Sophos UTM Manager administration guide for webadmin

Product version: 4.102
Document date: 26 June 2013
The specifications and information in this document are subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. This document may not be copied or distributed by any means, in whole or in part, for any reason, without the express written permission of Astaro GmbH & Co. KG. Translations of this original manual must be marked as follows: "Translation of the original manual".

© 2000–2013 Astaro GmbH & Co. KG.
All rights reserved.
Amalienbadstraße 41/Bau 52,
76227 Karlsruhe,
Germany
http://www.sophos.com

Sophos UTM, Sophos UTM Manager, Astaro Security Gateway, Astaro Command Center, Astaro Gateway Manager, and WebAdmin are trademarks of Astaro GmbH & Co. KG. Cisco is a registered trademark of Cisco Systems Inc. iOS is a trademark of Apple Inc. Linux is a trademark of Linus Torvalds. All further trademarks are the property of their respective owners.

Limited Warranty

No guarantee is given for the correctness of the information contained in this document. Please send any comments or corrections to nsg-docu@sophos.com.
# Contents

## 1 Installation  
1.1 System Requirements ................................................. 1
  1.1.1 Administration PC ............................................. 3
  1.1.2 Supported Devices ............................................ 3
  1.1.3 UPS Device Support ........................................... 4
  1.1.4 RAID Support .................................................. 4
1.2 Installation Instructions ........................................... 4
  1.2.1 Key Functions During Installation ............................ 5
  1.2.2 Special Options During Installation .......................... 5
  1.2.3 Installing Sophos UTM Manager ............................... 6
1.3 Basic Configuration ................................................ 9

## 2 WebAdmin ........................................................... 13
2.1 WebAdmin Menu .................................................... 13
2.2 Button Bar .......................................................... 14
2.3 Lists ................................................................. 15
2.4 Searching in Lists ................................................. 16
2.5 Dialog Boxes ....................................................... 17
2.6 Buttons and Icons ................................................. 18
2.7 Object Lists ........................................................ 20

## 3 Dashboard .......................................................... 23
3.1 Flow Monitor ....................................................... 24

## 4 Management .......................................................... 27
4.1 System Settings .................................................... 27
  4.1.1 Organizational ................................................. 28
  4.1.2 Hostname ....................................................... 28
  4.1.3 Time and Date ................................................ 28
  4.1.4 Shell Access .................................................. 30
  4.1.5 Reset Configuration or Passwords ............................ 32
4.2 WebAdmin Settings ................................................. 33
  4.2.1 General ......................................................... 33
  4.2.2 Access Control ................................................ 34
  4.2.3 HTTPS Certificate ............................................. 35
  4.2.4 User Preferences ............................................. 36
  4.2.5 Advanced ...................................................... 36
4.3 Sophos UTM Manager .............................................. 38
  4.3.1 General ......................................................... 39
8.2.3 Monthly ................................................................. 117
8.2.4 Yearly ................................................................. 117
8.3 Network Usage ..................................................... 117
  8.3.1 Daily ............................................................... 117
  8.3.2 Weekly ............................................................. 118
  8.3.3 Monthly ........................................................... 118
  8.3.4 Yearly ............................................................... 118
  8.3.5 Bandwidth Usage ............................................. 118
8.4 Network Protection ............................................... 119
  8.4.1 Daily ............................................................... 119
  8.4.2 Weekly ............................................................. 119
  8.4.3 Monthly ........................................................... 120
  8.4.4 Yearly ............................................................... 120
8.5 Executive Report .................................................. 120
  8.5.1 View Report ...................................................... 120
  8.5.2 Archived Executive Reports ................................. 120
  8.5.3 Configuration ................................................... 120
8.6 Log Settings ......................................................... 121
  8.6.1 Local Logging ................................................... 121
  8.6.2 Remote Syslog Server ....................................... 122
  8.6.3 Remote Log File Archives ................................ 123
8.7 Reporting Settings ................................................ 125
  8.7.1 Settings .......................................................... 125
9 Support ................................................................. 129
  9.1 Documentation .................................................. 129
  9.2 Printable Configuration ...................................... 130
  9.3 Contact Support ................................................ 130
  9.4 Tools ................................................................. 131
    9.4.1 Ping Check ................................................... 131
    9.4.2 Traceroute .................................................... 131
    9.4.3 DNS Lookup ................................................ 132
  9.5 Advanced .......................................................... 132
    9.5.1 Process List ................................................ 133
    9.5.2 LAN Connections .......................................... 133
    9.5.3 Routes Table ............................................... 133
    9.5.4 Interfaces Table ......................................... 133
    9.5.5 Config Dump ............................................... 133
    9.5.6 Resolve REF ............................................... 134
10 Log Off ............................................................... 135
1 Installation

The following topics are included in this chapter:

- System Requirements
- Installation Instructions
- Basic Configuration

1.1 System Requirements

The requirements for installing and using Sophos UTM Manager are dependent on the number of devices to administer. The following device ranges are available:

Small

- Allows to manage up to 20 devices
- Processor: Intel Celeron D with 1.6 GHz
- 512 (1024) MB DDR RAM
- 80 GB SATA hard drive
- 1 Gigabit PCI Ethernet network card
- 1 Mbit connection

Medium

- Allows to manage up to 50 devices
- Processor: Dual-Core with 2 x 1.8 GHz
- 1024 MB DDR RAM
- 80 GB SATA hard drive
- 2 Gigabit PCI Ethernet network cards
- 2 Mbit connection
Large

- Allows to manage up to 100 devices
- Processor: Intel Core2 Duo with 2 x 3.0 GHz
- 2 GB DDR RAM
- 120 GB SATA hard drive
- 2 Gigabit PCI Ethernet network cards
- 4 Mbit connection

Huge

- Allows to manage up to 200 devices
- Processor: Intel Xeon with 4 x 2.4 GHz
- 2/4 GB DDR RAM
- 160 GB SATA hard drive
- 4 Gigabit PCI Ethernet network cards
- 6 Mbit connection

Enterprise

- Allows to manage up to 300 devices
- Processor: Intel Xeon with 8 x 2.4 GHz
- 8 GB DDR RAM
- 200 GB SATA hard drive
- 4 Gigabit PCI Ethernet network cards
- 8 Mbit connection

Note – More information is included in the Release Notes.
1.1.1 Administration PC

The hardware and software requirements for the administration PC used are as follows:

- **Processor**: Clock signal frequency 2.4 GHz or higher, Dual-Core recommended for 250 devices.

- **Browser**: An HTTPS-capable browser such as Firefox 3.x or Microsoft’s Internet Explorer 7 or 8 or higher; JavaScript must be enabled. For best performance, we recommend the use of Firefox 3.5 or higher on a decent machine if you manage more than 10–25 devices.

In addition, the browser must be configured not to use a proxy for the IP address of the SUM’s internal network card (eth0).

1.1.2 Supported Devices

With the current version of Sophos UTM Manager up to 300 security systems may be managed. The following security systems are supported:

<table>
<thead>
<tr>
<th>Feature</th>
<th>V7</th>
<th>V8</th>
<th>V9</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic</td>
<td>7.300</td>
<td>8.000</td>
<td>9.000</td>
</tr>
<tr>
<td>VPN</td>
<td>7.401</td>
<td>8.000</td>
<td>9.000</td>
</tr>
<tr>
<td>Global Definitions</td>
<td>7.501</td>
<td>8.000</td>
<td>9.000</td>
</tr>
<tr>
<td>Reporting</td>
<td>7.501</td>
<td>8.000</td>
<td>9.000</td>
</tr>
<tr>
<td>Firewall/Packet Filter</td>
<td>7.506</td>
<td>8.000</td>
<td>9.000</td>
</tr>
<tr>
<td>Web Filter</td>
<td>7.506</td>
<td>8.000</td>
<td>9.000</td>
</tr>
<tr>
<td>VPN Enhancements</td>
<td>7.506</td>
<td>8.000</td>
<td>9.000</td>
</tr>
<tr>
<td>Privilege Restriction</td>
<td>7.507</td>
<td>8.002</td>
<td>9.000</td>
</tr>
<tr>
<td>2nd SUM Connection</td>
<td>7.507</td>
<td>8.002</td>
<td>9.000</td>
</tr>
<tr>
<td>Backup/Restore</td>
<td>–</td>
<td>8.200</td>
<td>9.000</td>
</tr>
<tr>
<td>Backup Rollout</td>
<td>–</td>
<td>8.201</td>
<td>9.000</td>
</tr>
<tr>
<td>On Demand Reporting</td>
<td>–</td>
<td>8.200</td>
<td>9.000</td>
</tr>
<tr>
<td>Global Object Import</td>
<td>–</td>
<td>–</td>
<td>9.000</td>
</tr>
<tr>
<td>Joining Devices</td>
<td>–</td>
<td>–</td>
<td>9.000</td>
</tr>
<tr>
<td>MSP Licensing</td>
<td>-</td>
<td>-</td>
<td>9.100</td>
</tr>
</tbody>
</table>
1.1.3 UPS Device Support

*Uninterruptible Power Supply* (UPS) devices maintain a continuous supply of electric power to connected equipment by supplying power from a separate source when utility power is not available. Sophos UTM Manager supports UPS devices of the manufacturers MGE UPS Systems and APC. The communication between the UPS device and Sophos UTM Manager is made via the USB interface.

As soon as the UPS device runs in battery operation, a notification is sent to the administrator. If the power failure persists for a longer period and the voltage of the UPS device approximates a critical value, another message will be sent to the administrator—Sophos UTM Manager will be shut down automatically.

**Note** – Please read the operation manual of the UPS device to connect the devices to Sophos UTM Manager. SUM will recognize the UPS device when booting via the USB interface. Only boot Sophos UTM Manager when you have connected the USB interfaces to each other.

1.1.4 RAID Support

A RAID (*Redundant Array of Independent Disks*) is a data storage scheme using multiple hard drives to share or replicate data among the drives. To ensure that the RAID system is detected and properly displayed on the Dashboard, you need to use a RAID controller that is supported by Sophos UTM Manager. Check the HCL to figure out which RAID controllers are supported. The HCL is available at the Sophos Knowledgebase. Use "HCL" as search term to locate the corresponding page.

1.2 Installation Instructions

What follows is a step-by-step guide of the installation process of Sophos UTM Manager Software.

Before you begin the installation, please make sure you have the following items available:

- The Sophos UTM Manager CD-ROM
- The license key for Sophos UTM Manager
1 Installation

The setup program will check the hardware of the system, and then install the software on your PC.

1.2.1 Key Functions During Installation

In order to navigate through the menus, use the following keys (please also note the additional key functions listed at the bottom of a screen):

- F1: Displays the context-sensitive help screen.
- Cursor keys: Use these keys to navigate through the text boxes (for example, the license agreement or when selecting a keyboard layout).
- Tab key: Move back and forth between text boxes, lists, and buttons.
- Enter key: The entered information is confirmed, and the installation proceeds to the next step.
- Space key: Select or unselect options marked with an asterisk.
- Alt-F2: Switch to the installation console.
- Alt-F4: Switch to the log.
- Alt-F1: Switch to the interactive bash shell.
- Alt-F1: Return to the main installation screen.

1.2.2 Special Options During Installation

Some screens offer additional options:

**View Log**: Opens the installation log.

**Support**: Opens the support dialog screen.

**To USB Stick**: Writes the installation log as zip file to a USB stick. Remember to insert a USB stick before confirming this option. The zip file can be used to solve installation problems, e.g. by the Sophos UTM Manager Support Team.

**Back**: Returns to the previous screen.

**Cancel**: Opens a confirmation dialog window to abort the installation.

**Help**: Opens the context-sensitive help screen.
### 1.2.3 Installing Sophos UTM Manager

1. **Boot your PC from CD-ROM drive.**
   The installation start screen is displayed.

   **Note** – You can always press F1 to access the help menu. Pressing F3 in the start screen opens a troubleshooting screen.

2. **Press Enter.**
   The *Introduction* screen is displayed.

3. **Select Start Installation.**
   The *Hardware Detection* screen is displayed.
   The software will check the following hardware components:
   - CPU
   - Size and type of hard disk drive
   - CD-ROM drive
   - Network interface cards
   - IDE or SCSI controllers

   If your system does not meet the minimum requirements, the installation will report the error and abort.

   As soon as the hardware detection is completed, the *Detected Hardware* screen is displayed for information purposes.

4. **Press Enter.**
   The *Select Keyboard* screen is displayed.

5. **Select your keyboard layout.**
   Use the Cursor keys to select your keyboard layout, e.g. *English (UK)*, and press Enter to continue.
   The *Select Timezone* screen is displayed.

6. **Select your area.**
   Use the Cursor keys to select your area, e.g. *Europe*, and press Enter to continue.
7. **Select your time zone.**
   Use the Cursor keys to select your time zone, e.g. *London*, and press Enter to continue.

   The *Date and Time* screen is displayed.

8. **Set date and time.**
   If date and time are not correct, you can change them here. Use the Tab key and the 
   Cursor keys to switch between text boxes. You can unselect the *Host clock is UTC* option 
   by pressing the Space key. Invalid entries will be rejected. Confirm your settings with the 
   Enter key.

   The *Select Admin Interface* screen is displayed.

9. **Select an internal network card.**
   In order to use the WebAdmin tool to configure the rest of Sophos UTM Manager, select 
   a network interface card to be the internal network card (eth0). Choose one of the avail- 
   able network cards from the list and confirm your selection with the Enter key.

   **Note** – Interfaces having an active connection are marked with [link].

   The *Network Configuration* screen is displayed.

10. **Configure the administrative network interface.**
    Define the IP address, network mask, and gateway of the internal interface which is 
    going to be the administrative network interface. The default values are:

    **Address:** 192.168.2.100
    **Netmask:** 255.255.255.0
    **Gateway:** none

    You need to change the gateway value only if you wish to use the WebAdmin interface 
    from a workstation outside the subnet defined by the netmask. Note that the gateway 
    itself must be within the subnet.¹

¹For example, if you are using a network mask of 255.255.255.0, the subnet is defined by the 
first three octets of the address: in this case, 192.168.2. If your administration computer has 
the IP address 192.168.10.5, it is not on the same subnet, and thus requires a gateway. The 
gateway router must have an interface on the 192.168.2 subnet and must be able to contact 
the administration computer. In our example, assume the gateway has the IP address 
192.168.2.1.
Confirm your settings with the Enter key.

If your CPU supports 64 bit the 64 Bit Kernel Support screen is displayed. Otherwise the installation continues with the Enterprise Toolkit screen.

11. **Install the 64-bit kernel.**
Select Yes to install the 64-bit kernel or No to install the 32-bit kernel.

The Enterprise Toolkit screen is displayed.

12. **Accept installation of the Enterprise Toolkit.**
The Enterprise Toolkit comprises the Sophos UTM Manager Software. You can decide to install Open Source software only. However, we advise to also install the Enterprise Toolkit to be able to use the full functionality of Sophos UTM Manager.

Press Enter to install both software packages or select No to install the Open Source software only.

The Installation: Partitioning screen is displayed.

13. **Confirm the warning message to start the installation.**
Please read the warning carefully. After confirming, all existing data on the PC will be destroyed.

If you want to cancel the installation and reboot instead, select No.

**Caution** – The installation process will delete all data on the hard disk drive.

The software installation process can take up to a couple of minutes.

The Installation Finished screen is displayed.

14. **Remove the CD-ROM, connect to the internal network, and reboot the system.**
When the installation process is complete, remove the CD-ROM from the drive and connect the eth0 network card to the internal network. Except for the internal network card (eth0), the sequence of network cards normally will be determined by PCI ID and by the kernel drivers. The sequence of network card names may also change if the hardware configuration is changed, especially if network cards are removed or added.

Then press Enter in the installation screen to reboot SUM. During the boot process, the IP addresses of the internal network cards are changed. The installation routine console (Alt+F1) may display the message "No IP on eth0" during this time.
After Sophos UTM Manager has rebooted (a process which, depending on your hardware, can take several minutes), ping the IP address of the eth0 interface to ensure it is reachable. If no connection is possible, please check if one of the following problems is present:

- The IP address of Sophos UTM Manager is incorrect.
- The IP address of the administrative computer is incorrect.
- The default gateway on the client is incorrect.
- The network cable is connected to the wrong network card.
- All network cards are connected to the same hub.

1.3 Basic Configuration

The second step of the installation is performed through WebAdmin, the web based administrative interface of Sophos UTM Manager. Prior to configuring basic system settings, you should have a plan how to integrate Sophos UTM Manager into your network. You must decide which functions you want it to provide. However, you can always reconfigure Sophos UTM Manager at a later time. So if you do not have planned how to integrate Sophos UTM Manager into your network yet, you can begin with the basic configuration right away.

1. **Start your browser and open WebAdmin.**
   Browse to the URL of Sophos UTM Manager (i.e., the IP address of eth0). In order to stay consistent with our configuration example above, this would be https://192.168.2.100:4444 (note the HTTPS protocol and port number 4444).

   To provide authentication and encrypted communication, Sophos UTM Manager comes with a self-signed security certificate. This certificate is offered to the web browser when an HTTPS-based connection to WebAdmin is established. For being unable to check the certificate’s validity, the browser will display a security warning. Once you have accepted the certificate, the initial login page is displayed.
1.3 Basic Configuration

2. **Fill out the Basic System Setup form.**
Enter accurate information of your company in the text boxes presented here. In addition, specify a password and valid email address for the administrator account. If you accept the license agreement, click the *Perform Basic System Setup* button to continue logging in. While performing the basic system setup, a number of certificates and certificate authorities are being created:

- **WebAdmin CA**: The CA with which the WebAdmin certificate was signed (see *Management > WebAdmin Settings > HTTPS Certificate*).

- **WebAdmin Certificate**: The digital certificate of WebAdmin (see *Management > Certificate Management > Certificates*).

The login page appears. (With some browsers it may, however, happen that you are presented another security warning because the certificate has changed according to your entered values.)
3. **Log into WebAdmin.**
   Type `admin` in the *Username* field and enter the password you have specified on the previous screen.

   The Dashboard page of WebAdmin is opened providing you with all system status information of the Sophos UTM Manager unit.

4. **Install your license.**
   Open the *Management > Licensing > Installation* tab. Click the Folder icon, browse for the license file and upload it. Click *Apply* to save your license.

5. **Configure the internal network interface.**
   Open the *Interfaces & Routing > Interfaces* tab and click the *Edit* button of your internal network interface (*eth0*). The settings for this interface are based on the information you provided during the installation of the software. Click *Save* to apply your changes.

   **Note** – If you change the IP address of the internal interface, you must connect to WebAdmin again using the new IP address.

6. **Select the uplink type for the external interface.**
   Click the *New interface* button to add an external interface. Enter a name and select the connection type of your uplink/Internet connection the external network card is going to use. The type of interface and its configuration depend on what kind of connection to the Internet you are going to use. Select a network card, enter an IP address, change the netmask and enter a default gateway if necessary. Click *Save* to apply your settings.

   The new interface is shown in the list, disabled. To enable it click the toggle switch. It turns green when the connection is established.
7. **Configure Gateway Manager.**
   Open *Management > Sophos UTM Manager* and configure Sophos UTM Manager settings such as access control and device security.

![Figure 3 WebAdmin: Dashboard](image)

8. **Confirm your settings.**
   If you encounter any problems while completing these steps, please contact the support department of your Sophos UTM Manager supplier. For more information, you might also want to visit the following websites:
   - Sophos UTM Manager Support Forum
   - Sophos Knowledgebase
2 WebAdmin

WebAdmin is the web-based administrative interface that allows you to configure every aspect of Sophos UTM Manager. WebAdmin consists of a menu and pages, many of which have multiple tabs. The menu on the left of the screen organizes the features of Sophos UTM Manager in a logical manner. When you select a menu item, such as Network Protection, it expands to reveal a submenu and the associated page opens. Note that for some menu items no page is associated. Then, the page of the previously selected menu or submenu item keeps being displayed. You have to select one of the submenu items, which opens the associated page at its first tab.

The procedures in this documentation direct you to a page by specifying the menu item, submenu item, and the tab, for example: "On the Interfaces & Routing > Interfaces > Hardware tab, configure ..."

![Figure 4 WebAdmin: Overview](image)

2.1 WebAdmin Menu

The WebAdmin menu provides access to all configuration options of Sophos UTM Manager, that is, there is no need for using a command line interface to configure specific parameters.

- **Dashboard**: The Dashboard graphically displays a snapshot of the current operating status of the Sophos UTM Manager unit.
- **Management**: Configure basic system and WebAdmin settings as well as all settings that concern the configuration of the Sophos UTM Manager unit.

- **Definitions & Users**: Configure network, service, and time period definitions as well as user accounts, user groups, and external authentication servers for use with the Sophos UTM Manager unit.

- **Interfaces & Routing**: Configure system facilities such as network interfaces as well as routing options, among other things.

- **Network Services**: Configure network services such as DNS and DHCP, among other things.

- **Logging & Reporting**: View log messages and statistics about the utilization of the Sophos UTM Manager unit and configure settings for logging and reporting.

- **Support**: Access to the support tools available at the Sophos UTM Manager unit.

- **Log Off**: Log out of the user interface.

### Searching The Menu

Above the menu a search box is located. It lets you search the menu for keywords in order to easily find menus concerning a certain subject. The search function matches the name of menus but additionally allows for hidden indexed aliases and keywords.

As soon as you start typing into the search box, the menu automatically reduces to relevant menu entries only. You can leave the search box at any time and click the menu entry matching your prospect. The reduced menu stays intact, displaying the search results, until you click the reset button next to it.

**Tip** – You can set focus on the search box via the keyboard shortcut \[CTRL+Y\].

### 2.2 Button Bar

The buttons in the upper right corner of WebAdmin provide access to the following features:

- **Username/IP**: Shows the currently logged in user and the IP address from which WebAdmin is accessed. If other users are currently logged in, their data will be shown, too.
• **Open Live Log**: Clicking this button opens the live log that is associated with the WebAdmin menu or tab you are currently on. To see a different live log without having to change the menu or tab, hover over the Live Log button. After some seconds a list of all available live logs opens where you can select a live log to display. Your selection is memorized as long as you stay on the same WebAdmin menu or tab.

**Tip** – You can also open live logs via the Open Live Log buttons provided on multiple WebAdmin pages.

• **Online Help**: Every menu, submenu, and tab has an online help screen that provides context-sensitive information and procedures related to the controls of the current WebAdmin page.

**Note** – The online help is version-based and updated by means of patterns. If you update to a new firmware version, your online help will also be updated, if available.

• **Reload**: To request the already displayed WebAdmin page again, always click the Reload button.

**Note** – Never use the reload button of the browser, because otherwise you will be logged out of WebAdmin.

### 2.3 Lists

Many pages in WebAdmin consist of lists. The buttons on the left of each list item enable you to edit, delete, or clone the item (for more information see section *Buttons and Icons*). To add an item to the list, click the *New …* button, where "…" is a placeholder for the object being created (e.g., interface). This opens a dialog box where you can define the properties of the new object.

![New interface button](image)

**Figure 5** WebAdmin: Example of a List
2.4 Searching in Lists

With the first drop-down list on the top you can filter all items according to their type or group. The second field on the top lets you search for items specifically. Enter a search string and click Find.

Lists with more than ten items are split into several chunks, which can be browsed with Forward (>>) and Backward (<<) buttons. With the Display drop-down list, you can temporarily change the number of items per page. Additionally, you can change the default setting for all lists on the Management > WebAdmin Settings > User Preferences tab.

The header of a list provides some functionality. Normally, clicking a header field sorts the list for that object field of that name, e.g. clicking the field Name sorts the list by the objects' names. The Action field in the header contains some batch options you can carry out on previously selected list objects. To select objects, select their checkbox. Note that the selection stays valid across multiple pages, that is, while browsing between pages of a list already selected objects stay selected.

Tip – Clicking on the Info icon will show all configuration options in which the object is used.

2.4 Searching in Lists

A filter field helps you to quickly reduce the number of items displayed in a list. This makes it much easier to find the object(s) you were looking for.

Important Facts

- A search in a list typically scans several fields for the search expression. A search in Users & Groups for example considers the username, the real name, the comment, and the first email address. Generally speaking, the search considers all texts which you can see in the list, excluding details displayed via the Info icon.

- The list search is case-insensitive. That means it makes no difference whether you enter upper- or lower-case letters. The search result will contain matches both with upper-case and lower-case letters. Searching explicitly for upper-case or lower-case letters is not possible.

- The list search is based on Perl regular expression syntax (although case-insensitive). Typical search expressions known from e.g. text editors like * and ? as simple wildcard characters or the AND and OR operators do not work in list search.
Examples

The following list is a small selection of useful search strings:

**Simple string:** Matches all words that contain the given string. For example, "inter" matches "Internet", "interface", and "printer".

**Beginning of a word:** Mark the search expression with a `\b` at the beginning. For example, `\binter` matches "Internet" and "interface" but not "printer".

**End of a word:** Mark the search expression with a `\b` at the end. For example, `http\b` matches "http" but not "https".

**Beginning of an entry:** Mark the search expression with a `^` at the beginning. For example, `^inter` matches "Internet Uplink" but not "Uplink Interfaces".

**IP addresses:** Searching for IP addresses, you need to escape dots with a backslash. For example, `192\.168` matches "192.168". To search more generally for IP addresses use `\d` which matches any digit. `\d+` matches multiple digits in a row. For example, `\d+.\d+.\d+.\d+` matches any IPv4 address.

---

**Note** – It makes sense to rather use an easy, fail-safe search expression which will lead to more matches than to rack your brains for a supposedly more perfect one which can easily lead to unexpected results and wrong conclusions.

You can find a detailed description of regular expressions and their usage in Sophos UTM Manager in the [Sophos Knowledgebase](#).

### 2.5 Dialog Boxes

Dialog boxes are special windows which are used by WebAdmin to prompt you for entering specific information. The example shows a dialog box for creating a new static route in the **Interfaces & Routing > Static Routing** menu.
Each dialog box can consist of various widgets such as text boxes, checkboxes, and so on. In addition, many dialog boxes offer a drag-and-drop functionality, which is indicated by a special background reading DND. Whenever you encounter such a box, you can drag an object into the box. To open the object list from where to drag the objects, click the Folder icon that is located right next to the text box. Depending on the configuration option, this opens the list of available networks, interfaces, users/groups, or services. Clicking the green Plus icon opens a dialog window letting you create a new definition. Some widgets that are not necessary for a certain configuration are grayed out. In some cases, however, they can still be edited, but having no effect.

**Note** – You may have noticed the presence of both Save and Apply buttons in WebAdmin. The Save button is used in the context of creating or editing objects in WebAdmin such as static routes or network definitions. It is always accompanied by a Cancel button. The Apply button, on the other hand, serves to confirm your settings in the backend, thus promptly activating them.

### 2.6 Buttons and Icons

WebAdmin has some buttons and functional icons whose usage is described here.

