configuration > System > Active Directory** page.

C.2.1 Appliance and AD Domain have the same name

The appliance and your Active Directory domain have been given the same name. These names cannot be the same. Change the hostname of the appliance on the **Network: Hostname** page, and then re-test the Active Directory settings by clicking **Verify Settings** on the **System: Active Directory** page.

C.2.2 Clock skew is too large

The time difference between the appliance and your Active Directory Kerberos server is greater than three minutes. Update the time on your Kerberos server, or adjust the NTP Server setting (set at the bottom of the **Configuration > System > Time Zone** page) to synchronize the appliance to the same NTP source as your Kerberos server.

**Note**
Microsoft Windows Server 2000 can be configured as an NTP source, see KB articles http://support.microsoft.com/kb/216734 and http://support.microsoft.com/kb/223184. Microsoft Windows Server 2003 is configured as an NTP source by default.

C.2.3 Could not auto-detect settings

Your network’s Active Directory settings could not be auto-detected by the appliance. Clear the **Auto-detect advanced settings** check box, and manually configure all the required fields on the **System: Active Directory** page.
C.2.4 Could not connect to Domain Controller

The appliance could not connect to the specified Active Directory domain controller, typically because the hostname cannot be resolved, or an error was made when it was entered. Check the Active Directory Domain Controller, update the required fields on the System: Active Directory page, and click Verify Settings again.

C.2.5 Could not join the domain

The appliance could not join the specified Active Directory domain, possibly due to insufficient privileges for the given Username and Password. Check the Active Directory Domain Controller, update the required fields on the System: Active Directory page, and click Verify Settings again.

C.2.6 Could not test Kerberos settings

The appliance could not reach your specified Active Directory Kerberos server or the specified Active Directory Domain Controller is not in your Kerberos server’s database. Update the required fields, check the Active Directory Kerberos server on the System: Active Directory page, and click Verify Settings again.

C.2.7 Could not test LDAP settings

The appliance could not authenticate to your specified Active Directory LDAP server, or the specified LDAP Base DN field is incorrect. Check the Active Directory Domain Controller, update the required fields on the System: Active Directory page, and click Verify Settings again.

C.2.8 Domain could not be found

The specified Active Directory domain could not be found. Check the Active Directory Domain Controller, update the required fields on the System: Active Directory page, and click Verify Settings again.

C.2.9 Hostname is too long

The appliance hostname cannot be longer than 15 characters to join the Active Directory domain. Update your Fully-qualified domain name on the Configuration > Network > Hostname page, and configure your Active Directory settings on the System: Active Directory page.

C.2.10 Invalid credentials

The appliance could not authenticate with the given Username and Password. Check the Active Directory Domain Controller, update the required fields on the System: Active Directory page, and click Verify Settings again.
C.2.11 LDAP search query timeout

The appliance is having trouble communicating with your Kerberos server and has timed out waiting for a response. Specifically, the appliance is unable to auto-detect the LDAP authentication DN field. Check your Kerberos server and firewall settings to ensure that they are communicating on the proper ports and that those ports are properly configured on your firewall, and then re-test the Active Directory settings by clicking Verify Settings on the System: Active Directory page.

C.2.12 No IPC share found

The appliance could not detect an IPC share on your Active Directory Domain Controller. Check the Active Directory Domain Controller, update the required fields on the System: Active Directory page, and click Verify Settings again.

C.2.13 No NETLOGON share found

The appliance could not detect a NETLOGON share on your Active Directory Domain Controller. Check the Active Directory Domain Controller, update the required fields on the System: Active Directory page, and click Verify Settings again.

C.2.14 Server appears to be in wrong domain

The specified Active Directory domain does not match the specified Active Directory Domain Controller. Check the Active Directory Domain Controller, update the required fields on the System: Active Directory page, and click Verify Settings again.

C.2.15 Server error

An error occurred when the appliance tried to join the Active Directory domain. If you receive this error, ensure that the following are true:

- The detected or configured Domain Controller is currently running.
- The required ports between the appliance and the Domain Controller are open bi-directionally; these are:

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Service</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>53</td>
<td>TCP &amp; UDP</td>
<td>dns</td>
<td>DNS query</td>
</tr>
<tr>
<td>88</td>
<td>TCP &amp; UDP</td>
<td>kerberos</td>
<td>Kerberos authentication</td>
</tr>
<tr>
<td>123</td>
<td>UDP</td>
<td>ntp</td>
<td>Clock synchronization</td>
</tr>
<tr>
<td>139</td>
<td>TCP</td>
<td>netbios-ssn</td>
<td>MS NetBIOS over TCP/IP</td>
</tr>
<tr>
<td>389</td>
<td>TCP &amp; UDP</td>
<td>ldap</td>
<td>LDAP synchronization</td>
</tr>
<tr>
<td>445</td>
<td>TCP</td>
<td>smb</td>
<td>MS server message block</td>
</tr>
<tr>
<td>Port</td>
<td>Protocol</td>
<td>Service</td>
<td>Purpose</td>
</tr>
<tr>
<td>------</td>
<td>----------</td>
<td>---------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>3268</td>
<td>TCP &amp; UDP</td>
<td>msgc</td>
<td>MS AD Global Catalog synchronization</td>
</tr>
</tbody>
</table>

Port 123 is only required if the **Network Time Protocol server** is set to the local Domain Controller on the **Configuration > System > Time Zone** page.

- The network connection between the appliance and the Domain Controller is working.

If the above checks fail to identify the problem, please contact Sophos Technical Support.

### C.2.16 Subdomain failed to authenticate

The configuration detection for one or more of your subdomains did not complete successfully. Click the "show details" link to see a list of the subdomains for which the settings could not be detected. Group policy for non-primary groups from those subdomains might not be applied as expected.

You can also check the following:

- The global catalog points to a single Active Directory forest containing a single Active Directory tree.
- The root domain of your Active Directory forest has an explicit trust relationship with all domains in the forest.
- The same administrator credentials work for all child domain controllers.
- All child domain controllers are accessible via the network and port 389 is open between the appliance and all domain controllers within the Active Directory forest.

If you cannot successfully connect to your Active Directory forest, you can manually change the port number for the Active Directory LDAP server (on the **Configuration > System > Active Directory** page) to 389 to force the appliance to access the Active Directory server as a single domain.

### C.2.17 Could not join the Secondary Domain Controller

The appliance could not join the specified **Secondary Domain Controller**. This may be because the **Secondary Domain Controller** is unreachable, or because the required object has not yet been replicated from the **Primary Domain Controller** to the **Secondary Domain Controller**.

### C.3 eDirectory Troubleshooting

The common error messages that you may encounter when configuring eDirectory access are described in this section, as are the corrective actions that you can take to respond to them. The following errors may be displayed at the bottom of the page when you click **Verify Settings** on the **Configuration > System > eDirectory** page.

**Important**

If your web appliance is having difficulty in identifying or correctly identifying a user then it is likely due to changes in your network topology or your eDirectory server. If there have been such changes, it is recommended that you turn **eDirectory integration to Off**, update your eDirectory settings, rerun **Verify Settings** and **Apply** those settings if the verify operation was successful.
C.3.1 Invalid credentials

The appliance could not authenticate with the given Authentication DN and Password. Update these fields on the Configuration > System > eDirectory page with the correct information, and click Verify Settings again.

