SOPHOS

Security made simple.

Sophos Management Appliance Configuration Guide

Product Version 4.3

Contents

1 Copyrights and Trademarks

2 Introduction

The purpose of this guide is to:

- continue assisting you with the installation and configuration of your Sophos appliance after you have completed the procedures described in the *Setup Guide*, which provides physical (rack) installation instructions for your Sophos appliance.
- provide you with pre-configuration planning information about the deployment of your appliance in your network.
- assist you with the basic configuration steps in the Sophos appliance setup wizard.
- List some essential post-configuration tasks that you should perform.

This guide assumes that you have already completed all of the steps in the *Setup Guide*.

While this guide contains enough information to prepare your appliance for live web traffic, it should not be considered a substitute for the *Online Help*, which contains complete instructions on configuring and managing your appliance. You can access the appliance's *Online Help* from the administrative web interface, and it also can be found on the Sophos Web Appliance Documentation site.

The Sophos Web Appliance Documentation site (http://wsa.sophos.com/docs/wsa/) provides access to the following manuals for the appliance:

- The Setup Guide (PDF) provides hardware installation instructions for the Web and Management Appliances.
- The SWA Configuration Guide (PDF) provides descriptions of the network deployment options and step-by-step instructions for the initial software installation and configuration of a Sophos Web Appliance.
- The SMA Configuration Guide (PDF) provides step-by-step instructions for the software side of an initial installation and configuration of a Sophos Management Appliance.
- The Online Help provides complete instructions on configuring and managing the Web and Management Appliance.
- The Release Notes list the New Features and the Resolved Issues for each release of the Web Appliance and Management Appliance software, as well as the Known Issues and Limitations for these products.

The Web Appliance Knowledge Base (http://www.sophos.com/support/knowledgebase/topics/1289/1293) is a collection of articles dealing with a variety of issues relating to the Web and Management Appliance, including:

- Common questions received by Sophos Web Appliance and Management Appliance Support.
- Technical issues that are not commonly encountered by Web Appliance and Management Appliance administrators.
- Technical issues that involve third-party hardware or software products that affect Web Appliance and Management Appliance deployment or operations.

The appliance setup wizard guides you through the processes of:

- Activating the Appliance
- Setting the Time Zone
- Configuring the Network Interface
- Setting the Hostname
- Testing Network Connectivity
- Registering and Updating your Appliance
- Configuring Central Management
- Setting Productivity Controls
- Setting the Alerts Recipients
- Setting your Organization's Support Contact Information

Although the wizard allows you to configure the appliance’s essential components, many additional configuration options are available in the administrative web interface, which launches automatically when you complete the wizard. The "Post-Installation Configuration" section of this guide describes the configuration options that you should set once installation is complete.

3 Features

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.

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.

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.

4 Integrating with Sophos Email Products

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

- To configure your Sophos Web or Management Appliance to route email via your Sophos Email Appliance:

  a) On your Sophos 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 Sophos 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 or Management Appliance to route email via your Sophos PureMessage for UNIX server:

  a) On your Sophos Web or Management Appliance, on the **Configuration** > **Network** > **Hostname** page, enter the IP address of your 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 Sophos 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 Sophos 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 Sophos 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 for UNIX server to access the internet via your Sophos Web Appliance:

  If you are using Active Directory, you must exclude your PureMessage server from authentication.

  a) On your Sophos Web Appliance, on the **Configuration** > **System** > **Connection Profiles** page, create a connection profile that includes the IP address of your PureMessage for UNIX server.

  b) On your Sophos 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 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

5 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 Sophos Web Appliances grouped together by a common Sophos 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.

Model	Processors	Memory (RAM)
WS100	dual-core, light-capacity	2 GB
WS500	dual-core, medium-capacity	2 GB
WS1000	dual-core, high-capacity	4 GB
WS1100	quad-core, high-capacity	8 GB
SM2000	quad-core, high-capacity	8 GB
SM5000	quad-core, high-capacity	8 GB
WS5000	quad-core, high-capacity	16 GB

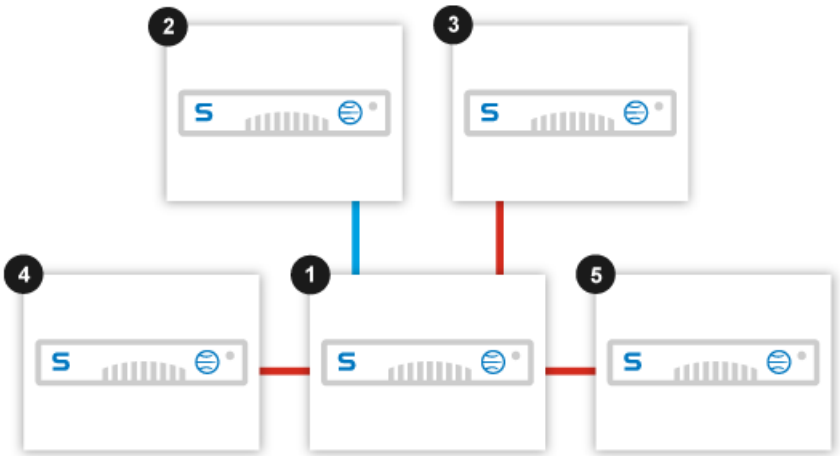
Note: The number of end users that an appliance can handle is determined by the frequency at which your organization's users browse the web throughout the day and the volume and nature of the files that they download and access. The number of users that a grouped deployment supports depends on the number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

