Teldat Security

User's Guide

Legal Notice

Warranty

This publication is subject to change.

Teldat offers no warranty whatsoever for information contained in this manual.

Teldat is not liable for any direct, indirect, collateral, consequential or any other damage connected to the delivery, supply or use of this manual.

Table of Contents

Chapter 1 About this guide

This user guide focuses on the Security application for the Teldat Atlas i6x .

1.1 Supported devices

The information contained in this guide only applies to the Atlas i6x equipped with an internal storage device and the Security application.

1.2 Who should read this manual?

This manual should be read by users who want to configure the Security application on an Atlas i6x .

1.3 When should I read this manual?

Read this guide as soon as you are ready to configure your security application. This manual describes the security application's functionalities and shows you how to configure the different parameters.

1.4 What is in this manual?

This user guide contains the following information:

- A brief comment on the purpose and operation of the Security application.
- How to configure the application using the Atlas i6x internal web.
- How to configure the application using text commands.
- A description of some general scenarios where the Security application could be used, together with the configuration process.
- Troubleshooting.

1.5 What is not in this manual?

This user guide does not contain information on the Atlas i6x hardware. Neither is it intended as a comprehensive guide for all aspects of the management operations available in the Management Platform, the Atlas i6x Application Host software and configuration, or other applications unrelated to security.It does not contain information on how to setup the device to connect to the Internet. For information on configuring the router, please see the relevant manuals for the different protocols at the following web site: *www.teldat.com* .

1.6 How is the information organized?

Chapter 1 explains how to use this guide and describes its contents. Chapter 2 introduces the Security application and offers a brief explanation of its features and components. Chapter 3 focuses on the web configuration method for this application. Chapter 4 presents another way of configuring the application (using text commands). Finally, chapter 5 shows scenarios whether the Security application could be used, as well as a step-by-step explanation of the configuration process.

In addition, this guide includes Appendices that provide additional information related to certain aspects of the Security application.

1.7 Technical support

Teldat, S.A. offers a technical support service. The device software can be regularly updated for maintenance reasons and for new features.

Contact information:

Web: www.teldat.com

Tel Nº: +34 918 076 565

Fax: +34 918 076 566

Email: support@teldat.com

Note

The manufacturer reserves the right to make changes and improvements to the software or hardware of this product, modifying the specifications of this manual without prior notice. The screen captures provided throughout the guide are for information purposes only. Some small modifications may exist in the current software.

1.8 About open-source software

Some of the product's software components contain copyrighted software that is licensed under GPL, GFDL, LGPL and other open source licenses. You may obtain the complete corresponding source code from us for a period of three years after our last shipment of this product by downloading this free of charge from Teldat, S.A.. If you would like the corresponding source code on a physical medium (such as CD-ROM), we may charge a cost for having to physically perform source distribution. This offer is valid to anyone in receipt of this information.

For more information about the software licenses for the Atlas i6x Application Host, please refer to the *About section* of the router's web configurator.

Chapter 2 What is Security application?

2.1 Teldat Security application

Network security is now a critical issue for any company. Security vulnerabilities, whatever their size, can cause all kinds of problems (unauthorized access to your systems, loss of data, periods of inactivity following a virus infection, etc.,). However, the concept of security goes beyond scanning and detecting malware with antivirus products. Forbidding access to potentially dangerous sites, identifying and marking annoying spam, and securing email traffic are also important aspects worth considering in the pursuit of a secure system.

The Security application is a suite of three integrated applications implementing a total security solution *for WEB and email*. Security application provides *antivirus*, *URL filtering* and *anti-spam* services. These services will be explained in more detail in the section on *Components* on page 3.

The Security application components can be easily customized by defining the following *entities*: groups, categories, URL user lists and email lists. All of them are briefly explained below. Further information on entity configuration can be found in the section on *Entities* on page 6.

- *Groups* allows you to group together several IP addresses and IP ranges for management purposes.
- *Categories* are predefined lists of URLs, domains and expressions associated with a particular subject (e.g., spyware, virus infected, drugs, weapons, etc.,). They provide you with an easy means of allowing/denying certain users access to particular types of Web content.
- *URL user lists* allow you to build your own lists of URLs, domains and expressions under a name of your choice. They are used in the same way as categories (allowing/denying access to particular types of web content).
- *Email lists* are sets of email addresses that you can use to allow mail from trusted addresses, or to block mail coming from well known spammers or undesirable senders.

2.2 Teldat Security application features

- *All in one web and mail security application*: the following three services are integrated within the application:
  - Web and email virus detection.
  - URL filtering.
  - Spam mail detection.
- *Simplify configuration*: the user no longer has to work with the configuration files of the integrated applications. This task has been eliminated to simplify the configuration process. It offers two ways of configuring the whole Security application:
  - Web configuration. This is the easiest way to configure the application on a device. With this method, you access the configuration web and change the parameters you wish to modify using a friendly web interface.
  - Text command configuration. This allows you to configure one or multiple devices from the Management platform using a text mode configuration that can be sent to the devices.
- *Easy customization*: allows the user to create his own lists of IP addresses, emails, URLs, domains and expressions, and to use predefined categories containing complete lists of URLs and domains related to several subjects, through entities.

2.3 Components

As mentioned above, Teldat Security application comprises three components, which we will now proceed to describe.

2.3.1 Antivirus

The Security application's antivirus service can detect many types of malicious software, including viruses. It runs as a daemon and can scan emails and files downloaded from the web. It will not be able to scan other files stored in the Atlas i6x hard drive. The antivirus detects viruses and moves any infected files to a quarantine folder, but cannot remove viruses from the files.

The antivirus service provided by the Security application is based on the use of ClamAV. ClamAV is the open source standard for mail gateway scanning software. It is high-performing, supports multiple file formats and allows for file and archive unpacking. The local antivirus database is updated with the latest threats once a day from the ClamAV databases. Further information on ClamAV can be found at the following link: *http://www.clamav.net*

2.3.2 URL filtering

When a user tries to access a blacklisted URL, Teldat Security application redirects the user to a blocking window and the browser informs the user that the URL has been blocked by the Security application because it is blacklisted. It is also possible to block access to all sites except those whitelisted. The lists of blocked/allowed sites may vary depending on the groups of accessing IP addresses.

The URL filter in Teldat Security application uses SquidGuard software to redirect. SquidGuard works with the Squid proxy software. Further information on SquidGuard can be found at the following link: *http://www.squidguard.org*

2.3.3 Anti-spam

The anti-spam service in Teldat Security application analyzes emails looking for spam messages. Email addresses can also be whitelisted or blacklisted so that messages are automatically accepted or considered spam.