<table>
<thead>
<tr>
<th>Buttons</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="View" /></td>
<td>Shows a dialog box with detailed information on the object.</td>
</tr>
<tr>
<td><img src="image" alt="Edit" /></td>
<td>Opens a dialog box to edit properties of the object.</td>
</tr>
<tr>
<td>Buttons</td>
<td>Meaning</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td><img src="image" alt="Delete" /></td>
<td>Deletes the object. If an object is still in use somewhere, there will be a warning. Not all objects can be deleted if they are in use.</td>
</tr>
<tr>
<td><img src="image" alt="Clone" /></td>
<td>Opens a dialog box for creating an object with identical settings/properties. Helps you to create similar objects without having to type all identical settings over and over again.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Functional Icons</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Info" /></td>
<td><strong>Info:</strong> Shows all configurations where the object is in use.</td>
</tr>
<tr>
<td><img src="image" alt="Details" /></td>
<td><strong>Details:</strong> Links to another WebAdmin page with more information about the topic.</td>
</tr>
<tr>
<td><img src="image" alt="Toggle switch" /></td>
<td><strong>Toggle switch:</strong> Enables or disables a function. Green when enabled, gray when disabled, and amber when configuration is required before enabling.</td>
</tr>
<tr>
<td><img src="image" alt="Folder" /></td>
<td><strong>Folder:</strong> Has two different functions: (1) Opens an object list (see section below) on the left side where you can choose appropriate objects from. (2) Opens a dialog window to upload a file.</td>
</tr>
<tr>
<td><img src="image" alt="Plus" /></td>
<td><strong>Plus:</strong> Opens a dialog window to add a new object of the required type.</td>
</tr>
<tr>
<td><img src="image" alt="Action" /></td>
<td><strong>Action:</strong> Opens a drop-down menu with actions. The actions depend on the location of the icon: (1) Icon in list header: the actions, e.g., <em>Enable</em>, <em>Disable</em>, <em>Delete</em>, apply to the selected list objects. (2) Icon in text box: with the actions <em>Import</em> and <em>Export</em> you can import or export text, and with <em>Empty</em> you delete the entire content. There is also a filter field which helps you to drill down a list to relevant elements. Note that the filter is case-sensitive.</td>
</tr>
<tr>
<td><img src="image" alt="Empty" /></td>
<td><strong>Empty:</strong> Removes an object from the current configuration when located in front of the object. Removes all objects from a box when located in the <em>Actions</em> menu. Objects are however never deleted.</td>
</tr>
<tr>
<td><img src="image" alt="Import" /></td>
<td><strong>Import:</strong> Opens a dialog window to import text with more than one item or line. Enhances adding multiple items without having to type them individually, e.g. a large blacklist to the URL blacklist. Copy the text from anywhere and enter it using CTRL+V.</td>
</tr>
</tbody>
</table>
2.7 Object Lists

<table>
<thead>
<tr>
<th>Functional Icons</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Image" /></td>
<td><strong>Export</strong>: Opens a dialog window to export all existing items. You can select a delimiter to separate the items, which can either be new line, colon, or comma. To export the items as text, mark the whole text in the <em>Exported Text</em> field and press <strong>CTRL+C</strong> to copy it. You can then paste it into all common applications using <strong>CTRL+V</strong>, for example a text editor.</td>
</tr>
<tr>
<td><img src="image2" alt="Image" /></td>
<td><strong>Sort</strong>: Using these two arrows, you can sort list elements by moving an element down or up, respectively.</td>
</tr>
<tr>
<td><img src="image3" alt="Image" /></td>
<td><strong>Forward/Backward</strong>: Depending on the location you can navigate through the pages of a long list, or move back and forth along the history of changes and settings.</td>
</tr>
<tr>
<td><img src="image4" alt="Image" /></td>
<td><strong>PDF</strong>: Saves the current view of data in a PDF file and then opens a dialog window to download the created file.</td>
</tr>
<tr>
<td><img src="image5" alt="Image" /></td>
<td><strong>CSV</strong>: Saves the current view of data in a CSV (comma-separated values) file and then opens a dialog window to download the created file.</td>
</tr>
</tbody>
</table>

2.7 Object Lists

An object list is a drag-and-drop list which is temporarily displayed on the left side of WebAdmin, covering the main menu.
An object list is opened automatically when you click the Folder icon (see section above), or you can open it manually via a keyboard shortcut (see Management > WebAdmin Settings > User Preferences).

The object list gives you quick access to WebAdmin objects like users/groups, interfaces, networks, and services to be able to select them for configuration purposes. Objects are selected simply by dragging and dropping them onto the current configuration.

According to the different existing object types, there are five different types of object lists. Clicking the Folder icon will always open the type required by the current configuration.
3 Dashboard

The Dashboard graphically displays a snapshot of the current operating status of Sophos UTM Manager.

The Dashboard displays by default when you log in to WebAdmin and shows the following information:

- **General Information**: Hostname, model, license ID, subscriptions, and uptime of the unit. The display color of a subscription switches to orange 30 days before its expiration date. During the last 7 days and after expiration, a subscription is displayed in red.

- **Version Information**: Information on the currently installed firmware and pattern versions as well as available updates.

- **Resource Usage**: Current system utilization, including the following components:
  - The CPU utilization in percent
  - The RAM utilization in percent. Please note that the total memory displayed is the part that is usable by the operating system. With 32-bit systems, in some cases that does not represent the actual size of the physical memory installed, as part of it is reserved for hardware.
  - The amount of hard disk space consumed by the log partition in percent
  - The amount of hard disk space consumed by the root partition in percent
  - The status of the UPS (uninterruptible power supply) module (if available)

- **Interfaces**: Name and status of configured network interface cards. In addition, information on the average bit rate of the last 75 seconds for both incoming and outgoing traffic is shown. The values presented are obtained from bit rate averages based on samples that were taken at intervals of 15 seconds. Clicking a traffic value of an interface opens a Flow Monitor in a new window. The Flow Monitor displays the traffic of the last ten minutes and refreshes automatically at short intervals. For more information on the Flow Monitor see chapter *Flow Monitor*.

- **Current System Configuration**: Enabled/disabled representation of the most relevant security features. Clicking one of the entries opens the WebAdmin page with the respective settings:
  - **Gateway Manager**: Displays the number of active (online) devices (gateways) compared to the total amount of known devices.
3.1 Flow Monitor

The Flow Monitor of Sophos UTM Manager is an application which gives quick access to information on network traffic currently passing the interfaces of SUM. It can be easily accessed via the Dashboard by clicking one of the interfaces at the top right. By clicking *All Interfaces* the Flow Monitor displays the traffic accumulated on all active interfaces. By clicking a single interface, the Flow Monitor displays the traffic of this interface only.

**Note** – The Flow Monitor opens in a new browser window. As pop-up blockers are likely to block this window it is advisable to deactivate pop-up blockers for WebAdmin.

The Flow Monitor provides two views, a chart and a table, which are described in the next sections. It refreshes every five seconds. You can click the *Pause* button to stop refreshing. After clicking *Continue* to start refreshing again, the Flow Monitor updates to the current traffic information.

**Chart View**

The Flow Monitor chart displays the network traffic for the past ten minutes. The horizontal axis reflects time, the vertical axis reflects the amount of traffic while dynamically adapting the scale to the throughput.

At the bottom of the chart view a legend is located which refers to the type of traffic passing an interface. Each type of traffic has a different color so that it can be easily distinguished in the chart.

When hovering the mouse cursor on a chart a big dot will appear, which gives detailed information of this part of the chart. The dot is clung to the line of the chart. As you move the mouse cursor the dot follows. In case a chart has several lines, the dot switches between them according to where you move the mouse cursor. Additionally, the dot changes its color depending on which line its information refer to, which is especially useful with lines running close to each other. The dot provides information on type and size of the traffic at the respective point of time.
3 Dashboard

3.1 Flow Monitor

Tabular View

The Flow Monitor table provides information on network traffic for the past five seconds:

#: Traffic is ranked based on its current bandwidth usage.

**Application**: Protocol or name of the network traffic if available. Unclassified traffic is a type of traffic unknown to the system. Clicking an application opens a window which provides information on the server, the port used, bandwidth usage per server connection, and total traffic.

**Clients**: Number of client connections using the application. Clicking a client opens a window which provides information on the client's IP address, bandwidth usage per client connection, and total traffic. Note that with unclassified traffic the number of clients in the table may be higher than the clients displayed in the additional information window. This is due to the fact that the term "unclassified" comprises more than one application. So, there might be only one client in the information window but three clients in the table, the latter actually being the connections of the single client to three different, unclassified applications.

**Bandwidth Usage Now**: The bandwidth usage during the last five seconds. Clicking a bandwidth opens a window which provides information on the download and upload rate of the application connection.

**Total Traffic**: The total of network traffic produced during the "lifetime" of a connection. Example 1: A download started some time in the past and still going on: the whole traffic produced during the time from the beginning of the download will be displayed. Example 2: Several clients using facebook: as long as one client keeps the connection open, the traffic produced by all clients so far adds up to the total traffic displayed. Clicking a total traffic opens a window which provides information on the overall download and upload rate of the application connection.
4 Management

This chapter describes how to configure basic system settings as well as the settings of the web-based administrative interface of Sophos UTM Manager, WebAdmin, among others. The Overview page shows statistics of the last WebAdmin sessions including possible changes. Click the Show button in the Changelog column to view the changes in detail.

In the State column, the end times of previous WebAdmin sessions are listed.

Note – You can end a WebAdmin session by clicking the Log off menu. If you close the browser without clicking the Log off menu, the session times out after the time span defined on the Management > WebAdmin Settings > Advanced tab.

The following topics are included in this chapter:

- System Settings
- WebAdmin Settings
- Sophos UTM Manager
- Licensing
- Up2Date
- Backup/Restore
- User Portal
- Notifications
- Customization
- SNMP
- Certificate Management
- Shutdown/Rerstart

4.1 System Settings

The tabs under System Settings allow you to configure basic settings of your SUM such as hostname, date, and time.
4.1 System Settings

4.1.1 Organizational

Enter the name and location of your organization and an email address to reach the person or group technically responsible for the operation of your Sophos UTM Manager. Note that this data is also used in certificates for WebAdmin.

4.1.2 Hostname

Enter the hostname of your SUM as a fully qualified domain name (FQDN) into this field, for example utm.example.com. A hostname may contain alphanumeric characters, dots, and hyphens. At the end of the hostname there must be a special designator such as com, org, or de. The hostname will be used in notification messages to identify SUM. Note that the hostname does not need to be registered in the DNS zone for your domain.

4.1.3 Time and Date

On your SUM, date and time should always be set correctly. This is needed both for getting correct information from the logging and reporting systems and to assure interoperability with other computers on the Internet.

Usually, you do not need to set the time and date manually. By default, automatic synchronization with public Internet time servers is enabled (see section Synchronize Time with Internet Server below).

In the rare case that you need to disable synchronization with time servers, you can change the time and date manually. However, when doing so, pay attention to the following caveats:

- Never change the system time from standard time to daylight saving time or vice versa. This change is always automatically covered by your time zone settings even if automatic synchronization with time servers is disabled.
- Never change date or time manually while synchronization with time servers is enabled, because automatic synchronization would typically undo your change right away. In case you must set the date or time manually, remember to first remove all servers from the NTP Servers box in the Synchronize Time with Internet Server section below and click Apply.
- After manually changing the system time, wait until you see the green confirmation message, stating that the change was successful. Then reboot the system (Management >
Shutdown/Rerstart). This is highly recommended as many services rely on the fact that
time is changing continuously, not abruptly. Jumps in time therefore might lead to mal-
function of various services. This advice holds universally true for all kind of computer sys-
tems.

- In rare cases, changing the system time might terminate your WebAdmin session. In
case this happens, log in again, check whether the time is now correctly set and restart
the system afterwards.

If you operate multiple interconnected SUMs that span several time zones, select the same time
zone for all devices, for example UTC (Coordinated Universal Time)—this will make log mes-
sages much easier to compare.

Note that when you manually change the system time, you will encounter several side-effects,
even when having properly restarted the system:

- **Turning the clock forward**
  - Time-based reports will contain no data for the skipped hour. In most graphs, this
time span will appear as a straight line in the amount of the latest recorded value.

- **Turning the clock backward**
  - There is already log data for the corresponding time span in time-based reports.
  - Most diagrams will display the values recorded during this period as compressed.
  - The elapsed time since the last pattern check (as displayed on the Dashboard)
    shows the value "never", even though the last check was in fact only a few minutes
    ago.
  - Automatically created certificates on SUM may become invalid because the begin-
    ning of their validity periods would be in the future.

Because of these drawbacks the system time should only be set once when setting up the sys-
tem with only small adjustments being made thereafter. This especially holds true if reporting
data needs to be processed further and accuracy of the data is important.

### Set Date And Time

To configure the system time manually, select date and time from the respective drop-down
lists. Click **Apply** to save your settings.

### Set Time Zone

To change the system's time zone, select an area or a time zone from the drop-down list. Click
**Apply** to save your settings.
4.1 System Settings

Changing the time zone does not change the system time, but only how the time is represented in output, for example in logging and reporting data. Even if it does not disrupt services, we highly recommend to reboot afterwards to make sure that all services use the new time setting.

**Synchronize Time With Internet Server**

To synchronize the system time using a timeserver, select one or more NTP servers. Click *Apply* after you have finished the configuration.

**NTP servers**: The *NTP Server Pool* is selected by default. This network definition is linked to the big virtual cluster of public timeservers of the *pool.ntp.org* project. In case your Internet service provider operates NTP servers for customers and you have access to these servers, it is recommended to remove the *NTP Server Pool* and use your provider’s servers instead. When choosing your own or your provider’s servers, using more than one server is useful to improve precision and reliability. The usage of three independent servers is almost always sufficient. Adding more than three servers rarely results in additional improvements, while increasing the total server load. Using both *NTP Server Pool* and your own or your provider’s servers is not recommended because it will usually neither improve precision nor reliability.

**Tip** – If you want client computers to be able to connect to these NTP servers, add them to the allowed networks on the *Network Services > NTP* page.

**Test Configured Servers**: Click this button if you want to test whether a connection to the selected NTP server(s) can be established from your device and whether it returns usable time data. This will measure the time offset between your system and the servers. Offsets should generally be well below one second if your system is configured correctly and has been operating in a stable state for some time.

Right after enabling NTP or adding other servers, it is normal to see larger offsets. To avoid large time jumps, NTP will then slowly skew the system time, such that eventually, it will become correct without any jumping. In that situation, please be patient. In particular, in this case, do *not* restart the system. Rather, return to check about an hour later. If the offsets decrease, all is working as it should.

**4.1.4 Shell Access**

Secure Shell (SSH) is a command-line access mode primarily used to gain remote shell access to SUM. It is typically used for low-level maintenance or troubleshooting. To access this shell you need an SSH client, which usually comes with most Linux distributions.
Allowed Networks
Use the Allowed networks control to restrict access to this feature to certain networks only. Networks listed here will be able to connect to the SSH service.

Authentication
In this section you can define an authentication method for SSH access and the strictness of access. The following authentication methods are available:

- Password (default)
- Public key
- Password and public key

To use Public Key Authentication you need to upload the respective public key(s) into the field Authorized keys for loginuser for each user allowed to authenticate via their public key(s).

Allow root login: You can allow SSH access for the root user. This option is disabled by default as it leads to a higher security risk. When this option is enabled, the root user is able to login via their public key. Upload the public key(s) for the root user into the field Authorized keys for root.

Click Apply to save your settings.

Shell User Passwords
Enter passwords for the default shell accounts root and loginuser. To change the password for one out of these two accounts only, just leave both input boxes for the other account blank.

Note – To enable SSH shell access, passwords must be set initially. In addition, you can only specify passwords that adhere to the password complexity settings as configured on the Definitions & Users > Authentication Servers > Advanced tab. That is, if you have enabled complex passwords, shell user passwords must meet the same requirements.

SSH Daemon Listen Port
This option lets you change the TCP port used for SSH. By default, this is the standard SSH port 22. To change the port, enter an appropriate value in the range from 1024 to 65535 in the Port number box and click Apply.
4.1.5 Reset Configuration or Passwords

The options on the Reset Configuration or Passwords tab let you delete the passwords of the shell users. In addition, you can execute a factory reset.

**Reset System Passwords:** Executing this function will reset the passwords of the following users:

- root (shell user)
- loginuser (shell user)
- admin (predefined administrator account)

In addition, to halt the system, select the **Shutdown System Afterwards** option.

**Security Note** – The next person connecting to the WebAdmin will be presented an *Admin Password Setup* dialog window. Thus, after resetting the passwords, you should usually quickly log out, reload the page in your browser, and set a new admin password.

Besides, shell access will not be possible anymore until you set new shell passwords on the **Management > System Settings > Shell Access** tab.

**Factory Reset:** This function resets the device back to the factory default configuration. The following data will be deleted:

- System configuration
- Logs and reporting data
- Update packages
- Licenses
- Passwords

However, the version number of Sophos UTM Manager Software will remain the same, that is, all firmware and pattern updates that have been installed will be retained.

**Note** – Sophos UTM Manager will shut down once a factory reset has been initiated.
4.2 WebAdmin Settings

The tabs under Management > WebAdmin Settings allow you to configure basic WebAdmin settings such as access control, the TCP port, user preferences, and the WebAdmin language, among other things.

4.2.1 General

On the WebAdmin Settings > General tab you can configure the WebAdmin language and basic access settings.

WebAdmin Language
Select the language of WebAdmin. The selected language will also be used for some WebAdmin output, e.g., the executive report. Note that this setting is global and applies to all users. Click Apply to save your settings.

After changing the language, it might be necessary to empty your browser cache to make sure that all texts are displayed in the correct language.

WebAdmin Access Configuration
Here you can configure which users and/or networks should have access to WebAdmin.

Allowed administrators: Sophos UTM Manager can be administered by multiple administrators simultaneously. In the Allowed administrators box you can specify which users or groups should have unlimited read and write access to the WebAdmin interface. By default, this is the group of SuperAdmins.

Allowed networks: The Allowed networks box lets you define the networks that should be able to connect to the WebAdmin interface. For the sake of a smooth installation of SUM, the default is Any. This means that the WebAdmin interface can be accessed from everywhere. Change this setting to your internal network(s) as soon as possible. The most secure solution, however, would be to limit the access to only one administrator PC through HTTPS.

Log access traffic: If you want to log all WebAdmin access activities in the firewall log, select the Log access traffic checkbox.
4.2 WebAdmin Settings

4.2.2 Access Control

On the WebAdmin Settings > Access Control tab you can create WebAdmin roles for specific users. This allows for a fine-grained definition of the rights a WebAdmin user can have.

There are two user roles predefined:

**Auditor**: Users having this role can view logging and reporting data.

**Readonly**: Users having this role can view everything in WebAdmin without being able to edit, create, or delete anything.

To assign users or groups one of these roles, click the Edit button and add the respective user(s) or group(s) to the Members box.

You can create further roles, according to your security policies. Do the following:

1. **On the Access Control tab, click New Role.**
   The Create Role dialog box opens.

2. **Make the following settings:**
   - **Name**: Enter a descriptive name for this definition.
   - **Members**: Add users and groups to this box who are to have this role.
   - **Grant read-only access** (optional): Select this checkbox to grant read-only access to all areas of WebAdmin to the given members.
   - **Rights**: This box contains different rights levels for the different functions of WebAdmin: auditor and manager. A manager has full administration rights for the respective function(s), whereas an auditor has only viewing rights. You can choose one or more rights by selecting the respective checkbox in front of a right.
     Example: You could give the user Jon Doe manager rights for Email Protection and additionally select the checkbox **Grant read-only access**. He would then be able to change settings in the Email Protection section and view all other areas of WebAdmin without being able to change anything there.
   - **Comment** (optional): Add a description or other information.

3. **Click Save.**
   Your settings will be saved.

To either edit or delete a role, click the corresponding buttons. Note that the Auditor and Readonly roles cannot be deleted.
4.2.3 HTTPS Certificate

On the Management > WebAdmin Settings > HTTPS Certificate tab you can import the WebAdmin CA certificate into your browser, regenerate the WebAdmin certificate, or choose a signed certificate to use for WebAdmin and User Portal.

During the initial setup of the WebAdmin access you have automatically created a local CA certificate on SUM. The public key of this CA certificate can be installed into your browser to get rid of the security warnings when accessing the WebAdmin interface.

To import the CA certificate, proceed as follows:

1. **On the HTTPS Certificate tab, click Import CA Certificate.**
   The public key of the CA certificate will be exported.

   You can either save it to disk or install it into your browser.

2. **Install the certificate** (optional).
   The browser will open a dialog box letting you choose to install the certificate immediately.

   **Note** – Due to different system times and time zones the certificate might not be valid directly after its creation. In this case, most browsers will report that the certificate has expired, which is not correct. However, the certificate will automatically become valid after a maximum of 24 hours and will stay valid for 27 years.

**Re-generate WebAdmin Certificate**

The WebAdmin certificate refers to the hostname you have specified during the initial login. If the hostname has been changed in the meantime, the browser will display a security warning. To avoid this, you can create a certificate taking the new hostname into account. For that purpose, enter the hostname as desired and click Apply. Note that due to the certificate change, to be able to continue working in WebAdmin, you probably need to reload the page via your web browser, accept the new certificate, and log back into WebAdmin.

**Choose WebAdmin/User Portal Certificate**

If you do not want to import the CA certificate but instead use your own signed certificate for WebAdmin and User Portal, you can select it here. However, for the certificate to be selectable from the drop-down list, you need to upload it first on the Management > Certificate Management > Certificates tab in PKCS#12 format, containing the certificate, its CA and its private key. To use the uploaded certificate, select it from the Certificates drop-down list and click Apply.
4.2 WebAdmin Settings

4.2.4 User Preferences

On the Management > WebAdmin Settings > User Preferences tab you can configure some user preferences such as global shortcuts and items per page for the currently logged in user.

WebAdmin Shortcuts Configuration

Here you can configure keyboard shortcuts to open and close the drag-and-drop object lists used in many configurations (for more information see WebAdmin > Object Lists) or to set the cursor focus on the menu search box (see also WebAdmin > WebAdmin Menu). Use the drop-down list to select a different modifier key and the text box to enter a different character. You can also turn off the keyboard shortcut by selecting Off from the drop-down list.

If you want to return to the default settings, click the Reset to Defaults button. Click Apply to save your settings.

Table Pager Options

Here you can globally define the pagination of tables for WebAdmin, i.e. how many items are displayed per page. Click the drop-down list and select a value. Click Apply to save your settings.

WebAdmin Browser Title Customization

Here you can change the label which is displayed on the WebAdmin browser window or tab. You can enter plain text and/or use the following variables:

- %h: hostname
- %u: username
- %i: remote IP address

The default setting is WebAdmin - User %u - Device %h which translates for example into WebAdmin - User admin - Device my_gateway.example.com. Click Apply to save your settings.

4.2.5 Advanced

WebAdmin Idle Timeout

Log Out After: In this field you can specify the period of time (in seconds) how long a WebAdmin session can remain idle before the administrator is forced to log in again. By default, the idle timeout is set to 300 seconds. The range is from 60 to 86,400 seconds.
Log Out on Dashboard: By default, when you have opened the Dashboard page of WebAdmin, the auto logout function is disabled. You can, however, select this option to enable the auto logout function for Dashboard, too.

WebAdmin TCP Port
By default, port 4444 is used as WebAdmin TCP port. In the TCP Port box you can enter either 443 or any value between 1024 and 65535. However, certain ports are reserved for other services. In particular, you can never use port 10443, and you cannot use the same port you are using for the User Portal or for SSL remote access. Note that you must add the port number to the IP address (separated by a colon) in the browser’s address bar when accessing WebAdmin, for example https://192.168.0.1:4444

Terms of Use
Your company policies might demand that users accept terms of use when they want to access WebAdmin. Select the checkbox Display "Terms of Use" After Login to enforce that users must accept the terms of use each time they log into WebAdmin. Users will then be presented the terms of use after having logged in. If they do not accept them they will be logged out again.

You can change the terms of use text according to your needs. Click Apply to save your settings.

Sophos UTM Improvement Program
You can help improving Sophos UTM Manager by allowing it to transfer anonymous general information of your current configuration as well as information about detected viruses to Sophos. That kind of information cannot and will not be tracked back to you. No user-specific information is collected, i.e., no user or object names, no comments, or other personalized information. However, URLs for which a virus was found will be transmitted if web filter antivirus scanning is enabled.

The information is encrypted and transmitted to Sophos using SSL. Once delivered, the data is stored in an aggregated form and made available to Sophos' software architects for making educated design decisions and thus improve future versions of Sophos UTM Manager.

If you enable the Send anonymous usage statistics option, SUM gathers the following information:

- Configuration and usage data: The system will send the following data to Sophos' servers once a week.
  - Hardware and license information (not the owner), for example:

      processor Intel(R) Core(TM)2 Duo CPU E8200 @ 2.66GHz
memory: 512MiB System Memory
eth0 network: 82545EM Gigabit Ethernet Controller
id: SUM
version: 4.000000
type: virtual
license: standard
mode: standalone
active_ips: 2
system_id: 58174596-276f-39b8-854b-ffa1886e3c6c
The system ID identifies your SUM only in the way that information of your system is not accidentally collected twice, e.g. after a re-installation.

- Features in use (only whether they are turned on or off), for example:
  main->backup->status: 1
  main->ha->status: off

- Amount of configured objects, for example:
  objects->interface->ethernet: 2
  objects->http->profile: 5

- CPU, memory and swap usage values in percent over the last seven days

- Virus data: The system writes the following data into a file that will be uploaded automatically to Sophos' servers every 15 minutes.
  - Information about viruses found by web protection, for example threat name, MIME type, URL of the request, or file size.

- Intrusion prevention data: The IPS log will be checked every minute for new alerts. If there is a new alert, the following data will be sent instantly to Sophos:
  - Information about the alert, for example snort rule identifier and timestamp.

### 4.3 Sophos UTM Manager

The tabs under Management > Sophos UTM Manager allow you to configure basic Gateway Manager settings such as the TCP port and language, access control for administrators and users as well as security aspects for connecting devices. From the Open Gateway Manager tab you can directly open the Gateway Manager in a new window.
4.3.1 General

**Gateway Manager Language:** Select the language of the Gateway Manager. Note that this applies to the current user profile only.

**Gateway Manager TCP Port:** By default, port (4422) is used as Gateway Manager TCP port. In the TCP Port box you can enter any value between 1024 and 65535. However, certain ports are reserved for other services. Note that you must add the port number to the IP address (separated by a colon) in the browser's address bar when accessing Gateway Manager, for example https://192.168.0.1:4422. Click Apply to save your settings.

4.3.2 Access Control

**Allowed Admins:** Gateway Manager can be administered by multiple administrators simultaneously. In the Allowed Admins box you can specify which users or groups should have unlimited device administrative access to the Gateway Manager interface. These users will also be able to initially grant rights to other, so called restricted users. By default, this box is empty due to tighten security of a freshly installed system.

**Allowed Users:** Gateway Manager also offers restricted login access for users, who are only allowed to monitor or manage devices based on rights specifically granted to them. In the Allowed Users box you can specify which users or groups should have access to the Gateway Manager interface with these limited permissions. By default, this box is empty.