C.3.2 Could not connect to server

The appliance could not connect to the given LDAP server and port. Update this field on the Configuration > System > eDirectory page, and click Verify Settings again.

Note
If the appliance cannot connect to the LDAP server, an error is displayed in the Detect Settings popup. If the address of the LDAP server is valid, a warning listing all incorrectly configured replicas is displayed.

Note
If the port is not specified, it defaults to 636.

C.3.3 Unable to establish Secure LDAP connection

While the appliance was able to connect to the server, it could not establish an LDAPS (encrypted) connection. Your eDirectory server must be set up for LDAPS connections. If your eDirectory server requires a client-side certificate, this is not supported, although setting client-side certificates to requested will not cause problems.

C.3.4 No users or groups returned from LDAP server

No users or groups were found on the specified server. This warning is issued when a base DN with no users is specified in the Base DN field, or the user specified in the Authentication DN does not have sufficient privileges to query the contents of the LDAP tree. Update these fields on the Configuration > System > eDirectory page, and click Verify Settings again. Additionally, increase the time limit on your eDirectory server, if it has run out.

C.3.5 Could not sync users from LDAP server

This message will display if the Base DN has a typo, if it doesn't exist, or if it is entered in an invalid format. Check this field on the Configuration > System > eDirectory page, and click Verify Settings again.

C.3.6 Invalid authentication DN

This error message is displayed if the Authentication DN field on the Configuration > System > eDirectory page has been entered in an unrecognized format, such as the dot-separated

Copyright © 2019 Sophos Limited
format, which is not supported. Check that this information has been properly entered in the form `cn=admin,o=company`, and click **Verify Settings** again.

### C.3.7 Unable to bind to LDAP server

Although the password has been entered correctly, the appliance could not authenticate with the server. This error message may be caused by a problem with the user object specified in the **Authentication DN** field. Correct this entry on the **Configuration > System > eDirectory** page, and click **Verify Settings** again.

### C.3.8 Server error

An error occurred when the appliance tried to connect to the eDirectory server. If you receive this error, ensure that the following are true:

- The configured eDirectory server is currently running.
- The required LDAPS port between the appliance and the eDirectory server is open bi-directionally for UDP and TCP communication. Unless you have configured a different port, the LDAPS default is port 636.
- The network connection between the appliance and the eDirectory server is working.
- The eDirectory server’s logs indicate that it is operating correctly.

If the above checks fail to identify the problem, please contact Sophos Technical Support.

### C.3.9 Network is unreachable

The appliance could not authenticate with the server as the network is unreachable. Correct this entry on the **Configuration > System > eDirectory** page, and click **Verify Settings** again.

### C.3.10 Could not resolve hostname

The appliance could not authenticate resolve the hostname of the server. Correct this entry on the **Configuration > System > eDirectory** page, and click **Verify Settings** again.

### C.4 Grouped Appliance Troubleshooting

This page describes the problems that can be encountered when joining a web appliance to a management appliance, and it provides solutions to these problems.

#### Join fails with Mismatched Software Load error message

**Problem**: Clicking **Join Management Appliance** produces a **Software versions to not match** error message at the **Verifying software version** check.

**Cause**: Installed software loads on the two appliances are different version.

**Solution**: On both appliances, go to the **Configuration > System > Updates** page and ensure that the latest software version is installed.
Previously joined web appliances are unable to join with a new (replacement) management appliance

**Problem**: When a management appliance is replaced with a new unit, and the previous unit’s configuration data backup is restored to the replacement unit, web appliances that were previously joined to the original management appliance are unable to communicate with the replacement management appliance.

**Cause**: Successfully joining previously joined web appliances to a replacement management appliance requires an additional step after configuration data is restored to the replacement management appliance, and after its fully qualified domain name and IP address are set.

**Solution**: After the replacement management appliance has had configuration data restored to it, and you have ensured that its fully qualified domain name and IP address are correct, each web appliance that was joined to the previous management appliance must be reverted to standalone mode, then be re-joined to the replacement management appliance.

New management appliance uploading web appliance data produces AD error alerts

**Problem**: When you join an established web appliance to a new management appliance, with the **Copy configuration and policy data from the first web appliance to join** option selected on the management appliance, the management appliance raises **Active Directory integration**, **Active Directory synchronization**, and possibly **Active Directory Trusted Domains synchronization** alerts.

**Cause**: The uploaded configuration data from the web appliance includes Active Directory access configuration, but the firewall between the new management appliance and the Active Directory server has not been configured to open the required ports.

**Solution**: Configure your firewall to provide access to the ports and services listed in the following tables.

### Table 3: External Connections

<table>
<thead>
<tr>
<th>Port</th>
<th>Function</th>
<th>Service</th>
<th>Protocol</th>
<th>Connection</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>Remote assistance</td>
<td>SSH</td>
<td>TCP</td>
<td>Outbound from appliance to sophos.com</td>
</tr>
<tr>
<td>22</td>
<td>Central configuration, status and reporting</td>
<td>SSH</td>
<td>TCP</td>
<td>Outbound from web appliance to management appliance (if not collocated)</td>
</tr>
<tr>
<td>25</td>
<td>Remote assistance notification</td>
<td>SMTP</td>
<td>TCP</td>
<td>Outbound from appliance to sophos.com</td>
</tr>
<tr>
<td>80</td>
<td>Outbound network web traffic</td>
<td>HTTP</td>
<td>TCP</td>
<td>Outbound from appliance to internet</td>
</tr>
<tr>
<td>123</td>
<td>Network time synchronization</td>
<td>NTP</td>
<td>UDP</td>
<td>Outbound from appliance to internet</td>
</tr>
<tr>
<td>Port</td>
<td>Function</td>
<td>Service</td>
<td>Protocol</td>
<td>Connection</td>
</tr>
<tr>
<td>------</td>
<td>----------</td>
<td>-----------</td>
<td>----------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td>443</td>
<td>Outbound network web traffic</td>
<td>HTTPS</td>
<td>TCP</td>
<td>Outbound from appliance to internet</td>
</tr>
</tbody>
</table>