The anti-spam service uses SpamAssassin software for spam detection. SpamAssassin updates once a day, downloading and installing new rules and configurations. Further information on SpamAssassin can be found at the following link: *http://spamassassin.apache.org*

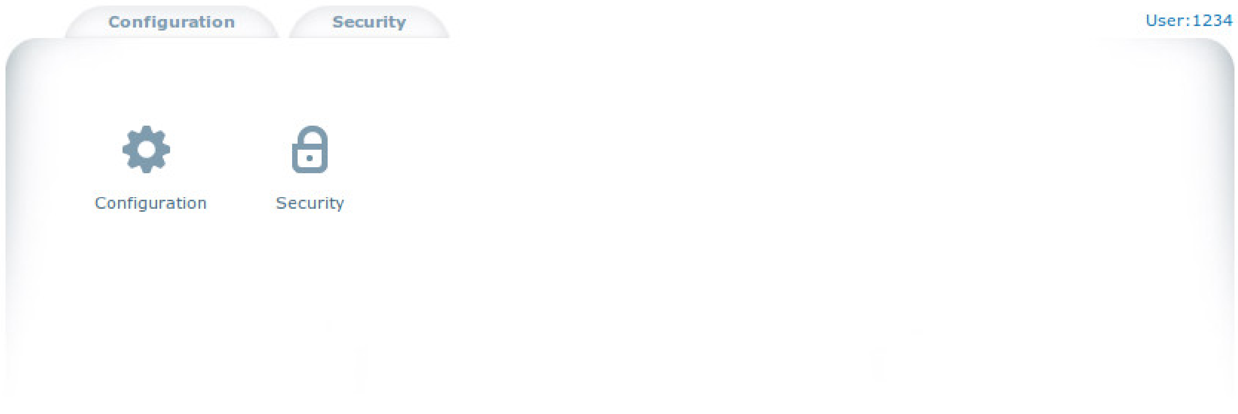
Chapter 3 Application web configuration

As with other applications installed on the Atlas i6x , there are two ways to configure the application: by using the Atlas i6x internal web, and by using text configuration (or a configuration template inside the management platform) to configure one or more devices simultaneously.This chapter describes how to configure the Security application using the web.

> **Note**
>
> The Security application will only behave properly if the general configuration is correct. Please refer to the appendix titled *General Configuration* on page 33 for information on how to configure the general settings.

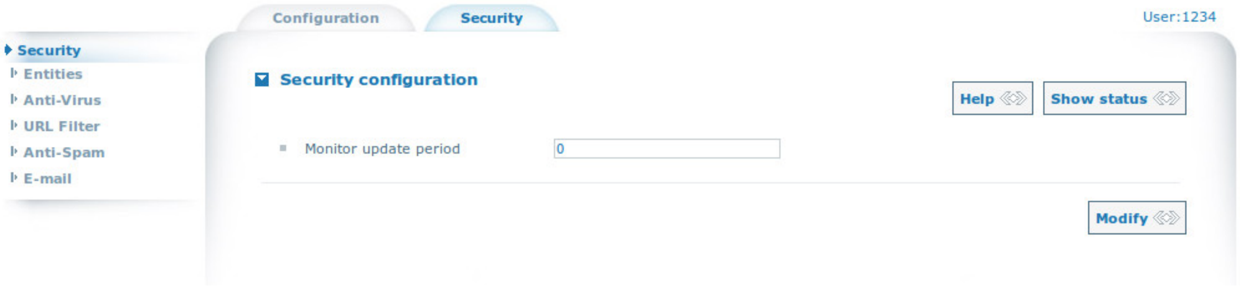
The application is represented by a padlock in the main window. You may click on the "Security" tab or the icon to access the application's configuration.

Fig. 3.1. Web configuration: main window



When you click on one icon, a new window opens. Click "Security" from the left-hand menu to enter the main configuration section.

Fig. 3.2. Security Web configuration



Security configuration

Monitor update period: 0

The previous figure shows only one configurable parameter: the monitor update interval (in seconds). Its default value is 0. This parameter sets the interval between updates of the numerical status information related to monitoring antivirus and anti-spam activity (number of virus detected, spam detected today, mails received today, total spam and total number of mails received). The maximum value for the monitor update interval is 86400 seconds (i.e., one day).

In the left-hand menu you will find the following configuration sections which are described below:

- Entities
- Antivirus

- URL Filter
- Anti-Spam
- Email

Click on them to access the corresponding configuration section.

> **Note**
>
> Summary of interface buttons:
>
> - ↑+ : Use this button to add a new entry to a table.
> - X : Use this button to remove an entry from a table.
> - Modify : Use this button to modify the value of the current section parameters. You must click this button before clicking any of the interface's other buttons (such as a table button), otherwise the whole page refreshes and you lose any modifications you have made.
> - Show status : Use this button to show status parameters.
> - Show conf : Use this button to return to the configuration section.

3.1 Entities

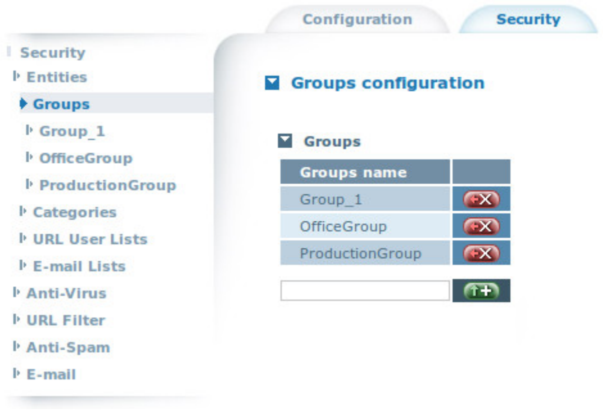
There are four types of entities: groups, categories, URL Users lists and email lists. These are displayed in the menu that appears on the left of the screen when you access the "Entities" section. You can access each of them by clicking on the relevant option in the left-hand menu.

Entities are used in other sections of the Security application to configure available services. *The entities created cannot be deleted if they are being used by any of the Security application's services.*

3.1.1 Groups

A group consists of a list of IP addresses, IP ranges or IPs with CIDR block. The table shown in the Groups window allows you to define new groups by adding a group name to the table. To add a new group, enter the name and press the ↑+ button. Other sections of the Security application, like the URL filter, can only be configured once the groups are defined. To remove a group, click on the X button next to the group entry that you want to delete. *Groups in use in any of the Security application's services cannot be deleted*.

Fig. 3.3. Entities configuration: Groups



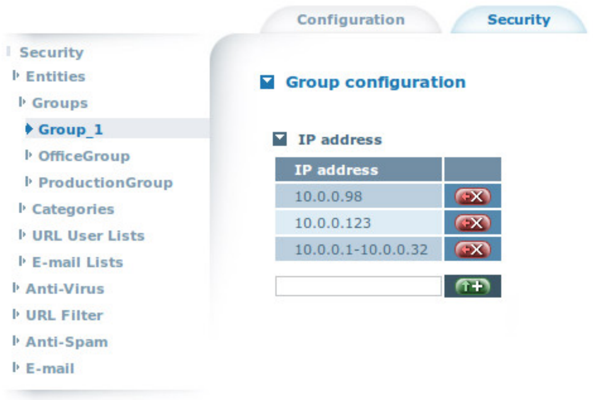
Groups configuration

Groups

Groups name	
Group_1	X
OfficeGroup	X
ProductionGroup	X
	↑+

Once a group has been added to the groups table, you can configure it by clicking the tag with the group name from the left-hand menu. The figure below shows the individual group configuration.

Fig. 3.4. Group configuration



Group configuration

IP address

IP address	
10.0.0.98	✕
10.0.0.123	✕
10.0.0.1-10.0.0.32	✕
	+

The Group configuration window contains a table with a list of IP addresses associated with the group. You can add IP addresses by typing in the address and clicking the + button. You can also enter an IP with CIDR block (e.g., 10.0.0.0/24) and IP ranges (e.g., 10.0.0.1-10.0.0.15). To remove an entry, press the ✕ icon next to the entry.

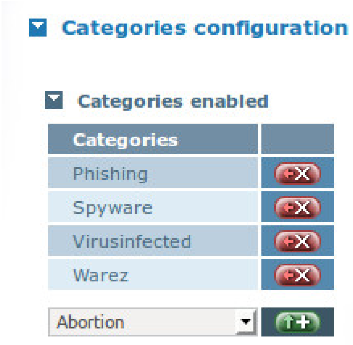
3.1.2 Categories

Categories are entities that are very similar to URL user lists (which will be explained in the next section). Like them, they consist of a list of domains, URLs and expressions (regular expressions that can match certain URLs).