**Allowed Networks:** The Allowed Networks box lets you define the networks that should be able to connect to the Gateway Manager interface. For the sake of a secure installation this box is empty by default. This means that the Gateway Manager interface cannot be accessed from anywhere until you properly define your security policy and finish all system administrative aspects of your installation. The most secure solution would be to limit the access to Gateway Manager to only one administrator PC through HTTPS. It is recommended to use internal network(s) in this setting in order to improve security.

4.3.3 Device Security

This tab provides settings for securing your device connections.
4.4 Licensing

**Device Authentication**
Here you can define whether devices need authentication to be able to connect to Sophos UTM Manager.

**Require Authentication**: Select this checkbox to only allow authenticated devices to connect to Sophos UTM Manager. Devices authenticate by means of a shared secret. Enter the shared secret into the Shared Secret field below.

**Note** – You need initially to securely distribute this shared secret to every device that shall be able to connect to Sophos UTM Manager. Please refer to the online help of your respective firewall and/or gateway product(s) for additional information on how to set the shared secret there.

**Automatic Update**: Select this checkbox to automatically update all connected (online) devices when you change the shared secret. Thus, there is no need to provide every device manually with the new shared secret which is useful when there are many devices.

**Device Access Control**

**Allowed Networks**: This box lets you define networks from where devices should be able to connect to Sophos UTM Manager. Due to security reasons this box is empty by default. This means that SUM prevents any unauthorized device access until all necessary device security configurations have been finalized. In order to improve and ensure security you should only add networks which actually belong to your organization.

**Note** – During basic setup a dedicated certificate for SUM will be created which will be used to secure device access.

4.3.4 Open Gateway Manager

**Open Gateway Manager**: Click this button to open SUM’s Gateway Manager in a new window.

4.4 Licensing

After downloading the Sophos UTM Manager installation files from the Sophos website, you receive an email with the license file. You can simply upload this license file on the Licensing
> Installation tab.

The license file additionally is available in the MyAstaro Portal.

With the license you have full automatic update support, i.e. you will be automatically informed about new firmware updates. Also, firmware and pattern updates can be downloaded (and installed) automatically.

The license comes with Web Support. You can use the Sophos UTM Manager Support Forum and the Sophos Knowledgebase.

### 4.4.1 Overview

The Licensing > Overview tab provides detailed information about your license and is divided into multiple areas:

- **Base License**: Shows basic license parameters such as ID, registration date, or type.
- **Support Services**: Shows the support level plus the date until it is valid. Sophos UTM Manager always comes with Web Support.

### 4.4.2 Installation

On the Management > Licensing > Installation tab you can upload and install a new license.

To install a license, proceed as follows:

1. **Open the Upload File dialog window.**
   
   Click the Folder icon next to the License file box.

   The Upload File dialog window opens.

2. **Select the license file.**
   
   Browse to the directory where your license file resides.

   Select the license file you want to upload.

3. **Click Start Upload.**
   
   Your license file will be uploaded.

4. **Click Apply.**
   
   Your license will be installed. Note that the new license will automatically replace any other license already installed.

   The installation of the license will take approximately 60 seconds.
4.5 Up2Date

The Management > Up2Date menu allows the configuration of the update service of Sophos UTM Manager. Regularly installed updates keep your SUM up-to-date with the latest bug-fixes, product improvements, and virus patterns. Each update is digitally signed by Sophos—any unsigned or forged update will be rejected.

There are two types of updates available:

- **Firmware updates**: A firmware update contains bug-fixes and feature enhancements for Sophos UTM Manager Software.

- **Pattern updates**: A pattern update keeps the online help up-to-date.

In order to download Up2Date packages, SUM opens a TCP connection to the update servers on port 443—allowing this connection without any adjustment to be made by the administrator. However, if there is another firewall in between, you must explicitly allow the communication via the port 443 TCP to the update servers.

4.5.1 Overview

The Management > Up2Date > Overview tab provides a quick overview whether your system is up-to-date. From here, you can install new firmware and pattern updates.

Up2Date Progress

This section is only visible when you have triggered an installation process. Click the button Watch Up2Date Progress in New Window to monitor the update progress. If your browser does not suppress pop-up windows, a new window showing the update progress will be opened. Otherwise you will have to explicitly allow the pop-up window.

**Note** – A backup will be sent to the standard backup email recipients before an installation process is started.
Firmware
The Firmware section shows the currently installed firmware version. If an update package is available, a button Update to Latest Version Now is displayed. Additionally, you will see a message in the Available Firmware Up2Dates section. You can directly download and install the most recent update from here. Once you have clicked Update To Latest Version Now, you can watch the update progress in new a window. For this, click the Reload button of WebAdmin.

Available Firmware Up2Dates
If you have selected Manual on the Configuration tab, you can see a Check for Up2Date Packages Now button in this section, which you can use to download firmware Up2Date packages manually. If there are more than one Up2Dates available, you can select which one you are going to install. You can use the Update to Latest Version Now button in the Firmware section if you want to install the most recent version directly.

There is a Schedule button available for each Up2Date with which you can define a specific date and time where an update is to be installed automatically. To cancel a scheduled installation, click Cancel.

A note on "implicit" installations: There can be a constellation, where you schedule an Up2Date package which requires an older Up2Date package to be installed first. This Up2Date package
will be automatically scheduled for installation before the actual Up2Date package. However, you can define a specific time for this package, too, but you cannot prevent its installation.

Pattern
The Pattern section shows the current version of the installed patterns. If you have selected Manual on the Configuration tab, you can see a Update Patterns Now button. Use this button to download and install new patterns if available.

Note – The current pattern version does not need to be identical with the latest available pattern version in order for the SUM unit to be working correctly. A deviation between the current and the latest available pattern version might occur when new patterns are available, which, however, do not apply to the unit you are using. What patterns are downloaded is dependent on your settings and hardware configuration.

4.5.2 Configuration
By default, new update packages are automatically downloaded to SUM.

Firmware Download Interval
This option is set to 15 minutes by default, that is Sophos UTM Manager checks every 15 minutes for available firmware updates. Sophos UTM Manager will automatically download (but not install) available firmware update packages. The precise time when this happens is distributed randomly within the limits of the selected interval. You can change the interval up to Monthly or you can disable automatic firmware download by selecting Manual from the drop-down list. If you select Manual you will find a Check for Up2Date Packages Now button on the Overview tab.

Pattern Download/Installation Interval
This option is set to 15 minutes by default, that is Sophos UTM Manager checks every 15 minutes for available pattern updates. Sophos UTM Manager will automatically download and install available pattern update packages. The precise time when this happens is distributed randomly within the limits of the selected interval. You can change the interval up to Monthly or you can disable automatic pattern download and installation by selecting Manual from the drop-down list. If you select Manual you will find a Update Patterns Now button on the Overview tab.
4.5.3 Advanced

The Management > Up2Date > Advanced tab lets you configure further Up2Date options such as selecting a parent proxy or Up2Date cache for your SUM.

**Note** – Update packages can be downloaded from Sophos UTM Manager FTP server.

**Manual Up2Date Package Upload:** If your SUM does not have direct access to the Internet or an Up2Date cache to download new update packages directly, you can upload the update package manually. To do so, proceed as follows:

1. **Open the Upload File dialog window.**
   Click the Folder icon next to the Up2Date file box.
   The Upload File dialog window opens.

2. **Select the update package.**
   Click Browse in the Upload File dialog window and select the update package you want to upload.

3. **Click Start Upload.**
   The update package will be uploaded to SUM.

4. **Click Apply.**
   Your settings will be saved.

**Parent Proxy**

A parent proxy is often required in those countries that require Internet access to be routed through a government-approved proxy server. If your security policy requires the use of a parent proxy, you can set it up here by selecting the host definition and port.

**Use a parent proxy:** Select the checkbox to enable parent proxy use. Enter the hostname and the port of the proxy.

**Proxy requires authentication:** If the parent proxy requires authentication, enter username and password here.

If a parent proxy is configured, Sophos UTM Manager fetches both firmware and pattern Up2Dates from it.
4.5.4 Cache

On the Management > Up2Date > Cache tab you can enable the Up2Date Cache of SUM. The Up2Date Cache is a function that centrally downloads and then provides pattern updates and firmware updates to connected (managed) Sophos devices. This is useful to save bandwidth, since not every device needs to download updates individually. To enable the Up2Date cache function, proceed as follows:

1. **Enable the Up2Date Cache.**
   Click the toggle switch.
   The toggle switch turns amber and the Up2Date Cache area becomes editable.

2. **Make the following settings:**
   **Port:** Enter a port where the Up2Date Cache will provide the updates to the devices.
   You can enter any value between 1024 and 65535. However, certain ports are reserved for other services. By default, port 8080 is used.

   **Cache** (optional): Click the Clear button if you want to empty the cache manually. This operation might take some time to complete and it is recommended not to invoke it repeatedly.

   **Allowed Networks** (optional): Here you can define the device networks that should be able to use the Up2Date Cache. Due to security reasons this box is empty by default. This means that the Up2Date Cache cannot be accessed until all necessary access control configurations have been finalized. In order to tighten and ensure security you should only add networks which actually belong to your organization.

3. **Click Apply.**
   Your settings will be saved.

**Note** – Please consider that the Up2Date Cache is acting as a proxy to the actual Up2Date servers and hence will not allow connection requests to other destinations than the official Up2Date servers.

4.6 Backup/Restore

The backup restoring function allows you to save the SUM settings to a file on a local disk. This backup file allows you to install a known good configuration on a new or misconfigured system.
Be sure to make a backup after every system change. This will ensure that the most current settings are always available. In addition, keep your backups in a safe place, as it also contains security-relevant data such as certificates and cryptographic keys. After generating a backup, you should always check it for readability. It is also a good idea to use an external program to generate MD5 checksums, for this will allow you to check the integrity of the backup later on.

4.6.1 Backup/Restore

On the Management > Backup/Restore > Backup/Restore tab you can create backups, import backups, as well as restore, download, send, and delete existing backups.

Available Backups

This section is only visible if at least one backup has been created before, either by the automatic backup function or manually (see section Create Backup).

All backups are listed giving date and time of their creation, their SUM version number, the user who created it, and the comment.

You can decide whether to download, restore, delete, or send a backup.

- **Download**: Opens a dialog window where you can decide to download the file encrypted (provide password) or unencrypted. Click Download Backup. You are prompted to select a location in the file system for the downloaded backup to reside.

  - **Encrypt before downloading**: Before downloading or sending it, you have the option to encrypt the backup. Encryption is realized with Blowfish cipher in CBC mode. Provide a password (second time for verification). You will be asked for this password when importing the backup. The file extension for encrypted backups is ebf, for unencrypted backups abf.

  **Note** – A backup does include administrator passwords, the high availability passphrase if configured, as well as all RSA keys and X.509 certificates. Since this information is confidential, it is good practice to enable encryption.

- **Restore**: Replaces the current system settings by the settings stored in a backup. You will have to log in again afterwards. If the selected backup contains all data you can log in directly. If the selected backup does not contain all data (see section Create Backup) you will have to enter the necessary data during the login procedure. If only the host data has been removed in the selected backup you can add an additional administrative email
address if you want. It will be used where no recipient is given and as additional address where multiple recipients are possible.

- **Restoring backups from USB flash drive:** You can also restore unencrypted backup files (file extension `.abf`) from a FAT formatted USB flash drive such as a simple USB stick. To restore a backup from a USB flash drive, copy the backup file to the USB flash drive and plug the device into Sophos UTM Manager prior to boot up. If several backup files are stored on the device, the lexicographically first file will be used (numbers precede letters). For example, suppose the backup files `utm_manager_backup_2013-04-17.abf` and `2012-03-20_utm_manager_backup.abf` are both stored on the USB flash drive. During the boot up, the second file will be used because it begins with a number, although it is much older than the other one.

In addition, a lock file is created after the successful recovery of a backup, preventing the installation of the same backup over and over again while the USB flash drive is still being plugged in. However, if you want to install a previous backup once again, you must first reboot with no USB flash drive plugged in. This will delete all lock files. When you now boot with the USB flash drive plugged in again, the same backup can be installed.

- **Delete:** Deletes a backup from the list. Using the Delete icon on the bottom of the list, you can delete all selected backups. To select backups, click the checkboxes to the left of the backups or use the checkbox on the bottom to select all backups.

- **Send:** Opens a dialog window where you can decide to send the file encrypted (provide password) or unencrypted. Click **Send Now** to send the backup. Recipients will be the standard recipients, that is, the backup will be sent to the address(es) provided on the **Automatic Backups** tab.

  - **Encrypt before sending:** See **Encrypt before downloading** above.

### Create Backup
Backups are not only useful to restore your system after an (unwanted) change or failure. Moreover, they can be used as templates to set up systems that should have a similar configuration so that those systems are already pre-configured in some way which can save you a lot of time. For that, you can strip certain information from a backup before it is created, e.g. hostname, certificates, etc.

To create a backup with the current system state, proceed as follows:
1. **In the Create Backup section, enter a comment** (optional).
   The comment will be displayed along with the backup in the backup list.

2. **Make the following settings** (optional):
   - **Remove unique site data**: Select this option to create the backup without host-specific data. This includes hostname, system ID, SNMP data, HA data, license, shell user passwords, and anonymization passwords as well as all certificates, public and private keys, fingerprints and secrets of Email Protection, Web Protection, Client Authentication, IPsec, SSL VPN, RED, WebAdmin, Web Application Firewall, and proxies. Such backups are a convenient means to set up multiple similar systems. There are some things to consider though: 1) After restoring you are presented the basic system setup. 2) Only the first interface is configured, the primary IP address being the one that has been configured during installation. All other interfaces will be disabled and set to IP address 0.0.0.0.
   - **Remove administrative mail addresses**: Select this option to additionally remove the administrator email addresses used in various parts of SUM, e.g. postmaster addresses in Email Protection, notifications, etc. This option is especially useful for IT partners who set up Sophos UTM Manager devices at customers' sites.

3. **Click Create Backup Now**.
   The backup appears in the list of available backups.

   If a backup is created with one or both of the options selected, the backup entry contains a respective additional comment.

**Import Backup**
To import a backup, click the Folder icon and select a backup file to upload, then click **Start Upload**. When importing an encrypted backup file, you must provide the correct passphrase prior to importing the backup. Note that the backup will not instantly be restored. Instead, it will be added to the **Available Backups** list.
4.6.2 Automatic Backups

On the Management > Backup/Restore > Automatic Backup tab you can configure several options dealing with the automatic generation of backups. To have backups created automatically, proceed as follows:

1. **Enable automatic backups on the Automatic Backups tab.**
   
   Click the toggle switch.
   
   The toggle switch turns green and the Options and Send Backups by Email areas become editable.

2. **Select the interval.**
   
   Automatic backups can be created at various intervals.
   
   You can choose between daily, weekly, and monthly.

3. **Specify the maximum number of backups to be stored.**
   
   Backups are stored up to the number you enter here. Once the maximum has been reached, the oldest backups will be deleted.
   
   Note that this applies to automatically created backups only. Backups created manually and backups created automatically before a system update will not be deleted.

4. **Click Apply.**
   
   Your settings will be saved.

To save you the work of backing up your SUM manually, the backup feature supports emailing the backup file to a list of defined email addresses.

**Recipients:** Automatically generated backups will be sent to users contained in the Recipients box. Multiple addresses can be added. By default, the first administrator’s email address is used.

**Encrypt email backups:** In addition, you have the option to encrypt the backup (Triple DES encryption).

**Password:** Once you have selected the Encrypt email backups option, provide a password (second time for verification). You will be prompted for this password when importing the backup.

Automatically created backups will appear in the Available Backups list on the Backup/Restore tab, marked with the System flag indicating the Creator. From there, they can be restored, downloaded, or deleted as any backup you have created by yourself.
4.7 User Portal

The User Portal of Sophos UTM Manager is a special browser-based application on the unit enabling authorized users to change their password. That way, users who are allowed to use the Gateway Manager but not the WebAdmin can nonetheless change their password. It can be accessed by browsing to the URL of Sophos UTM Manager, for example, https://192.168.2.100 (note the HTTPS protocol and the missing port number 4444 you would normally enter for accessing the WebAdmin interface).

For more information on how to exclude users from WebAdmin see section Management > WebAdmin Settings > Access Control. Information on how to give users access to the Gateway Manager can be found in section Management > Sophos UTM Manager > Access Control.

On the login page, users can select a language from the drop-down list located on the right side of the header bar.

![User Portal: Welcome Page](image)

**Figure 9** User Portal: Welcome Page
4.7 User Portal

4.7.1 Global

On the Management > User Portal > Global tab you can enable the User Portal. Additionally you can specify which networks and which users should be granted access to the User Portal.

To enable User Portal access, proceed as follows:

1. **Enable the User Portal.**
   - Click the toggle switch.
   - The toggle switch turns amber and the End-User Portal Options area becomes editable.

2. **Select the allowed networks.**
   - Select the networks that should be allowed to access the User Portal.

3. **Select the allowed users.**
   - Select the users or user groups that should be able to access the User Portal.
   - If you do not want to grant access to all users, unselect the Allow all users checkbox and select the users and user groups individually.

4. **Click Apply.**
   - Your settings will be saved.

4.7.2 Advanced

On the Advanced tab you can configure an alternative hostname and port number for the User Portal as well as language and security options.

**Language**

During login, the User Portal fetches the language settings of the web browser and loads the respective locales to display the portal in the same language as the browser defaults. For browser language settings that are not available for the User Portal, you can select here which language will be the fallback language. Users have additionally the option to select a language on the User Portal login page.

**Security**

The User Portal uses cookies to track sessions. Persistent cookies permit to return after having closed a session without having to log in again. They can always be deleted from user-side, however, by using the Log Out button of the User Portal.
Network Settings
Hostname: By default, this is SUM's hostname as given on the Management > System Settings > Hostname tab. However, if you want to grant access to the User Portal for users gaining access over the Internet, it might be necessary to enter an alternative hostname here that can be publicy resolved.

Listen Address: Default value is Any. When using the web application firewall you need to give a specific interface address for the service to listen for User Portal connections. This is necessary for the User Portal connection handler and the web application firewall to be able to differentiate between the incoming SSL connections.

Port: By default, port 443 for HTTPS is selected. You can change the port to any value in the range from 1024 to 65535. Note that you cannot select either 10443 or the WebAdmin TCP Port, which is configured on the Management > WebAdmin Settings > Advanced tab. Independent of the defined port, the User Portal can always be accessed via HTTPS only.

Welcome Message
You can customize the welcome message of the User Portal. Simple HTML markup and hyperlinks are allowed.

Note – Changing the welcome message is not possible when using a home use license.

4.8 Notifications
Sophos UTM Manager comes with a notification feature that informs you immediately about all sorts of security-relevant events occurring on SUM, either by email or SNMP trap. All events that might possibly be of interest to an administrator are represented by various error, warning, and information codes. What notifications are sent depends on the selection you have configured on the Notifications tab.

4.8.1 Global
On the Management > Notifications > Global tab you can configure the sender address (i.e., the From address) to be taken for notification emails sent by SUM. By default, this is do-not-reply@fw-notify.net. If you want to change this address, it is advisable to enter an email
address of your domain, as some mail servers might be configured to check whether a given sender address really exists.

In addition, you can specify the recipients of SUM notifications. By default, this is the administrator's email address you had entered during the initial setup.

**Limit Notifications:** Some security-relevant events such as detected intrusion attempts will create a lot of notifications, which may quickly clog the notification recipients' email inboxes. For this reason, Sophos UTM Manager has sensible default values to limit the number of notifications sent per hour. If you disable this option, every security-relevant event will create a notification, provided the event is configured so as to send a notification on the Management > Notifications > Notifications tab.

### Device Specific Text

Here you can enter a description of Sophos UTM Manager, e.g. its location, which will be displayed in the notifications sent.

#### 4.8.2 Notifications

Notifications are divided into three categories:

- **CRIT:** Messages informing about critical events that might render SUM inoperable.
- **WARN:** Warnings about potential problems that need your attention, for example, exceeding thresholds.
- **INFO:** Merely informational messages such as the restart of a system component, for example.

You can select whether you want to send the notification as email or SNMP trap.

#### 4.8.3 Advanced

In case your SUM cannot send emails directly, you can configure a smarthost to send the emails. Proceed as follows:

1. **Enable External SMTP on the Management > Notifications > Advanced tab.**
   Click the toggle switch.

2. **Enter your smarthost.**
   You can use drag-and-drop. The port is preset to the default SMTP port 25.
- **Use TLS**: Select this checkbox if you want to enforce TLS when sending notifications. Note that notifications will not be sent if the smarthost does not support TLS.

3. **Specify the authentication settings.**
   If the smarthost requires authentication, check the Authentication checkbox and enter the corresponding username and password.

4. **Click Apply.**
   Your settings will be saved.

### 4.9 Customization

The tabs under *Management > Customization* allow you to customize and localize email notifications and status messages created by Sophos UTM Manager, making it possible to adapt those messages to both your policy and your corporate identity.

**Note** – Customization is not possible when using a home use license.

### 4.9.1 Global

On the *Management > Customization > Global* tab you can customize global display options for the system messages presented to users. Note that UTF-8/Unicode is supported.

**Company Logo**

You can upload your own logo/banner (in *png* format only), which is used for email notifications.

To upload a logo:

1. **Open the Upload file dialog window.**
   Click the Folder icon next to the *Upload new logo* box.

   The *Upload file* dialog window opens.

2. **Select the logo.**
   Browse to the location where the logo that you want to upload resides.

   Once you have selected the logo, click *Start Upload.*

3. **Click Apply.**
   The logo will be uploaded, replacing the file that is already installed.
Custom Company Text
Customize the message that will be displayed beneath the company logo. For example, you might want to enter the administrator’s contact data here.

4.10 SNMP
The Simple Network Management Protocol (SNMP) is used by network management systems to monitor network-attached devices such as routers, servers, and switches. SNMP allows the administrator to make quick queries about the condition of each monitored network device. You can configure Sophos UTM Manager to reply to SNMP queries or to send SNMP traps to SNMP management tools. The former is achieved with so-called management information bases (MIBs). An MIB specifies what information can be queried for which network device. Sophos UTM Manager supports SNMP version 2 and 3 and the following MIBs:

- DISMAN-EVENT-MIB: Event Management Information Base
- HOST-RESOURCES-MIB: Host Resources Management Information Base
- IF-MIB: Interfaces Group Management Information Base
- IP-FORWARD-MIB: IP Forwarding Table Management Information Base
- IP-MIB: Management Information Base for the Internet Protocol (IP)
- NOTIFICATION-LOG-MIB: Notification Log Management Information Base
- RFC1213-MIB: Management Information Base for Network Management of TCP/IP-based Internet: MIB II
- SNMPv2-MIB: Management Information Base for the Simple Network Management Protocol (SNMP)
- TCP-MIB: Management Information Base for the Transmission Control Protocol (TCP)
- UDP-MIB: Management Information Base for the User Datagram Protocol (UDP)

In order to get Sophos UTM Manager system information, an SNMP manager must be used that has at least the RFC1213-MIB (MIB II) compiled into it.

4.10.1 Query
On the Management > SNMP > Query page you can enable the usage of SNMP queries.

To configure SNMP queries, proceed as follows:
1. **Enable SNMP Queries.**
   Click the toggle switch.

   The sections *SNMP Version* and *SNMP Access Control* become editable.

2. **Select the SNMP version.**
   In the *SNMP Version* section, select a version from the drop-down list. SNMP version 3 requires authentication.

3. **Select allowed networks.**
   Networks listed in the *Allowed networks* box are able to query the SNMP agent running on Sophos UTM Manager. Note that the access is always read-only.

   - **Community String:** When using version 2, enter a community string. An SNMP community string acts as a password that is used to protect access to the SNMP agent. By default, the SNMP community string is "public", but you can change it to any setting that best suits your needs.

     **Note** – Allowed characters for the community string are: (a-z), (A-Z), (0-9), (+), (-), (@), (.), (-), (blank).

   - **Username/Password:** When using version 3, authentication is required. Enter a username and password (second time for verification) to enable the remote administrator to send queries. The password must have at least eight characters. SNMP v3 uses SHA for authentication and AES for encryption. Note that username and password are used for both of them.

4. **Click Apply.**
   Your settings will be saved.

Furthermore, you can enter additional information about SUM.

**Device Information**

The *Device Information* text boxes can be used to specify additional information about SUM such as its name, location, and administrator. This information can be read by SNMP management tools to help identify SUM.

**Note** – All SNMP traffic (protocol version 2) between SUM and the *Allowed networks* is not encrypted and can be read during the transfer over public networks.
Sophos UTM Manager Notifier MIB
This section allows you to download the Sophos UTM Manager notifier MIB which contains the definitions of the Sophos UTM Manager SNMP notification based on your current settings for the notification traps.

4.10.2 Traps
In the Traps tab you can define an SNMP trap server to which notifications of relevant events occurring on SUM can be sent as SNMP traps. Note that special SNMP monitoring software is needed to display those traps.

The messages that are sent as SNMP traps contain so-called object identifiers (OID), for example, .1.3.6.1.4.1.9789, which belong to the private enterprise numbers issued by IANA. Note that .1.3.6.1.4.1 is the iso.org.dod.internet.private.enterprise prefix, while 9789 is Astaro's Private Enterprise Number. The OID for notification events is 1500, to which are appended the OIDs of the type of the notification and the corresponding error code (000–999). The following notification types are available:

- **DEBUG** = 0
- **INFO** = 1
- **WARN** = 2
- **CRIT** = 3

Example: The notification "INFO-302: New firmware Up2Date installed" will use the OID .1.3.6.1.4.1.9789.1500.1.302 and has the following string assigned:

```
[<HOST>] [INFO] [302]
```

Note that `<HOST>` is a placeholder representing the hostname of the system and that only type and error code from the notification's subject field are transmitted.

To select an SNMP trap server, proceed as follows:

1. **Click New SNMP Trap Sink.**
   The Create New SNMP Trap Sink dialog box opens.

2. **Make the following settings:**
   - **Host:** The host definition of the SNMP trap server.
Community string: An SNMP community string acts as a password that is used to protect access to querying SNMP messages. By default, the SNMP community string is set to "public". Change it to the string that is configured on the remote SNMP trap server.

Note – Allowed characters for the community string are: (a-z), (A-Z), (0-9), (+), (_), (@), (.), (-), (blank).

Comment (optional): Add a description or other information.

3. Click Save.
The new SNMP trap server will be listed on the Traps tab.

4.11 Certificate Management

The Management > Certificate Management menu is the central place to manage all certificate-related operations of Sophos UTM Manager. This includes creating or importing X.509 certificates as well as uploading so-called Certificate Revocation Lists (CRLs), among other things.

4.11.1 Certificates

On the Management > Certificate Management > Certificates tab you can create or import public key certificates in the X.509 standard format. Such certificates are digitally signed statements usually issued by a Certificate Authority (CA) binding together a public key with a particular Distinguished Name (DN) in X.500 notation.

All certificates you create on this tab contain an RSA key. They are signed by the self-signed certificate authority (CA) VPN Signing CA that was created automatically using the information you provided during the initial login to the WebAdmin interface.