Table 4: Internal Connections

<table>
<thead>
<tr>
<th>Port</th>
<th>Function</th>
<th>Service</th>
<th>Protocol</th>
<th>Connection</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>Backups using passive FTP</td>
<td>FTP</td>
<td>TCP</td>
<td>Outbound from appliance to FTP server</td>
</tr>
<tr>
<td>22</td>
<td>Central configuration, status and reporting</td>
<td>SSH</td>
<td>TCP</td>
<td>Outbound from web appliance to management appliance (if collocated)</td>
</tr>
<tr>
<td>53</td>
<td>DNS queries</td>
<td>DNS</td>
<td>UDP</td>
<td>Outbound from appliance to LAN</td>
</tr>
<tr>
<td>80</td>
<td>Administrative web interface</td>
<td>HTTP</td>
<td>TCP</td>
<td>Inbound from LAN to appliance</td>
</tr>
<tr>
<td>88</td>
<td>Kerberos authentication</td>
<td>KERBEROS</td>
<td>TCP/UDP</td>
<td>Inbound/outbound between appliance and AD server</td>
</tr>
<tr>
<td>139</td>
<td>MS NetBIOS session</td>
<td>NETBIOS-SSN</td>
<td>TCP/UDP</td>
<td>Inbound/outbound between appliance and AD server</td>
</tr>
<tr>
<td>389</td>
<td>Directory services synchronization</td>
<td>LDAP</td>
<td>TCP/UDP</td>
<td>Inbound/outbound between appliance and AD server</td>
</tr>
<tr>
<td>443</td>
<td>Administrative web interface</td>
<td>HTTPS</td>
<td>TCP</td>
<td>Inbound from LAN to appliance</td>
</tr>
<tr>
<td>445</td>
<td>MS server message block</td>
<td>SMB</td>
<td>TCP/UDP</td>
<td>Inbound/outbound between appliance and AD server</td>
</tr>
<tr>
<td>636</td>
<td>LDAP synchronization</td>
<td>LDAPS</td>
<td>TCP</td>
<td>Inbound/outbound between appliance and AD server</td>
</tr>
<tr>
<td>1024–1300, 49152–65535</td>
<td>Dynamic RPC</td>
<td>RPC</td>
<td>TCP</td>
<td>Inbound/outbound between appliance and AD server</td>
</tr>
<tr>
<td>3268</td>
<td>MS AD Global Catalog synchronization</td>
<td>MSGC</td>
<td>TCP/UDP</td>
<td>Inbound/outbound between appliance and AD server</td>
</tr>
<tr>
<td>8080</td>
<td>Proxy (end user web browsing)</td>
<td>HTTP/HTTPS</td>
<td>TCP</td>
<td>Inbound/outbound between LAN and appliance</td>
</tr>
</tbody>
</table>
New web appliance join produces an AD integration alert and blocks all users’ web access

**Problem:** When you join a new web appliance to a configured management appliance, the web appliance raises an Active Directory integration alert, and web access is blocked for all of the web appliance’s users.

**Cause:** The configuration data downloaded from the management appliance includes Active Directory access configuration, but the firewall between the new web appliance and the Active Directory server has not been configured to open the required ports.

**Solution:** You can either configure your firewall to provide access to the ports and services listed in the preceding tables, or you can configure the new web appliance to use a local Active Directory server, although the appliance must still have access to the ports and services indicated in the preceding tables.

**Related concepts**
- Understanding Mode and Model Differences (page 42)
- Updates (page 113)
- Grouping Web Appliances (page 37)

**Related tasks**
- Configuring Active Directory Access (page 123)

## C.5 HTTPS Compatibility

This section describes several areas of compatibility to be aware of prior to enabling HTTPS scanning. It is instructive to first review how HTTPS web requests work, and how HTTPS scanning operates.

In normal usage, the following things occur when a user accesses an HTTPS secured website:

1. The browser negotiates a secure connection directly to the remote site. Once connected, the user can inspect the certificate authority if needed. If the remote site uses an unrecognized certificate authority, the user will be first prompted by the browser to inspect and accept this site’s certificate authority.

2. The certificate authority contains a key that verifies the authenticity of the encrypted content that is received from the secure website, and which the SSL software decrypts.

3. Any information that the user submits to the secure website is also encrypted, and the authenticity of their submission is similarly verified by the certificate authority.

The web appliance provides two security features related to this process: certificate validation and HTTPS scanning.

### Certificate Validation

Often, end users have little knowledge about the reliability of a certificate authority, so they will often accept certificate authorities without knowing if they are from trusted sources. To overcome this problem, the web appliance includes most reliable certificate authorities, and it can automatically validate certificate authorities from the Sophos certificate authority list. You can also add custom certificate authorities. This allows you to prevent users from accepting certificate authorities.
HTTPS Scanning

To provide secure sessions between commercial or banking sites and users, HTTPS encrypts web content between the website server and the user’s browser. While the traffic between the two is encrypted during an HTTPS session, the content that is delivered is no less likely to be infected with viruses or other malware.

To scan encrypted content, the content must first be decrypted, then scanned, then re-encrypted for delivery to the requesting end-user’s browser. Doing this maintains the privacy of the encrypted content, as the process is done automatically without human eyes viewing the content.

However, because the traffic has been decrypted, the original site certificate cannot be used by the browser to authenticate the connection, so the original certificate is replaced by one generated automatically on the appliance using a Sophos-generated certificate authority. This replaces the original certificate, which requires that you download and install the Sophos-generated certificate authority into your users’ browsers. This can be done as a centralized system administration operation using Group Policy Objects.

Note
For more information, see the knowledgebase article Installing the Sophos-Generated Certificate Authority in Your Users’ Browsers.

In greater detail, here is how the web appliance handles HTTPS scanning:

1. You, the administrator, download the Sophos certificate authority from the web appliance and install it in your user’s browsers.
The user requests a secure web page through the web appliance.

The secure site and the web appliance negotiate a secure connection.
The web appliance creates a certificate for its secure session with the user.

The returned page goes through the following process:

5a The secure site sends an HTTPS page to the web appliance.
5b The web appliance decrypts the page.
5c The web appliance scans the contents.
5d The web appliance re-encrypts the page.
5e The web appliance sends the re-encrypted page to the user, whose browser decrypts the page using the certificate authority installed in Step 1.

Note
For more information about obtaining the certificate to install on your users’ browsers, see Downloading the Certificate Authority.
HTTPS Compatibility with Sites

Many financial sites require that clients use a specific certificate authority to establish an HTTPS session with the financial institution's site. During HTTPS scanning, the appliance replaces the client certificate with its own certificate. Therefore, financial institutions that require special client certificates do not support HTTPS scanning. It is highly recommended that administrators enable the option to **Exempt Financial & Investment sites from HTTPS scanning** for maximum compatibility. This option is enabled by default when HTTPS scanning is enabled.

Some web services are incompatible with proxies that scan HTTPS content, and, therefore, it is recommended that you exempt them from HTTPS scanning. Of these, the Webex service **webex.com** is exempted from HTTPS scanning by default.

Some software applications use HTTPS for registration and expect specific certificates from the systems that are registering. When HTTPS scanning is enabled and the appliance generates its own certificate, such applications may not operate correctly. Of these, the Windows Vista activation site, **sls.microsoft.com**, is exempted from HTTPS scanning by default.

For a complete list of known sites that are incompatible with HTTPS scanning, refer to the section **Managing HTTPS Scanning Exemptions** (page 105), and add sites from the list to be exempt from HTTPS scanning as required.

**Related tasks**
- Configuring Certificate Validation (page 106)
- Adding a Certificate from a Web Site (page 107)
- Adding a Root Authority Certificate (page 108)
- Configuring HTTPS Scanning (page 104)

C.6 Images Display as Gray

When images are loaded in a browser or third-party application directly from a *blocked or warned* site, the images will be displayed as gray boxes. If a user visits a site that policy blocks or warns against, the appliance presents a page describing what is happening, but the images are displayed as gray boxes.

Some third-party applications import images from the web as well. For instance, Microsoft Office 2007 can display and download clip art from the web. But, a site that it pulls images from may be *blocked or warned* in the appliance policy. These images will not be displayed in the Clip Art browser in Office 2007.

To allow access you can right click the image in the browser and add an exception for that site in **Configuration > Group Policy > Local Site List**.

**Related tasks**
- Configuring the Local Site List (page 96)
- Searching Recent Activity (page 181)
D Interpreting Log Files

This page provides the information required to interpret a web appliance log file.