The Categories window displays a table where you can select different categories and add them to the table using the + button. This allows them to be used in other sections of the Security application configuration web. *Categories cannot be created by the user.* A predefined list of categories can be found in the Appendix titled *Categories list* on page 36. Some examples of categories include spyware, drugs or gardening. A category's list of domains, URLs and expressions are always linked to the name of the category. A category can be removed from the table by pressing the ✕ button. *Categories in use in any of the Security application's services cannot be removed.*

A category's list of domains, URLs and expressions are downloaded from the management platform when the category is enabled, i.e., when it has been added to the categories table. Categories update once a day, between 00:00 and 01:00, downloading their lists. There are four categories enabled by default: physing, spyware, virusinfected and warez.

Fig. 3.5. Entities configuration: Categories



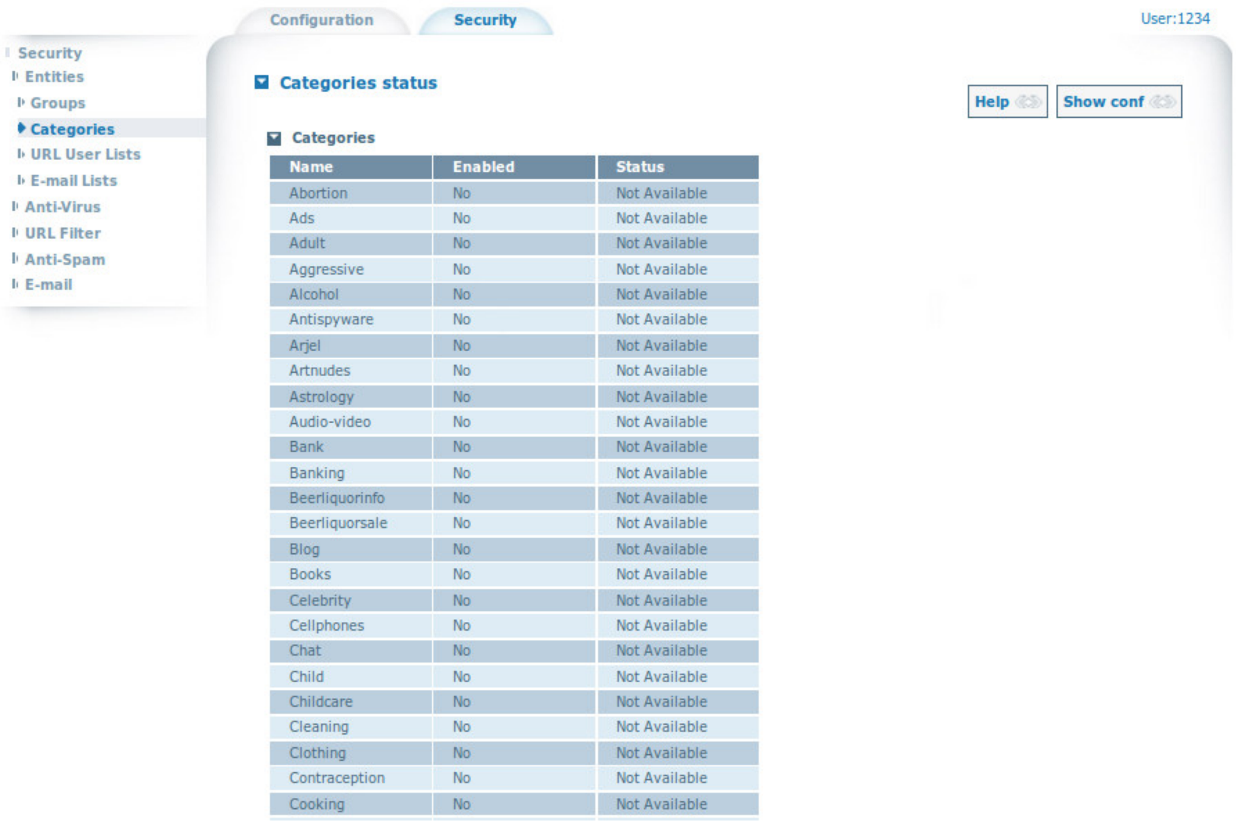
Categories configuration

Categories enabled

Categories	
Phishing	✕
Spyware	✕
Virusinfected	✕
Warez	✕
Abortion	+

You can view the status of the categories, by clicking the Show status button. The status window displays a table (see below) with the names of all the categories registered, whether they are enabled or not and their status (available or not available). Categories are enabled when they have been included in the categories configuration table, like the categories in the previous image. They are also available when a category has been downloaded successfully. Any category not yet downloaded, will appear in the table as not available.

Fig. 3.6. Entities configuration: Categories status

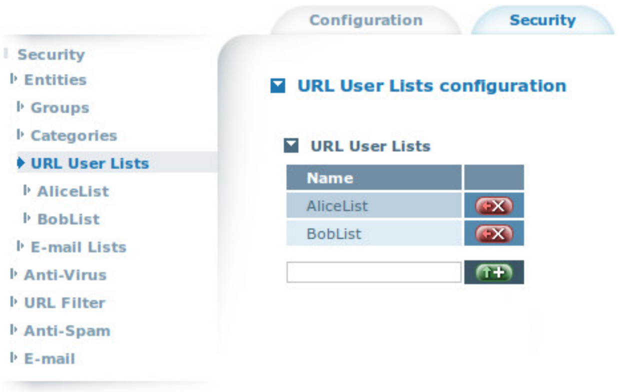


Name	Enabled	Status
Abortion	No	Not Available
Ads	No	Not Available
Adult	No	Not Available
Aggressive	No	Not Available
Alcohol	No	Not Available
Antispyware	No	Not Available
Arjel	No	Not Available
Artnudes	No	Not Available
Astrology	No	Not Available
Audio-video	No	Not Available
Bank	No	Not Available
Banking	No	Not Available
Beerliquorinfo	No	Not Available
Beerliquorsale	No	Not Available
Blog	No	Not Available
Books	No	Not Available
Celebrity	No	Not Available
Cellphones	No	Not Available
Chat	No	Not Available
Child	No	Not Available
Childcare	No	Not Available
Cleaning	No	Not Available
Clothing	No	Not Available
Contraception	No	Not Available
Cooking	No	Not Available

3.1.3 URL User Lists

URL user lists are categories created by the user. They consist of a list of domains, URLs and expressions that must be manually entered by the user, rather than downloaded as happens with the categories. User lists are also useful in other configuration sections. You can add new URL user lists names by pressing the the + button in the table in the URL user lists configuration section. You will then be able to configure them. Press the X button to remove a user list. As with the other entities, *URL user lists in use in any of the Security application's services cannot be deleted*.

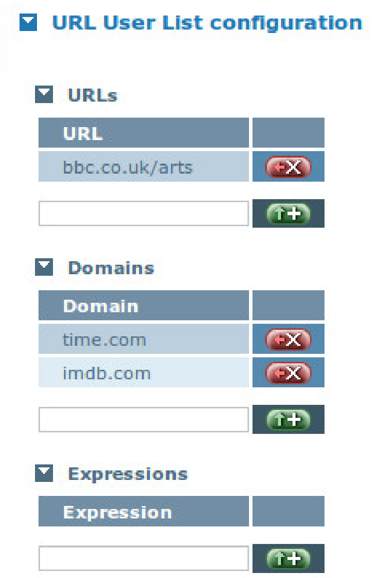
Fig. 3.7. Entities configuration: URL User Lists



Name	
AliceList	X
BobList	X
	+

You can access the URL User Lists by pressing on the URL User List name in the left-hand menu. Three tables can be configured for each URL User List (see image below). Use the + and X buttons to add and remove items from these tables.