Scaling and Deployment

Your organization can either grow to require more than one appliance, or—if your organization is a new Sophos 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

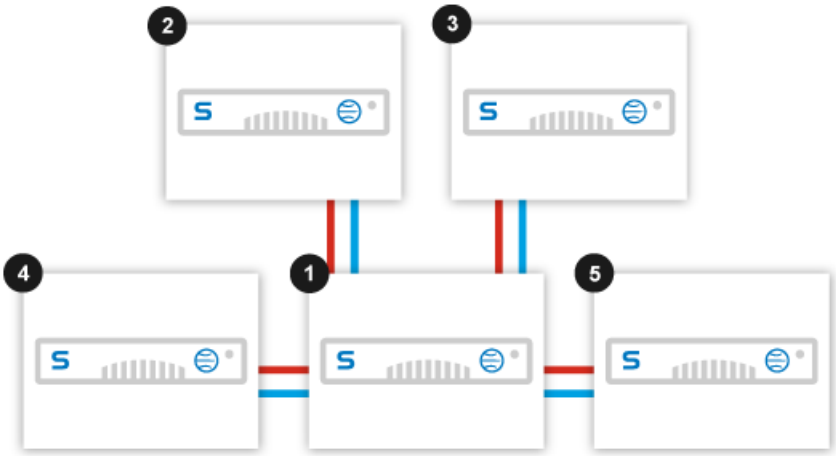
1. Join your organization's original, already-configured Web Appliance (2) to the Management Appliance (1).

   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 (1). This can be done in any order, whether the new Web Appliances are in the same location (3) or in remote locations ((4) and (5)).

   The new Web Appliances that are joined—(3), (4), and (5)—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 2 and 3 or in remote locations 4 and 5, are joined (in any order) to the Management Appliance 1 (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 1 and distributed to the Web Appliances—2, 3, 4, 5—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

Sophos Web Appliances can operate in standalone or joined mode. You can also join a Sophos 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.”

6 Initial Configuration

This section describes the steps required to register your appliance with Sophos and perform the initial activation and configuration of your appliance. You begin by activating your appliance, after which the setup wizard launches.

In the wizard, you perform the required networking configuration. The appliance then registers with Sophos and retrieves the latest software updates and threat definitions. Next, you set more of the initial configuration options for the appliance and, upon completion, the Dashboard page of the appliance's administrative web interface is launched.

Note: You can modify all of the configuration options set in the wizard from within the appliance's administrative web interface.

To prepare for installation and initial configuration:

1. On your organization's firewall, configure access to the following ports for external and internal connections for the appliance.

   External Connections

   These services are typically used for connections between your Web Appliance(s) and locations outside of your organization's network.

Port	Function	Service	Protocol	Connection
22	Remote assistance	SSH	TCP	Outbound from appliance to sophos.com
22	Central configuration, status and reporting	SSH	TCP	Outbound from Web Appliance to Management Appliance (if not collocated)
25	Remote assistance notification	SMTP	TCP	Outbound from appliance to sophos.com
80	Outbound network web traffic	HTTP	TCP	Outbound from appliance to internet
123	Network time synchronization	NTP	UDP	Outbound from appliance to internet
443	Outbound network web traffic	HTTPS	TCP	Outbound from appliance to internet

   Note: Opening ports 80 and 443 is a standard best practice. However, certain web sites may also require other ports to be opened.

Internal Connections

These services are typically used for connections within your organization's network and your Web Appliance(s) or between appliances themselves, if you have multiple appliances.

Port	Function	Service	Protocol	Connection
21	Backups using passive FTP	FTP	TCP	Outbound from appliance to FTP server
22	Central configuration, status and reporting	SSH	TCP	Outbound from Web Appliance to Management Appliance (if collocated)
53	DNS queries	DNS	UDP	Outbound from Appliance to LAN
80	administrative web interface	HTTP	TCP	Inbound from LAN to appliance
88	Kerberos authentication	KERBEROS	TCP/UDP	Inbound/outbound between appliance and AD server
139	MS NetBIOS session	NETBOSSSN	TCP/UDP	Inbound/outbound between appliance and AD server
389	Directory services synchronization	LDAP	TCP/UDP	Inbound/outbound between appliance and AD server
443	administrative web interface	HTTPS	TCP	Inbound from LAN to appliance
445	MS server message block	SMB	TCP/UDP	Inbound/outbound between appliance and AD server
636	LDAP synchronization	LDAPS	TCP	Inbound/outbound between appliance and eDirectory server
3268	MS AD Global Catalog synchronization	MSGC	TCP/UDP	Inbound/outbound between appliance and AD server
8080	Proxy (end user web browsing)	HTTP/HTTPS	TCP	Inbound/outbound between LAN and appliance

2. Gather the information that you will need to perform the installation and initial configuration of the appliance.

You will need the following information:

- The email message from Sophos that contains the activation code for your appliance.
- IP address, network mask, and fully qualified domain name for the appliance.
- IP address of the default gateway (the router on your LAN).
- IP address of the DNS servers.
- The email addresses of those in your organization who will receive alerts.
- The contact information for the person in your organization thatSophos should notify about support issues for your appliance.