This file is saved as part of a system backup that is configured on the Configuration > System > Backup page, if you have the Transaction log files at least once daily at midnight option selected, and you have chosen to back up the logs in the Sophos format. If you have chosen to back up the logs in the Squid format, see the Squid log format page.

Introduction

The appliance keeps a log (called sophos_log) of all requests it processes. The following is an example of a sophos_log entry:

```
h=10.99.115.13 u="DOMAIN\johnsmith" s=200 X=- t=1336666489 T=284453 Ts=0 act=1 cat="0x220000002a" app=-- rsn=- threat="-" type="text/html" ctype="text/html" sav-ev=4.77 sav-dv=2012.5.10.4770003 uri-dv=-- in=1255 out=26198 meth=GET ref="-" ua="Mozilla/5.0 (Windows NT 6.1; WOW64; rv:12.0)
Gecko/20100101 Firefox/12.0"
req="GET http://www.google.ca/ HTTP/1.1" dom="google.ca" filetype="-" rule="0"
filesize=25815 axtime=0.048193 fttime=0.049360 scantime=0.011 src_cat="0x2f0000002a"
labs_cat="0x2f0000002a" dcat_prox="-" target_ip="74.162.127.94"
labs_rule_id="0"
reqtime=0.027 adtime=0.001625 ftbypass=- os=Windows authn=53
auth_by=portal_cache
dnstime=0.000197 quotatime=- sandbox=-
```

```
h=192.168.98.38 u="SILKNET2\t\xc3\xe5m\xc3\xe5sj\xc3\xb3n\xc3\xa9\xc3\xa4s\xc3\xb7m\xc3\xa4s\xc3\xb3n\xc3\xa4s\xc3\xa9s" s=200 X=X t=1178921655 T=3444378 Ts=3 act=1 cat=0x220000001a rsn=- threat="-" type="application/x-exe" ctype="application/x-msdos-program" sav-ev=4.17
cache=MISS in=905 out=236936 meth=GET
req="GET http://funnel-web.ca.sophos.com/mime/ exe.exe HTTP/1.1"
dom="sophos.com"
filetype="exe.exe" rule="3479751" filesize=266360 axtime=0.001234
fttime=0.000235 scantime=0.010 src_cat=0x3200001d53 labs_cat=0x0200000012
dcat_prox="-"
target_ip="192.168.3.125" labs_rule_id="3479751" reqtime=0.056
adtime=0.000003
```
### Data Fields

The following table explains the keys used in the `sophos_log` file.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ep</strong></td>
<td>This setting is optional and is only displayed if you are using Endpoint Web Control. A value of <code>ep=1</code> means the browsing occurred on the endpoint computer, and that this entry was then uploaded to the appliance.</td>
</tr>
<tr>
<td><strong>sxl</strong></td>
<td>This setting is optional. An entry of <code>sxl=y</code> or <code>sxl=n</code> indicates if an SXL lookup for a particular transaction was successful or not.</td>
</tr>
<tr>
<td><strong>h</strong></td>
<td>Remote host (the IP address that sent the request).</td>
</tr>
<tr>
<td><strong>u</strong></td>
<td>Remote user who made the request (null if user authentication is off). Note that the second entry example above shows how UTF-8 usernames are encoded in the log file.</td>
</tr>
<tr>
<td><strong>s</strong></td>
<td>HTTP status code sent back to the client.</td>
</tr>
</tbody>
</table>
| **X** | The connection status when the response was completed:  
- `X` = connection aborted before the response completed,  
- `+` = connection may be kept alive after the response is sent,  
- `-` = connection will be closed after the response is sent. |
| **t** | Timestamp (in seconds) of when the request was first received since the UNIX Epoch, i.e. 1970-01-01 00:00:00 UTC). |
| **T** | Time in microseconds required to serve this request. |
| **Ts** | Time required (in seconds) to serve this request. |
| **act** | Action code that identifies the outcome of the request:  
- `-7` = User is shown a sandbox analysis page.  
- `-6` = User attempted to proceed on a quota page, but the request was blocked.  
- `-5` = Block page displayed: daily quota time exceeded.  
- `-4` = Quota time warning displayed.  
- `-3` = User proceeded but request was blocked.  
- `-2` = Request was warned.  
- `-1` = Request was blocked.  
- `1` = Request was allowed.  
- `2` = Request was warned and user decided to proceed.  
- `3` = User proceeded.  
- `4` = User accepts a quota time and proceeds.  
- `5` = Requested proceeded after quota accepted. |
<p>| <strong>cat</strong> | Matched URI category ID (e.g. <code>0x200000034</code>). The <code>n</code> indicates the risk level: 0=unclassified, 1=trusted, 2=low, 3=medium, and 4=high. For a full listing of the values used with the cat key, see the section <a href="#">Category Codes</a> below. |
| <strong>app</strong> | Application identified by the appliance. |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rsn</td>
<td>Reason code that identifies why a particular request was blocked. The supported codes are listed below; however, this list is subject to change.</td>
</tr>
<tr>
<td></td>
<td>1401 = Blocked because request contains a virus,</td>
</tr>
<tr>
<td></td>
<td>1402 = Blocked by Local or Sophos URI list,</td>
</tr>
<tr>
<td></td>
<td>1403 = Blocked by file type,</td>
</tr>
<tr>
<td></td>
<td>1404 = Blocked because the request is encrypted and could not be scanned,</td>
</tr>
<tr>
<td></td>
<td>1405 = Blocked because the virus scanner timed out when trying to scan the request,</td>
</tr>
<tr>
<td></td>
<td>1406 = Blocked by policy,</td>
</tr>
<tr>
<td></td>
<td>1407 = Blocked because the originating server failed SSL certificate validation,</td>
</tr>
<tr>
<td></td>
<td>1408 = Blocked ‘Range’ requests,</td>
</tr>
<tr>
<td></td>
<td>1409 = Blocked by tag.</td>
</tr>
<tr>
<td></td>
<td>1410 = Blocked (Lookup failed)</td>
</tr>
<tr>
<td></td>
<td>1411 = Blocked because of application control.</td>
</tr>
<tr>
<td></td>
<td>1412 = Blocked by Sandstorm</td>
</tr>
<tr>
<td>threat</td>
<td>Malware/Virus name detected by the scanner.</td>
</tr>
<tr>
<td>type</td>
<td>MIME type identified by the appliance.</td>
</tr>
<tr>
<td>ctype</td>
<td>Content-Type indicated by the originating server.</td>
</tr>
<tr>
<td>sav-ev</td>
<td>Sophos Anti-virus engine version used for this request.</td>
</tr>
<tr>
<td>sav-dv</td>
<td>Sophos Anti-virus data version used for this request.</td>
</tr>
<tr>
<td>uri-dv</td>
<td>Sophos URI list version used for this request.</td>
</tr>
<tr>
<td>cache</td>
<td>Cache HIT or MISS (whether the request was served from the appliance cache).</td>
</tr>
<tr>
<td>in</td>
<td>Amount of data (including headers, in bytes) received from the client by the appliance for this request.</td>
</tr>
<tr>
<td>out</td>
<td>Amount of data (including headers, in bytes) sent out by the appliance to the client for this request.</td>
</tr>
<tr>
<td>meth</td>
<td>HTTP request method (i.e. POST/GET/CONNECT).</td>
</tr>
<tr>
<td>ref</td>
<td>HTTP &quot;referrer&quot; field, populated if this request was referred by another (e.g. request for an image that is part of a web page).</td>
</tr>
<tr>
<td>ua</td>
<td>User-Agent of the client that’s making this request.</td>
</tr>
<tr>
<td>req</td>
<td>HTTP request string (including request method, URL requested, and request protocol).</td>
</tr>
<tr>
<td>dom</td>
<td>Domain portion of the request URI.</td>
</tr>
<tr>
<td>filetype</td>
<td>Sophos filetype category (e.g. both ‘application/x-gzip’ &amp; ‘application/x-bzip2’ belong to the category ‘archive.compress’).</td>
</tr>
<tr>
<td>rule</td>
<td>Policy rule ID matched for this request. Local Site List categorization rules are prefixed with ‘LSL-‘. Sophos categorization rules are not documented.</td>
</tr>
<tr>
<td>filesize</td>
<td>Size of the file served for this request (does not include HTTP protocol overhead).</td>
</tr>
<tr>
<td>axtime</td>
<td>Amount of time (in seconds) it took to perform access checks.</td>
</tr>
<tr>
<td>fftime</td>
<td>Amount of time (in seconds) it took to perform file-typing.</td>
</tr>
<tr>
<td>scantime</td>
<td>Amount of time (in seconds) it took to perform scanning.</td>
</tr>
<tr>
<td>src_cat</td>
<td>Internal use only.</td>
</tr>
<tr>
<td>labs_cat</td>
<td>Internal use only.</td>
</tr>
<tr>
<td>dcat_prox</td>
<td>Internal use only.</td>
</tr>
<tr>
<td>target_ip</td>
<td>The IP address that the request resolves to.</td>
</tr>
<tr>
<td>labs_rule_id</td>
<td>Internal use only.</td>
</tr>
<tr>
<td>reqtime</td>
<td>Amount of time (in seconds) that a web resource is in the queue for scanning.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>adtime</td>
<td>Amount of time (in seconds) it took to perform Active Directory or eDirectory authentication.</td>
</tr>
<tr>
<td>ftbypass</td>
<td>Internal use only.</td>
</tr>
<tr>
<td>os</td>
<td>If you have specified a connection profile for authentication, this is the type of operating system or device that was detected.</td>
</tr>
<tr>
<td>auth_by</td>
<td>The form of authentication that succeeded (for example, &quot;bypass,&quot; &quot;portal,&quot; &quot;kerb&quot;).</td>
</tr>
<tr>
<td>authn</td>
<td>Internal use only.</td>
</tr>
<tr>
<td>dnstime</td>
<td>Amount of time (in seconds) it took to get a DNS response. This can help troubleshoot DNS latency issues.</td>
</tr>
<tr>
<td>quotatime</td>
<td>The number of quota minutes used. This relates to the number of minutes allowed for this quota. This is configured in the Naming &amp; Scheduling tab of the Additional Policy wizard: Configuration &gt; Group Policy &gt; Additional Policies.</td>
</tr>
<tr>
<td>sandbox</td>
<td>Identifies whether a download should be sent to the sandbox component of Sophos Sandstorm.</td>
</tr>
</tbody>
</table>