To generate a certificate, proceed as follows:

1. On the Certificates tab, click New Certificate.
The Add Certificate dialog box opens.

2. Make the following settings:
   Name: Enter a descriptive name for this certificate.

   Method: To create a certificate, select Generate (for more information on uploading certificates, see below).
4.11 Certificate Management

Key size: The length of the RSA key. The longer the key, the more secure it is. You can choose among key sizes of 1024, 2048, or 4096 bits. Select the maximum key size compatible with the application programs and hardware devices you intend to use. Unless longer keys cause critical performance issues for your specific purposes, do not reduce the key size in order to optimize performance.

VPN ID type: You have to define a unique identifier for the certificate. The following types of identifiers are available:

- Email address
- Hostname
- IP address
- Distinguished name

VPN ID: Depending on the selected VPN ID type, enter the appropriate value into this text box. For example, if you selected IP address from the VPN ID type list, enter an IP address into this text box. Note that this text box will be hidden when you select Distinguished Name from the VPN ID type list.

Use the drop-down lists and text boxes from Country to Email to enter identifying information about the certificate holder. This information is used to build the Distinguished Name, that is, the name of the entity whose public key the certificate identifies. This name contains a lot of personal information in the X.500 standard and is supposed to be unique across the Internet. If the certificate is for a road warrior connection, enter the name of the user in the Common name box. If the certificate is for a host, enter a hostname.

Comment (optional): Add a description or other information.

3. **Click Save.**
   The certificate appears on the Certificates list.

To delete a certificate click the button **Delete** of the respective certificate.

Alternatively, to upload a certificate, proceed as follows:

1. **On the Certificates tab, click New Certificate.**
   The Add Certificate dialog box opens.

2. **Make the following settings:**
   - **Name:** Enter a descriptive name for this certificate.
   - **Method:** Select Upload.
File type: Select the file type of the certificate. You can upload certificates being one of the following types:

- **PKCS#12 (Cert+CA):** PKCS refers to a group of *Public Key Cryptography Standards* (PKCS) devised and published by RSA laboratories. The PKCS#12 file format is commonly used to store private keys with accompanying public key certificates protected with a container passphrase. You must know this container passphrase to upload files in this format.

- **PEM (Cert only):** A Base64 encoded *Privacy Enhanced Mail* (PEM) file format with no password required.

File: Click the Folder icon next to the File box and select the certificate you want to upload.

Comment (optional): Add a description or other information.

3. Click Save.
   The certificate appears on the Certificates list.

To delete a certificate click the button Delete of the respective certificate.

You can download the certificate either in PKCS#12 or as PEM format. The PEM file only contains the certificate itself, while the PKCS#12 file also contains the private key as well as the CA certificate with which it was signed.

### 4.11.2 Certificate Authority

On the *Management > Certificate Management > Certificate Authority* tab you can add new *Certificate Authorities* to the unit. Generally speaking, a certificate authority or *Certification Authority* (CA) is an entity which issues digital certificates for use by other parties. A CA attests that the public key contained in the certificate belongs to the person, organization, host, or other entity noted in the certificate by signing the certificate signing request with the private key of the CA's own certificate. Such a CA is therefore called a signing CA.

On SUM, the signing CA was created automatically using the information you provided during the initial login to SUM. Thus, all certificates you create on the *Certificates* tab are self-signed certificates, meaning that the issuer and the subject are identical. However, you can alternatively import a signing CA by third-party vendors. In addition, to verify the authenticity of a host or user requesting an IPsec connection, you can also use alternative CA certificates whose private keys are unknown. Those CA certificates are called verification CAs and can be added on this tab as well.
4.11 Certificate Management

**Important Note** – You can have multiple verification CAs on your system, but only one signing CA. So if you upload a new signing CA, the previously installed signing CA automatically becomes a verification CA.

To import a CA, proceed as follows:

1. **On the Certificate Authority tab, click Import CA.**
   The Import CA dialog box opens.

2. **Make the following settings:**
   - **Name:** Enter a descriptive name for this CA.
   - **Type:** Select the type of CA you are going to import. You can choose between verification CAs or signing CAs. A verification CA must be available in the PEM format, while a signing CA must be available in the PKCS#12 format.
   - **CA Certificate:** Click the Folder icon next to the CA Certificate box and select the certificate you want to import. Note that if you are to upload a new signing CA, you must enter the password with which the PKCS#12 container was secured.
   - **Comment (optional):** Add a description or other information.

3. **Click Save.**
   The new CA certificate appears on the Certificate Authority list.

To delete a CA click the button **Delete** of the respective CA.

The signing CA can be downloaded in PKCS#12 format. You will then be prompted to enter a password, which will be used to secure the PKCS#12 container. In addition, verification CAs can be downloaded in PEM format.

### 4.11.3 Revocation Lists (CRLs)

A CRL is a list of certificates (more precisely, their serial numbers) which have been revoked, that is, are no longer valid, and should therefore not be relied upon. On the Management > Certificate Management > Revocation Lists (CRLs) tab you can upload the CRL that is deployed within your PKI.

To upload a CRL, proceed as follows:

1. **On the Revocation Lists (CRLs) tab, click Upload CRL.**
   The Upload CRL dialog box opens.
2. **Make the following settings:**
   - **Name:** Enter a descriptive name for this CRL.
   - **CRL File:** Click the Folder icon next to the *CRL File* box and select the CRL you want to upload.
   - **Comment** (optional): Add a description or other information.

3. **Click Save.**
   The new CRL appears on the list of revocation lists.

To delete a CRL click the button *Delete* of the respective CRL.

### 4.11.4 Advanced

On the *Management > Certificate Management > Advanced* tab you can re-generate the VPN Signing CA that was created during the initial setup of the unit. The VPN Signing CA is the certificate authority with which digital certificates are signed that are used for remote access and site-to-site VPN connections. The old VPN signing CA will be kept as verification CA.

**Re-generate Signing CA**

You can renew all user certificates using the current signing CA. This becomes relevant once you have installed an alternative VPN Signing CA on the *Certificate Authority* tab.

**Caution** – The SUM and all user certificates will be re-generated using the new signing CA. This will break certificate-based site-to-site and remote access VPN connections.

### 4.12 Shutdown and Restart

On this tab you can manually shut down or restart Sophos UTM Manager.

**Shutdown:** This action allows you to shut down the system and to stop all services in a proper manner. For systems without a monitor or LCD display, the end of the shutdown process is signaled by an endless series of beeps at intervals of one second.

To shut down Sophos UTM Manager, proceed as follows:

1. **Click **Shutdown (Halt) the System Now.**

2. **Confirm the warning message.**
   When asked "Really shut down the system?", click OK.
The system is going down for halt.

Depending on your hardware and configuration, this process may take several minutes to complete. Only after the system has completely shut down you should turn off the power. If you turn off the power without the system being shut down properly, the system will check the consistency of its file system during the next booting, meaning that the boot-up process will take much longer than usual. In the worst case, data may have been lost.

The system will beep five times in a row to indicate a successful system start.

**Restart:** This action will shut down the system completely and reboot. Depending on your hardware and configuration, a complete restart can take several minutes.

To restart Sophos UTM Manager, proceed as follows:

1. **Click Restart (Reboot) the System Now.**
2. **Confirm the warning message.**
   When asked "Really restart the system?", click OK.

   The system is going down for halt and reboot.
5 Definitions & Users

This chapter describes how to configure network and service definitions used throughout Sophos UTM Manager. The Definitions Overview page in WebAdmin shows the number of network definitions according to type as well as the numbers of service definitions according to protocol type.

The pages of the Definitions & Users menu allow you to define networks and services that can be used in all other configuration menus in one central place. This allows you to work with the names you define rather than struggling with IP addresses, ports, and network masks. Another benefit of definitions is that you can group individual networks and services together and configure them all at once. If, for example, you assign certain settings to these groups at a later time, these settings will apply to all networks and services contained therein.

Additionally, this chapter describes how to configure user accounts, user groups, and external authentication servers of Sophos UTM Manager as well as authentication for client PCs.

The following topics are included in this chapter:

- Network Definitions
- Service Definitions
- Users & Groups
- Authentication Servers

5.1 Network Definitions

The Definitions & Users > Network Definitions menu lets you create hosts, networks, and network groups as well as MAC address definitions. The definitions created here can be used in many other WebAdmin configurations.

5.1.1 Network Definitions

The Definitions & Users > Network Definitions > Network Definitions tab is the central place for defining hosts, networks, and network groups on SUM. The definitions created here can be used on many other WebAdmin configuration menus.
Opening the tab, by default, all network definitions are displayed. Using the drop-down list on top of the list, you can choose to display network definitions with certain properties.

**Tip** – When you click on the Info icon of a network definition in the *Network Definitions* list, you can see all configuration options in which the network definition is used.

The network table also contains static networks, which were automatically created by the system and which can neither be edited nor deleted:

- **Interface Address**: A definition of this type will be added for each network interface. It contains the current IP address of the interface. Its name consists of the interface name with ",(Address)" appended to it.

- **Interface Broadcast Address**: A definition of this type will be added for each Ethernet-type network interface. It contains the current IPv4 broadcast address of the interface. Its name consists of the interface name with ",(Broadcast)" appended to it.

- **Interface Network Address**: A definition of this type will be added for each Ethernet-type network interface. It contains the current IPv4 network of the interface. Its name consists of the interface name with ",(Network)" appended to it.

- **Internet**: A network definition bound to the interface which serves as default gateway. Making use of it in your configuration should make the configuration process easier. With uplink balancing enabled, the definition *Internet* is bound to *Uplink Interfaces*.

**Note** – User network objects authenticated via client authentication will always be shown as unresolved due to performance reasons.

To create a network definition, proceed as follows:

1. **On the Network Definitions tab, click New Network Definition.**
   The *Create New Network Definition* dialog box opens.

2. **Make the following settings:**
   (Note that further parameters of the network definition will be displayed depending on the selected definition type.)

   - **Name**: Enter a descriptive name for this definition.
   - **Type**: Select the network definition type. The following types are available:
Host: A single IP address. Provide the following information:
- IPv4 address: The IP address of the host (note that you cannot enter the IP address of a configured interface).
- DHCP Settings (optional): In this section you can create static mappings between hosts and IP address. For that purpose, you need a configured DHCP server (see Network Services > DHCP > Servers).

Note – To avoid an IP address clash between regularly assigned addresses from the DHCP pool and those statically mapped make sure that the latter are not in the scope of the DHCP pool. For example, a static mapping of 192.168.0.200 could result in two systems receiving the same IP address if the DHCP pool is 192.168.0.100 – 192.168.0.210.

IPv4 DHCP: Select the IPv4 DHCP server to be used for static mapping.

MAC addresses: Enter the MAC addresses of the hosts’ network interface cards. The MAC addresses are usually specified in a format consisting of six groups of two hexadecimal digits, separated by colons (e.g., 00:04:76:16:EA:62).

DNS Settings (optional): If you do not want to set up your own DNS server but need static DNS mappings for a few hosts of your network, you can enter these mappings in this section of the respective hosts. Note that this only scales for a limited number of hosts and is by no means intended as a replacement of a fully operable DNS server.
- Hostname: Enter the fully qualified domain name (FQDN) of the host.
- Reverse DNS: Select the checkbox to enable the mapping of the host’s IP address to its name. Note that although several names can map to the same IP address, one IP address can only ever map to one name.
- Additional hostnames: Click the Plus icon to add additional hostnames for the host.

DNS host: A DNS hostname, dynamically resolved by the system to produce an IP address. DNS hosts are useful when working with dynamic IP endpoints. The system will re-resolve these definitions periodically according to the TTL (Time To Live) values and update the definition with the new IP address (if any). Provide the following information:
- Hostname: The hostname you want to resolve.
5.1 Network Definitions

- **DNS group**: Similar to DNS host, but can cope with multiple RRs (Resource Records) in DNS for a single hostname.

- **Network**: A standard IP network, consisting of a network address and a netmask. Provide the following information:
  - **IPv4 address**: The network address of the network (note that you cannot enter the IP address of a configured interface).
  - **Netmask**: The bit mask used to tell how many bits in an octet(s) identify the subnetwork, and how many bits provide room for host addresses.

- **Range**: Select to define a whole IPv4 address range. Provide the following information:
  - **IPv4 from**: First IPv4 address of the range.
  - **IPv4 to**: Last IPv4 address of the range.

- **Network group**: A container that includes a list of other network definitions. You can use them to bundle networks and hosts for better readability of your configuration. Once you have selected **Network group**, the **Members** box appears where you can add the group members.

- **Availability group**: A group of hosts and/or DNS hosts sorted by priority. Alive status of all hosts is checked with ICMP pings at an interval of 60 seconds, by default. The host with the highest priority and an alive status is used in configuration. Once you have selected **Availability group**, the **Members** box appears where you can add the group members.

**Comment** (optional): Add a description or other information.

3. **Optionally, make the following advanced settings:**
   The options displayed depend on the selected **Type** above.

   **Interface** (optional): You can bind the network definition to a certain interface, so that connections to the definition will only be established via this interface.

   **Monitoring type** (only with type **Availability group**): Select the service protocol for the alive status checks. Select either **TCP** (TCP connection establishment), **UDP** (UDP connection establishment), **Ping** (ICMP Ping), **HTTP Host** (HTTP requests), or **HTTPS Hosts** (HTTPS requests) for monitoring. When using **UDP** a ping request will be sent initially which, if successful, is followed by a UDP packet with a payload of 0. If ping does not succeed or the ICMP port is unreachable, the host is regarded as down.
Port (only with monitoring type TCP or UDP): Number of the port the request will be sent to.

URL (optional, only with monitoring types HTTP Host or HTTPS Host): URL to be requested. You can use other ports than the default ports 80 or 443 by adding the port information to the URL, e.g., http://example.domain:8080/index.html. If no URL is entered, the root directory will be requested.

Interval: Enter a time interval in seconds at which the hosts are checked.

Timeout: Enter a maximum time span in seconds for the hosts to send a response. If a host does not respond during this time, it will be regarded as dead.

Always resolved: This option is selected by default, so that if all hosts are unavailable, the group will resolve to the host which was last available. Otherwise the group will be set to unresolved if all hosts are dead.

4. Click Save.
The new definition appears on the network definition list.

To either edit or delete a network definition, click the corresponding buttons.

5.1.2 MAC Address Definitions

The Definitions & Users > Network Definitions > MAC Address Definitions tab is the central place for defining MAC address definitions, i.e., lists of MAC addresses. A MAC address definition can be used like a network definition. Additionally it can be used to further restrict a rule based on hosts/IP addresses to only match devices which have one of the defined MAC addresses.

Tip – When you click on the Info icon of a MAC address definition, you can see all configuration options in which the definition is used.

To create a MAC address definition, proceed as follows:

1. On the MAC Address Definitions tab, click New MAC Address List.
The Create MAC Address List dialog box opens.

2. Make the following settings:
   Name: Enter a descriptive name for this definition.
MAC addresses: Click the Plus icon to enter individual MAC addresses subsequently or use the Action icon to import a list of MAC addresses via copy and paste. The MAC addresses are usually specified in a format consisting of six groups of two hexadecimal digits, separated by colons (e.g., 00:04:76:16:EA:62).

Hosts: Add the hosts whose MAC addresses you want to add to the MAC address definition. The MAC addresses defined in the DHCP Settings section of the host definition will be added to the MAC address list.

Note – You can either enter MAC addresses or hosts or both.

Comment (optional): Add a description or other information.

3. Click Save.
The new definition appears on the MAC Address Definition list.

To either edit or delete a MAC address definition, click the corresponding buttons.

5.2 Service Definitions

On the Definitions & Users > Service Definitions page you can centrally define and manage services and service groups. Services are definitions of certain types of network traffic and combine information about a protocol such as TCP or UDP as well as protocol-related options such as port numbers. You can use services to determine the types of traffic accepted or denied by SUM.

Tip – When you click on the Info icon of a service definition in the Service Definitions list, you can see all configuration options in which the service definition is used.

To create a service definition, proceed as follows:

The Create New Service Definition dialog box opens.

2. Make the following settings:
(Note that further parameters of the service definition will be displayed depending on the selected definition type.)

   Name: Enter a descriptive name for this definition.
Type of Definition: Select the service type. The following types are available:

- **TCP**: Transmission Control Protocol (TCP) connections use port numbers ranging from 0 to 65535. Lost packets can be recognized through TCP and be requested again. In a TCP connection, the receiver notifies the sender when a data packet was successfully received (connection related protocol). TCP sessions begin with a three way handshake and connections are closed at the end of the session. Provide the following information:
  - **Destination Port**: Enter the destination port either as single port number (e.g., 80) or as a range (e.g., 1024:64000), using a colon as delimiter.
  - **Source Port**: Enter the source port either as single port number (e.g., 80) or as a range (e.g., 1024:64000), using a colon as delimiter.

- **UDP**: The *User Datagram Protocol* (UDP) uses port numbers between 0 and 65535 and is a stateless protocol. Because it does not keep state, UDP is faster than TCP, especially when sending small amounts of data. This statelessness, however, also means that UDP cannot recognize when packets are lost or dropped. The receiving computer does not signal the sender when receiving a data packet. When you have selected *UDP*, the same configuration options can be edited as for TCP.

- **TCP/UDP**: A combination of TCP and UDP appropriate for application protocols that use both sub protocols such as DNS. When you have selected *TCP/UDP*, the same configuration options can be edited as for TCP or UDP.

- **ICMP**: The *Internet Control Message Protocol* (ICMP) is chiefly used to send error messages, indicating, for example, that a requested service is not available or that a host or router could not be reached. Once you have opted for *ICMP*, select the ICMP code/type.

- **IP**: The *Internet Protocol* (IP) is a network and transport protocol used for exchanging data over the Internet. Once you have selected *IP*, provide the number of the protocol to be encapsulated within IP, for example 121 (representing the SMP protocol).

- **ESP**: The *Encapsulating Security Payload* (ESP) is a part of the IPsec tunneling protocol suite that provides encryption services for tunneled data via VPN. Once you have selected ESP or AH, provide the *Security Parameters Index* (SPI), which identifies the security parameters in combination with the IP address. You can either enter a value between 256 and 4,294,967,296 or keep the default setting given as the range from 256 to 4,294,967,296 (using a colon as delimiter),
especially when using automatic IPsec key exchange. Note that the numbers 1-255 are reserved by the Internet Assigned Numbers Authority (IANA).

- **AH**: The Authentication Header (AH) is a part of the IPsec tunneling protocol suite and sits between the IP header and datagram payload to maintain information integrity, but not secrecy.

- **Group**: A container that includes a list of other service definitions. You can use them to bundle service definitions for better readability of your configuration. Once you have selected Group, the Members box opens where you can add group members (i.e., other service definitions).

**Comment** (optional): Add a description or other information.

3. **Click Save**.
   The new definition appears on the Service Definitions list.

To either edit or delete a definition, click the corresponding buttons.

**Note** – The type of definition cannot be changed afterwards. If you want to change the type of definition, you must delete the service definition and create a new one with the desired settings.

### 5.3 Users & Groups

The Definitions & Users > Users & Groups menu lets you create users and groups for WebAdmin access as well as for remote access, User Portal access, email usage etc.

#### 5.3.1 Users

On the Definitions & Users > Users & Groups > Users tab you can add user accounts to SUM. In its factory default configuration, Sophos UTM Manager has one administrator called **admin**.

**Tip** – When you click on the Info icon of a user definition in the Users list, you can see all configuration options in which the user definition is used.

When you specify an email address in the New User dialog box, an X.509 certificate for this user will be generated simultaneously while creating the user definition, using the email address as the certificate's VPNID. On the other hand, if no email address is specified, a certificate will be
created with the user's *Distinguished Name* (DN) as VPN ID. That way, if a user is authenticated by means of a backend group such as eDirectory, a certificate will be created even if no email address is set in the corresponding backend user object.

Because the VPN ID of each certificate must be unique, each user definition must have a different and unique email address. Creating a user definition with an email address already present in the system will fail.

To add a user account, proceed as follows:

1. **On the Users tab, click New User.**
   The *Create New User* dialog box opens.

2. **Make the following settings:**
   - **Username:** Enter a descriptive name for this user (e.g. jdoe). Note that for using remote access via PPTP or L2TP over IPsec, the username may only contain ASCII printable characters\(^1\).
   - **Real name:** Enter the user's real name (e.g. John Doe).
   - **Email address:** Enter the user's primary email address.
   - **Additional email addresses** (optional): Enter additional email addresses of this user.
   - **Authentication:** Select the authentication method. The following methods are available:
     * **Local:** Select to authenticate the user locally on SUM.
     * **Remote:** Select to authenticate the user using one of the external authentication methods supported by Sophos UTM Manager. For more information, see *Definitions & Users > Authentication Servers*.
     * **None:** Select to prevent the user from authentication completely. This is useful, for example, to disable a user temporarily without the need to delete the user definition altogether.
   - **Password:** Enter a user password (second time for verification). Only available if you selected *Local* as authentication method. Note that Basic User Authentication does not support umlauts. Note that for using remote access via PPTP or L2TP over IPsec, the password may only contain ASCII printable characters\(^2\).

---

\(^1\)http://en.wikipedia.org/wiki/ASCII#ASCII_printable_characters

\(^2\)http://en.wikipedia.org/wiki/ASCII#ASCII_printable_characters
**Backend sync**: Some basic settings of the user definition such as the real name or the user's email address can be updated automatically by synchronizing the data with external backend authentication servers (only available if you selected *Remote* as authentication method). Note that the option will automatically be set according to the *Enable Backend Sync on Login* option on the *Authentication Servers > Advanced* tab, if the user is selected for prefetching.

*Note* – Currently, only data with Active Directory and eDirectory servers can be synchronized.

**X.509 certificate**: Once the user definition has been created, you can assign an X.509 certificate for this user when editing the user definition. By default, this is the certificate that was automatically generated upon creating the user definition. However, you can also assign a third-party certificate, which you can upload on the *Management > Certificate Management > Certificates* tab.

**Comment (optional)**: Add a description or other information.

3. **Click Save.**
   The new user account appears on the *Users* list.

If you want to make this user a regular administrator having access to the web-based administrative interface WebAdmin, add the user to the group of *SuperAdmins*, which is configured on the *Definitions & Users > Users & Groups > Groups* tab in WebAdmin.

*Note* – If you have deleted a user object and want to create a user object with the same name, make sure you have also deleted the certificate associated with this user on the *Management > Certificate Management > Certificates* tab. Otherwise you will get an error message stating that an item with that name already exists.

You can download remote access certificates and/or configurations of users for whom some sort of remote access has been enabled. For that, select the checkbox in front of the respective users and select the desired option from the *Actions* drop-down list in the list header. Remote access users can also download those files themselves when they are allowed to use the User Portal.
5.3.2 Groups

On the Definitions & Users > Users & Groups > Groups page you can add user groups to SUM. In its factory default configuration, Sophos UTM Manager has one user group called Super-Admins. If you want to assign administrative privileges to users, that is, granting access to WebAdmin, add them to the group of SuperAdmins; this group should not be deleted.

Tip – When you click on a group definition in the Groups list, you can see all configuration options in which the group definition is used.

To add a user group, proceed as follows:

1. **On the Groups tab, click New Group.**
   The Create New Group dialog box opens.

2. **Make the following settings:**
   - **Group name**: Enter a descriptive name for this group. Note that this name does not need to correspond to the names of your backend groups.
   - **Group type**: Select the type of the group. You can choose between a group of static members and two group types promoting dynamic membership.
     - **Static members**: Select the local users who shall become member of this group.
     - **Backend membership**: Users are dynamically added to a group definition if they have been successfully authenticated by one of the supported authentication mechanisms. To proceed, select the appropriate backend authentication type:
       - **Active Directory**: An Active Directory user group of SUM provides group memberships to members of Active Directory server user groups configured on a Windows network. Enter the name of the Active Directory server groups the user is a member of. For more information, see Definitions & Users > Authentication Servers > Servers.
       - **eDirectory**: An eDirectory user group of SUM provides group memberships to members of eDirectory user groups configured on an eDirectory network. Enter the name of the eDirectory groups the user is a member of. For more information, see Definitions & Users > Authentication Servers > Servers.
- **RADIUS**: Users are automatically added to a RADIUS backend group when they have been successfully authenticated using the RADIUS authentication method.

- **TACACS+**: Users are automatically added to a TACACS+ backend group when they have been successfully authenticated using the TACACS+ authentication method.

- **LDAP**: Users are automatically added to an LDAP backend group when they have been successfully authenticated using the LDAP authentication method.

**Limit to backend group(s) membership** (optional): For all X.500-based directory services you can restrict the membership to various groups present on your backend server if you do not want all users of the selected backend server to be included in this group definition. The group(s) you enter here once selected this option must match a *Common Name* as configured on your backend server. Note that if you select this option for an Active Directory backend, you can omit the `CN=` prefix. If you select this option for an eDirectory backend, you can use the eDirectory browser that lets you conveniently select the eDirectory groups that should be included in this group definition. However, if you do not use the eDirectory browser, make sure to include the `CN=` prefix when entering eDirectory containers.

**Check an LDAP attribute** (optional): If you do not want all users of the selected backend LDAP server to be included in this group definition, you can select this checkbox to restrict the membership to those users matching a certain LDAP attribute present on your backend server. This attribute is then used as an LDAP search filter. For example, you could enter `groupMembership` as attribute with `CN=Sales,O=Example` as its value. That way you could include all users belonging to the sales department of your company into the group definition.

**Comment** (optional): Add a description or other information.

3. **Click Save.**
   
The new user group appears on the *Groups* list.

To either edit or delete a group, click the corresponding buttons.
5.4 Authentication Servers

On the Definitions & Users > Authentication Servers page databases and backend servers of external user authentication services can be managed. External user authentication allows you to validate user accounts against existing user databases or directory services on other servers of your network. Authentication services currently supported are:

- Novell's eDirectory
- Microsoft's Active Directory
- RADIUS
- TACACS+
- LDAP
5.4 Authentication Servers

5.4.1 Global Settings

The Definitions & Users > Authentication Servers > Global Settings tab lets you configure basic authentication options. The following options are available:

**Create users automatically:** When this option is selected, Sophos UTM Manager will automatically create a user object whenever an unknown user of a configured backend group successfully authenticates against one of the various authentication services supported by Sophos UTM Manager. For example, if you configure a RADIUS backend group and you add this group as a member to one of the roles defined on the Management > WebAdmin Settings > Access Control tab, Sophos UTM Manager will automatically create a user definition for a RADIUS user who has successfully logged in to WebAdmin.

- **Automatic User Creation for Facilities:** Automatic user creation can be enabled or disabled for specific services. Users are only created for enabled services. This option is not available—and automatic user creation is disabled for all facilities—when the Create users automatically option is not selected.

For user objects created automatically an SSL certificate will be generated. Note, however, that automatic user creation will fail in case of an email address conflict, for the user definition to be created automatically must not have configured an email address that is already present on the system. All email addresses must be unique within the system because they are used as identifiers for X.509 certificates.

| Important Note – Authentication (i.e., the action of determining who a user is) and authorization (i.e., the action of determining what a user is allowed to do) for a user whose user object was created automatically are always done on the remote backend server/directory service. Therefore, automatically created user objects in Sophos UTM Manager are useless if the corresponding backend server is not available or if the user object has been deleted on the remote site. |

Note also that Sophos UTM Manager caches user authentication data it has retrieved from a remote authentication server for 300 seconds. For this reason, changes made to the remote user settings will only take effect after the cache has expired.