Fig. 3.8. URL user list configuration



URL User List configuration

URLs

URL	
bbc.co.uk/arts	X

Domains

Domain	
time.com	X
imdb.com	X

Expressions

Expression	

3.1.3.1 URLs

The URLs in the table shall become part of the user list once the URL Filter blacklists/whitelists that list, or when it becomes part of the anti-virus's safe URLs and domains list.

3.1.3.2 Domains

The domains in the table shall become part of the user list once the URL Filter blacklists/whitelists that list, or when it becomes part of the anti-virus's safe URLs and domains list.

3.1.3.3 Expressions

If a URL matches one of the expressions in the table, it is considered to be included in the URLs list. All kinds of regular expressions can be entered here, for example:

- Match all URLs containing three or more consecutive "x":

```
xxx+
```

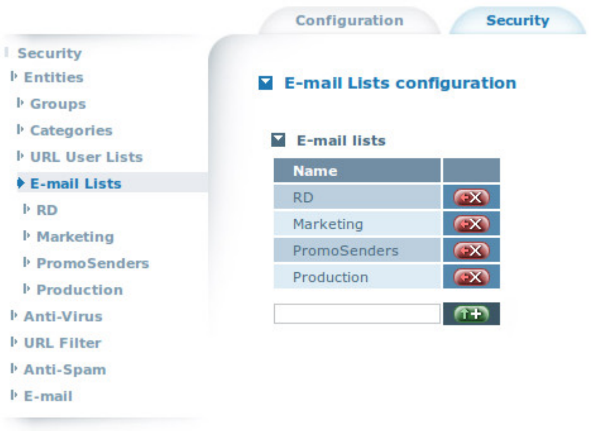
- Match all URLs ending in ".tk":

```
^http://.*\.tk$
```

3.1.4 Email lists

An email list entity consists of a list of email addresses.You can add new email lists by pressing the + button in the table in the Email lists window. The left-hand menu will include tags with the names of the registered email lists. *Lists in use in any of the application's services cannot be removed.* Click the X button to remove a list.

Fig. 3.9. Entities configuration: email lists



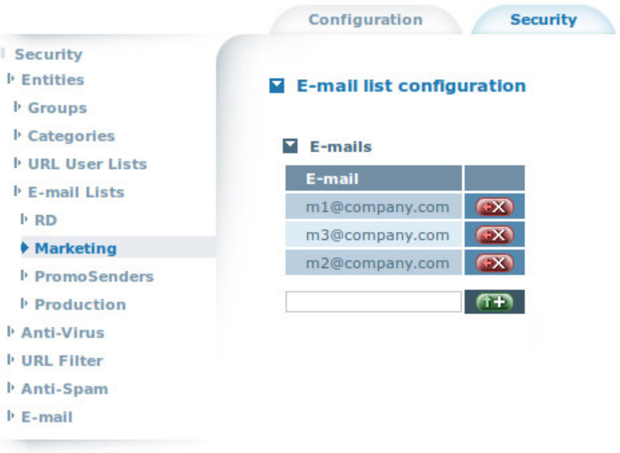
E-mail Lists configuration

E-mail lists

Name	
RD	✕
Marketing	✕
PromoSenders	✕
Production	✕
	+

Press on an entry from the left-hand menu to access the email list configuration window (see image below). You can use the + and ✕ buttons to add email addresses to the table.

Fig. 3.10. emails list configuration



E-mail list configuration

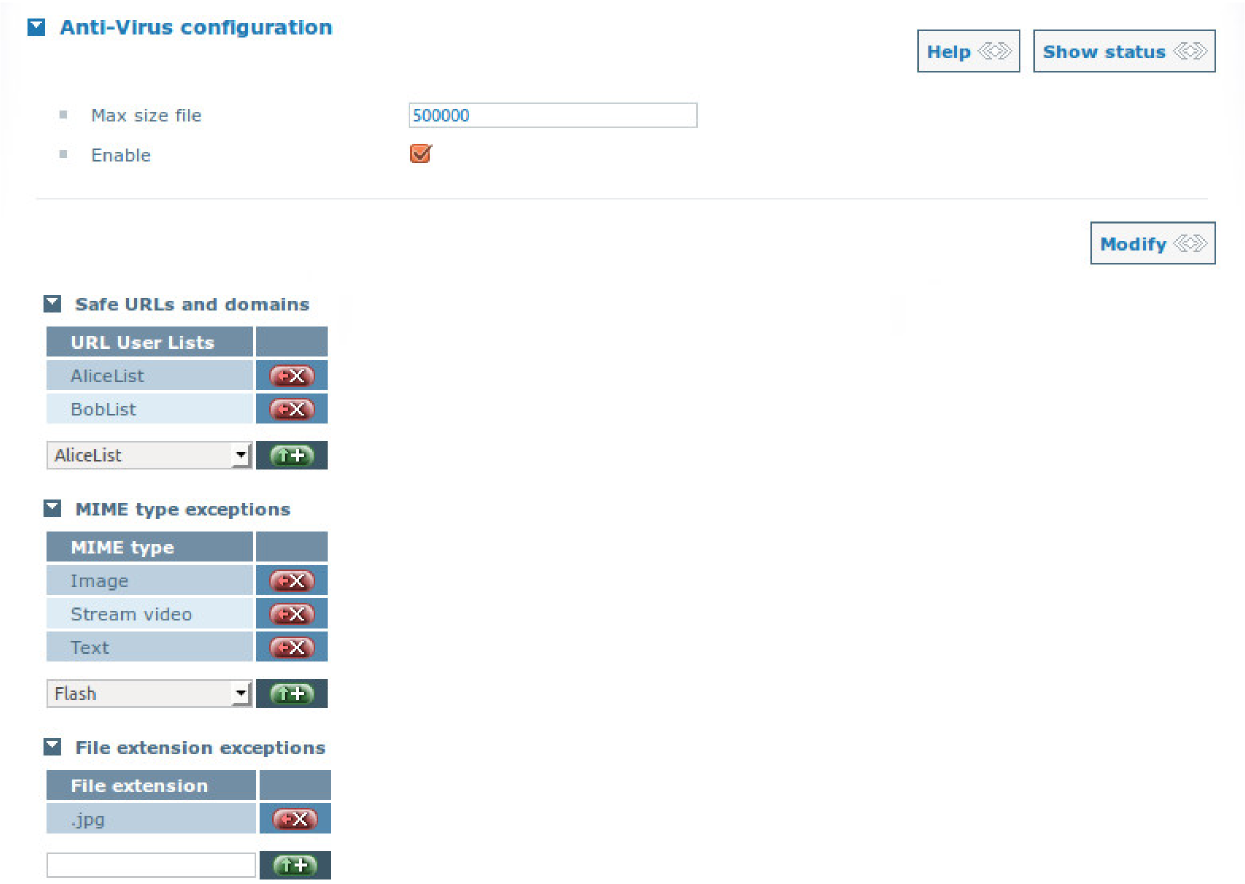
E-mails

E-mail	
m1@company.com	✕
m3@company.com	✕
m2@company.com	✕
	+

3.2 Antivirus configuration: scan web and mail

The Anti-Virus configuration window (see image below) shows two configurable parameters at the top that may be changed by clicking on the Modify button, and three tables for the user to add or remove elements using the + and ✕ buttons. This section will explain all of the antivirus configuration parameters.