### Special Notes

The basic format is `[key]=value` where there is no whitespace between the key, the equals character or the value. The value may be enclosed in quotes, e.g. `[key]="value"`. Values that contain embedded whitespace will always use quote delimiters. Implementers are encouraged to check for, and remove if found, surrounding unescaped quote characters for each value.

Each log line is terminated by a newline character (ASCII LF, 0x10). Since these log files may be moved between computers that could reformat the text file, implementers are encouraged to recognize and accept log lines terminated by any of the standard text line termination schemes: newline, carriage return (ASCII CR, 0x0D) or LF+CR as used by Windows/DOS.

Quotes (" ") and backslashes (\) within a value are escaped by prepending a backslash. Keys will never contain such characters.

Null values may be represented by an empty string (e.g. `[key]=""`) or a dash character (e.g. `[key]=--` or `[key]="--"). Any value containing only a dash character should be treated as if the value was not specified. Some fields will contain a null string if the value would otherwise be undefined (e.g. for a blocked request, the filetype field will be meaningless).

The appliance supports Unicode usernames when authenticating users to an Active Directory or eDirectory server. In these cases the user field will contain a UTF-8 string; the non-printable bytes are escaped using the `\x` prefix followed by the hexadecimal representation of the raw bytes (e.g. `\xAF`). In the example above, 'SILKNET2\t\xc3\xb5\xc3\xa4\xc3\xb3\xc3\xa9s' translates to 'SILKNET2\tömásjónés', where the username is:

<table>
<thead>
<tr>
<th>Character</th>
<th>Unicode</th>
</tr>
</thead>
<tbody>
<tr>
<td>t</td>
<td>U+0074, Latin Small Letter T</td>
</tr>
<tr>
<td>ø</td>
<td>U+00F5, Latin Small Letter O with Tilde</td>
</tr>
<tr>
<td>m</td>
<td>U+006D, Latin Small Letter M</td>
</tr>
<tr>
<td>å</td>
<td>U+00E4, Latin Small Letter A with Diaeresis</td>
</tr>
<tr>
<td>s</td>
<td>U+0073, Latin Small Letter S</td>
</tr>
<tr>
<td>j</td>
<td>U+006A, Latin Small Letter J</td>
</tr>
<tr>
<td>ò</td>
<td>U+00F3, Latin Small Letter O with Acute</td>
</tr>
<tr>
<td>n</td>
<td>U+006E, Latin Small Letter N</td>
</tr>
<tr>
<td>é</td>
<td>U+00E9, Latin Small Letter E with Acute</td>
</tr>
<tr>
<td>s</td>
<td>U+0073, Latin Small Letter S</td>
</tr>
</tbody>
</table>

The list of supported fields will change. Implementers are encouraged to silently ignore fields containing an unrecognized key.
The order of fields contained in each log line will change. Implementers are encouraged to parse fields using methods that do not rely on specific ordering.

Category Codes

The following table explains the values used with the `cat` key. The $n$ indicates the risk level: 0=unclassified, 1=trusted, 2=low, 3=medium, and 4=high.