**Authentication Cache**

Every time Sophos UTM Manager gets a user request, e.g., http, from a yet unknown user and authentication is required, the Sophos User Authentication (SUA) writes an entry to the
authentication cache. Over time, in environments with frequently changing users it can be reasonable to empty the cache from time to time. Also, if you want to force an immediate new authentication for all users. Use the button **Flush Authentication Cache** to empty the authentication cache.

An authentication is valid for 300 seconds. During this time, other authentication requests by the same user are looked up directly in the cache. This technique takes load off backend authentication services like eDirectory.

**Note** – Flushing the cache does not affect users that are remotely logged on.

**Live Log**

**Open Live Log:** Click the button to see the log of the **Sophos User Authentication** (SUA) in a new window.

### 5.4.2 Servers

On the **Definitions & Users > Authentication Servers > Servers** tab, you can create one or more authentication servers, such as eDirectory, Active Directory, LDAP, RADIUS, and TACACS+.

#### 5.4.2.1 eDirectory

Novell eDirectory is an X.500 compatible directory service for centrally managing access to resources on multiple servers and computers within a given network. eDirectory is a hierarchical, object-oriented database that represents all the assets in an organization in a logical tree. Those assets can include people, servers, workstations, applications, printers, services, groups, and so on.

To configure eDirectory authentication, proceed as follows:

1. **On the Servers tab, click New Authentication Server.**
   The dialog box **Create New Authentication Server** opens.

2. **Make the following settings:**
   - **Backend:** Select eDirectory as backend directory service.
   - **Position:** Select a position for the backend server. Backend servers with lower numbers will be queried first. For better performance, make sure that the backend server that is likely to get the most requests is on top of the list.
   - **Server:** Select (or add) an eDirectory server.
5.4 Authentication Servers

SSL: Select this option to enable SSL data transfer. The Port will then change from \texttt{389} (LDAP) to \texttt{636} (ldaps = LDAP over SSL).

Port: Enter the port of the eDirectory server. By default, this is port \texttt{389}.

Bind DN: The \textit{Distinguished Name} (DN) of the user to bind to the server with. This user is needed if anonymous queries to the eDirectory server are not allowed. Note that the user must have sufficient privileges to obtain all relevant user object information from the eDirectory server in order to authenticate users. eDirectory users, groups, and containers can be specified by the full distinguished name in LDAP notation, using commas as delimiters (e.g., \texttt{CN=administrator,DC=intranet,DC=example,DC=com}).

Password: Enter the password of the bind user.

Test server settings: Pressing the \textit{Test} button performs a bind test with the configured server. This verifies that the settings on this tab are correct, and the server is up and accepting connections.

Base DN: The starting point relative to the root of the LDAP tree where the users are included who are to be authenticated. Note that the base DN must be specified by the full distinguished name (FDN) in LDAP notation, using commas as delimiters (e.g., \texttt{O=Example,OU=RnD}). Base DN may be empty. In this case, the base DN is automatically retrieved from the directory.

Username: Enter the username of a test user to perform a regular authentication.

Password: Enter the password of the test user.

Authenticate example user: Click the \textit{Test} button to start the authentication test for the test user. This verifies that all server settings are correct, the server is up and accepting connections, and users can be successfully authenticated.

3. Click \textit{Save}.

The server will be displayed in the \textit{Servers} list.

5.4.2.2 Active Directory

Active Directory (AD) is Microsoft’s implementation of a directory service and is a central component of Windows 2000/2003 servers. It stores information about a broad range of resources residing on a network, including users, groups, computers, printers, applications, services, and any type of user-defined objects. As such it provides a means of centrally organizing, managing, and controlling access to these resources.
The Active Directory authentication method allows you to register Sophos UTM Manager at a Windows domain, thus creating an object for Sophos UTM Manager on the primary domain controller (DC). SUM is then able to query user and group information from the domain.

Note – SUM supports Active Directory 2003 and newer.

To configure Active Directory authentication, proceed as follows:

1. **On the Servers tab, click New Authentication Server.** The dialog box Create New Authentication Server opens.

2. **Make the following settings:**
   - **Backend:** Select Active Directory as backend directory service.
   - **Position:** Select a position for the backend server. Backend servers with lower numbers will be queried first. For better performance, make sure that the backend server that is likely to get the most requests is on top of the list.
   - **Server:** Select (or add) an Active Directory server.
   - **SSL:** Select this option to enable SSL data transfer. The Port will then change from 389 (LDAP) to 636 (ldaps = LDAP over SSL).
   - **Port:** Enter the port of the Active Directory server. By default, this is port 389.
   - **Bind DN:** The full Distinguished Name (DN) of the user to bind to the server in LDAP notation. This user is needed if anonymous queries to the Active Directory server are not allowed. The bind user must have sufficient privileges to obtain all relevant user object information from the Active Directory server in order to authenticate users; a requirement usually met by the administrator of the domain.

Each DN consists of one or more Relative Distinguished Names (RDN) constructed from some attributes of the Active Directory user object and includes its username, the node where it resides, and the top-level DN of the server, all specified in LDAP notation and separated by commas.

- The username must be the name of the user who is able to access the directory and is to be specified by the CN designator (e.g., CN=user). While using a popular account with domain permissions, such as "admin" is possible, it is highly recommended for best practices that the user not have admin rights, as it is sufficient for them to have read permission on all objects of the subtree starting at the given base DN.
5.4 Authentication Servers

- The information of the node where the user object resides must include all sub-nodes between the root node and the user object and is usually comprised of so-called organizational units and common name components. Organizational units (indicated by the combined folder/book icon in the Microsoft Management Console) are to be specified by the OU designator. Note that the order of the nodes is from the lowest to the highest node, that is, the more specific elements come first (e.g., OU=Management_US, OU=Management). On the other hand, default Active Directory containers (indicated by a simple Folder icon) such as the pre-defined Users node are to be specified using the CN designator (e.g., CN=Users).

- The top-level DN of the server can consist of several domain components, each specified by the DC designator. Note that the domain components are given in the same order as the domain name (for example, if the domain name is example.com, the DN part would be DC=example, DC=com).

An example bind user DN for a user named administrator whose object is stored in the Users container in a domain called example.com would look like this:

\[CN=administrator, CN=Users, DC=example, DC=com\]

**Figure 11** Authentication: Microsoft Management Console

Now, suppose you create an organizational unit called Management with the subnode Management_US and move the administrator user object into it, the DN of the administrator would change to:

\[CN=administrator, OU=Management_US, OU=Management, DC=example, DC=com\]

**Password:** Enter the password of the bind user.

**Test server settings:** Pressing the Test button performs a bind test with the configured server. This verifies that the settings on this tab are correct, and the server is up and accepts connections.
**Base DN:** The starting point relative to the root of the LDAP tree where the users are included who are to be authenticated. Note that the base DN must be specified by the full distinguished name (FDN) in LDAP notation, using commas as delimiters (e.g., O=Example,OU=RnD). Base DN may be empty. In this case, the base DN is automatically retrieved from the directory.

**Username:** Enter the username of a test user to perform a regular authentication.

**Password:** Enter the password of the test user.

**Authenticate example user:** Click the *Test* button to start the authentication test for the test user. This verifies that all server settings are correct, the server is up and accepting connections, and users can be successfully authenticated.

3. **Click Save.**
   The server will be displayed in the *Servers* list.

### 5.4.2.3 LDAP

LDAP, an abbreviation for *Lightweight Directory Access Protocol*, is a networking protocol for querying and modifying directory services based on the X.500 standard. Sophos UTM Manager uses the LDAP protocol to authenticate users for several of its services, allowing or denying access based on attributes or group memberships configured on the LDAP server.

To configure LDAP authentication, proceed as follows:

1. **On the Servers tab, click New Authentication Server.**
   The dialog box *Create New Authentication Server* opens.

2. **Make the following settings:**
   **Backend:** Select LDAP as backend directory service.

   **Position:** Select a position for the backend server. Backend servers with lower numbers will be queried first. For better performance, make sure that the backend server that is likely to get the most requests is on top of the list.

   **Server:** Select (or add) an LDAP server.

   **SSL:** Select this option to enable SSL data transfer. The Port will then change from 389 (LDAP) to 636 (ldaps = LDAP over SSL).

   **Port:** Enter the port of the LDAP server. By default, this is port 389.
5.4 Authentication Servers

**Bind DN:** The *Distinguished Name* (DN) of the user to bind to the server with. This user is mandatory. For security reasons, anonymous queries to the LDAP server are not supported. Note that the user must have sufficient privileges to obtain all relevant user object information from the LDAP server in order to authenticate users. LDAP users, groups, and containers can be specified by the full distinguished name in LDAP notation, using commas as delimiters (e.g., CN=administrator,DC=intranet,DC=example,DC=com).

**Password:** Enter the password of the bind user.

**Test server settings:** Pressing the *Test* button performs a bind test with the configured server. This verifies that the settings on this tab are correct, and the server is up and accepts connections.

**User attribute:** Select the user attribute that is to be used as the filter for searching the LDAP directory. The user attribute contains the actual login name each user is prompted for, for example by remote access services. The following user attributes can be selected:

- **CN** (Common Name)
- **SN** (Surname)
- **UID** (User ID)

If usernames in your LDAP directory are not stored in any of these forms, select <<Custom>> from the list and enter your custom attribute into the *Custom* field below. Note that this attribute must be configured on your LDAP directory.

**Base DN:** The starting point relative to the root of the LDAP tree where the users are included who are to be authenticated. Note that the base DN must be specified by the full distinguished name (FDN) in LDAP notation, using commas as delimiters (e.g., O=Example,OU=RnD). Base DN may be empty. In this case, the base DN is automatically retrieved from the directory.

**Username:** Enter the username of a test user to perform a regular authentication.

**Password:** Enter the password of the test user.

**Authenticate example user:** Click the *Test* button to start the authentication test for the test user. This verifies that all server settings are correct, the server is up and accepting connections, and users can be successfully authenticated.
3. **Click Save.**
   The server will be displayed in the **Servers** list.

### 5.4.2.4 RADIUS

RADIUS, the acronym of *Remote Authentication Dial In User Service* is a widespread protocol for allowing network devices such as routers to authenticate users against a central database. In addition to user information, RADIUS can store technical information used by network devices, such as supported protocols, IP addresses, routing information, and so on. This information constitutes a user profile, which is stored in a file or database on the RADIUS server.

The RADIUS protocol is very flexible, and servers are available for most operating systems. The RADIUS implementation on SUM allows you to configure access rights on the basis of proxies and users. Before you can use RADIUS authentication, you must have a running RADIUS server on the network. Whereas passwords are encrypted using the RADIUS secret, the username is transmitted in plain text.

To configure RADIUS authentication, proceed as follows:

1. **On the Servers tab, click New Authentication Server.**
   The dialog box *Create New Authentication Server* opens.

2. **Make the following settings:**
   - **Backend:** Select RADIUS as backend directory service.
   - **Position:** Select a position for the backend server. Backend servers with lower numbers will be queried first. For better performance, make sure that the backend server that is likely to get the most requests is on top of the list.
   - **Server:** Select (or add) a RADIUS server.
   - **Port:** Enter the port of the RADIUS server. By default, this is port 1812.
   - **Shared Secret:** The shared secret is a text string that serves as a password between a RADIUS client and a RADIUS server. Enter the shared secret.
   - **Test server settings:** Pressing the Test button performs a bind test with the configured server. This verifies that the settings on this tab are correct, and the server is up and accepts connections.
   - **Username:** Enter the username of a test user to perform a regular authentication.
   - **Password:** Enter the password of the test user.
5.4 Authentication Servers

**NAS identifier:** Select the appropriate NAS identifier from the list. For more information see the Note and the table below.

**Authenticate example user:** Click the Test button to start the authentication test for the test user. This verifies that all server settings are correct, the server is up and accepting connections, and users can be successfully authenticated.

3. **Click Save.**
   The server will be displayed in the Servers list.

**Note** – Each user authentication service of Sophos UTM Manager such as the Gateway Manager or the WebAdmin querying the RADIUS server sends a different identifier (NAS identifier) to the RADIUS server. That way, the various services can be differentiated on the RADIUS server, which is useful for authorization purposes, that is, the granting of specific types of service to a user. Below you can find the list of user authentication services and their corresponding NAS identifier.

<table>
<thead>
<tr>
<th>User Authentication Service</th>
<th>NAS Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway Manager</td>
<td>acc</td>
</tr>
<tr>
<td>User Portal</td>
<td>portal</td>
</tr>
<tr>
<td>WebAdmin</td>
<td>webadmin</td>
</tr>
</tbody>
</table>

Table 2: RADIUS NAS Identifiers

### 5.4.2.5 TACACS+

TACACS+ (the acronym of *Terminal Access Controller Access Control System*) is a proprietary protocol by Cisco Systems, Inc. and provides detailed accounting information and administrative control over authentication and authorization processes. Whereas RADIUS combines authentication and authorization in a user profile, TACACS+ separates these operations. Another difference is that TACACS+ utilizes the TCP protocol (port 49) while RADIUS uses the UDP protocol.

To configure TACACS+ authentication, proceed as follows:

1. **On the Servers tab, click New Authentication Server.**
   The dialog box Create New Authentication Server opens.
2. **Make the following settings:**

   **Backend:** Select TACACS+ as backend directory service.

   **Position:** Select a position for the backend server. Backend servers with lower numbers will be queried first. For better performance, make sure that the backend server that is likely to get the most requests is on top of the list.

   **Server:** Select (or add) a TACACS+ server.

   **Port:** Enter the port of the TACACS+ server. By default, this is port 49.

   **Key:** Enter the authentication and encryption key for all TACACS+ communication between Sophos UTM Manager and the TACACS+ server. The value for the key to be entered here should match the one configured on the TACACS+ server. Enter the key (second time for verification).

   **Test server settings:** Pressing the Test button performs a bind test with the configured server. This verifies that the settings on this tab are correct, and the server is up and accepting connections.

   **Username:** Enter the username of a test user to perform a regular authentication.

   **Password:** Enter the password of the test user.

   **Authenticate example user:** Click the Test button to start the authentication test for the test user. This verifies that all server settings are correct, the server is up and accepting connections, and users can be successfully authenticated.

3. **Click Save.**
   The server will be displayed in the Servers list.

### 5.4.3 Advanced

**Block Password Guessing**
This function can be used to prevent password guessing. After a configurable number of failed login attempts (default: 3), the IP address trying to gain access to one of the facilities will be blocked for a configurable amount of time (default: 600 seconds).

**Drop packets from blocked hosts:** If enabled, all packets coming from blocked hosts will be dropped for the specified time. This option serves to avoid DoS attacks.

**Facilities:** The check will be performed for the selected facilities.

**Never block networks:** Networks listed in this box are exempt from this check.
Local Authentication Passwords
Using this option, you can force the use of strong passwords for administrators or locally registered users having administrative privileges. You can configure password complexity to adhere to the following security requirements:

- Minimum password length, default is eight characters
- Require at least one lowercase character
- Require at least one uppercase character
- Require at least one numeral
- Require at least one non-alphanumeric character

To enable the selected password properties select the *Require complex passwords* checkbox and click *Apply*.

Prefetch Directory Users
Users from eDirectory or Active Directory can be synchronized with SUM. This will pre-create user objects on SUM such that these user objects already exist, when the user logs in. The synchronization process can run weekly or daily.

To enable prefetching, make the following settings:

**Server:** The drop-down list contains servers that have been created on the *Servers* tab. Select a server for which you want to enable prefetching.

**Prefetch interval:** Select an interval to prefetch users. To run the synchronization weekly, select the day of the week when synchronization should start. To run the synchronization daily, select *Daily*.

**Prefetch time:** Select a time to prefetch users.

**Groups:** To specify which groups should be pre-created, enter the groups here. You can use the integrated LDAP browser to select these groups.

**Enable Backend Sync on Login** (optional): With every prefetch event, the *Backend sync* option of the involved users (*Users & Groups > Users* tab) will be set to the value defined here. If the option is enabled, the users' *Backend sync* option will be enabled, if the option is disabled, the users' *Backend sync* option will be disabled.

Click *Apply* to save your settings.

**Prefetch Now:** Click this button to start prefetching immediately.
Open Prefetch Live Log: Click this button to open the prefetch live log.
6 Interfaces & Routing

This chapter describes how to configure interfaces and network-specific settings in Sophos UTM Manager. The Network Statistics page in WebAdmin provides an overview of today's top ten accounting services, top source hosts, and concurrent connections. Each of the sections contains a Details link. Clicking the link redirects you to the respective reporting section of WebAdmin, where you can find more statistical information.

The following topics are included in this chapter:

- Interfaces
- Static Routing

6.1 Interfaces

The Interfaces menu allows you to configure and manage all network cards installed on SUM and also all interfaces with the external network (Internet) and interfaces to the internal networks (LAN, DMZ).

**Note** – While planning your network topology and configuring SUM, take care to note which interface is connected to which network. In most configurations, the network interface with SysID eth1 is chosen as the connection to the external network.

The following sections explain how to manage and configure different interface types on the tabs Interfaces, Additional Addresses, Link Aggregation, Uplink Balancing, Multipath Rules, and Hardware.

6.1.1 Interfaces

On the Interfaces tab you can configure network cards and virtual interfaces. The list shows the already defined interfaces with their symbolic name, hardware device, and current addresses. The interface status is also displayed. By clicking the toggle switch, you can activate and deactivate interfaces. Please note that interface groups do not have a toggle switch.
When you click the Info icon of an interface definition in the Interfaces list, you can see all configuration options in which the interface definition is used.

Newly added interfaces may show up as **Down** while they are in the process of being set up. You can select to edit and delete interfaces by clicking the respective buttons.

### 6.1.1.1 Automatic Interface Network Definitions

Each interface on your SUM has a symbolic name and a hardware device assigned to it. The symbolic name is used when you reference an interface in other configuration settings. For each interface, a matching set of network definitions is automatically created by SUM:

- A definition containing the current IP address of the interface, its name consisting of the interface name and the *(Address)* suffix.
- A definition containing the network attached to the interface, its name consisting of the interface name and the *(Network)* suffix.
- A definition containing the broadcast address of the interface, its name consisting of the interface name and the *(Broadcast)* suffix.

One interface with the symbolic name *Internal* is already predefined. It is the management interface and will typically be used as the "internal" SUM interface. If you want to rename it, you should do so right after the installation.

### 6.1.1.2 Group

You can combine two or more interfaces to a group. Groups can ease your configuration tasks. When creating multipath rules, you need to configure a group if you want to balance traffic over a defined group of uplink interfaces only instead of using all uplink interfaces.

To configure a **Group** interface, proceed as follows:

**On the Interfaces tab, click New Interface.**

1. The Create New Interface dialog box opens.

2. **Make the following settings:**
   - **Name:** Enter a descriptive name for the interface.
   - **Type:** Select *Group* from the drop-down list.
   - **Interfaces:** Add the interfaces to be grouped.
Comment (optional): Add a description or other information.

3. **Click Save.**
   The group is added to the interface list. Groups do not have a status.

To show only interfaces of a certain type, select the type of the interfaces you want to have displayed from the drop-down list. To either edit or delete an interface, click the corresponding buttons.

### 6.1.1.3 Interface Types

The following list shows which interface types can be added to SUM, and what type of hardware is needed to support them:

**Group:** You can organize your interfaces in groups. In appropriate configurations, you can then select a single interface group instead of multiple interfaces individually.

**3G/UMTS:** This is an interface based on a USB modem stick. The stick needs to be plugged in and SUM needs to be rebooted before interface creation.

**Ethernet DHCP:** This is a standard Ethernet interface with DHCP.

**Ethernet Static:** This is a normal Ethernet interface, with 10, 100, or 1000 Mbit/s bandwidth.

**Ethernet VLAN:** VLAN (Virtual LAN) is a method to have multiple layer-2 separated network segments on a single hardware interface. Every segment is identified by a "tag", which is just an integer number. When you add a VLAN interface, you will create a "hardware" device that can be used to add additional interfaces (aliases), too.

### 6.1.1.4 3G/UMTS

Sophos UTM Manager supports network connections via 3G/UMTS USB sticks.

To configure a 3G/UMTS interface, proceed as follows:

- **On the Interfaces tab, click New Interface.**
  1. The Create New Interface dialog box opens.

- **Make the following settings:**
  - **Name:** Enter a descriptive name for the interface.
  - **Type:** Select 3G/UMTS from the drop-down list.
6.1 Interfaces

**Hardware:** Select a USB modem stick from the drop-down list. Note that you need to reboot after you plugged the USB stick in.

**Network:** Select the mobile network type, which is either **GSM/W-CDMA, CDMA,** or **LTE.**

**IPv4 default GW** (optional): Select this option if you want to use the default gateway of your provider.

**PIN** (optional): Enter the PIN of the SIM card if a PIN is configured.

**APN Autoselect:** (optional): By default, the APN (Access Point Name) used is retrieved from the USB modem stick. If you unselect the checkbox, enter APN information into the APN field.

**Username/Password** (optional): If required, enter a username and password for the mobile network.

**Dial String** (optional): If your provider uses a different dial string, enter it here. Default is *99#.

**Comment** (optional): Add a description or other information.

3. **Optionally, make the following advanced settings:**

**Init String:** Enter the string to initialize the USB modem stick. Remember that it might become necessary to adjust the init string to the USB modem stick. In this case, the init string can be gathered from the associated USB modem stick manual. If you do not have the required documentation available, keep the default setting **ATZ.**

**Reset String:** Enter the reset string for the USB modem stick. Keep in mind that it might be necessary to adjust the reset string to the USB modem stick. In this case you can gather it from the associated USB modem stick manual. If you do not have the required documentation available, keep the default setting **ATZ.**

**MTU:** Enter the maximum transmission unit for the interface in bytes. You must enter a value fitting your interface type here if you want to use traffic management. A sensible value for the interface type is entered by default. Changing this setting should only be done by technically adept users. Entering wrong values here can render the interface unusable. An MTU size greater than 1500 bytes must be supported by the network operator and the network card (e.g., Gigabit interface). By default, an MTU of 1500 bytes is set for the **3G/UMTS** interface type.
Asymmetric (optional): Select this option if your connection’s uplink and downlink bandwidth are not identical and you want the Dashboard to reflect this. Then, two textboxes are displayed, allowing you to enter the maximum uplink bandwidth in either MB/s or KB/s. Select the appropriate unit from the drop-down list.

Displayed Max (optional): Here you can enter the maximum downlink bandwidth of your connection, if you want the Dashboard to reflect it. The bandwidth can be given in either MB/s or KB/s. Select the appropriate unit from the drop-down list.

4. Click Save.
   The system will now check the settings for validity. After a successful check the new interface will appear in the interface list. The interface is not yet enabled (toggle switch is gray).

5. Enable the interface.
   Click the toggle switch to activate the interface.

   The interface is now enabled (toggle switch is green). The interface might still be displayed as being Down. The system requires a short time to configure and load the settings. Once the Up message appears, the interface is fully operable.

To show only interfaces of a certain type, select the type of the interfaces you want to have displayed from the drop-down list. To either edit or delete an interface, click the corresponding buttons.

6.1.1.5 Ethernet Static

To configure a network card for a static Ethernet connection to an internal or external network, you must configure the network card with an IP address and netmask.

To configure a static Ethernet interface, proceed as follows:

   On the Interfaces tab, click New Interface.

1. The Create New Interface dialog box opens.

2. Make the following settings:
   Name: Enter a descriptive name for the interface.

   Type: Select Ethernet Static from the drop-down list.

   Hardware: Select an interface from the drop-down list.
Tip – For an external connection (e.g., to the Internet) choose the network card with SysID eth1.

**IPv4 address:** Enter the IP address of the interface.

**Netmask:** Select a network mask (IPv4).

**IPv4 default GW** (optional): Select this option if you want to use a statically defined default gateway.

**Default GW IP** (optional): Enter the IP address of the default gateway.

**Comment** (optional): Add a description or other information.

3. **Optionally, make the following advanced settings:**
   - **MTU:** Enter the maximum transmission unit for the interface in bytes. You must enter a value fitting your interface type here if you want to use traffic management. A sensible value for the interface type is entered by default. Changing this setting should only be done by technically adept users. Entering wrong values here can render the interface unusable. An MTU size greater than 1500 bytes must be supported by the network operator and the network card (e.g., Gigabit interface). By default, an MTU of 1500 bytes is set for the *Ethernet Static* interface type.
   - **Proxy ARP:** To enable the function, select the checkbox. By default, the *Proxy ARP* function is disabled (Off). This option is available on broadcast-type interfaces. When you switch it on, SUM will "attract" traffic on that interface for hosts "behind" it and pass it on. It will do that for all hosts that it has a direct interface route for. This allows you to build "transparent" network bridging while still doing firewalling. Another use for this feature is when your ISP’s router just puts your "official" network on its Ethernet interface (does not use a host route).
   - **Asymmetric** (optional): Select this option if your connection’s uplink and downlink bandwidth are not identical and you want the Dashboard to reflect this. Then, two textboxes are displayed, allowing you to enter the maximum uplink bandwidth in either MB/s or KB/s. Select the appropriate unit from the drop-down list.
   - **Displayed Max** (optional): Here you can enter the maximum downlink bandwidth of your connection, if you want the Dashboard to reflect it. The bandwidth can be given in either MB/s or KB/s. Select the appropriate unit from the drop-down list.
4. **Click Save.**  
The system will now check the settings for validity. After a successful check the new interface will appear in the interface list. The interface is not yet enabled (toggle switch is gray).

5. **Enable the interface.**  
Click the toggle switch to activate the interface.

The interface is now enabled (toggle switch is green). The interface might still be displayed as being *Down*. The system requires a short time to configure and load the settings. Once the *Up* message appears, the interface is fully operable.

To show only interfaces of a certain type, select the type of the interfaces you want to have displayed from the drop-down list. To either edit or delete an interface, click the corresponding buttons.

### 6.1.1.6 Ethernet VLAN

In order to connect SUM to the virtual LANs, the system requires a network card with a tag-capable driver. A tag is a 4-byte header attached to packets as part of the Ethernet header. The tag contains the number of the VLAN that the packet should be sent to: the VLAN number is a 12-bit number, allowing up to 4095 virtual LANs. In WebAdmin this number is referred to as the **VLAN tag**.

**Note** – Sophos maintains a list of supported tag-capable network interface cards. The Hardware Compatibility List (HCL) is available at the Sophos Knowledgebase. Use "HCL" as search term to locate the corresponding page.

To configure an Ethernet VLAN interface, proceed as follows:

- **On the Interfaces tab, click New Interface.**
  1. The *Create New Interface* dialog box opens.

- **Make the following settings:**
  - **Name**: Enter a descriptive name for the interface.
  - **Type**: Select *Ethernet VLAN* from the drop-down list.
  - **Hardware**: Select an interface from the drop-down list.
  - **VLAN Tag**: Enter the VLAN tag to use for this interface.
**IPv4 address**: Enter the IP address of the interface.