Fig. 3.11. Antivirus configuration



Anti-Virus configuration

- Max size file: 500000
- Enable: ☑

Safe URLs and domains

URL User Lists	
AliceList	✕
BobList	✕
AliceList	+

MIME type exceptions

MIME type	
Image	✕
Stream video	✕
Text	✕
Flash	+

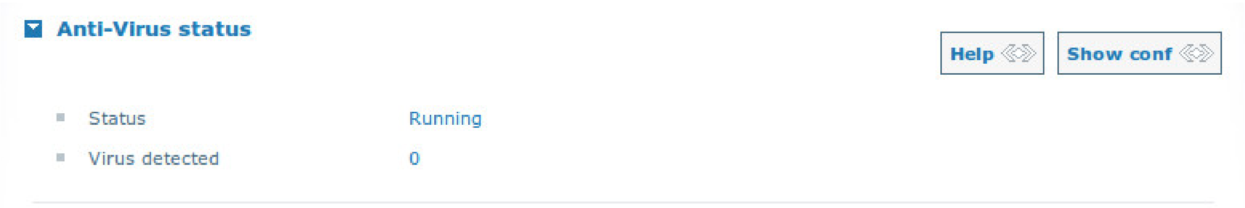
File extension exceptions

File extension	
.jpg	✕
	+

The antivirus service in the Security application will run as a daemon, scanning all the files downloaded from the Web and email. The Security application allows you to define three types of file exceptions that will not be analyzed by the antivirus: files from safe URLs and domains, files of certain MIME types and files with particular extensions. The antivirus will be automatically updated each day between 00:00 and 01:00 to maintain optimal detection capability.

The Antivirus section also contains a status window that you can access by clicking on the Show status button. This window (see image below) allows you to view the status of the antivirus service (running or stopped), and the number of viruses detected per day.

Fig. 3.12. Antivirus status



Anti-Virus status

- Status: Running
- Virus detected: 0

3.2.1 Maximum file size (bytes)

This is the largest file size that the antivirus will scan. The default value is 500000. This value is large enough to allow most files to be analyzed, while avoiding the scanning of large files that would take too long to analyze. There is, however, no limit in this parameter value.

3.2.2 Enable antivirus

Check this box to enable the antivirus. The Security application will not perform any antivirus scanning if this box is left unchecked.

3.2.3 Safe URLs and domains

Here you can add any of the URL user lists registered in the URL user lists section (*URL User Lists* on page 8). The antivirus will be disabled for any URL or domain matching an expression pattern included in any of the lists in the table.

3.2.4 MIME type exceptions

Adding this to the exceptions table prevents the antivirus from scanning a file with matching Content-Type. The options included by default are image, stream video and text. The MIME types available are:

- image
- stream video
- text
- flash
- javascript

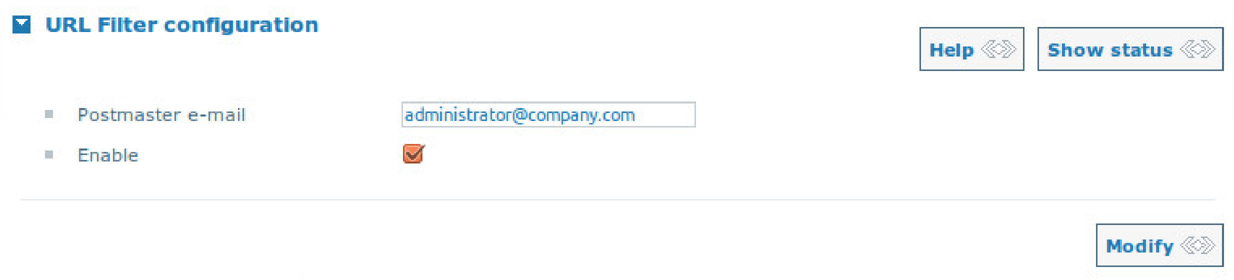
3.2.5 File extension exceptions

The antivirus will not scan any file with the extensions added to this table.

3.3 URL filter configuration: block access to URLs

As you can see in the image below, this configuration section has two parameters. This section contains further information on both. The left-hand menu contains a Rules tag. Click on this tag to enter the Rules configuration window.

Fig. 3.13. URL filter config



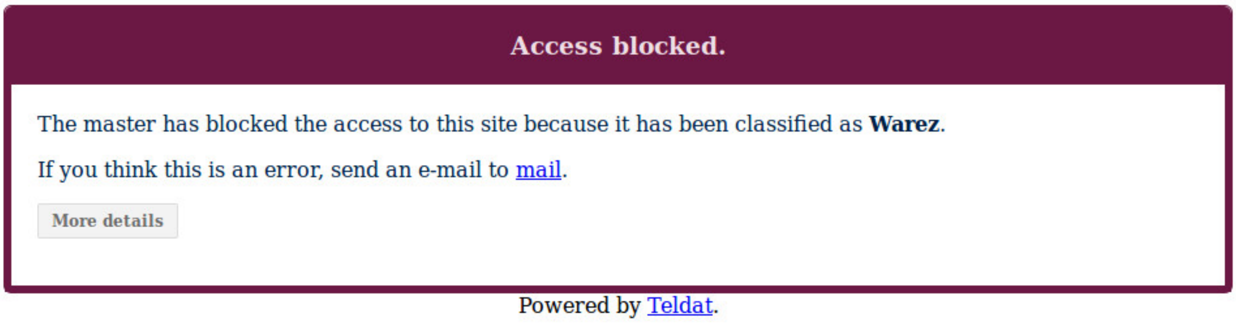
URL Filter configuration

Postmaster e-mail: administrator@company.com

Enable: ☑

The URL filter service controls user access rights to the web. It performs this task using several rules that you can define (the way rules are configured is described below). Each rule has a source group that is the set of IP addresses whose access the rule is going to control. There are two options: the user can choose to allow the source group IP addresses to access all web sites except those blacklisted by the rule, or the user can choose to restrict access only to a white list of approved sites defined by the rule. When a user tries to access a blocked site, he is redirected to a block screen (see image below) that contains information on why that URL is blocked and/or the administrator's contact email.

Fig. 3.14. URL filter: blocked URL



Access blocked.

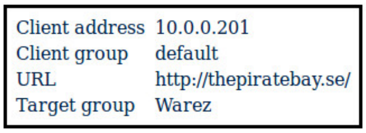
The master has blocked the access to this site because it has been classified as **Warez**.

If you think this is an error, send an e-mail to mail.

Powered by Teldat.

You can click the “More Details” button to view the client address, the group that the client belongs to and that the rule applies to, the requested URL and the target group (i.e., the category or URL user list included in the rule's blacklist).

Fig. 3.15. URL filter: blocked URL details



Client address	10.0.0.201
Client group	default
URL	http://thepiratebay.se/
Target group	Warez

Click the Show status button in the status window to view the total number of requests sent.

3.3.1 Postmaster email

This is the contact email that will be displayed in the block screen sent to the browser of the user who is trying to access a forbidden URL.