Note: Ensure that you have completed all of the steps in the*Setup Guide*, opened the indicated ports, and gathered the information listed above before you begin the appliance setup wizard. Running the setup wizard is documented in the following sections of this guide.

6.1 Activating the Appliance

To activate your appliance:

1. Prepare the laptop or other system that you will connect directly to the appliance by setting the subnet mask to 255.255.255.0 and the IP address to 172.24.24.1.
2. Connect your laptop via an ethernet cable to the **Config** port on the rear of the appliance.
3. Using a supported browser, connect to `https://172.24.24.173`.

   Important: You may need to add this address to Internet Explorer's Trusted Sites. When prompted to "continue to this website", accept the invalid certificate.

4. Enter the activation code contained in an email message from Sophos, or if you are installing the appliance as a 30-day trial, click **Try Now**.

   The login page is displayed:

5. Set and confirm an administrator password of at least 6 characters.

6. Click **Login**.

   The **End User License** page is displayed. Optionally, print the end user license agreement by clicking **Print** to display a printable version of the license agreement. Use your browser's built-in options to print the agreement.

   Important: Do not interrupt the installer once it begins. Doing so can damage the system to the point that it may require return to the factory to be re-imaged.

7. Read the License Agreement fully (scrolling to the bottom of the license agreement activates the "accept" option below), select **I accept the terms of the License Agreement**, and click **Next**.

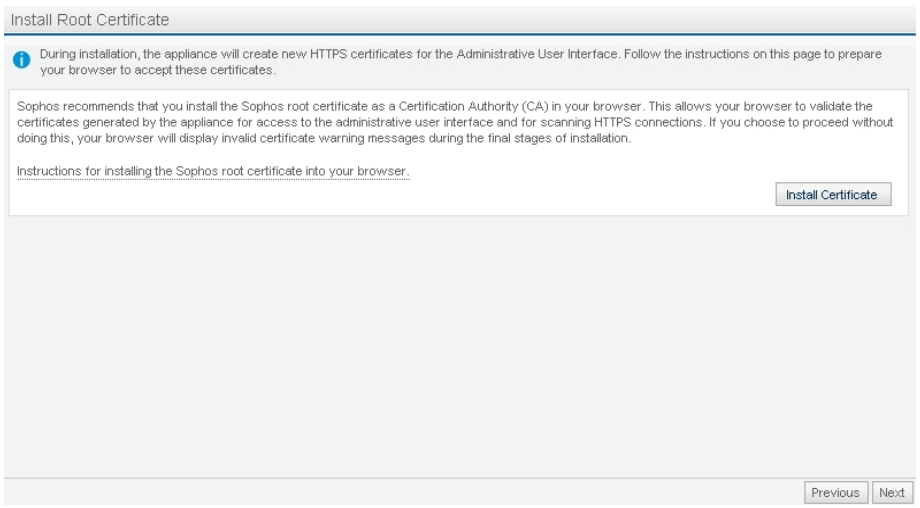
   The **3rd Party Notice** page is displayed. You may print the notice by clicking **Print**.

8. Read the 3rd party notice fully, and click **Next** to proceed to the Install Root Certificate on page 16 page of the wizard.

6.2 Install Root Certificate

To install the root certificate:

The root certificate must be installed in the browser from which you will access the appliance's administrative web interface in order to use this administrative interface. This certificate can always be added later, but choosing not to install the root certificate at this stage will result in invalid certificate warning messages being displayed during the final stages of this setup wizard.



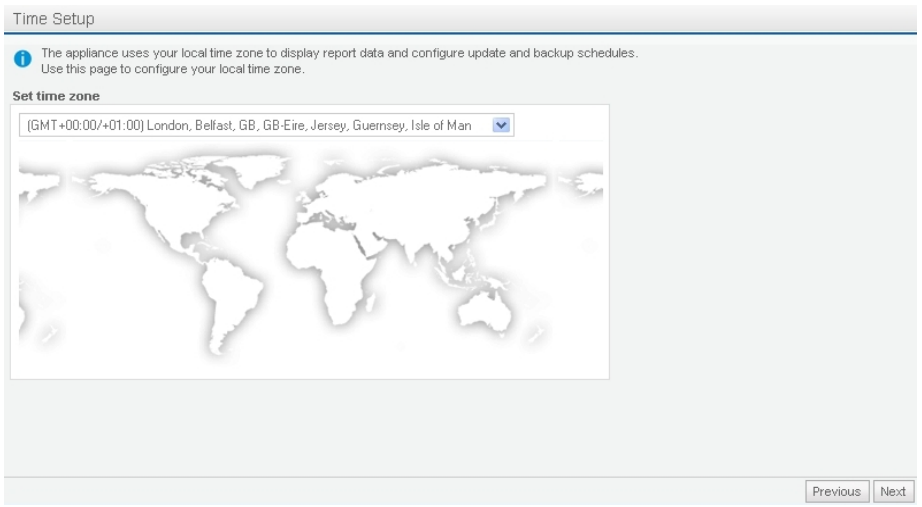
1. Click **Install Certificate**.