<table>
<thead>
<tr>
<th>Category ID</th>
<th>User-visible category name</th>
<th>Category ID</th>
<th>User-visible category name</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0n00000000</td>
<td>Uncategorized</td>
<td>0x2n0000001C</td>
<td>Kid's Sites</td>
</tr>
<tr>
<td>0x2n00000001</td>
<td>Adult/Sexually Explicit</td>
<td>0x2n0000001D</td>
<td>Motor Vehicles</td>
</tr>
<tr>
<td>0x2n00000002</td>
<td>Advertisements &amp; Pop-Ups</td>
<td>0x2n0000001E</td>
<td>News</td>
</tr>
<tr>
<td>0x2n00000003</td>
<td>Alcohol &amp; Tobacco</td>
<td>0x2n0000001F</td>
<td>Peer-to-Peer</td>
</tr>
<tr>
<td>0x2n00000004</td>
<td>Arts</td>
<td>0x2n00000020</td>
<td>Personals and Dating</td>
</tr>
<tr>
<td>0x2n00000005</td>
<td>Blogs &amp; Forums</td>
<td>0x2n00000021</td>
<td>Philanthropic &amp; Professional Orgs.</td>
</tr>
<tr>
<td>0x2n00000006</td>
<td>Business</td>
<td>0x2n00000022</td>
<td>Phishing &amp; Fraud</td>
</tr>
<tr>
<td>0x2n00000007</td>
<td>Chat</td>
<td>0x2n00000023</td>
<td>Photo Searches</td>
</tr>
<tr>
<td>0x2n00000008</td>
<td>Computing &amp; Internet</td>
<td>0x2n00000024</td>
<td>Politics</td>
</tr>
<tr>
<td>0x2n00000009</td>
<td>Criminal Activity</td>
<td>0x2n00000025</td>
<td>Proxies &amp; Translators</td>
</tr>
<tr>
<td>0x2n0000000A</td>
<td>Downloads</td>
<td>0x2n00000026</td>
<td>Real Estate</td>
</tr>
<tr>
<td>0x2n0000000B</td>
<td>Education</td>
<td>0x2n00000027</td>
<td>Reference</td>
</tr>
<tr>
<td>0x2n0000000C</td>
<td>Entertainment</td>
<td>0x2n00000028</td>
<td>Religion</td>
</tr>
<tr>
<td>0x2n0000000D</td>
<td>Fashion &amp; Beauty</td>
<td>0x2n00000029</td>
<td>Ringtones/Mobile Phone Downloads</td>
</tr>
<tr>
<td>0x2n0000000E</td>
<td>Finance &amp; Investment</td>
<td>0x2n0000002A</td>
<td>Search Engines</td>
</tr>
<tr>
<td>0x2n0000000F</td>
<td>Food &amp; Dining</td>
<td>0x2n0000002B</td>
<td>Sex Education</td>
</tr>
<tr>
<td>0x2n00000010</td>
<td>Gambling</td>
<td>0x2n0000002C</td>
<td>Shopping</td>
</tr>
<tr>
<td>0x2n00000011</td>
<td>Games</td>
<td>0x2n0000002D</td>
<td>Society &amp; Culture</td>
</tr>
<tr>
<td>0x2n00000012</td>
<td>Government</td>
<td>0x2n0000002E</td>
<td>Spam URLs</td>
</tr>
<tr>
<td>0x2n00000013</td>
<td>Hacking</td>
<td>0x2n0000002F</td>
<td>Sports</td>
</tr>
<tr>
<td>0x2n00000014</td>
<td>Health &amp; Medicine</td>
<td>0x2n00000030</td>
<td>Spyware</td>
</tr>
<tr>
<td>0x2n00000015</td>
<td>Hobbies &amp; Recreation</td>
<td>0x2n00000031</td>
<td>Streaming Media</td>
</tr>
<tr>
<td>0x2n00000016</td>
<td>Hosting Sites</td>
<td>0x2n00000032</td>
<td>Tasteless &amp; Offensive</td>
</tr>
<tr>
<td>0x2n00000017</td>
<td>Illegal Drugs</td>
<td>0x2n00000033</td>
<td>Travel</td>
</tr>
<tr>
<td>0x2n00000018</td>
<td>Infrastructure</td>
<td>0x2n00000034</td>
<td>Violence</td>
</tr>
<tr>
<td>0x2n00000019</td>
<td>Intimate Apparel &amp; Swimwear</td>
<td>0x2n00000035</td>
<td>Weapons</td>
</tr>
<tr>
<td>0x2n0000001A</td>
<td>Intolerance &amp; Hate</td>
<td>0x2n00000036</td>
<td>Web-based email</td>
</tr>
<tr>
<td>0x2n0000001B</td>
<td>Job Search &amp; Career Development</td>
<td>0x2n10000037</td>
<td>Custom</td>
</tr>
</tbody>
</table>

Sandbox codes

The following table explains the values used with the `sandbox` key.
<table>
<thead>
<tr>
<th>Sophos log</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sandbox=-</td>
<td>Engine reports sandboxing is not needed.</td>
</tr>
<tr>
<td>sandbox=1</td>
<td>Engine reports sandboxing is needed, file is not sent for analysis.</td>
</tr>
<tr>
<td>sandbox=2</td>
<td>File is sent to cloud to be analyzed</td>
</tr>
<tr>
<td>sandbox=3</td>
<td>Sandbox fast response: file is clean.</td>
</tr>
<tr>
<td>sandbox=4</td>
<td>Sandbox cloud response: file is clean.</td>
</tr>
<tr>
<td>sandbox=-1</td>
<td>Sandbox fast response: file is malicious.</td>
</tr>
<tr>
<td>sandbox=-2</td>
<td>Sandbox fast response: error occurred.</td>
</tr>
<tr>
<td>sandbox=-3</td>
<td>Sandbox cloud response: file is malicious.</td>
</tr>
<tr>
<td>sandbox=-4</td>
<td>Sandbox cloud response: error occurred.</td>
</tr>
</tbody>
</table>

**Related tasks**

Automating Backups (page 120)
E Copyrights and Trademarks

Sophos Web Appliance and Sophos Management Appliance Copyright © 2000-2016 Sophos Limited. All rights reserved.

Sophos and Sophos Anti-Virus are registered trademarks of Sophos Limited.

The Sophos Web Appliance and Sophos Management Appliance are licensed in accordance with the terms of the Sophos Appliance License Agreement. A copy of this license agreement can be found at http://www.sophos.com/legal.

This Sophos appliance includes or may include:

- Software developed by the Apache Software Foundation (http://www.apache.org/). A copy of the license agreement for this software can be found at www.apache.org/licenses/LICENSE-2.0.txt.

- Software originally written by Laurent Bedubourg. Copyright © 2004-2005 Laurent Bedubourg.


- Software originally written by David Turner, Robert Wilhelm, and Werner Lemberg. Portions of this software are copyright © 2008 The FreeType Project www.freetype.org. All rights reserved.


- Software originally written by Thomas G. Lane. This software is based in part on the work of the Independent JPEG Group.


- Software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

- Portions copyright © 1999-2008 The PHP Group. All rights reserved.

- Software originally written by Victor A. Abell. Copyright 1994 Purdue Research Foundation, West Lafayette, Indiana 47907. All rights reserved.

- Software originally written by Janek Schleicher. Copyright © 2002 Janek Schleicher.

- Software originally written by Julian R Seward.

- Software originally written by Henry Spencer. Copyright © 1986 by University of Toronto.

- Cryptographic software written by Eric A. Young and software written by Tim J. Hudson.


- Software originally written by Lennart Poettering. Copyright © 2004 Lennart Poettering.


Permission to use, copy, modify, and distribute this software and its documentation for any purpose with or without fee is hereby granted, provided that the above copyright notice appears
in all copies and that both the copyright notice and this permission notice appear in supporting
documentation, and that the name University of Delaware not be used in advertising or publicity
pertaining to distribution of the software without specific, written prior permission. The University
of Delaware makes no representations about the suitability this software for any purpose. It is
provided "as is" without express or implied warranty.

- Software originally written by Marc Alexander Lehmann, Copyright © 2007 Marc Alexander
  Lehmann.

License: Redistribution and use in source and binary forms, with or without modification, are
permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions
  and the following disclaimer.