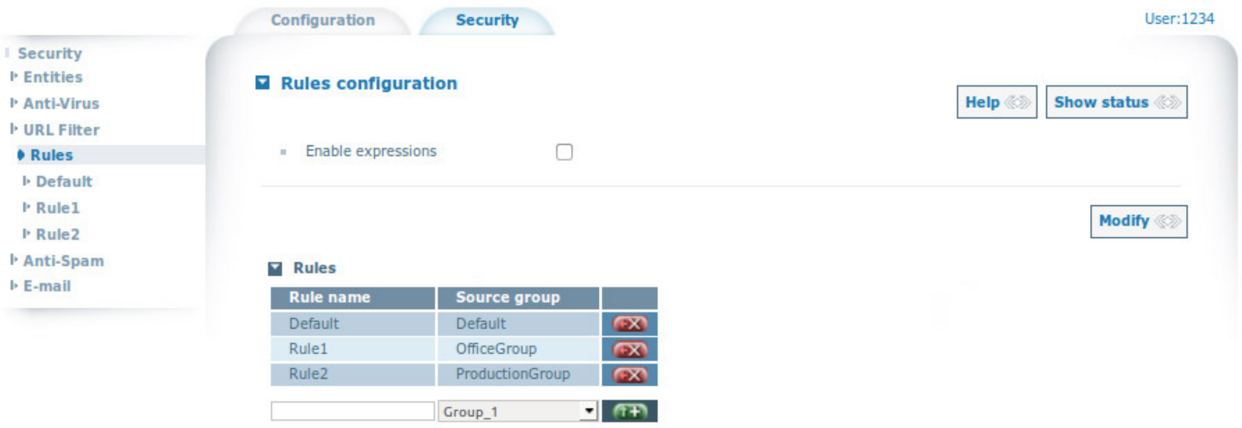
3.3.2 Enable URL filter

This check box enables URL filtering.

3.3.3 Creating and configuring rules

The rules configuration window contains both a check box for enabling expressions and a table of rules (see image below). Ticking the "Enable expressions" box allows the expressions defined in the URL user lists entities to be used when those lists are selected in the individual rule configuration (more information on this can be found further on). The rules table has a default rule. Before you can add new rules, you must first define a group in the entities groups section (see *Entities* on page 6). To add a rule, select one of the available groups as a source group (see *Source group* on page 14), type a name for the rule and click the + button. If there are no more available groups, the screen will shown a “Cannot add elements” message. Once you have clicked the "add" button, the rule name will appear in the left-hand menu. You can configure the rules in the table by clicking on a rule name in the left-hand menu. The access rights controlled by each rule will only apply to its source group. Use the ✕ button to remove rules.

Fig. 3.16. URL filter: rules



Rules configuration

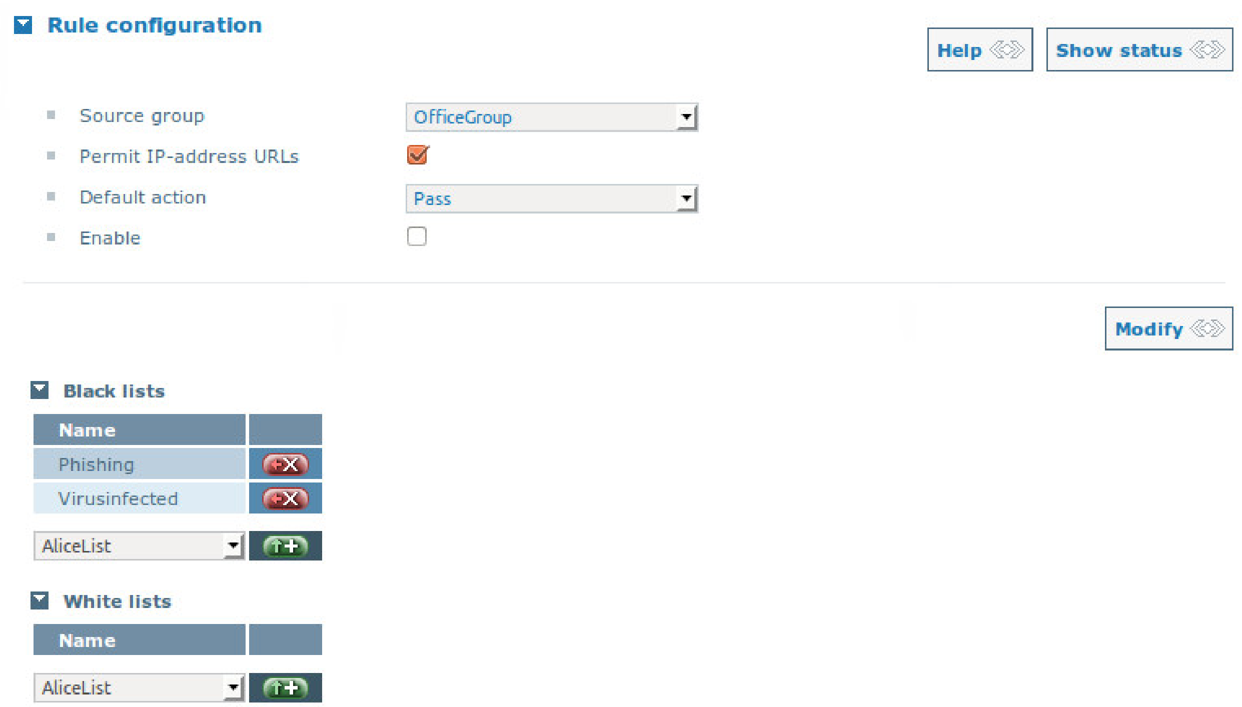
- Enable expressions □

Rules

Rule name	Source group	
Default	Default	✕
Rule1	OfficeGroup	✕
Rule2	ProductionGroup	✕
	Group_1	+

As shown in the following figure, a rule's individual configuration window has four configurable parameters and two lists.

Fig. 3.17. Rule configuration



Rule configuration

- Source group: OfficeGroup
- Permit IP-address URLs: ☑
- Default action: Pass
- Enable: □

Black lists

Name	
Phishing	✕
Virusinfected	✕
AliceList	+

White lists

Name	
AliceList	+

To view the number of blocked requests, access the status window by clicking the Show status button from the rule's configuration window.

3.3.3.1 Source group

Selects a group entity. A list of IP addresses or IP ranges will be defined in the groups section. The access rights defined by the rule will only apply to the sources included in the group's IP addresses list. You cannot use the same source group for two rules.

3.3.3.2 Permit IP-address URLs

This parameter is checked by default and allows IP-address URLs to be used. Fully qualified domain names must be used if you leave the parameter unchecked.

3.3.3.3 Default action

Selects the default action to apply to the rule: pass or block. Select Pass if you want to grant users access to any non-blacklisted URLs. Block will prevent users from accessing URLs that have not been whitelisted.

3.3.3.4 Enable

Check this box to enable the use of the rule.

3.3.3.5 Black lists

You can select the entities (categories and URL user lists) that will be blocked by the URL filter. Any of the available categories and URL user lists defined in the Entities configuration section can be selected here.