**Netmask**: Select a network mask (IPv4).

**IPv4 default GW** (optional): Select this option if you want to use a statically defined default gateway.

**Default GW IP** (optional): Enter the IP address of the default gateway.

**Comment** (optional): Add a description or other information.

3. **Optionally, make the following advanced settings:**
   **MTU**: Enter the maximum transmission unit for the interface in bytes. You must enter a value fitting your interface type here if you want to use traffic management. A sensible value for the interface type is entered by default. Changing this setting should only be done by technically adept users. Entering wrong values here can render the interface unusable. An MTU size greater than 1500 bytes must be supported by the network operator and the network card (e.g., Gigabit interface). By default, an MTU of 1500 bytes is set for the Ethernet VLAN interface type.

   **Proxy ARP**: To enable the function, select the checkbox. By default, the Proxy ARP function is disabled (Off).

   This option is available on broadcast-type interfaces. When you switch it on, SUM will "attract" traffic on that interface for hosts "behind" it and pass it on. It will do that for all hosts that it has a direct interface route for. This allows you to build "transparent" network bridging while still doing firewalling. Another use for this feature is when your ISP’s router just puts your "official" network on its Ethernet interface (does not use a host route).

   **Asymmetric** (optional): Select this option if your connection's uplink and downlink bandwidth are not identical and you want the Dashboard to reflect this. Then, two textboxes are displayed, allowing you to enter the maximum uplink bandwidth in either MB/s or KB/s. Select the appropriate unit from the drop-down list.

   **Displayed Max** (optional): Here you can enter the maximum downlink bandwidth of your connection, if you want the Dashboard to reflect it. The bandwidth can be given in either MB/s or KB/s. Select the appropriate unit from the drop-down list.

4. **Click Save**.

   The system will now check the settings for validity. After a successful check the new interface will appear in the interface list. The interface is not yet enabled (toggle switch is gray).
5. **Enable the interface.**
   Click the toggle switch to activate the interface.

   The interface is now enabled (toggle switch is green). The interface might still be displayed as being *Down*. The system requires a short time to configure and load the settings. Once the *Up* message appears, the interface is fully operable.

To show only interfaces of a certain type, select the type of the interfaces you want to have displayed from the drop-down list. To either edit or delete an interface, click the corresponding buttons.

### 6.1.1.7 Ethernet DHCP

To configure an *Ethernet DHCP* interface, proceed as follows:

- **On the Interfaces tab, click New Interface.**
  1. The *Create New Interface* dialog box opens.
  2. **Make the following settings:**
     - **Name:** Enter a descriptive name for the interface.
     - **Type:** Select *Ethernet DHCP* from the drop-down list.
     - **Hardware:** Select an interface from the drop-down list.

   **Tip** – For an external connection (e.g., to the Internet) choose the network card with SysID *eth1*. Please note that one network card cannot be used as both a *Ethernet DHCP* and a *PPP over Ethernet* (PPPoE-DSL) or *PPTP over Ethernet* (PPPoA-DSL) connection simultaneously.

- **IPv4 default GW** (optional): Select this option if you want to use the default gateway of your provider.

- **Comment** (optional): Add a description or other information.

3. **Optionally, make the following advanced settings:**
   - **Hostname:** If your ISP requires to receive the hostname of your system, enter it here.
   - **MTU:** Enter the maximum transmission unit for the interface in bytes. You must enter a value fitting your interface type here if you want to use traffic management. A sensible value for the interface type is entered by default. Changing this setting should only be done by technically adept users. Entering wrong values here can render the interface
An MTU size greater than 1500 bytes must be supported by the network operator and the network card (e.g., Gigabit interface). By default, an MTU of 1500 bytes is set for the Ethernet DHCP interface type.

**Proxy ARP:** To enable the function, select the checkbox. By default, the Proxy ARP function is disabled (Off). This option is available on broadcast-type interfaces. When you switch it on, SUM will "attract" traffic on that interface for hosts "behind" it and pass it on. It will do that for all hosts that it has a direct interface route for. This allows you to build "transparent" network bridging while still doing firewalling. Another use for this feature is when your ISP's router just puts your "official" network on its Ethernet interface (does not use a host route).

**Asymmetric (optional):** Select this option if your connection's uplink and downlink bandwidth are not identical and you want the Dashboard to reflect this. Then, two textboxes are displayed, allowing you to enter the maximum uplink bandwidth in either MB/s or KB/s. Select the appropriate unit from the drop-down list.

**Displayed Max** (optional): Here you can enter the maximum downlink bandwidth of your connection, if you want the Dashboard to reflect it. The bandwidth can be given in either MB/s or KB/s. Select the appropriate unit from the drop-down list.

4. **Click Save.**
   The system will now check the settings for validity. After a successful check the new interface will appear in the interface list. The interface is not yet enabled (toggle switch is gray).

5. **Enable the interface.**
   Click the toggle switch to activate the interface.
   The interface is now enabled (toggle switch is green). The interface might still be displayed as being Down. The system requires a short time to configure and load the settings. Once the Up message appears, the interface is fully operable.

To show only interfaces of a certain type, select the type of the interfaces you want to have displayed from the drop-down list. To either edit or delete an interface, click the corresponding buttons.

### 6.1.2 Additional Addresses

One network card can be configured with additional IP addresses (also called *aliases*). This function allows you to manage multiple logical networks on one physical network card. It can also be
used to assign further addresses to a SUM running NAT (Network Address Translation).

To configure additional addresses on standard Ethernet interfaces, proceed as follows:

1. **On the Additional Addresses tab, click New Additional Address.**
   The Create New Additional Address dialog box opens.

2. **Make the following settings:**
   - **Name:** Enter a descriptive name for the new additional address.
   - **On Interface:** Select an interface from the drop-down list to which the address is to be assigned.
   - **IPv4 Address:** Enter the additional IP address of the interface.
   - **Netmask:** Select a netmask from the drop-down list.
   - **Comment (optional):** Add a description or other information.

3. **Click Save.**
   The system will now check the settings for validity. After a successful check the new interface will appear in the interface list. The interface is not yet enabled (toggle switch is gray).

4. **Enable the additional address.**
   Click the toggle switch to activate the additional address.

   The additional address is now enabled (toggle switch is green). The additional address might still be displayed as being Down. The system requires a short time to configure and load the settings. Once the *Up* message appears, the additional address is fully operable.

To either edit or delete an additional address, click the corresponding buttons.

### 6.1.3 Hardware

The Interfaces & Routing > Interfaces > Hardware tab lists all configured interfaces showing information such as the Ethernet mode of operation or the MAC address. On SUM hardware devices, for each interface, auto negotiation can be enabled or disabled.

**Auto Negotiation:** Usually, the Ethernet mode of operation (1000BASE-T full-duplex, 100BASE-T full-duplex, 100BASE-T half-duplex, 10BASE-T full-duplex, 10BASE-T half-duplex, and so on) between two network devices is automatically negotiated by choosing the best possible mode of operation supported by both devices, where higher speed (e.g. 1000 Mbit/sec) is preferred over lower speed (e.g. 100 Mbit/sec), and full duplex is preferred over half duplex at the same speed.
6.1 Interfaces

**Caution** – For proper 1000 Mbit/sec operation, auto negotiation is always required and mandatory by IEEE Std 802.3ab. Thus, be careful to never switch Auto Negotiation off for any interface with Link mode 1000BASE-T. The timing of your network link may fail, causing service degradation or failure. For 100 Mbit/sec and 10 Mbit/sec operation, auto negotiation is optional, but still recommended for use whenever possible.

Auto negotiation is enabled by default. In the rare case that you need to switch it off, click the Edit button of the corresponding interface card and change the setting in the appearing dialog box Edit NIC Parameters via the drop-down list Link Mode. Note that the drop-down list is only available with SUM hardware devices. Click Save to save your changes.

**Caution** – Be careful when disabling auto negotiation, as this might lead to mismatches, resulting in a significant performance decrease or even disconnect. If the respective network interface card is your interface to WebAdmin you may lose access to WebAdmin!

In case one of your interfaces lost its network link due to manipulation of auto negotiation or speed settings, just changing the settings back will typically not bring the interface back to normal operation: Changing auto negotiation or speed settings on disconnected interfaces is not reliable. Therefore first switch on auto negotiation and then reboot SUM to bring back normal operation.

**HA Link Monitoring**: If high availability is enabled, all configured interfaces are monitored for link status. In case of a link failure, a takeover is triggered. If a configured interface is not always connected (e.g. management interface) please disable HA link monitoring for the corresponding interface. Otherwise all HA nodes will stay in status UNLINKED. To disable HA link monitoring click the Edit button of the corresponding interface card and change the setting in the appearing dialog box Edit NIC Parameters. Click Save to save your changes.

**Set Virtual MAC**: Sometimes it is useful to be able to change the MAC address of a device. For example, there are some ISPs where the modem must be reset when the device connected to it changes and by that the MAC address of that device. By setting the MAC address to the value of the former device, a reset of the modem can be avoided.

SUM, however, does not overwrite the original MAC address of the device but instead sets a virtual MAC address. To do so, click the Edit button of the corresponding interface card. In the appearing dialog box Edit NIC Parameters, select the checkbox Set Virtual MAC and enter a valid MAC address. Click Save to save your changes.
To restore the original MAC address, click the Edit button of the corresponding interface card. In the appearing dialog box Edit NIC Parameters, unselect the checkbox Set Virtual MAC. Click Save to save your changes.

6.2 Static Routing

Every computer connected to a network uses a routing table to determine the path along which an outbound data packet must be sent to reach its destination. For example, the routing table contains the information whether the destination address is on the local network or if the data packet must be forwarded to a router. If a router is involved, the table contains information about which router is to be used for which network.

Two types of routes can be added to the routing table of Sophos UTM Manager: standard static routes and policy routes. With static routes, the routing target is exclusively determined by the packet's destination address. With policy routes, however, it is possible to make routing decisions based on the source interface, source address, service, or destination address.

**Note** – You do not need to set additional routes for networks attached to SUM's interfaces, as well as default routes. The system inserts these routes automatically.

6.2.1 Standard Static Routes

The system automatically inserts routing entries into the routing table for networks that are directly connected to the system. Manual entries are necessary in those cases where there is an additional router which is to be accessed via a specific network. Routes for networks, that are not directly connected and that are inserted to the routing table via a command or a configuration file, are called static routes.

To add a standard static route, proceed as follows:

1. **On the Standard Static Routes tab click New Static Route.**
   The Create New Static Route dialog box opens.

2. **Make the following settings:**
   - **Route type:** The following route types are available:
     - **Interface route:** Packets are sent out on a particular interface. This is useful in two cases. First, for routing on dynamic interfaces (PPP), because in this case the IP address of the gateway is unknown. Second, for defining a default route having
6.2 Static Routing

- a gateway located outside the directly connected networks.
  - **Gateway route**: Packets are sent to a particular host (gateway).
  - **Blackhole route**: Packets are discarded silently. This is useful in connection with OSPF or other dynamic adaptive routing protocols to avoid routing loops, route flapping, and the like.

**Network**: Select the destination networks of data packets SUM must intercept.

**Interface**: Select the interface through which the data packets will leave SUM (only available if you selected *Interface Route* as route type).

**Gateway**: Select the gateway/router to which SUM will forward data packets (only available if you selected *Gateway Route* as route type).

**Comment** (optional): Add a description or other information.

3. **Optionally, make the following advanced setting**:
   - **Metric**: Enter a metric value which can be an integer from 0 to 4294967295 with a default of 5. The metric value is used to distinguish and prioritize routes to the same destination. A lower metric value is preferred over a higher metric value. IPsec routes automatically have the metric 0.

4. **Click Save**.
   The new route appears on the *Standard Static Route* list.

5. **Enable the route**.
   Click the toggle switch to activate the route.

To either edit or delete a route, click the corresponding buttons.

### 6.2.2 Policy Routes

When a router receives a data packet, it normally decides where to forward it based on the destination address in the packet, which is then used to look up an entry in a routing table. However, in some cases, there may be a need to forward the packet based on other criteria. Policy-based routing allows for forwarding or routing of data packets according to your own policies.

To add a policy route, proceed as follows:

1. **On the Policy Routes tab click New Policy Route**.
   The *Create New Policy Route* dialog box opens.
2. **Make the following settings:**

   **Position:** The position number, defining the priority of the policy route. Lower numbers have higher priority. Routes are matched in ascending order. Once a route has matched, routes with a higher number will not be evaluated anymore.

   **Route type:** The following route types are available:

   - **Interface route:** Packets are sent out on a particular interface. This is useful in two cases. First, for routing on dynamic interfaces (PPP), because in this case the IP address of the gateway is unknown. Second, for defining a default route having a gateway located outside the directly connected networks.

   - **Gateway route:** Packets are sent to a particular host (gateway).

   **Source interface:** The interface on which the data packet to be routed has arrived. The *Any* setting applies to all interfaces.

   **Source network:** The source network of the data packets to be routed. The *Any* setting applies to all networks.

   **Service:** The service definition that matches the data packet to be routed. The drop-down list contains all predefined services as well as the services you have defined yourself. These services allow you to specify precisely which kind of traffic should be processed. The *Any* setting matches any combination of protocols and source and destination ports.

   **Destination network:** The destination network of the data packets to be routed. The *Any* setting applies to all networks.

   **Target interface:** The interface for the data packets to be sent to (only available if you selected *Interface Route* as route type).

   **Gateway:** Select the gateway/router to which the gateway will forward data packets (only available if you selected *Gateway Route* as route type).

   **Comment** (optional): Add a description or other information.

3. **Click Save.**

   The new route appears on the *Policy Routes* list.

4. **Enable the route.**

   Click the toggle switch to activate the route.

To either edit or delete a route, click the corresponding buttons.
7 Network Services

This chapter describes how to configure several network services of Sophos UTM Manager for your network.

The following topics are included in this chapter:

- DNS
- NTP

7.1 DNS

The tabs of the Network Services > DNS menu contain miscellaneous configuration options, all related to the Domain Name System (DNS), a system primarily used to translate domain names (computer hostnames) to IP addresses.

7.1.1 Global

**Allowed Networks**

You can specify the networks that are to be allowed to use SUM as a recursive DNS resolver. Typically, you will select your internal networks here.

**Note** – If you already run an internal DNS server, for example as part of Active Directory, you should leave this box empty.

**DNSSEC**

The Domain Name System Security Extensions (DNSSEC) is a set of extensions to DNS to enhance security. It works by digitally signing DNS lookup records using public-key cryptography. If unselected, the SUM accepts all DNS records. If selected, the SUM validates incoming DNS requests with regard to DNSSEC signing. Only correctly signed records will be accepted from signed zones.
Note – If selected, DNS records might be rejected by DNSSEC-incapable forwarders that are manually installed or assigned by ISP. In this case, on the Forwarders tab, remove the DNS forwarders from the box and/or disable the Use forwarders assigned by ISP checkbox.

Flush Resolver Cache
The DNS proxy uses a cache for its records. Each record has an expiration date (TTL, time-to-live) at which it will be deleted, which is normally one day. However, you can empty the cache manually e.g. if you want recent changes in DNS records to take effect immediately, not having to wait for the TTL to expire. To empty the cache, click Flush Resolver Cache Now.

7.1.2 Forwarders
On the Network Services > DNS > Forwarders tab you can specify so-called DNS forwarders. A DNS forwarder is a Domain Name System (DNS) server on a network used to forward DNS queries for external DNS names to DNS servers outside of that network. If possible, add a DNS forwarder to your configuration. This should be a host "near" your site, preferably one provided by your Internet provider. It will be used as a "parent" cache. This will speed up DNS requests considerably. If you do not specify a forwarding name server, the root DNS servers will be queried for zone information first, taking a longer time to complete requests.

To create a DNS forwarder, proceed as follows:

1. Select a DNS forwarder.
   Select or add a DNS forwarder.
   **Use Forwarders Assigned By ISP** (optional): Select the Use Forwarders Assigned by ISP checkbox to forward DNS queries to the DNS servers of your ISP. When this box is checked, all forwarders automatically assigned by your ISP will be listed in the line below the box.

2. Click Apply.
   Your settings will be saved.

7.1.3 Request Routing
Suppose you run your own internal DNS server, this server could be used as an alternate server to resolve DNS queries for a domain you do not want to be resolved by DNS forwarders.
On the Network Services > DNS > Request Routing tab you can define routes to your own DNS servers.

To create a DNS request route, proceed as follows:

1. **On the Request Routing tab, click New DNS Request Route.**
   The Create New DNS Request Route dialog box opens.

2. **Make the following settings:**
   - **Domain:** Enter the domain for which you want to use an alternate DNS server.
   - **Target servers:** Select one or more DNS servers to use for resolving the domain entered above.
   - **Comment** (optional): Add a description or other information.

3. **Click Save.**
   The new route appears on the DNS Request Route list and is immediately active.

To either edit or delete a DNS request route, click the corresponding buttons.

### 7.1.4 DynDNS

Dynamic DNS, or DynDNS for short, is a domain name service which allows static Internet domain names to be assigned to a computer with a varying IP address. You can sign up for the DynDNS service at the website of the respective DynDNS service provider to get a DNS alias that will automatically be updated when your uplink IP address changes. Once you have registered to this service, you will receive a hostname, username, and password, which are necessary for the configuration.

To configure DynDNS, proceed as follows:

1. **On the DynDNS tab, click New DynDNS.**
   The Create New DynDNS dialog box opens.

2. **Make the following settings:**
   - **Type:** The following DynDNS services are available:
     - **DNS Park:** Official website: [www.dnspark.com](http://www.dnspark.com)
     - **DtDNS:** Official website: [www.dtdns.com](http://www.dtdns.com)
     - **DynDNS:** Standard DNS service of the service provider Dynamic Network Services Inc. (Dyn). Official website: [www.dyndns.com](http://www.dyndns.com)
- **DynDNS-custom**: Custom DNS service of the service provider Dynamic Network Services Inc. (Dyn) ([www.dyndns.com](http://www.dyndns.com)). Custom DNS is designed primarily to work with domains owned or registered by yourself.

- **easyDNS**: Official website: [www.easydns.com](http://www.easydns.com)

- **FreeDNS**: Official website: [freedns.afraid.org](http://freedns.afraid.org)

- **Namecheap**: Official website: [www.namecheap.com](http://www.namecheap.com)

- **zoneedit**: Official website: [www.zoneedit.com](http://www.zoneedit.com)

**Note** – In the **Server** field the URL is displayed to which the SUM sends the IP changes.

**Assign** (not with type FreeDNS): Define the IP address the DynDNS name is to be associated with. Selecting **IP of Local Interface** is useful when the interface in question has a public IP address. Typically, you will use this option for your DSL uplink. When you select **First public IP on the default route** no interface needs to be specified. Instead, your SUM will send a WWW request to a public DynDNS server which in return will respond with the public IP you are currently using. This is useful when your SUM does not have a public IP address but is located inside a private network, connected to the Internet via a masquerading router.

**Note** – FreeDNS always uses the first public IP address on the default route.

**Interface** (not with type FreeDNS, only with IP of local interface): Select the interface for which you want to use the DynDNS service, most likely this will be your external interface connected to the Internet.

**Hostname**: Enter the domain name you received from your DynDNS service provider (e.g., example.dyndns.org). **Note** that you need not adhere to a particular syntax for the hostname to be entered here. What you must enter here exclusively depends on what your DynDNS service provider requires. Apart from that, you can also use your DynDNS hostname as the gateway's main hostname, which, however, is not mandatory.

**Aliases** (optional): Use this box to enter additional hostnames which should point to the same IP address as the main hostname above (e.g., mail.example.com, example.com).
MX (optional, only with type DNS Park, DynDNS, or easyDNS): Mail exchangers are used for directing mail to specific servers other than the one a hostname points to. MX records serve a specific purpose: they let you specify the host (server) to which mail for a specific domain should be sent. For example, if you enter mail.example.com as Mail Exchanger, mail addressed to user@example.com would be delivered to the host mail.example.com.

MX priority (optional, only with type DNS Park): Enter a positive integer number indicating whether the specified mail server should be preferred for delivery of mail to the domain. Servers with lower numbers are preferred over servers with higher numbers. You can usually leave the field blank because DNS Park uses a default value of 5 which is appropriate for almost all purposes. For technical details about mail exchanger priorities, see RFC 5321.

Backup MX (optional, only with type DynDNS or easyDNS): Select this checkbox only if the hostname named in the Hostname text box is to serve as main mail exchanger. Then the hostname from the MX text box will only be advertised as a backup mail exchanger.

Wildcard (optional, only with type DynDNS or easyDNS): Select this option if you want subdomains to point to the same IP address as your registered domain. Using this option an asterisk (*) will be added to your domain serving as a wildcard (e.g., *.example.dyndns.org), thus making sure that, for example, www.example.dyndns.org will point to the same address as example.dyndns.org.

Username: Enter the username you received from the DynDNS service provider.

Password: Enter the password you received from the DynDNS service provider.

Comment (optional): Add a description or other information.

3. Click Save.
   The new DynDNS appears on the DynDNS list. The service is still disabled (toggle switch is gray).

4. Enable DynDNS.
   Click the toggle switch to enable the DynDNS service.
   The service is now enabled (toggle switch is green).

To either edit or delete a DynDNS, click the corresponding buttons.

You can use multiple DynDNS objects at the same time. When all settings for two hostnames are identical, it is recommended to use the Aliases option—instead of creating two distinct objects.
7.2 NTP

The menu Network Services > NTP allows you to configure an NTP server for the connected networks. The Network Time Protocol (NTP) is a protocol used for synchronizing the clocks of computer systems over IP networks. Instead of just synchronizing the time of Sophos UTM Manager, which can be configured on the Management > System Settings > Time and Date tab, you can explicitly allow certain networks to use this service as well.

To enable the use of NTP time synchronization for specific networks, proceed as follows:

1. **Enable the NTP server.**
   - Click the toggle switch.

2. **Select Allowed networks.**
   - Select the networks that should be allowed to access the NTP server.

3. **Click Apply.**
   - Your settings will be saved.
8 Logging & Reporting

This chapter describes the logging and reporting functionality of Sophos UTM Manager.

Sophos UTM Manager provides extensive logging capabilities by continuously recording various system and network protection events. The detailed audit trail provides both historical and current analysis of various network activities to help identify potential security threats or to troubleshoot occurring problems.

The reporting function of Sophos UTM Manager provides real-time information of its managed devices by collecting current log data and presenting it in a graphical format.

The Log Partition Status page in WebAdmin shows the status of the log partition of your Sophos UTM Manager unit, including information about the disk space left and fillup rate as well as a four-week histogram of the log partition utilization. As the fillup rate is the difference between the measurement point and the starting point divided by the time elapsed, the value is somewhat inaccurate in the beginning but becomes more precise the longer the system is up.

The following topics are included in this chapter:

- View Log Files
- Hardware
- Network Usage
- Network Protection
- Executive Report
- Log Settings
- Reporting Settings

Reporting Charts

Sophos UTM Manager displays reporting data in line charts and pie charts. Due to their interactivity, those charts allow a fine-grained access to information.
Line Charts

Interacting with line charts is easy: When hovering the mouse cursor on a chart a big dot will appear, which gives detailed information of this part of the chart. The dot is clung to the line of the chart. As you move the mouse cursor the dot follows. In case a chart has several lines, the dot switches between them according to where you move the mouse cursor. Additionally, the dot changes its color depending on which line its information refer to, which is especially useful with lines running close to each other.

![Figure 12 Reporting: Example of a Line Chart](image)

Pie Charts

Similar to line charts, you can interact with pie charts: Direct the mouse cursor to a piece of a pie chart. This piece will immediately be extracted from the rest of the pie, the tooltip showing detailed information of the extracted piece.

![Figure 13 Reporting: Example of a Pie Chart](image)

8.1 View Log Files

The Logging & Reporting > View Log Files menu offers the possibility to view different kind of log files and to search in log files.
8.1.1 Today's Log Files

On the Logging & Reporting > View Log Files > Today’s Log Files tab all current logs can easily be accessed.

This tab provides various actions that can be applied to all log files. The following actions are available:

- **Live Log**: Opens a pop-up window allowing you to view the log file in real-time. New lines are added to the log file on the fly. If you select Autoscroll, the pop-up window will automatically scroll down to always display the most recent log. In addition, the pop-up window also contains a filter text box that allows you to limit the display of new logs to only those records that match the filter.

- **View**: Opens a pop-up window that shows the log file in its current state.

- **Clear**: Deletes the contents of the log file.

Using the drop-down list in the table footer, you can either download selected log files as a zip file or clear their contents simultaneously.

8.1.2 Archived Log Files

On the Logging & Reporting > View Log Files > Archived Log Files tab you can manage the log file archive. All log files are archived on a daily basis. To access an archived log file, select the subsystem of Sophos UTM Manager for which logs are written as well as a year and month.

All available log files that match your selection will be displayed in chronological order. You can either view the archived log file or download it in zip file format.

Using the drop-down list in the table footer, you can either download selected log files as a zip file or delete them simultaneously.

8.1.3 Search Log Files

The tab Logging & Reporting > View Log Files > Search Log Files enables you to search through your local log files for various time periods. First, select the log file you want to search through, then enter the search term and select the time range. If you select Custom Time Frame from the Select Time Frame list, you can specify a start and end date. After clicking the
8.2 Hardware

The Logging & Reporting > Hardware menu provides overview statistics about the utilization of hardware components for several time periods.

8.2.1 Daily

The Hardware > Daily tab provides overview statistics about the following hardware components of the last 24 hours:

- CPU Usage
- Memory/Swap Usage
- Partition Usage

**CPU Usage:** The histogram displays the current processor utilization in percent.

**Memory/Swap Usage:** The utilization of memory and swap in percent. The swap usage heavily depends on your system configuration. The activation of system services such as Intrusion Prevention or the proxy servers will result in a higher memory usage. If the system runs out of free memory, it will begin to use swap space, which decreases the overall performance of the system. The used swap space should be as low as possible. To achieve that, increase the total amount of memory available to your system.

**Partition Usage:** The utilization of selected partitions in percent. All charts show three graphs, each representing one hard disk drive partition:

- **Root:** The root partition is the partition where the root directory of Sophos UTM Manager is located. In addition, this partition stores update packages and backups.
- **Log:** The log partition is the partition where log files and reporting data is stored. If you run out of space on this partition, please adjust your settings under Logging & Reporting > Log Settings > Local Logging.
- **Storage:** The storage partition is the partition where the database, temporary data, cached Up2Dates, and configuration files are located.
8.2.2 Weekly

The *Hardware > Weekly* tab provides overview statistics about selected hardware components for the last seven days. The histograms are described in the *Daily* section.

8.2.3 Monthly

The *Hardware > Monthly* tab provides overview statistics about selected hardware components for the last four weeks. The histograms are described in the *Daily* section.

8.2.4 Yearly

The *Hardware > Yearly* tab provides overview statistics about selected hardware components for the last twelve months. The histograms are described in the *Daily* section.