   For full instructions on installing the root certificate that are specific to your browser, click "**Instructions for installing the Sophos root certificate into your browser.**"

2. Click **Next** to proceed to the Time Zone on page 17 page of the wizard.

6.3 Time Zone

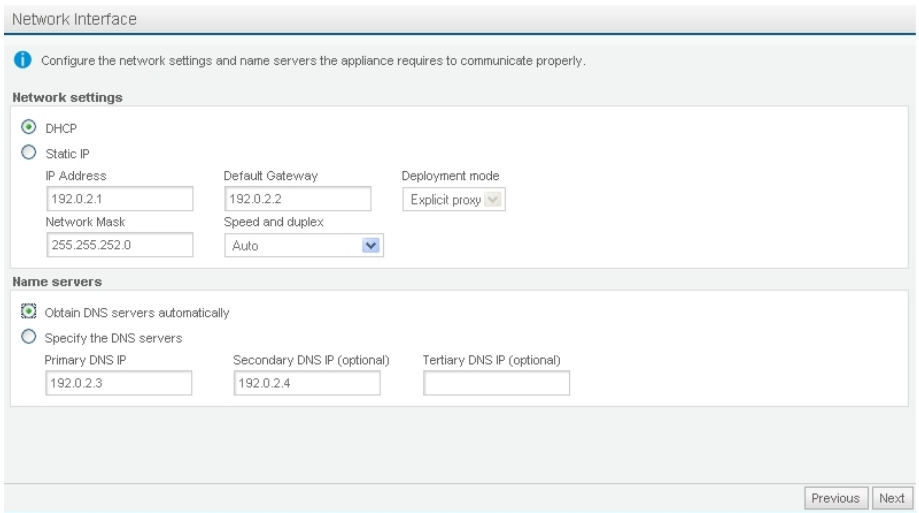
To set the time zone:



1. From the drop-down list, select the appropriate time zone for your region.
2. Click **Next** to proceed to the Network Interface on page 17 page of the wizard.

6.4 Network Interface

The appliance's network settings and name servers are configured on the **Network Interface** page of the wizard.



To configure network interface settings:

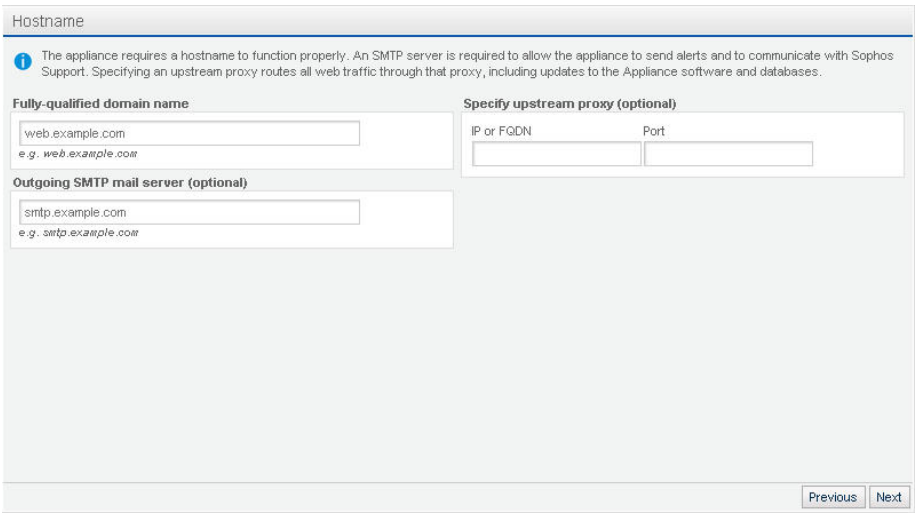
1. In the **Network settings** section, do one of the following:
   - *To configure network settings with DHCP*, accept the default **DHCP** option.
   - *To configure a static IP address*, select **Static IP** and configure the following:
     1. In the **IP Address** text box, enter the address for the appliance.
     2. In the **Network Mask** text box, enter the mask (for example, 255.255.0.0).
     3. In the **Default Gateway** text box, enter the address of the default gateway (that is, the router on your LAN).
     4. On the **Speed and duplex** drop-down list, accept the **Auto** option. (If you select another setting from the drop-down list, it must match the speed of your ethernet switch to ensure that the appliance operates correctly.)

2. In the **Name servers** section, do one of the following:
   - Select **Obtain DNS servers automatically**. (If you selected the **DHCP** option in the previous step, this option will be the only one available.)
   - Select **Specify the DNS servers**. Then, in the **Primary DNS IP** text box, enter a DNS IP address. Optionally, enter secondary and tertiary addresses.

3. Click **Next** to proceed to Hostname on page 18 configuration.

6.5 Hostname

You must assign a hostname for the appliance. Additionally, if you plan to connect to the internet through an upstream proxy server, you must assign a server address and port number for that server.