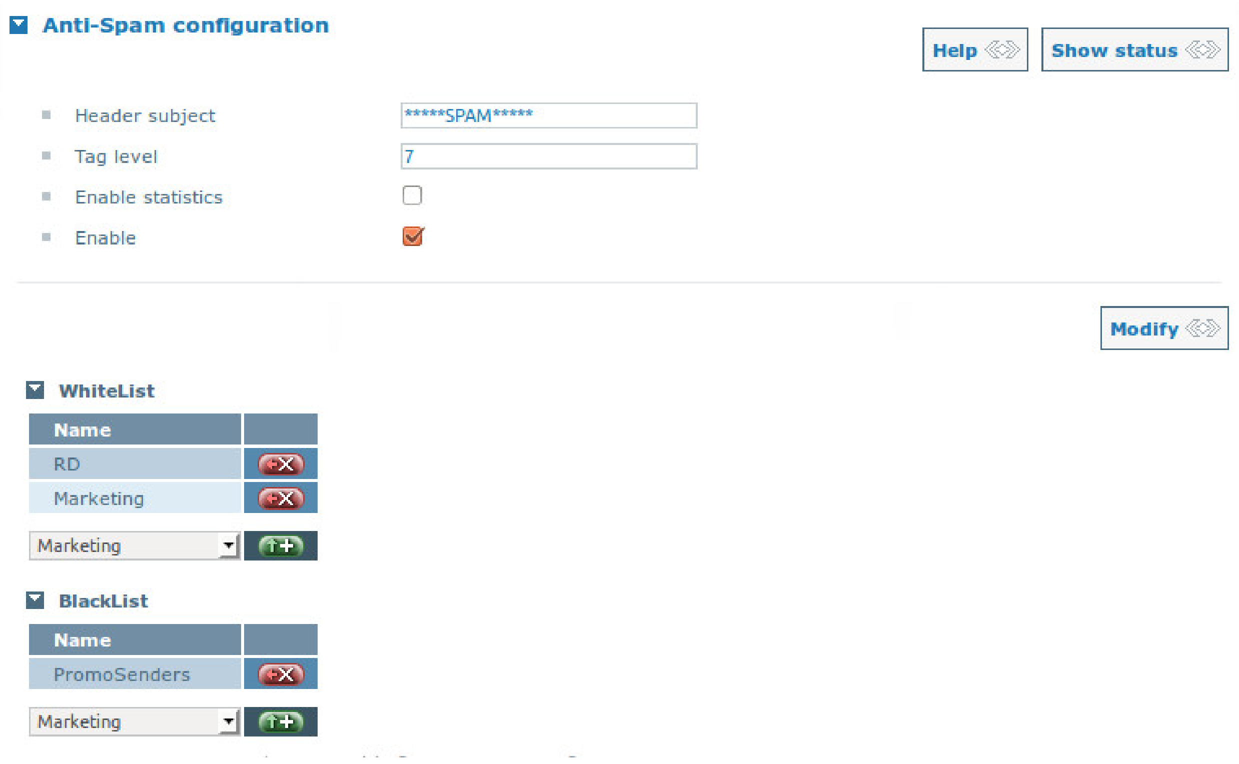
3.3.3.6 White lists

You can select the entities (categories and URL user lists) that will not be blocked by the URL filter. Any of the available categories and URL user lists defined in the Entities configuration section can be selected here.

3.4 Anti-Spam configuration

The image shows the Anti-Spam configuration window. Changes in some configuration parameters can be saved using the Modify button and lists can be added to or removed from white and black lists using the ↑+ and +X icons.

Fig. 3.18. Anti-Spam configuration



Anti-Spam configuration

Header subject: *****SPAM*****

Tag level: 7

Enable statistics: □

Enable: ☑

WhiteList

Name	
RD	+X
Marketing	+X

Marketing ↑+

BlackList

Name	
PromoSenders	+X

Marketing ↑+

The Anti-spam service in the Security application will analyze email traffic in search of spam. The application allows you to add white lists of trusted email addresses to ensure that mails from these addresses will never be treated as spam. You can also insert blacklists containing the email addresses of well-known spammers and undesirable senders so that their mail is marked as spam. The Anti-spam service will be automatically updated each day between 00:00 and 01:00 to maintain optimal detection capability.

You can click on the Show status button to view Anti-Spam status and statistics. This information includes:

- Status: running or stopped
- Spam detected today
- Mail today
- Total spam detected
- Total mail

3.4.1 Header subject

This is a string that will be added to the Subject header of the spam emails to identify them. By default it is “******SPAM******”.

3.4.2 Tag level

Sets the threshold at which a message is considered spam. In the Security application, it is set to 7 by default.

3.4.3 Enable statistics

Enables statistical data to be stored in the SQL database.

3.4.4 Enable

Check this box to enable the Security application's Anti-Spam service.

3.4.5 Whitelist

Emails from a whitelisted email address will always be tagged as no-spam.

3.4.6 Blacklist

Emails from a blacklisted email address will always be tagged as spam.

Note

Email lists cannot be selected in the white and blacklists until they have been registered in the email lists entities configuration section. You will receive a "Cannot add elements" message if you try to select an email list that has not yet been registered.

3.5 Email: configure email for antivirus and anti-spam services

This section allows you to configure an email for antivirus and/or anti-spam mail scanning.

When an email is configured to enable virus scanning and spam detection, the application does the following: the email traffic received in the mail ports (configurable by the user) is redirected to internal ports (also configurable by the user) where two daemons are listening. If SSL is enabled, traffic received in the SSL port is also forwarded to an internal port. The same happens with with STARTTLS (only for SMTP). The daemons listening on the internal ports are p3scan for POP3 and smtp-gated for SMTP. These daemons know whether antivirus or anti-spam services have been enabled and use these services to analyze the data before sending it on to its destination. The email is not sent if malware or spam is detected. Instead, detection statistics are increased and the user may receive a notification.

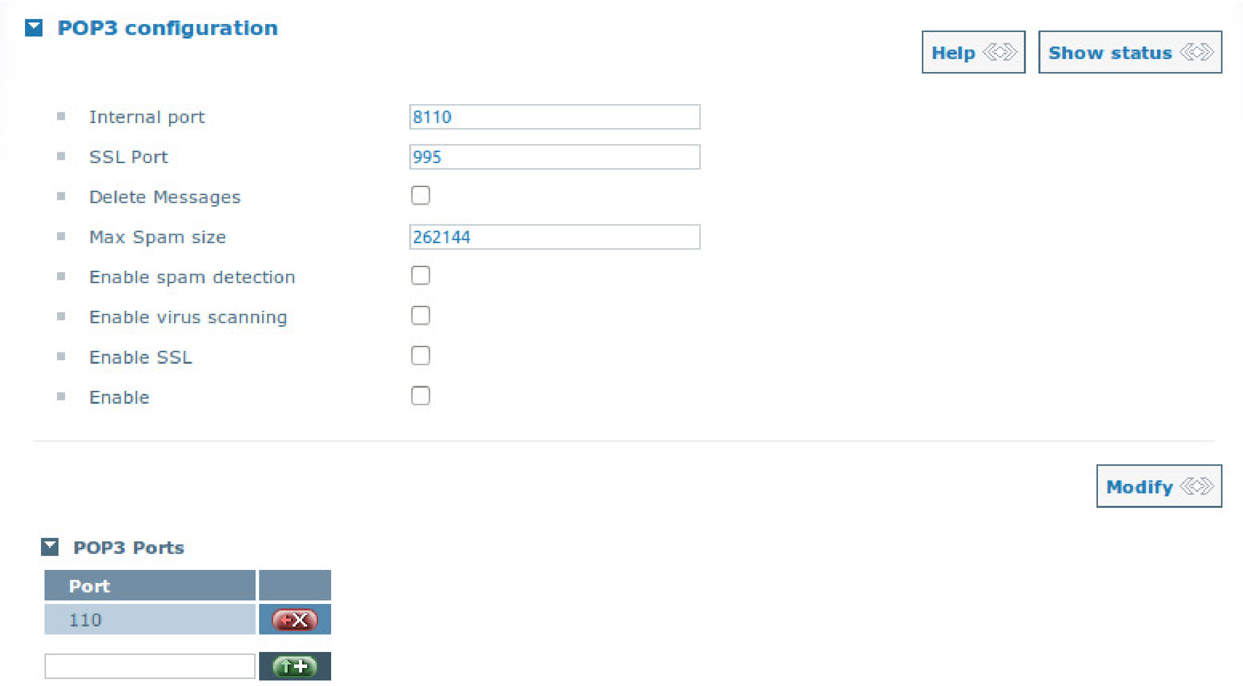
The left-hand menu of the Email configuration window displays two options: POP3 and SMTP. Click on the tags to access their configuration windows.