8.3 Network Usage

The tabs of the *Logging & Reporting > Network Usage* menu provide overview statistics about the traffic passing each interface of Sophos UTM Manager for several time periods. Each chart presents its data using the following units of measurement:

- u (Micro, $10^{-6}$)
- m (Milli, $10^{-3}$)
- k (Kilo, $10^3$)
- M (Mega, $10^6$)
- G (Giga, $10^9$)

Note that the scaling can range from $10^{-18}$ to $10^8$.

8.3.1 Daily

The *Network Usage > Daily* tab provides overview statistics about the traffic passing each configured interface of the last 24 hours.

Each histogram shows two graphs:
8.3 Network Usage

- **Inbound**: The average incoming traffic for that interface, in bits per second.
- **Outbound**: The average outgoing traffic for that interface, in bits per second.

The Concurrent Connections chart shows you the total of concurrent connections.

8.3.2 Weekly

The Network Usage > Weekly tab provides overview statistics about the traffic passing each configured interface of the last seven days. The histograms are described in the **Daily** section.

8.3.3 Monthly

The Network Usage > Monthly tab provides overview statistics about the traffic passing each configured interface of the last four weeks. The histograms are described in the **Daily** section.

8.3.4 Yearly

The Network Usage > Yearly tab provides overview statistics about the traffic passing each configured interface of the last twelve months. The histograms are described in the **Daily** section.

8.3.5 Bandwidth Usage

The Network Usage > Bandwidth Usage tab presents comprehensive data about the network traffic which was transferred to/from and through the device.

From the first drop-down list, select the type of data to display, e.g., **Top Clients** or **Top Services By Client**. Select the desired entry, and, if an additional box is displayed, specify the respective filter argument. Additionally, using the drop-down list below, you can filter the entries by time. Always click **Update** to apply the filters.

On the **By Client** and **By Server** views you can manually provide an IP/Network, as well as network ranges (e.g., 192.168.1.0/24 or 10/8). On the **By Services** views you can enter protocol and service, separated by comma (e.g., **TCP,SMTP,UDP,6000**). If you do not supply the protocol, TCP will be assumed (e.g. **HTTP** is also valid).

On the **Top Clients** and **Top Servers** views, if an IP or a hostname is clicked in the result table, it will automatically be used as a filter for the **Top Services By Client** or **Top Services By Server** view. On the **Top Services**, **Top Applications**, and **Top Application Categories** views, if you click a service, an application, or an application category in the result table, it will automatically be
used as a filter for the Top Clients by Service, Top Clients by Application, or Top Clients by Category view.

Please note that the labels IN and OUT for traffic may vary depending on the point of view.

By default, 20 entries per page are displayed. If there are more entries, you can jump forward and backward using the Forward and Backward icons, respectively. In the Number of rows drop-down list, you can increase the number of entries displayed per page.

You can sort all data by clicking the table column headers. For example, if you want to sort all hosts by incoming traffic, click on IN in the table heading. Thus, hosts causing the most incoming traffic will be listed first. Note that the data for traffic is given in kibibytes (KiB) and mebibytes (MiB), both of which are base-2 units of computer storage (e.g., 1 kibibyte = 2\(^{10}\) bytes = 1 024 bytes).

You can download the data in PDF or Excel format by clicking one of the corresponding icons in the top right corner of the tab. The report is generated from the current view you have selected. Additionally, by clicking the Pie Chart icon—if present—you can get a pie chart displayed above the table.

8.4 Network Protection

The tabs of the Logging & Reporting > Network Protection menu provide overview statistics about relevant network protection events detected by Sophos UTM Manager.

8.4.1 Daily

The Daily tab provides an overview statistic about the firewall violations of the last 24 hours.

Firewall Violations: Every data packet that is dropped or rejected is counted as a firewall violation. The number of firewall violations is calculated over a time span of five minutes.

8.4.2 Weekly

The Weekly tab provides an overview statistic about firewall violations of the last seven days. The histograms are described in the Daily section.
8.4.3 Monthly

The *Monthly* tab provides an overview statistic about firewall violations of the last four weeks. The histograms are described in the *Daily* section.

8.4.4 Yearly

The *Yearly* tab provides an overview statistic about firewall violations of the last twelve months. The histograms are described in the *Daily* section.

8.5 Executive Report

In the menu *Logging & Reporting > Executive Report* you can create a collection of the most important reporting data presented in graphical format to show network utilization for a number of services.

8.5.1 View Report

On the *Logging & Reporting > Executive Report > View Report* tab you can create a complete executive report based on the individual reports in the tabs and pages of the *Reporting* menu. Click the button *Generate Report Now* to open a window showing the executive report.

8.5.2 Archived Executive Reports

The *Executive Report > Archived Executive Reports* tab provides an overview of all archived executive reports. Only those executive reports will be archived for which archiving has been selected on the *Configuration* tab.

8.5.3 Configuration

On the *Executive Report > Configuration* tab you can make the settings for executive reports.

**Daily Executive Report**

**Daily executive report:** If enabled, a daily executive report is created.
8 Logging & Reporting

8.6 Log Settings

In the Logging & Reporting > Log Settings menu you can configure basic settings for local and remote logging.

8.6.1 Local Logging

On the Logging & Reporting > Log Settings > Local Logging tab you can make the settings for local logging. Local logging is enabled by default.

However, to activate local logging in case it was disabled, proceed as follows:

1. **On the Local Logging tab enable local logging.**
   
   Click the toggle switch.

   The toggle switch turns green and the areas on this tab become editable.

2. **Select a time frame when log files are to be deleted.**
   
   From the drop-down list select what action is to be applied automatically on log files.

   *Never delete log files* is selected by default.

3. **Click Apply.**

   Your settings will be saved.
Thresholds
Here you can define thresholds for local logging which are bound to certain actions that are to be carried out if a threshold is reached. The following actions are available:

- **Nothing**: No actions will be initiated.
- **Send notification**: A notification will be sent to the administrator stating that the threshold was reached.
- **Delete oldest log files**: Oldest log files will be deleted until the remaining amount is below the configured threshold or until the log file archive is empty. In addition, a notification of that event will be sent to the administrator.
- **Shutdown system**: The system will be shut down. A notification of that event will be sent to the administrator.
  
  In case of a system shutdown, the administrator has to change the configuration of the local logging, configure log file deletion or move away/delete log files manually. If the reason for the system shutdown persists, the system will shut down itself again the next time the log cleaning process runs, which happens daily at 12:00 AM (i.e., at midnight).

Click Apply to save your settings.

8.6.2 Remote Syslog Server
On the Logging & Reporting > Log Settings > Remote Syslog Server tab you can make the settings for remote logging. This function allows you to forward log messages from SUM to other hosts. This is especially useful for networks using a host to collect logging information from several SUMs. The selected host must run a logging daemon that is compatible to the syslog protocol.

To configure a remote syslog server, proceed as follows:

1. **On the Remote Syslog Server tab enable remote syslog.**
   
   Click the toggle switch.
   
   The toggle switch turns amber and the Remote Syslog Settings area becomes editable.

2. **Click the Plus icon in the Syslog Servers box to create a server.**
   
   The Add Syslog Server dialog box opens.

3. **Make the following settings:**
   
   **Name**: Enter a descriptive name for the remote syslog server.
**Server:** Add or select the host that should receive log data from SUM.

**Caution** – Do not use one of SUM’s own interfaces as a remote syslog host, since this will result in a logging loop.

**Port:** Add or select port which is to be used for the connection.

4. **Click Apply.**
   
   Your settings will be saved.

**Remote Syslog Buffer**

In this area you can change the buffer size of the remote syslog. The buffer size is the number of log lines kept in the buffer. Default is 1000. Click **Apply** to save your settings.

**Remote Syslog Log Selection**

This area is only editable when remote syslog is enabled. Select the checkboxes of the logs that should be delivered to the syslog server. You can select all logs at once by selecting the option **Select All.** Click **Apply** to save your settings.

**8.6.3 Remote Log File Archives**

On the *Logging & Reporting > Log Settings > Remote Log File Archives* tab you can make the settings for remote archiving of log files. If remote log file archiving is enabled, the log files of the past day are packed and compressed into one file, which is transferred to a remote log file storage. Using the drop-down list you can select your preferred transfer method.

To configure a remote log file archive, proceed as follows:

1. **Enable the Remote Log File Archives function.**
   
   Click the toggle switch.
   
   The toggle switch turns amber and the *Remote Log File Archive* area becomes editable.

2. **Select the log file archiving method.**
   
   From the drop-down list, select your preferred archiving method. Depending on your selection, the related configuration options for each archiving method will be displayed below. You can choose between the following archiving methods:

   - **FTP Server:** The *File Transfer Protocol* (FTP) method needs the following parameters to be set:
8.6 Log Settings

- **Host**: Host definition of the FTP server.
- **Service**: TCP port the server is listening on.
- **Username**: Username for the FTP server account.
- **Password**: Password for the FTP server account.
- **Path**: Remote (relative) path where the log files are stored.

- **SMB (CIFS) Share**: The SMB method needs the following parameters to be set:
  - **Host**: Host definition of the SMB server.
  - **Username**: Username for the SMB account.
  - **Password**: Password for the SMB account.

  **Security Note** – The password will be saved plain-text in the configuration file. It is therefore advisable to create a user/password combination uniquely for this logging purpose.

- **Share**: SMB share name. Enter the path or the network share information where the log files are to be transferred to, e.g. `/logs/log_file_archive`.

- **Workgroup/Domain**: Enter the workgroup or domain the log file archive is part of.

- **Secure Copy (SSH Server)**: To use the SCP method, it is necessary that you add the public SSH DSA key to the authorized keys of your SCP server. On a Linux system, you can simply cut and paste the SSH DSA key and add it to the `~/.ssh/authorized_keys` file of the configured user account. During the installation, Sophos UTM Manager creates a new SSHDSA key. For security reasons, this SSH DSA key is not included in backups. After a new installation or the installation of a backup, you must therefore store the new SSH DSA key on the remote server to be able to securely copy your log file archives to the SCP server. The SCP method requires the following settings:
  - **Host**: Host definition for the SCP server.
  - **Username**: Username for the SCP server account.
  - **Path**: Remote (full) path where the log files should be stored.
  - **Public DSA key**: On the remote storage host, add the provided public DSA key to the list of authorized keys.
Send by email: To have the log file archive sent by email, enter a valid email address.

3. Click Apply.
Your settings will be saved.

If the transfer fails, the archive will remain on SUM. During each run of the log cleaning process, SUM tries to deliver all remaining archives.

8.7 Reporting Settings

In the Logging & Reporting > Reporting Settings menu you can make settings for the reporting functions such as enabling/disabling certain features of reporting, setting time frames and amounts for keeping data. Additionally, you can anonymize data to enhance privacy protection.

8.7.1 Settings

The Settings tab allows you to define reporting actions and the time period reporting data will be kept on the system before it is automatically deleted. The following report topics can be set:

- Authentication
- Firewall
- Network Usage

Use the checkboxes on the left side to enable or disable reporting for a certain report topic. By default, all report topics are enabled.

Use the drop-down lists on the right to determine how long reporting data is kept.

Note – Disabling needless reports will lower the base load of your machine and can reduce performance bottlenecks. Try to keep time frames as short as possible since high amounts of stored data result in a higher base load and decreased responsiveness on the dynamical reporting pages.

The settings on this tab do not affect the log file archives.

Executive Report Settings

In this area you can define respectively the number of executive reports to keep:
8.7 Reporting Settings

- Daily reports: 60 at maximum
- Weekly reports: 52 at maximum
- Monthly reports: 12 at maximum

Click Apply to save your settings.

For more information on the executive report and its options, see Logging & Reporting > Executive Report.

**PDF Paper Settings**

The default paper format for the PDF executive report is A4. Using the drop-down list you can alternatively select Letter or Legal. Click Apply to save your settings.

**CSV Delimiter Settings**

Here you can define which delimiter is used when exporting reporting data to CSV format. Please note that with Windows operating systems the delimiter should match the regional settings of your system to make sure that the exported data will be displayed correctly in a spreadsheet program like e.g., Excel.

**IPFIX Accounting**

By means of IPFIX you can export IPv4 flow data of SUM to a provider for e.g. monitoring, reporting, accounting, or billing purposes.

Internet Protocol Flow Information Export (IPFIX) is a message-based protocol for exporting accounting information in a universal way. The accounting information is collected by an exporter and sent to a collector. A typical set of accounting information for an IPv4 flow consists of source address, destination address, source port, destination port, bytes, packets, and network traffic classification data.

If enabled, SUM serves as exporter: It exports IPFIX accounting data. The collector generally is located at a provider’s site where the accounting data of one or more of your SUMs is aggregated and analyzed. During the system setup at your provider, you will be given the hostname and you have to define a unique Observation Domain ID (OID) per exporter, i.e., SUM. Enter this data into the corresponding fields.

Data is exported on UDP port 4739. A single network connection uses two IPFIX flows—one for the export direction, one for the reply.
Security Note – Be aware that with IPFIX the accounting data will be transmitted unencrypted. It is therefore recommended to send the data via private network only.

Click Apply to save your settings.
9 Support

This chapter describes the support tools available for Sophos UTM Manager.

The pages of the Support menu contain many customer support related features ranging from various web links, through contact information, to the output of useful network tools that are used to determine important network properties without the need to access SUM’s command-line interface.

The following topics are included in this chapter:

- Documentation
- Contact Support
- Tools
- Advanced

In addition, the main page of the Support menu contains web links to the following information resources:

- Knowledgebase (KB): Official knowledgebase of Sophos NSG contains numerous information on configuring Sophos UTM Manager.
- Known Issues List (KIL): The list of known problems that cannot be fixed or for which a workaround is available.
- Hardware Compatibility List (HCL): The list of hardware that is compatible to Sophos UTM Manager Software.
- Up2Date Information: Sophos NSG Up2Date blog, which informs about product improvements and firmware updates.

9.1 Documentation

Online Help
This section gives a description of how to open and use the online help.

Manual Download
Select if you want to download the Administration Guide for SUM WebAdmin or for SUM Gateway Manager as well as the language of the guide and click Start download. Note that you
need a special reader to open PDF documents such as Adobe's Reader or Xpdf.

Cross Reference – Administration Guides from former SUM versions and other documentation can be downloaded from the Sophos Knowledgebase.

9.2 Printable Configuration

On the Support > Printable Configuration page you can create a detailed report of the current WebAdmin configuration.

Note – The printable configuration is opened in a new window. Depending on your browser it may be necessary to allow pop-up windows for WebAdmin.

The structure of the printable configuration matches the WebAdmin menu structure to facilitate finding the corresponding configuration options in WebAdmin.

The printable configuration browser page consists of an overview page, called index, and several subpages. Links to subpages are highlighted blue. Subpages give detailed information to the respective topic. You can always return from a subpage to the index by clicking the Back to the index link at the bottom of the subpage.

There are two more viewing options for the printable configuration:

- WebAdmin format
- Confd format

You can find the links to these viewing options at the bottom of the index page.

9.3 Contact Support

Sophos offers a comprehensive range of customer support services for its security solutions. Based on the support/maintenance level, you have various levels of access and committed response time by the Sophos service department and/or Sophos NSG Certified Partners.

All support cases concerning Sophos UTM Manager are processed via the MyAstaro Licensing Portal. You may open a support case via a web form by clicking Open Support Ticket in New Window.
9.4 Tools

The tabs of the Support > Tools menu display the output of useful network tools that can be used to determine important network properties without the need to access SUM's command-line interface. The output of the following tools can be viewed:

- Ping
- Traceroute
- DNS Lookup

9.4.1 Ping Check

The program ping is a computer network tool used to test whether a particular host is reachable across an IP network. Ping works by sending ICMP echo request packets to the target host and listening for ICMP echo response replies. Using interval timing and response rate, ping estimates the round-trip time and packet loss rate between hosts.

To make a ping check, proceed as follows:

1. **Select the ping host.**
   Select the host you want to ping. In the Ping Host box, you can select a host for which a host definition exists. Alternatively, you can also select Custom hostname/IP address and enter a custom hostname or IP address into the textbox below.

2. **Select the IP version** (only available if IPv6 is globally enabled).
   From the IP version drop-down list, select IPv4 or IPv6.

3. **Click Apply.**
   The output of the ping check will be displayed in the Ping Check Result area.

9.4.2 Traceroute

The program traceroute is a computer network tool used to determine the route taken by packets across an IP network. It lists the IP addresses of the routers that were involved in transporting the packet. If the packet's route cannot be determined within a certain time frame, traceroute will report an asterisk (*) instead of the IP address. After a certain number of failures, the check will end. An interruption of the check can have many causes, but most likely it is caused by a firewall along the network path that blocks traceroute packets.
To trace a route, proceed as follows:

1. **Specify the traceroute host.**
   Select the host you want to trace the route to. In the *Traceroute host* box, you can select a host for which a host definition exists. Alternatively, you can also select *Custom hostname/IP address* and enter a custom hostname or IP address into the textbox below.

2. **Select the IP version** (only available if IPv6 is globally enabled).
   In the *IP version* drop-down list, select *IPv4* or *IPv6*.

3. **Print hop addresses numerically rather than symbolically and numerically** (optional).
   Selecting this option saves a nameserver address-to-name lookup for each gateway found on the path.

4. **Click Apply.**
   The output of traceroute will be displayed in the *Traceroute Result* area.

### 9.4.3 DNS Lookup

The program *dig* (short for *Domain Information Groper*) is a network tool for interrogating DNS name servers. It performs DNS lookups and displays the answers that are returned from the name server(s) that were queried.

To make a DNS lookup, proceed as follows:

1. **Specify the hostname/IP address.**
   Enter the hostname or IP address of the host for which you want to determine DNS information.

2. **Select Enable verbose output** (optional).
   Select this option to generate lengthy output showing more information.

3. **Click Apply.**
   The output of *dig* will be displayed in the *DNS Lookup Result* area.

### 9.5 Advanced

The *Support > Advanced* menu displays even more information on your SUM and gives access to advanced features. It gives overview of running processes and local network connections and you can view the routing table and the interfaces table. Additionally, you can download a
support package for debugging and recovery purposes and find background information about internally used configuration references which you may encounter in log files.

### 9.5.1 Process List

The program *ps* displays a header line followed by lines containing information about your processes that have controlling terminals. This information is sorted by controlling terminal, then by process ID.

### 9.5.2 LAN Connections

The program *netstat* (short for *Network Statistics*) is a network tool that displays a list of the active Internet connections a computer currently has, both incoming and outgoing.

### 9.5.3 Routes Table

The program *ip* is a network tool for controlling TCP/IP networking and traffic control. Invoked with the parameter `route show table all` it displays the contents of all routing tables of SUM.

### 9.5.4 Interfaces Table

The table shows all configured interfaces of Sophos UTM Manager, both network interface cards and virtual interfaces. The program *ip* invoked with parameter `addr` displays interfaces and their properties.

### 9.5.5 Config Dump

For debugging or recovery purposes it is useful to gather as many information as possible about your installation of Sophos UTM Manager. The support package that can be downloaded from the *Support > Advanced > Config Dump* tab provides exactly this. The zip file contains the following items:

- The entire dump of SUM’s configuration (*storage.abf*). Note that this is no genuine backup file—it does not contain any passwords, among other things—and can be used for debugging purposes only.
- Information on the hardware present in the system (hwinfo).
- Information on the software packages installed on the system (swinfo).

### 9.5.6 Resolve REF

For debugging purposes you can resolve configuration references internally used by the system. If you encounter a reference somewhere in the logs, you can paste the reference string here (e.g., REF_DefaultSuperAdmin). The tab will then display an excerpt of the configuration daemon's data structure.
10 Log Off

You can log out of SUM by clicking the Log Off menu entry. If you do not log out properly or if you close the web browser inadvertently, you might not be able to log in again for approximately 30 seconds.

**Note** – You will be logged out if you visit a different website during a session. In this case, you will have to log in again.
A

**Address Resolution Protocol**
Used to determine the Ethernet MAC address of a host when only its IP address is known.

**Advanced Configuration and Power Interface**
The ACPI specification is a power management standard that allows the operating system to control the amount of power distributed to the computer's devices.

**Advanced Programmable Interrupt Controller**
Architecture for dealing with interrupts in multi-processor computer systems.

**Astaro Command Center**
Software for monitoring and administering multiple Astaro gateway units by means of a single interface. Starting with version 4, the software was renamed Sophos UTM Manager (SUM).

**Astaro Security Gateway**
Software for unified threat management, including mail and web security. Starting with version 9, the software was renamed Unified Threat Management (UTM).

**Authentication Header**
IPsec protocol that provides for anti-replay and verifies that the contents of the packet have not been modified in transit.

**Autonomous System**
Collection of IP networks and routers under the control of one entity that presents a common routing policy to the Internet.

**B**

**Bounce Address Tag Validation**
Name of a method designed for determining whether the return address specified in an e-mail message is valid. It is designed to reject bounce messages to forged return addresses.

**Broadcast**
The address used by a computer to send a message to all other computers on the network at the same time. For example, a network with IP address 192.168.2.0 and network mask 255.255.255.0 would have a broadcast address of 192.168.2.255.

**C**

**Certificate Authority**
Entity or organization that issues digital certificates for use by other parties.

**Cipher Block Chaining**
Refers in cryptography to a mode of operation where each block of plaintext is "XORed" with the previous ciphertext block before being encrypted. This way, each ciphertext block is dependent on all plaintext blocks up to that point.
Cluster
Group of linked computers, working together closely so that in many respects they form a single computer.

Dynamic Host Configuration Protocol
Protocol used by networked devices to obtain IP addresses.

E
Encapsulating Security Payload
IPsec protocol that provides data confidentiality (encryption), anti-replay, and authentication.

Explicit Congestion Notification
Explicit Congestion Notification (ECN) is an extension to the Internet Protocol and allows end-to-end notifications of network congestion without dropping packets. ECN only works if both endpoints of a connection successfully negotiate to use it.

F
File Transfer Protocol
Protocol for exchanging files over packet-switched networks.

G
Generic Routing Encapsulation
Tunneling protocol designed for encapsulation of arbitrary kinds of network layer packets inside arbitrary kinds of network layer packets.

GeoIP
Technique to locate devices worldwide by means of satellite imagery.
H

H.323
Protocol providing audio-visual communication sessions on packet-switched networks.

High Availability
System design protocol that ensures a certain absolute degree of operational continuity.

Hypertext Transfer Protocol
Protocol for the transfer of information on the Internet.

Hypertext Transfer Protocol over Secure Socket Layer
Protocol to allow more secure HTTP communication.

I

IDENT
Standard protocol that helps identify the user of a particular TCP connection.

Internet Control Message Protocol
Special kind of IP protocol used to send and receive information about the network’s status and other control information.

Internet Protocol
Data-oriented protocol used for communicating data across a packet-switched network.

Internet Relay Chat
Open protocol enabling the instant communication over the Internet.

Internet service provider
Business or organization that sells to consumers access to the Internet and related services.

IP Address
Unique number that devices use in order to identify and communicate with each other on a computer network utilizing the Internet Protocol standard.

Link-state advertisement
Basic communication means of the OSPF routing protocol for IP.

MAC Address
Unique code assigned to most forms of networking hardware.

Managed Security Service Provider
Provides security services for companies.

Management Information Base
Type of database used to manage the devices in a communications network. It comprises a collection of objects in a (virtual) database used to manage entities (such as routers and switches) in a network.

Masquerading
Technology based on NAT that allows an entire LAN to use one public IP address to communicate with the rest of the Internet.
**Message-Digest algorithm 5**
Cryptographic hash function with a 128-bit hash value.

**Multipurpose Internet Mail Extensions**
Internet Standard that extends the format of e-mail to support text in character sets other than US-ASCII, non-text attachments, multi-part message bodies, and header information in non-ASCII character sets.

**MX record**
Type of resource record in the Domain Name System (DNS) specifying how e-mails should be routed through the Internet.

**Network Address Translation**
System for reusing IP addresses.

**Network Time Protocol**
Protocol for synchronizing the clocks of computer systems over packet-switched networks.

**Not-so-stubby area**
In the OSPF protocol, a type of stub area that can import autonomous system (AS) external routes and send them to the backbone, but cannot receive AS external routes from the backbone or other areas.

**Open Shortest Path First**
Link-state, hierarchical interior gateway protocol (IGP) for network routing.

**OpenPGP**
Protocol combining strong public-key and symmetric cryptography to provide security services for electronic communications and data storage.

**Port**
Virtual data connection that can be used by programs to exchange data directly. More specifically, a port is an additional identifier—in the cases of TCP and UDP, a number between 0 and 65535—that allows a computer to distinguish between multiple concurrent connections between the same two computers.

**Portscan**
Action of searching a network host for open ports.

**Post Office Protocol version 3**

**Privacy Enhanced Mail**
Early IETF proposal for securing e-mail using public key cryptography.

**Protocol**
Well-defined and standardized set of rules that controls or enables the connection, communication, and data transfer between two computing endpoints.

**Proxy**
Computer that offers a computer network service to allow clients to make indirect network connections to other network services.
**R**

**Real-time Blackhole List**
Means by which an Internet site may publish a list of IP addresses linked to spamming. Most mail transport agent (mail server) software can be configured to reject or flag messages which have been sent from a site listed on one or more such lists. For webservers as well it is possible to reject clients listed on an RBL.

**Redundant Array of Independent Disks**
Refers to a data storage scheme using multiple hard drives to share or replicate data among the drives.

**Remote Authentication Dial In User Service**
Protocol designed to allow network devices such as routers to authenticate users against a central database.

**Router**
Network device that is designed to forward packets to their destination along the most efficient path.

**S**

**Secure Shell**
Protocol that allows establishing a secure channel between a local and a remote computer across packet-switched networks.

**Secure Sockets Layer**
Cryptographic protocol that provides secure communications on the Internet, predecessor of the Transport Layer Security (TLS).

**Secure/Multipurpose Internet Mail Extensions**
Standard for public key encryption and signing of e-mail encapsulated in MIME.

**Security Parameter Index**
Identification tag added to the header while using IPsec for tunneling the IP traffic.

**Sender Policy Framework**
Extension to the Simple Mail Transfer Protocol (SMTP). SPF allows software to identify and reject forged addresses in the SMTP MAIL FROM (Return-Path), a typical annoyance of e-mail spam.

**Session Initiation Protocol**
Signalization protocol for the setup, modification and termination of sessions between two or several communication partners. The text-oriented protocol is based on HTTP and can transmit signalization data through TCP or UDP via IP networks. Thus, it is the base among others for Voice-over-IP videotelephony (VoIP) and multimedia services in real time.

**Shared Secret**
Password or passphrase shared between two entities for secure communication.

**Simple Mail Transfer Protocol**
Protocol used to send and receive e-mail across packet-switched networks.
**Single sign-on**
Form of authentication that enables a user to authenticate once and gain access to multiple applications and systems using a single password.

**SOCKetS**
Internet protocol that allows client-server applications to transparently use the services of a network firewall. SOCKS, often called the Firewall Traversal Protocol, is currently at version 5 and must be implemented in the client-side program in order to function correctly.

**Sophos UTM Manager**
Software for monitoring and administering multiple UTM units by means of a single interface. Formerly known as Astaro Command Center.

**Source Network Address Translation**
Special case of NAT. With SNAT, the IP address of the computer which initiated the connection is rewritten.