1. Configure your appliance's hostname by typing it in the **Fully qualified domain name** text box.

   Note: The length of the first element of the fully qualified domain name (the hostname) must be no more than 15 characters.

2. Optionally, set your outgoing mail server by typing the fully qualified domain name of your organization's outgoing SMTP mail server in the **Outgoing SMTP mail server (optional)** text box.

   This is required if your organization's firewall will not permit the appliance to send email directly to the internet. Email is used to send your remote assistance request and, optionally, alert notifications to Sophos.

3. Optionally, specify an upstream proxy by typing the IP address or the fully qualified domain name of the upstream proxy in the **Specify upstream proxy (optional)** section's **IP or FQDN** text box and typing the port number by which you access your organization's web proxy (usually 8080) in the **Specify upstream proxy (optional)** section's **Port** text box.

   Note: The currently supported upstream proxy configurations are:

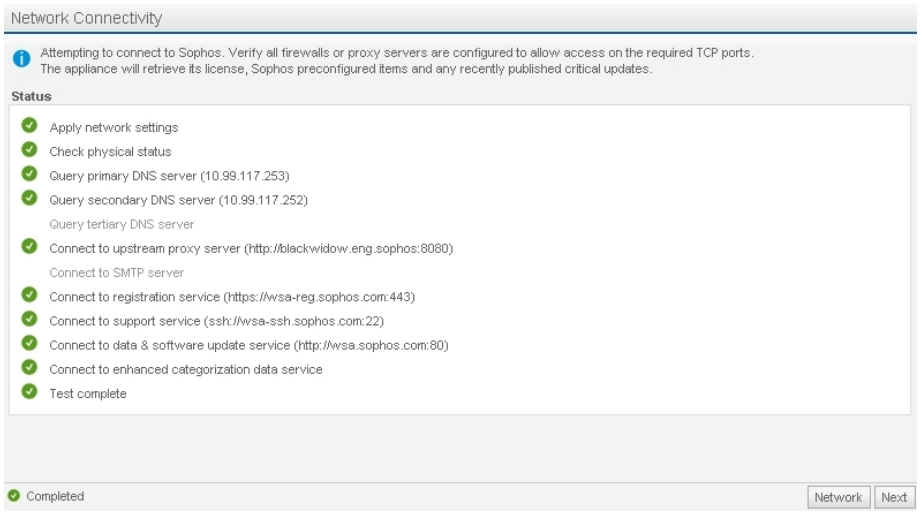
   - **Squid:** without user authentication.
   - **ISA Server 2006 Standard Edition:** in firewall and proxy mode without user authentication.

   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* or to the "Initial Configuration" page of this guide to review specific ports that the appliance uses for external and internal connections.

4. Click **Next** to proceed to Network Connectivity on page 19.

6.6 Network Connectivity

With network configuration complete, this page of the wizard applies and tests the appliance's network configuration and its connection to Sophos.



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 was successful.
- A yellow exclamation mark icon indicates that the test produced a warning.

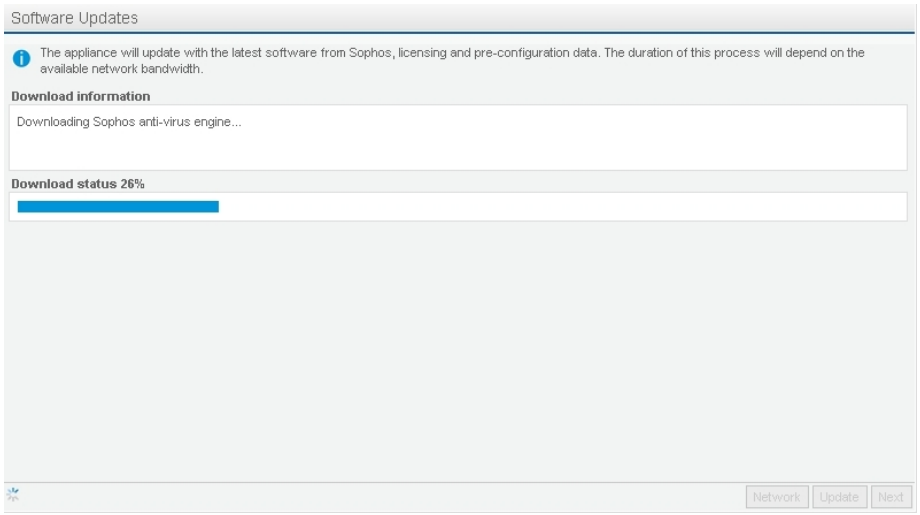
- A red "x" icon indicates that the test failed.

If you see any warning or error icons, click **Network Settings** to return to the **Network Interface** page, where you can correct the configuration.

When the test has completed successfully, click **Next** to proceed to Software Updates on page 20.

6.7 Register and Update

The appliance will now use the activation code to register with Sophos. Once registered, the appliance is authorized to receive threat definitions and software updates. The appliance will not begin registering and updating until you click **Update**.