- Redistributions in binary form must reproduce the above copyright notice, this list of
  conditions and the following disclaimer in the documentation and/or other materials provided
  with the distribution.

This software is provided by the copyright holders and contributors "as is" and any express
or implied warranties, including, but not limited to, the implied warranties of merchantability
and fitness for a particular purpose are disclaimed. In no event shall the copyright owner or
contributors be liable for any direct, indirect, incidental, special, exemplary, or consequential
damages (including, but not limited to, procurement of substitute goods or services; loss of use,
data, or profits; or business interruption) however caused and on any theory of liability, whether
in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the
use of this software, even if advised of the possibility of such damage.

- Software licensed in accordance with Oracle’s Berkeley DB open source license. Source code
  for the Debian Linux packages that rely on Oracle’s Berkely DB product, as well as the applicable
distribution of the Oracle Berkeley DB packages, are available upon request via mail order by
submitting a request to Sophos; via email to wsasupport@sophos.com; or via the web at http://

- Some software programs that are licensed (or sublicensed) to the user under the GNU General
  Public License (GPL) or other similar Free Software licenses, which, among other rights, permit
the user to copy, modify and redistribute certain programs, or portions thereof, and have access
to the source code. The GPL requires for any software licensed under the terms of the GPL,
which is distributed in an executable binary format, that the source code for such software
also be made available to the users of the binary form. For any such software covered under
the GPL, the source code is available via mail order by submitting a request to Sophos; via
email to wsasupport@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

- Some libraries that are licensed (or sublicensed) to the user under the GNU Lesser General Public
License (LGPL) using a suitable shared library mechanism for linking with such libraries. A copy of
the license agreement for any such included software can be found at http://www.gnu.org/licenses/
lGPL.html.

- Other software programs whose copyright notices are included within the source code for such
  programs in accordance with their license terms.
The OpenLDAP Public License
Version 2.8, 17 August 2003

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions in source form must retain copyright statements and notices,

2. Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution, and

3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time. Each revision is distinguished by a version number. You may use this Software under terms of this license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission. Title to copyright in this Software shall at all times remain with copyright holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Copyright 1999-2003 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved. Permission to copy and distribute verbatim copies of this document is granted.
F Contacting Sophos

Sophos Technical Support

If you encounter a problem with your Sophos product, or if it does not function as described in the documentation, contact Sophos Technical Support: http://www.sophos.com/support/

Corporate Contact Information

To contact your local Sophos office, see: http://sophos.com/companyinfo/contacting/
G Glossary

G.1 Active Directory

Microsoft’s implementation of LDAP (Lightweight Directory Access Protocol) on Windows. Active Directory provides LDAP-like directory services for managing identities and permissions of users throughout a network. Active Directory is a hierarchical, object-oriented database in which each object represents a single entity (for example, a user or group).

G.2 adware

Software that displays advertising in your system’s GUI (graphical user interface). Adware is often installed unknowingly by someone who is downloading and installing free software.

G.3 certificate

Certificates used by the appliance are public key certificates known as X.509 certificates. These encryption keys are associated with a specific identity or organization, and they allow the identity of the certificate holder to be verified. Identity verification is an important component of ensuring secure communication. Without it, it is possible for even encrypted communication to be redirected or compromised by an untrustworthy third party.

Certificates include information such as the hostname they are to be used with, a digital signature from a certificate authority, a start date, and an expiry date. To be considered valid, a certificate must:

• not yet be expired.
• have a digital signature from a trusted certificate authority.
• have a hostname associated with it that matches the hostname of the machine that is using the certificate.

Note

If your web appliance has several hostnames associated with it, it is important that you ensure the hostname presented to other machines matches your certificate(s) exactly.

By default, the web appliance uses what is known as a self-signed certificate. A self-signed certificate is a certificate that has been signed by the creator of a certificate, rather than by a third-party CA. This can be useful for providing encryption functionality when verification of the host’s identity by an external CA is not needed. In this case, the host acts as its own CA. This can be the case when the web appliance needs to verify its identity to a limited set of hosts, such as communication within a company, or with business partners.
G.4 certificate authority

Certificate authorities are trusted third parties. They can be root authorities (i.e. explicitly trusted). They can have identities that can be verified by checking with other trusted certificate authorities (such as the root authorities). Or you can choose to designate a CA as trusted (such as an authority within your organization).

G.5 Classless Inter-Domain Routing

Classless Inter-Domain Routing (CIDR) is an internet address assignment and aggregation strategy. CIDR, pronounced “cider” or “cedar”, is a refinement to the way IP addresses are interpreted that replaces the previous generation of IP address syntax (the Class A, B, and C addressing scheme). It allows greater flexibility when dividing ranges of IP addresses into separate networks, thus providing more efficient use of increasingly scarce IPv4 addresses. The CIDR strategy is described in RFC 1519.

G.6 command and control center

A command and control center is a computer that controls a botnet. A command and control center (C&C or C2) is a computer that controls a botnet (a network of compromised computers). Some botnets use distributed command and control systems, making them more resilient. From the command and control center, hackers can instruct multiple computers to perform their desired activities. Command and control centers are often used to launch distributed denial-of-service attacks because they can instruct a vast number of computers to perform the same action at the same time.

G.7 eDirectory

A multi-platform server application from Novell that supports LDAP (Lightweight Directory Access Protocol). eDirectory is a hierarchical, object-oriented database that allows access to LDAP clients.

G.8 FTP-over-HTTP

A configuration to proxy browser-based connections to FTP sites.

“FTP-over-HTTP” refers to proxying browser-based connections to FTP sites. It is not related to FTP servers that provide HTTP front ends as an alternative (for example, as is done on many open source mirror sites). “FTP-over-HTTP” works as follows:

1. Configure your browser to use the web appliance for FTP.
   
   This will cause your browser to communicate to the proxy (web appliance) via HTTP for both HTTP and FTP requests.

2. Enter an ftp:// URL in your browser.

3. Your browser makes an HTTP connection to the proxy, requesting the ftp:// URL.

4. The web appliance makes an FTP connection to the site requested and retrieves the file or directory listing.
• If it is a directory listing, the web appliance decorates it with HTML and returns that to the browser.

• If it is a file, the web appliance scans it and returns it to the browser (a patience page is returned first if the download takes a long time).

If you do not configure your browser to use the web appliance for FTP, entering ftp:// URL requests will bypass the proxy, and your browser will communicate with the FTP server via the FTP protocol.

G.9 Group Policy Object

A collection of settings that defines user or computer settings for a group of users or computers. The settings stored in Group Policy Objects reference Active Directory units such as sites and domains.

G.10 group

List of users to which differentiated policy settings can be applied. Lists of users that the Sophos email and URL filtering products use as a basis for the policy settings that determine which filtering actions are performed for which users.

G.11 Kerberos

A network authentication protocol. Kerberos issues “tickets” that allow users to securely prove their identities.

G.12 latency

The time delay added to a page load or file download. The time delay between the moment something is initiated, such as a URL request made in a user’s browser, and the moment its first effect begins, such as the moment when that URL first starts to load in the browser’s content pane.

G.13 malware

Malware includes viruses, worms, and Trojan horses. Malware, or malicious software, refers to programs that are designed to damage or disrupt a computer. Malware is generally installed without the user’s knowledge and describes various types of malicious code, including viruses, worms and Trojan horses.