**Spanning Tree Protocol**
Network protocol to detect and prevent bridge loops.

**Subnet mask**
The subnet mask (also called netmask) of a network, together with the network address, defines which addresses are part of the local network and which are not. Individual computers will be assigned to a network on the basis of the definition.

**Symmetric Multiprocessing**
The use of more than one CPU.

**Time-to-live**
8-bit field in the Internet Protocol (IP) header stating the maximum amount of time a packet is allowed to propagate through the network before it is discarded.

**Transmission Control Protocol**
Protocol of the Internet protocol suite allowing applications on networked computers to create connections to one another. The protocol guarantees reliable and in-order delivery of data from sender to receiver.

**Transport Layer Security**
Cryptographic protocol that provides secure communications on the Internet, successor of the Secure Sockets Layer (SSL).

**Unified Threat Management**
Software for unified threat management, including mail and web security. Formerly known as Astaro Security Gateway.

**Uniform Resource Locator**
String that specifies the location of a resource on the Internet.

**Uninterruptible power supply**
Device which maintains a continuous supply of electric power to connected equipment by supplying power from a separate source when utility power is not available.
Up2Date
Service that allows downloading relevant update packages from the Sophos server.

User Datagram Protocol
Protocol allowing applications on networked computers to send short messages sometimes known as datagrams to one another.

Virtual Private Network
Private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol such as PPTP or IPsec.

Voice over IP
Routing of voice conversations over the Internet or through any other IP-based network.

WebAdmin
Web-based graphical user interface of Sophos/Astaro products such as UTM, SUM, ACC, ASG, AWG, and AMG.

Windows Internet Naming Service
Microsoft's implementation of NetBIOS Name Server (NBNS) on Windows, a name server and service for NetBIOS computer names.

X
X.509
Specification for digital certificates published by the ITU-T (International Telecommunications Union – Telecommunication). It specifies information and attributes required for the identification of a person or a computer system.
List of Figures

Figure 1  WebAdmin: Initial Login Page .................................................. 10
Figure 2  WebAdmin: Regular Login Page ............................................. 11
Figure 3  WebAdmin: Dashboard ........................................................... 12
Figure 4  WebAdmin: Overview .............................................................. 13
Figure 5  WebAdmin: Example of a List ................................................ 15
Figure 6  WebAdmin: Example of a Dialog Box ..................................... 18
Figure 7  WebAdmin: Dragging an Object From the Object List Networks .................................................. 21
Figure 8  Up2Date: Progress Window ...................................................... 43
Figure 9  User Portal: Welcome Page ...................................................... 51
Figure 10 Groups: eDirectory Browser of Sophos UTM Manager ........... 77
Figure 11 Authentication: Microsoft Management Console .................. 82
Figure 12 Reporting: Example of a Line Chart ...................................... 114
Figure 13 Reporting: Example of a Pie Chart ........................................ 114
Index

3

3G/UMTS (interface type) 93
  MTU 94

A

access control 12
  logging of traffic 33
  to Gateway Manager 39
  to SSH 31
  to SUM 40
  to WebAdmin 33-34
Active Directory 77, 80
  backend servers 81
Base DN 83
  groups 88
  port number 81
  prefetching with 88
  supported versions 81
Admin Password Setup (dialog window) 32
administration guide
  download of 129
  language of 129
administrative interface 7
administrator 72
  contact data 56
  password of 32
    setting of 10
  WebAdmin access 33
administrator manual See administration guide
agent, SNMP 57
aliases, IP addresses 100
APC (manufacturer) 4
area, system settings 6
Astaro’s Portal See MyAstaro Portal
auditor (user right) 34
auditor (user role) 34
  authentication 77-78
    cache for 78
      clearance of 79
    global settings 78
    live log 79
      of clients 65-66
      of users 73
  authentication servers 79
    Active Directory 77, 80
    eDirectory 77, 79
    external 65, 77
    LDAP 77, 83
    RADIUS 77-78, 85
    TACACS+ 77, 86
  authentication services 86
  authorization
    of users 86
  automatic backups 50
    deletion of 50
    download of 50
    emailing of 50
    encryption of 50
    interval of creation 50
    password protection 50
    restoration of 50
    storage of 50
  autonegotiation, interfaces 101
  availability groups 68
    always resolved 69
    monitoring interval 69

B

backend directory services See directory services
backend servers
  Active Directory 81
  eDirectory 79
  LDAP 83
  RADIUS 85
  TACACS+ 87
backups
  as templates 49
automatic 50
  before Up2Date installation 42
  deletion of 50
  download of 50
  emailing of 42, 50
  encryption of 50
  interval of creation 50
  password protection 50
  restoration of 50
  storage of 50
available 47, 49-50
confidential information and 47
content of 47
creation of 46-48
creator of 47, 50
deletion of 48
download of 47
emailing of 48
  recipients of 48
  encryption of 47
file extensions 47
import of 48-50
lock files and 48
password protection 47
readability of 47
restoration of 46-47
  from USB flash drive 48
SSH DSA keys and 124
storage of 47
version number 47
bandwidth monitor See flow monitor
bandwidth usage, reporting 118
base license 41
basic configuration 9
basic system setup 10
battery operation, UPS 4
bit mask 68
bit rate, network cards 23
blocked IP address, due to failed logins 87
Blowfish (cipher) 47
browser See web browser
button bar, of WebAdmin 14
buttons, in WebAdmin 18
C
cache 46
  for authentication 78
  clearance of 79
  for Up2Dates 24, 45
CBC mode (Cipher Block Chaining) 47
CD-ROM drive, system requirements 6
CD-ROM, for installation 4
certificate authority 59, 61
  download of 62
  import of 62
  signing CA 61
    for VPN 63
  verification CA 61
  WebAdmin certificate 10, 35
certificates 59
  deletion of 60
  download of 61
  generation of 59, 72
  import of 60
  information contained in 28
  invalid 29
  management of 59
    of User Portal 35
    of WebAdmin 10, 35
  public keys, import of 59
  revocation lists 59, 62
  self-signed, of system 9, 59, 61
  SSL, of users 78
time, time zones, and 35
  validity of 9, 35
  VPN ID 60, 72
  VPN ID type 60
X.509 59
  of users 72
changes, of WebAdmin settings 27
charts, reporting 114
client authentication 65-66
codes, of notifications 53
command-line access 30, See also shell access
community string, SNMP 57, 59
cOMPANY information 10
company logo, customization of 55
company text, customization of 56
complexity, password 31, 88
configuration 9
  of system 23
  of Up2Dates 44
  of WebAdmin, overview 130
reset of 32
configuration dump, support 133
connection types, for Internet uplink 11
console  See shell access
contact data, administrator 56
controllers
  IDE 6
  SCSI 6
CPU usage 23, 116
CPU, system requirements 6
CRL  See certificates, revocation lists
CSV export, delimiter 126
customer support, Sophos UTM 130
customization
  home use license and 55
  of company logo 55
  of company text 56
  of email notifications 55
  of system messages 55
D
Dashboard 11, 13, 23
  RAID display 4
date 28
  NTP servers 28, 30
  setting of 7
    manual 28-29
daylight saving time 28
definitions 65
  of MAC addresses 69
  of networks 65
  of services 70
detection, hardware 5-6
device information, SNMP 57
device security 12, 39
devices
  supported 3
DHCP
  IP address pool 67
dig (network tool) 132
directory services 77, 79
  Active Directory 77, 80
eDirectory 77, 79
  LDAP 77, 83
  RADIUS 77, 85
  TACACS+ 77, 86
Distinguished Name 59, 80-81, 84
DN  See Distinguished Name
DNS 107
  cache, clearance of 108
  DNSSSEC 107
  DynDNS 109
  forwarders 108
    by ISP 108
  groups 68
  hostname of system and 28
  hosts 67, 132
    time-to-live 67
  lookup 131-132
  records, time-to-live 108
  reverse DNS 67
  servers 108
    allowed networks 107
    internal 107-108
    root 108
    zone information 108
documentation, administrator 129
domain controllers  See directory services
DoS, intrusion prevention 87
DSA keys, SSH 124
  backups and 124
  public 124

Index
dynamic IP endpoints 67
DynDNS 109

E
eDirectory 77, 79
  backend servers 79
  Base DN 80
  groups 88
  port number 80
  prefetching with 88
email addresses
  conflict of 78
  unique 78
email recipients
  of backups 42
  of executive reports 121
  of logfile archives 125
end-user portal See User Portal
Enterprise Toolkit, installation of 8
Ethernet DHCP (interface type) 93, 99
  MTU 99
Ethernet Static (interface type) 93, 95
  MTU 96
  proxy ARP 96
Ethernet VLAN (interface type) 93, 97
  MTU 98
  proxy ARP 98
Ethernet, modes of operation 101
Excel (format)
  delimiter 126
  download of reporting data in 119
executive reports 120
  archived 120
  configuration of 120
  generation of 120
  number of 125
  PDF settings 126
  settings of 125
  view of 120
external interfaces 11

F
  factory reset 32
  system shutdown 32
  file extensions
    of backups 47
  filter field, of lists 16
  firewall
    reporting of 119
  firmware updates 42-43
    download of 43-44
    installation of 42-44
    scheduling of 43
  firmware version 23, 43
  flow monitor 23-24
    adaption of 95-96, 98, 100
  forwarders, DNS 108
  FQDN
    hostname and 28
  FTP
    servers
      as log file archive 123
      of Sophos UTM 45
    Fully Qualified Domain Name See FQDN

G
  Gateway Manager 38
    access to 39-40, 51
    language of 39
    starting 40
    status of 23
    TCP port of 39
gateway units See devices
gateways See devices
groups
  availability groups 68
  DNS groups 68
  network groups 68
  service groups 70, 72
  user groups 75
hard disk
erasure of 8
size and type 6
usage of 23
hardware
   interfaces 101
   minimum requirements 6
   reporting on 116-117
Hardware Compatibility List 4, 97, 129
hardware detection 5-6
HCL  See Hardware Compatibility List
HDD  See hard disk
help, online 42
high availability
   link monitoring 102
   takeover 102
home use license
   customization and 55
hostname, system 35
   configuration of 28
   DNS and 28
HTTPS
   WebAdmin CA certificate 10, 35
   WebAdmin certificate 35
IANA 58
ICMP
   echo request 131
   echo response 131
icons, in WebAdmin 18
   Info icon 16
IDE controllers 6
idle timeout, WebAdmin 36
improvement program, Sophos UTM 37
Info icon 16
   interface definitions 92
   MAC address definitions 69
   network definitions 66
   service definitions 70
user definitions 72
initial login page 9
installation 1, 124
   abortion of 6
   and basic configuration 9
   duration of 8
   from CD-ROM 4
   hardware requirements 6
   key functions during 5
   of Enterprise Toolkit 8
   of Open Source Software 8
   problems after 9
   system reboot after 8
   warning message 8
installation instructions 4
Interface Address 66
Interface Broadcast Address 66
Interface Network Address 66
interfaces 91
   administrative 7
   automatic definitions of 92
   autonegotiation of 101
   configuration of 91
   external 11, 96, 99
   flow monitor 23-24
   groups 92-93
   Info icon 92
   internal 7, 11
   of name "Internal" 92
   of status "Down" 92, 95, 97, 99-100
   of status "Up" 95, 97, 99-100
   table of 133
   types of 93, 95, 97, 99-100
      3G/UMTS 93
      Ethernet DHCP 93, 99
      Ethernet Static 93, 95
      Ethernet VLAN 93, 97
      group 92-93
      virtual 91
internal interfaces 7, 11
internal network card 7
Internet (network definition) 66
<table>
<thead>
<tr>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet time servers  See NTP servers</td>
</tr>
<tr>
<td>Internet uplink, connection type  11</td>
</tr>
<tr>
<td>IP addresses</td>
</tr>
<tr>
<td>additional  100</td>
</tr>
<tr>
<td>aliases of  100</td>
</tr>
<tr>
<td>blocking of  87</td>
</tr>
<tr>
<td>IP endpoints, dynamic  67</td>
</tr>
<tr>
<td><strong>K</strong></td>
</tr>
<tr>
<td>key functions, during installation  5</td>
</tr>
<tr>
<td>keyboard layout, selection of  6</td>
</tr>
<tr>
<td>keyboard shortcuts, in WebAdmin  36</td>
</tr>
<tr>
<td>Knowledgebase, Sophos  4, 12, 41, 97, 129-130</td>
</tr>
<tr>
<td>Known Issues List, Sophos UTM  129</td>
</tr>
<tr>
<td><strong>L</strong></td>
</tr>
<tr>
<td>language, Gateway Manager  39</td>
</tr>
<tr>
<td>language, WebAdmin 33</td>
</tr>
<tr>
<td>LDAP  77, 83</td>
</tr>
<tr>
<td>backend servers  83</td>
</tr>
<tr>
<td>Base DN  84</td>
</tr>
<tr>
<td>port number  83</td>
</tr>
<tr>
<td>user attribute  84</td>
</tr>
<tr>
<td>LDAP browser  88</td>
</tr>
<tr>
<td>LDAP over SSL  80-81, 83</td>
</tr>
<tr>
<td>license  23</td>
</tr>
<tr>
<td>base license  41</td>
</tr>
<tr>
<td>information on  41</td>
</tr>
<tr>
<td>installation of  41</td>
</tr>
<tr>
<td>purchase of  40</td>
</tr>
<tr>
<td>reset of  32</td>
</tr>
<tr>
<td>license key  4</td>
</tr>
<tr>
<td>licensing  40</td>
</tr>
<tr>
<td>support services  41</td>
</tr>
<tr>
<td>line charts, reporting  114</td>
</tr>
<tr>
<td>link monitoring, high availability  102</td>
</tr>
<tr>
<td>Linux, SSH and  30</td>
</tr>
<tr>
<td>lists  15</td>
</tr>
<tr>
<td>Info icon  16</td>
</tr>
<tr>
<td>search in  16</td>
</tr>
<tr>
<td>live logs  15</td>
</tr>
<tr>
<td>load, system  23</td>
</tr>
<tr>
<td>reduction of  125</td>
</tr>
<tr>
<td>local logging  121</td>
</tr>
<tr>
<td>thresholds of  122</td>
</tr>
<tr>
<td>localization, of system messages  55</td>
</tr>
<tr>
<td>lock files and backups  48</td>
</tr>
<tr>
<td>log files</td>
</tr>
<tr>
<td>archive of  115, 123</td>
</tr>
<tr>
<td>email  125</td>
</tr>
<tr>
<td>FTP server  123</td>
</tr>
<tr>
<td>SMB share  124</td>
</tr>
<tr>
<td>SSH server  124</td>
</tr>
<tr>
<td>deletion of  115, 122</td>
</tr>
<tr>
<td>download of  115</td>
</tr>
<tr>
<td>live log  115</td>
</tr>
<tr>
<td>of today  115</td>
</tr>
<tr>
<td>reset of  32</td>
</tr>
<tr>
<td>search in  114-115</td>
</tr>
<tr>
<td>view of  114-115</td>
</tr>
<tr>
<td>log off  135</td>
</tr>
<tr>
<td>log partition</td>
</tr>
<tr>
<td>histogram of, utilization  113</td>
</tr>
<tr>
<td>status of  113</td>
</tr>
<tr>
<td>usage of  23</td>
</tr>
<tr>
<td>logging  113</td>
</tr>
<tr>
<td>local  121</td>
</tr>
<tr>
<td>thresholds of  122</td>
</tr>
<tr>
<td>notifications and  122</td>
</tr>
<tr>
<td>remote  122</td>
</tr>
<tr>
<td>settings of  28, 121</td>
</tr>
<tr>
<td>time gaps  29</td>
</tr>
<tr>
<td>time settings  28</td>
</tr>
<tr>
<td>using syslog  122</td>
</tr>
<tr>
<td>login page</td>
</tr>
<tr>
<td>initial  9</td>
</tr>
<tr>
<td>standard  10</td>
</tr>
<tr>
<td>login problems  135</td>
</tr>
<tr>
<td>logins, failed  87</td>
</tr>
<tr>
<td>loginuser</td>
</tr>
<tr>
<td>password of  32</td>
</tr>
<tr>
<td>logout  135</td>
</tr>
<tr>
<td>automatic  135</td>
</tr>
</tbody>
</table>
M

MAC address definitions
  creation of 69
  Info icon 69
maintenance levels, support 130
Management Information Base, SNMP 56
manager (user right) 34
manual, administrator 129
  language of 129
memory
  usage of 116
menu, WebAdmin 13
  search box 14
MGE UPS Systems (manufacturer) 4
MIB See Management Information Base, SNMP
Microsoft Active Directory See Active Directory
monitoring
  of link status, high availability 102
  of network 56
MTU
  3G/UMTS 94
  Ethernet DHCP 99
  Ethernet Static 96
  Ethernet VLAN 98
MyAstaro Portal 41

N

NAS identifiers, RADIUS 86
NAT 101
netmask 68
netstat 133
network activities 113
network cards 6
  bit rate 23
  configuration of 91
  flow monitor 23-24
  internal 7
  name of 23
  sequence of 8
  status of 23
  SysIDs 96, 99
network definitions
  availability groups 68
  bind to interface 68
  creation of 66
  DNS groups 68
  DNS hosts 67
  hosts 67
  Info icon 66
  Internet 66
  network groups 68
  types of 66
network groups 68
network interfaces See interfaces
network mask See netmask
network monitoring 56
Network Protection
  reporting of 119-120
network services 107
  DNS 107
  NTP 112
network statistics 133
  overview of 91
network usage, reporting 117-118
networks 65
  definition of 65
  never blocked 87
  static 66
notifications 28, 53-54
  by email 53-54
    customization of 55
  codes of 53
  device-specific text 54
  limiting of 54
  logging and 122
  recipients 54
  smarthosts and 54
  SNMP trap 53-54
  types of 54
  notifier MIB of Sophos, SNMP 58
Novell eDirectory See eDirectory
Index

NTP 112
NTP servers 28, 30, 112
testing of 30

O
object identifier, SNMP traps 58
object lists 20
keyboard shortcuts 36
OID, SNMP traps 58
online help, update of 42
Open Source software, installation of 8
operating status, system 23
organizational information, system 28
OSPF 104

P
packet loss 131
pagination, tables 36
parent proxies
    as Up2Date cache 45
    authentication at 45
partition usage 116
    log partition 116
    root partition 23, 116
    storage partition 116
Partner Portal, Sophos NSG 130
password
    for shell 31
    of administrator 11, 32
        setting of 10
    of loginuser 32
        setting of 31
    of root 32
        setting of 31
    of users
        change of 51
        setting of 73
    of WebAdmin 11
    reset of 32
password complexity 31, 88
password guessing 87
pattern updates 42
    download of 44
    installation of 42, 44
    online help 42
pattern version 23, 44
PCI ID 8
PDF (format)
    download of reporting data in 119
PEM (file format) 61
pie charts, reporting 114
ping 131
ping check 9, 131
    availability group 68
PKCS#12 container (file format) 61
policy routes 103-104
port number
    of Active Directory 81
    of eDirectory 80
    of Gateway Manager 39
    of LDAP 83
    of RADIUS 85
    of SSH 31
    of TACACS+ 87
    of User Portal 52
    of WebAdmin 9
preferences
    of user 36
prefetching, authentication
    groups 88
        interval of 88
        time of 88
        with Active Directory 88
        with eDirectory 88
problems, after installation 9
process list, support 133
processor 6
protocols
    LDAP 83
    NTP 112
    of routing 104
    RADIUS 85
    syslog 122
TACACS+ 86
proxy ARP (function)
  with Ethernet Static 96
  with Ethernet VLAN 98
proxy server, government-approved See parent proxies
ps (support tool) 133
public keys, SSH DSA 124
R
RADIUS 77-78, 85
  backend servers 85
  NAS identifiers 86
  port number 85
  protocol of 85
  shared secret 85
RAID
  controllers 4
  display on Dashboard 4
  support for 4
RAM
  usage of 23
  readonly (user role) 34
reboot, system
  after installation 8
  manual 63
recipients
  of emails See email recipients
  of notifications 54
regular expressions 16
Relative Distinguished Name 81
remote log file archive 123
  email 125
  FTP server 123
  SMB share 124
  SSH server 124
remote syslog server 122
reporting 113
  activation of 125
  bandwidth usage 118
  charts 113
  deactivation of 125
  executive reports 120
  firewall 119
  hardware information 116-117
  IPFIX 126
  line charts 114
  Network Protection 119-120
  network traffic 117-118
  network usage 117-118
  pie charts 114
  settings of 28, 125
  time frames 125
  time gaps 29
  time settings 28
  reporting data
    automatic deletion 125
    download of 119, 126
    reset of 32
  request routing 108
  resolve REF 134
  resource usage 23
  restart, system 63
  reverse DNS 67
  revocation lists 59, 62
  rights, user 34
  root DNS servers 108
  root password 32
  route flapping 104
  routing
    automatic 103
    policy routes 103-104
    request routing 108
    standard static routes 103
    static routing 103
    routing loops 104
    routing protocols 104
    routing table 103-104, 133
  RSA keys
    and backups 47
S
  SCP servers 124
  SCSI controllers 6
Index

search box, of menu 13
  keyboard shortcut 36
Secure Copy, archiving method 124
Secure Shell 30, See also SSH
security certificate See certificates
security threats
  identification of 113
security warning, web browser 9-10, 35
self-signed certificate
  of system 9
servers
  DNS 107
    for authentication 79
  NTP 112
  SCP 124
service definitions
  change type of 72
  creation of 70
  Info icon of 70
service groups 70, 72
services
  definition of 70
  network services 107
  using AH 72
  using ESP 71
  using ICMP 71
  using IP 71
  using TCP 70
  using UDP 70
sessions, WebAdmin, overview of 27
shell access 30
  after password reset 32
  setting passwords for 31-32
shutdown, system 32, 63
  after factory reset 32
  logging thresholds and 122
signing certificate authority 61
  for VPN 63
Simple Network Management
  Protocol See SNMP
smarthosts
  notifications and 54
SMB share, as log file archive 124
SNMP 56
  agent 57
  community string 57, 59
  device information 57
  error codes 58
  queries 56
  Sophos notifier MIB 58
  traps 53, 56, 58
  Sophos Knowledgebase 4, 12, 41, 97, 129-130
  Sophos NSG Partner Portal 130
  Sophos NSG Support Forum 12, 41
  Sophos User Authentication 78-79
    live log 79
  Sophos UTM FTP server 45
  Sophos UTM improvement program 37
  Sophos UTM Manager
    access control 40
    access to 39
  Sophos UTM Up2Date Blog 129
  Sophos UTM User Portal See User Portal
SSH 30
  access control 31
  authentication methods 31
  clients 30
  daemon listen port 31
  Linux and 30
  port number 31
  public keys 31
  SSH DSA keys 124
  backups and 124
  public 124
  SSH server, as log file archive 124
SSL
  LDAP over 80-81, 83
  SSL certificates
    identifiers of 78
    of users 78
  standard static routes 103
  standard time 28
  static routing 103
statistic overview
  of network 91
status
  of log partition 113
  operating, of system 23
subnet 7
subscriptions, license
  information on 41
SuperAdmins (user group) 74-75
support 12, 129
  configuration dump 133
  contact information 130
  resolve REF 134
    Sophos NSG Partner Portal 130
support cases 130
Support Forum, Sophos NSG 12, 41
support levels 130
support services 41, 130
support tools 131
  DNS lookup 131-132
    ip 133
    netstat 133
    ping 131
    ps 133
    traceroute 131
supported devices 3
swap usage 116
symbols See icons, in WebAdmin
SysIDs, network cards 96, 99
syslog protocol 122
syslog server
  buffer size 123
  log selection 123
  remote 122
system
  configuration of 23
    reset of 32
  organizational information 28
reboot of
    after installation 8
    manual 63
    settings of 9, 27
shutdown of 63
  after factory reset 32
system load 23
  reduction of 125
system messages
  customization of 55
system requirements 1
  administration pc 3
T
table
  of interfaces 133
  routing table 103-104, 133
tables See also lists
  pagination of 36
  sorting data 119
TACACS+ 77, 86
  backend servers 87
  key for authentication/encryption 87
  port number 87
tags, VLAN 97
takeover, high availability 102
templates
  backup templates 49
terms of use, WebAdmin 37
time 28
  certificates and 35
daylight saving time 28
NTP 112
  NTP servers 28, 30
  setting of 7
    manual 28-29
    standard time 28
  synchronization of 112
  time gaps 29
time-to-live 67
time zone 28
  certificates and 35
  setting of 7, 29
timeout, WebAdmin 36
toggle switch, in WebAdmin 19
tools, support 131
  DNS lookup 131-132
  ip 133
  netstat 133
  ping 131
  ps 133
  traceroute 131
traceroute 131
traffic monitor See flow monitor
traps, SNMP 58
TTL See time-to-live

U
UMTS (interface type) 93
uninterruptible power supply 4
  battery operation 4
  notifications and 4
  recognition of 4
  status of 23
Up2Date Blog, Sophos UTM 129
Up2Date cache 45
  parent proxies 45
  status of 24
Up2Date Information, Sophos UTM 129
Up2Dates 42
  configuration of 44
  connection problems 42
  digital signature 42
  download of 42-43
  installation of 42-43
    implicit 43
  manual upload 45
  of firmware 43
  of patterns 44
  packages, reset of 32
  scheduling of 43
  system backup, automatic and 42
  update servers 42
update servers 42
uplink, Internet (connection type) 11
UPS See uninterruptible power supply
user definitions 72
  administrator privileges 74
  backend synchronization 74
  email addresses and 73
  Info icon 72
User Portal 51
  access control to 52
  certificate of 35
  cookies of 52
  hostname of 52
  language of 52
  listen address of 53
  port number 52
  Web Application Firewall and 53
  welcome message 53
user preferences 36
user rights 34
  auditor 34
  manager 34
user roles 34
  auditor 34
  readonly 34
users 65, 72
  access to Gateway Manager 51
  access to WebAdmin 51
  authentication of 73
  authorization of 86
  automatic creation of 78
  certificate of 74
  currently logged in 14
  disabling of 73
  password
    change of 51
    setting of 73
  user groups 65, 72, 75
UTC 29

V
verification certificate authority 61
version 23
  of firmware 23
  of patterns 23
virtual interfaces 91
virtual LAN  See VLAN
VLAN 97
tags 97
VPN
  signing certificate authority 63

W
warning message, at installation 8
web browser
  certificates and 9
  security warning 9-10, 35
WebAdmin 13
  access control to 33-34
  administrators 11, 33
  browser tab title 36
  button bar of 14
  buttons in 18
  certificate of 10, 35
    information contained in 28
configuration, overview 130
Dashboard 13, 23
dialog boxes in 17
icons in 18
keyboard shortcuts 36
language of 33
lists in 15
logging of access traffic 33
menu of 13
object lists 20
password for 11
port number 9, 37
protocol of 9
sessions, overview 27
settings of 33
  monitoring of changes 27
terms of use 37
timeout of 36
user roles 34
version of 23

X
X.509 certificates
  backups and 47
  creation of 59
  import of 59
  of users 72

Z
zone information, DNS 108