To register and update the appliance:

1. Click **Update**.

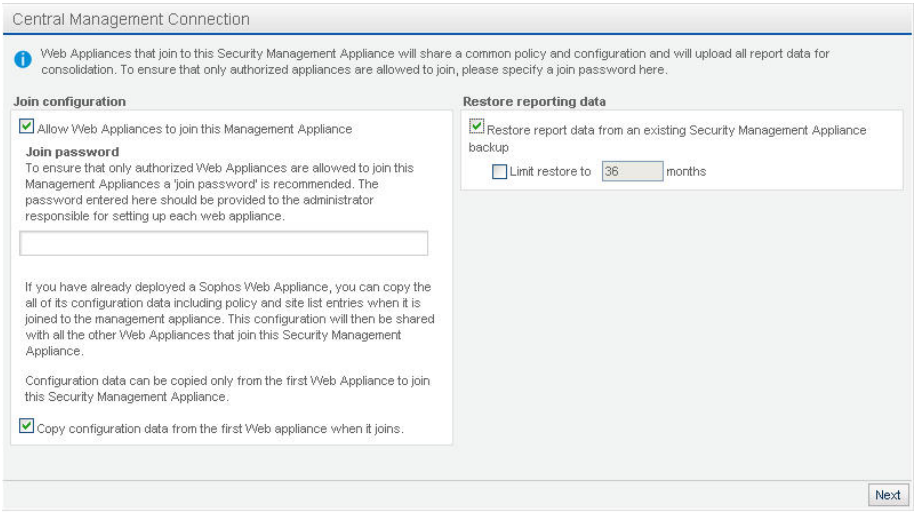
   The appliance registers with Sophos, updates the software, and updates the security and control data.

   Once updating is complete, the appliance may reboot.

2. When the appropriate message is displayed, click the **Next** button to proceed with the installation while the download continues in the background.

6.8 Central Management

The Management Appliance allows you to configure the way that it handles join requests from Web Appliances.



- To temporarily prevent Web Appliances from joining the Management Appliance:

  Clear the **Allow Web Appliance to join this Management Appliance** check box.

- To require joining Web Appliances to provide a password:

  Enter the password in the **Join password** text box.

- To prevent the Management Appliance from adopting the policies and configuration of the first Web Appliance that joins it:

  Clear the **Copy configuration data from the first Web Appliance when it joins** check box.

- To restore report data to the Management Appliance:

  Select the **Restore report data from an existing Sophos Management Appliance** check box.

- Once you have selected the option that you want, click **Next**.

  If you selected the **Restore report data from an existing Sophos Management Appliance** check box, proceed to Restore Reports.

  If you did not select the **Restore report data from an existing Sophos Management Appliance** check box, but you did select the **Copy configuration data from the first Web Appliance when it joins** check box, proceed to the Summary on page 25 page.

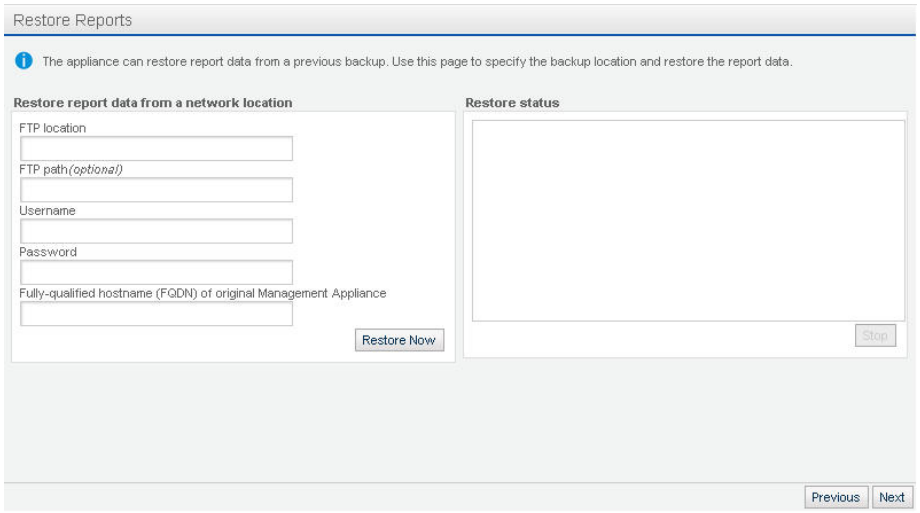
  If you did not select the **Restore report data from an existing Sophos Web Appliance** check box, and you cleared the **Copy configuration data from the first Web Appliance when it joins** check box, proceed to the Productivity Options on page 23 page.

Related tasks

Restore Reports on page 22

6.9 Restore Reports

You can only access this page if you selected the **Restore report data from an existing Sophos Management Appliance** check box on the **Central Management** page. This page of the Management Appliance setup wizard allows you to configure access to the FTP server to which you previously backed up report data.



1. In the **Restore report data from a network location** panel, fill in the following FTP server access and Management Appliance information:
   - **FTP location**: Enter the URL to the FTP server.
   - **FTP path (optional)**: Optionally, enter the path to the location of the backed up report data if this data is in a directory other than the home directory of the FTP user or the FTP server's root directory.
   - **Username**: The username of the FTP account used to back up the original report data.
   - **Password**: The password for the FTP user account that you entered in the **Username** text box.
   - **Fully-qualified hostname (FQDN) of original Management Appliance**: The hostname of the previous Management Appliance that originally backed up the report data that you now want to restore.
2. Click **Restore Now**.