G.14 network mask

Specifies which are the subnetwork and host parts of an IP address. Also known as a subnet mask, netmask or address mask, the network mask is used to specify which parts of the dotted quad of an IP address identify the subnetwork the host is on and which parts identify the host itself. Network masks are usually represented in either dotted quad notation (for example, 255.255.255.0) or CIDR notation (for example, 192.0.2.0/24).
G.15 NT LAN Manager

A Microsoft IIS web server integrated authentication method.

(Also known as Windows NT Challenge/Response authentication; recently updated and renamed Integrated Windows Authentication) NTLM is a Microsoft IIS (Internet Information Services) integrated authentication method. NTLM is used by such Microsoft applications as Active Directory and Sharepoint.

Note that NTLM has the following restriction: NTLM can get past a firewall, but is generally stopped by proxies because NTLM is connection-based, and proxies do not necessarily keep connections established. Applications such as Sharepoint inside an enterprise that require Integrated Windows Authentication (which includes NTLM authentication and Kerberos v5 authentication) should add the local IP address of servers hosting these applications to the browser’s proxy exemption list.

G.16 phishing

Acquisition of identity/passwords by false bank emails and websites. (Also known as carding and spoofing) Attempting to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an apparently official electronic communication, such as an email or an instant message. The term phishing arises from the use of increasingly sophisticated lures to “fish” for users’ financial information and passwords. Sophos email and URL filtering products are configured by default to detect phishing schemes.

G.17 policy

The web appliance’s URL filtering rules.

The appliance provides configuration options that enable you to set whether you will Allow user access to each of over 50 categories of URLs, and, if access is allowed, whether you want to Warn users that they have requested a URL that violates your organization’s browsing policy. This set of options constitutes the policy.

You can set the default policy on the Configuration > Group Policy > Default Policy page. You can set a special hours policy (for example, to allow less restrictive browsing during lunch hour and after regular business hours) on the Configuration > Group Policy > Special Hours page. Also, you can set numerous additional policies to grant groups or specified users extraordinary access, optionally for a limited time, on the Configuration > Group Policy > Additional Policies page.

G.18 potentially unwanted application

Potentially unwanted applications include spyware and adware.

Potentially unwanted applications (PUAs) are applications that, although not malicious, can affect performance of client machines or potentially introduce security and related risks into your organization. Some applications that may be classified as PUAs may have legitimate uses, but these should be installed only with the system administrator’s knowledge and at his or her discretion.

Sophos is an active member of the Anti Spyware Coalition (ASC). When classifying PUAs, SophosLabs uses the following broad definitions, which are derived from the ASC risk model.
Adware
- Application that often has the primary function of delivering advertising to the desktop.
- Software that tracks internet usage and/or collects potential Personally Identifiable Information (PII) data from a user’s computer for the purposes of selling this information, or associated information, to a third party.
- Usually unknowingly installed on systems without specific user interaction.
- Includes Advertising Display Software and Tracking Software as defined by ASC.

System Monitors
- Commercially or freely available software whose primary function is to monitor the use of the local computer.
- Commonly marketed as PC surveillance software.
- Usually installed with user interaction.
- Of interest to corporate networks to ensure that users do not make unauthorized use of such software.
- Applications for which some customers may want to authorize use.
- Include Tracking Software as defined by ASC.

Remote Administration Tools
- Commercial or freely available tools used for remotely accessing and controlling one or more computers.
- Usually installed and used with user interaction.
- Occasionally used legitimately in small businesses.
- Include Remote Control Software as defined by ASC that is not classified as malware.

Dialers
- Any application whose primary function is to dial a premium rate phone number.
- Can be installed without specific user interaction.
- Include Dialing software as defined by ASC.

Hacking Tools
- Applications that can be used to assist hackers to gain entry to a network, computer, or software program.
- Examples are port scanners, password crackers, and vulnerability scanners.
- Usually installed and used with user interaction.
- Have been known to be used in conjunction with malicious software.
- Can be used legitimately for assessing network security.
- Include Security Analysis Software as defined by ASC.

Other PUAs
- Include any software not categorized above that may be considered by a network administrator to be unsuitable for an enterprise network. For example:
  - Adware-bundled, -supported, or -affiliated software, such as P2P applications.
  - Trial versions of server applications that are commonly used in a malicious context.
  - Chat clients commonly used in a malicious context.
— Server applications such as FTP, Telnet, IRC, or SMTP commonly used in a malicious context.

**G.19 proxy**

A secure server through which internal clients connect to the internet. A service that allows clients to make indirect network connections to other networks, for example, an HTTP proxy for use by hosts with no direct connection to the internet. A client connects to the proxy server, then requests a connection, file, or other resource available on a different server. The proxy provides the resource either by connecting to the specified server or by serving it from a cache. In some cases, the proxy may alter the client’s request or the server’s response for various purposes. A proxy server can also serve as a firewall.

**G.20 Proxy Automatic Configuration**

PAC files script appropriate proxy routing by URL characteristics.

Proxy Automatic Configuration (PAC) is a way to automatically set the appropriate proxy for a given URL request. This is done by developing a JavaScript file with a `.pac` extension that is used by users’ browsers and which evaluates their URL requests and forwards each request to the appropriate proxy. This approach has the advantage of being completely within the control of network administrators and of operating transparently from the perspective of end users. Explaining how to create, implement and maintain PAC files is beyond the scope of this documentation. For details on the development and use of PAC files, you can start with Mozilla.org’s [PAC End User Guide](https://developer.mozilla.org/en-US/docs/Web/HTTP/PAC_EndUserGuide) for Firefox and Microsoft’s [Automatic Discovery of Firewall and Web Proxy Clients](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc746623(v=ws.10)) page.

**G.21 SophosLabs**

A 24/7 network of skilled analysts who respond to evolving security threats. The SophosLabs organization is a global network of highly skilled analysts who have been protecting businesses from known and emerging threats for more than 20 years. Focused on rapidly evolving threats like viruses, spam, phishing schemes, spyware and other malware, SophosLabs provides both proactive and rapid solutions for all Sophos customers. Our global network of threat analysis centers ensures Sophos is able to respond to new threats without compromise, achieving the highest levels of customer satisfaction and protection in the industry.

**G.22 spyware**

Software that covertly gathers information on users’ internet activities. Spyware gathers user information through the user’s internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the internet. Once installed, the spyware monitors user activity on the internet, and transmits that information in the background to someone else.

**G.23 Trojan**

A seemingly legitimate computer program designed to do damage. A seemingly legitimate computer program that has been intentionally designed to disrupt and damage computer activity. Trojans
are sometimes used in conjunction with viruses. A backdoor Trojan is a program that allows other computer users to gain access to your computer across the internet.

G.24 virus

Often viruses will disrupt computer systems or damage the data they contain. A virus requires a host program and will not infect a computer until it has been run. Some viruses spread across networks by making copies of themselves or may forward themselves via email. The term 'virus' is often used generically to refer to both viruses and worms.

G.25 Web Cache Communication Protocol

WCCP provides a way to redirect web traffic in real time on networks that use Cisco routers and switches. WCCP allows for clustering, failover, load balancing and the transparent deployment of web proxy and security products without additional network configuration or hardware.

G.26 worm

Unlike a virus, it has the ability to self-replicate and often will use email and the internet to spread.