   The report data restore process begins, with the status of that process displayed in the **Restore status** panel.
3. Optionally, click **Stop** if you want to halt the report restore process.

   The downloaded, or partially downloaded, backed up report data will be deleted if you choose to halt the process by clicking **Stop**.
4. Once the restore process has completed successfully, click **Next**.

If you selected the **Copy configuration data from the first Web Appliance when it joins** check box on the previous page, proceed to the Summary on page 25 page.

If you cleared the **Copy configuration data from the first Web Appliance when it joins** check box on the previous page, proceed to the Productivity Options on page 23 page.

Related tasks

Central Management on page 20

6.10 Productivity Options

The appliance uses categorizations of URLs to enforce your organization's user browsing policy. Use the **Productivity Options** page of the wizard to select how strict or lenient you want these settings to be.

To set the appliance's productivity filtering option:

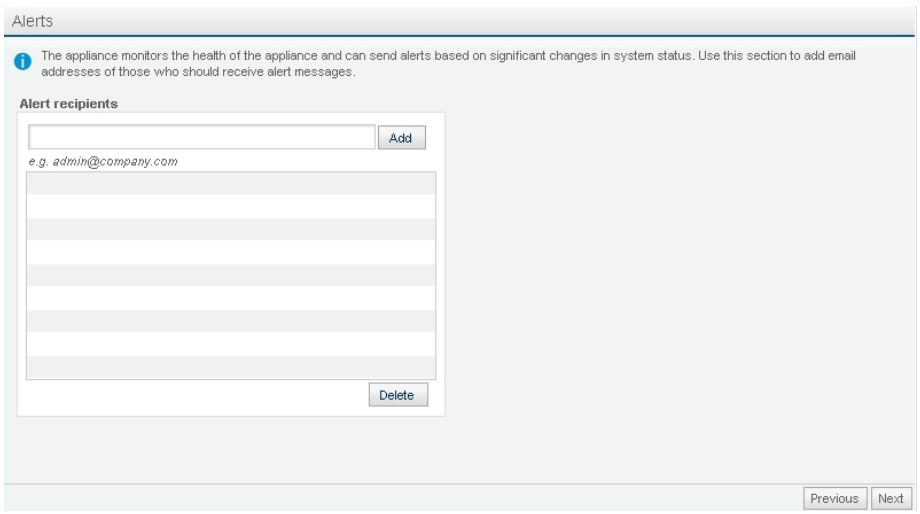
1. Select one of the **Productivity filtering options**.

   Generally, the top-most option is the most permissive, with successive options getting increasingly strict. The exception is the last option, which displays warning messages to users who try to access non-business related sites instead of blocking access to them. To see the details of what categories of sites are blocked, select an option and view the list of blocked categories in the **Description** information box.

2. Once you have selected the option, click **Next** to proceed to Alerts on page 23.

6.11 Alerts

Use the **Alerts** page of the wizard to set the email addresses of those in your organization who should receive alert messages from the appliance about significant changes to the appliance's system status. Critical and non-critical error alerts are configured separately on the **Support Contact** page of the wizard.



To configure the handling of system status alert email messages for the appliance:

1. Set the email address(es) for the recipient(s) of system alerts by entering the full email address of the intended recipient in the **Alert recipients** text box and clicking **Add**.

   The email address that you entered is added to the list below.

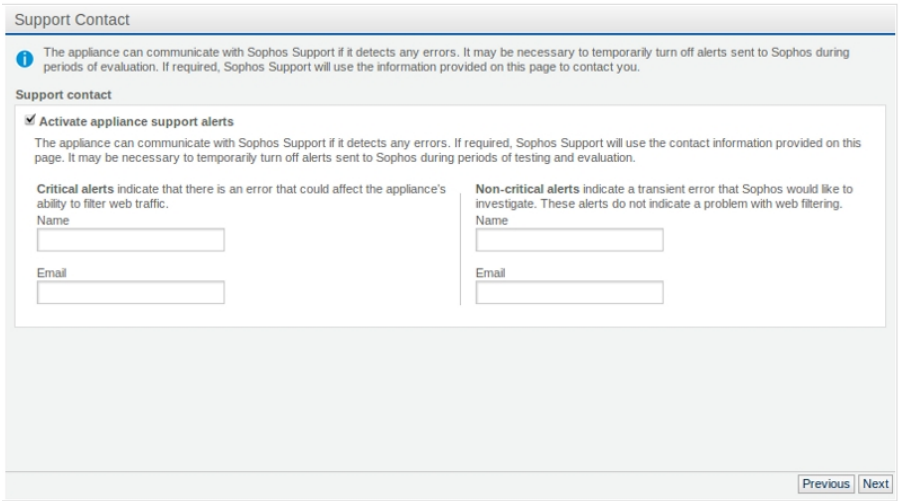
2. Optionally, remove an email address from the list of contacts by selecting the check box to the right of the email address that you want to remove from the list and clicking **Delete**.

   The selected email address is deleted from the list.

3. Once you have set the handling of the system status alerts, click **Next** to proceed to Support Contact on page 24, where you configure the names of people in your organization that Sophos Technical Support can contact if the appliance detects any errors.

6.12 Support Contact

The **Support Contact** page prompts you to provide information that Sophos Technical Support can use to contact the appropriate person in your organization if the appliance ever has a critical problem.



To provide contact information to Sophos Technical Support:

1. Select **Activate appliance support alerts**.
2. For **Critical alerts**, provide the **Name** and **Email** of the person who should receive these messages.
3. For **Non-critical alerts**, provide the **Name** and **Email** of the person who Sophos should contact.

   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.

4. Once you have set your support contact information, click **Next** to proceed to the configuration settings Summary on page 25.

6.13 Summary

The configuration **Summary** page displays an overview of all of your configuration settings that you can view or print before committing the changes.

To use the **Summary** page:

1. Scroll through the summary to read all of the configuration settings and confirm that they are all set as you want them.
2. If you choose to change any of the settings, repeatedly click **Previous** to return to the page required.

   The changes that you have made will persist as you navigate back and forth through the pages.

3. Optionally, once you have confirmed that all of the settings are as required, print the summary for your records and future reference by clicking **Print**.
4. Once you are satisfied that the configuration settings are all as required and you have printed the summary, click **Finish**.

   Your configuration settings are applied and the **Dashboard** page of the appliance's administrative web interface is displayed.

   This will also trigger the generation of a new hostname-specific site certificate, which may take as long as a minute or two.

   Note: URL data downloads begin in the **Software Updates** stage; however, this is a large list of sites, pages, and files, so the downloading is done in the background to speed up the setup process. If you click **Finish** on the **Summary** page before the data download is complete, an alert message will appear, warning you that this data has not yet finished downloading. You can proceed (click **OK**) without any problems, but it is important to understand that the full protection offered by the Web Appliance will not be available until the URL data download is complete.

   If you do proceed, the following indicators will show the state of the URL data download:

   - The System status in will be in a warning state (amber) until the data download is complete (although this may escalate to a critical state [red] if there are 6 or more download errors during the initial download).
   - The Dashboard's "URL test" will be unavailable (grayed out) until initial data download is complete.
   - The System status will change back to normal (green) when the download is complete.

5. Log out and disconnect the cable from the **Config** ethernet port and restore your laptop's previous LAN settings. Do not connect the “Config” port to your LAN.
6. Connect to the appliance through your organization's LAN via a web browser.

   The URL for your appliance should be:

   ```
   https://[appliance-hostname].[your-organization].[domain]/index.php
   ```

Related tasks

Post-Installation Configuration on page 27

7 Post-Installation Configuration

When the wizard closes, the **Dashboard** of the appliance's administrative web interface is displayed. There are still some important configuration tasks that should be completed that were not available in the wizard. These tasks are listed in the **Post installation** checklist on the **Configuration** home page.

7.1 Setting General Options

Note: On this page, the available features are:

- On a standalone Web Appliance: the **Cache settings**, **Additional Options**, **SophosLabs** , and **Logging mode** options.
- On a joined Web Appliance: the **Cache settings** options.
- On a Management Appliance: the **Options**, **SophosLabs** , and **Logging mode** options.

Use the **Configuration** > **Global Policy** > **General Options** page to set a variety of Web Appliance's policy-related filtering options.

- 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.

- To clear the cache, click **Clear Cache**.
- 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 (e.g. SafeSearch, YouTube Safety)** check box, and click **Apply**.

  Internet search engines such as Google, MSN, bing.com, and Yahoo! offer their users an option to filter out search results that contain inappropriate content (SafeSearch). The appliance can enforce SafeSearch for these search engines, while still permitting users access to these search engines.

  Once the SafeSearch option has been enabled, search results for web pages and thumbnail images are filtered for Google, MSN, bing.com, and Yahoo!, even if users disable the SafeSearch option on any of these sites (your users' preferences are overridden). Additionally, video search results for YouTube, MSN, bing.com, and Yahoo! are filtered when SafeSearch is enforced.

  Note: While the appliance can enforce SafeSearch for the above search engines, the SafeSearch filtering is implemented by individual search engines, and the behavior may vary amongst search engines. As such, it is possible that some unwanted content may be displayed in search results. The functionality of SafeSearch as implemented by these search engines and the ability of the appliance to control this feature is beyond Sophos's control and may change without notice.

- 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.
- To share data with Sophos that will help improve the protection provided by your Web Appliance, select the **SophosLabs** check box, and click **Apply**.

  Note: No data shared with Sophos will contain information in which user identities are shown or can be deduced.

- To exclude username 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.

- 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.
- To limit access to Google accounts and services to only the domains you specify, select the **Enable Google Application control** check box and enter one or more domains that you wish to allow.

7.2 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”.

7.2.1 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.

7.3 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.

7.4 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.

7.4.1 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**.

Related tasks

Modifying Notification Page Text on page 34

7.4.2 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**.

Related tasks

Setting Global Notification Options on page 34

8 Contacting Sophos

Sophos 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/