3.5.1 POP3

When POP3 is enabled (see *Enable* on page 18), all connections to a POP3 server received in a port of the POP3 ports lists (see *POP3 ports* on page 18) will be redirected to an internal port (see*Internal port* on page 17) where the p3scan service listens. The Linux kernel provides the P3scan with the the original destination (the email server) so that the latter can connect to it. All data received from the client will be sent to the server, and vice versa. However, the necessary parts of the protocol are parsed and emails sent from the server are stored in a file for virus scanning and spam detection (as long as these two options are enabled, see *Enable spam detection* on page 18 and*Enable SSL* on page 18). If the email is safe, it is sent. If not, it is replaced with a spam or virus notification. The infected email can be deleted if required (see *Delete messages* on page 17).

Click on the Show status button to see whether POP3 is running or has been stopped.

Fig. 3.19. POP3 configuration



- Internal port 8110
- SSL Port 995
- Delete Messages □
- Max Spam size 262144
- Enable spam detection □
- Enable virus scanning □
- Enable SSL □
- Enable □

Port	
110	✕
	+

3.5.1.1 Internal port

The TCP port receiving redirected traffic from the POP3 ports (see *POP3 ports* on page 18).

3.5.1.2 SSL port

SSL port.

3.5.1.3 Delete messages

When this box is checked, infected messages are deleted once the user has been informed, instead of being kept in a Virus Directory.

3.5.1.4 Max spam size (bytes)

Sets the maximum message size a message can have in order to be analyzed for spam. A message that exceeds this number will not be processed. The size is specified in bytes and the default value is 262144. The maximum message size is 256 MB.

3.5.1.5 Enable spam detection

Check this box to enable spam detection. *The Anti-spam service (see Anti-Spam configuration on page 15) must be enabled to activate spam detection.*

3.5.1.6 Enable virus scanning

Check this box to enable antivirus scanning.The *Antivirus service (see Antivirus configuration: scan web and mail on page 10) must be enabled to activate virus scanning.*

3.5.1.7 Enable SSL

Enable the use of SSL.

3.5.1.8 Enable

Enable POP3.

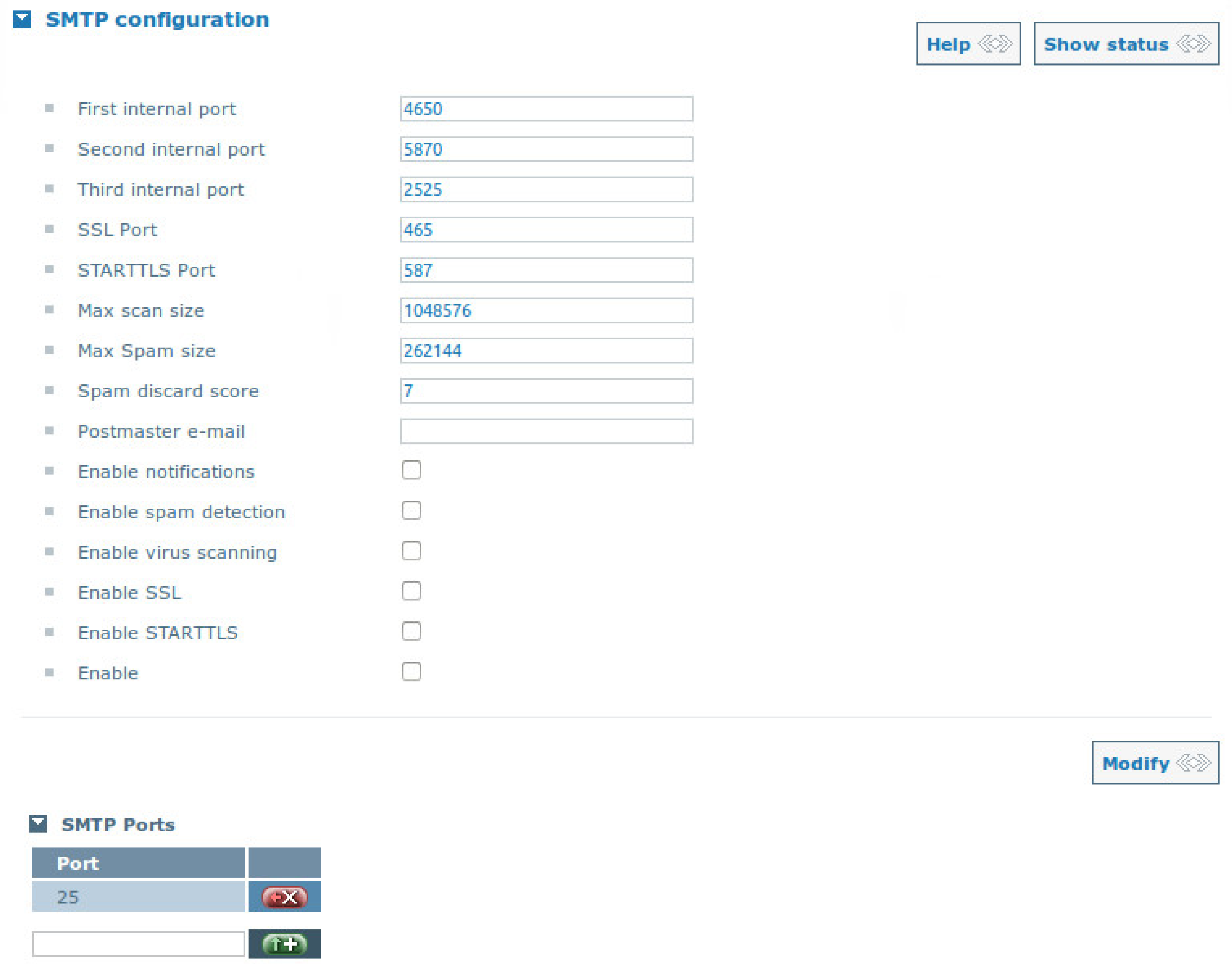
3.5.1.9 POP3 ports

Emails received on these ports are redirected to the internal port. The SSL port cannot be added to POP3 ports. You can add and remove ports by clicking on the ✚ and ✖ buttons.

3.5.2 SMTP

By enabling SMTP you activate an smtp-gated service, by which a server has the ability to scan, recognize and block mail containing spam or viruses. It acts like proxy, intercepting outgoing SMTP connections and scanning session data on-the-fly. When a message is infected, the SMTP session is terminated. Emails coming from the SMTP port (see *SMTP ports* on page 20), the SSL port (see*SSL port* on page 19) or the STARTTLS port (see *STARTTLS port* on page 19), will be redirected to the designated internal ports (see*First internal port* on page 19,*Second internal port* on page 19,*Third internal port* on page 19), where smtp-gated listens.

Fig. 3.20. SMTP configuration



SMTP configuration

First internal port	4650
Second internal port	5870
Third internal port	2525
SSL Port	465
STARTTLS Port	587
Max scan size	1048576
Max Spam size	262144
Spam discard score	7
Postmaster e-mail	
Enable notifications	☐
Enable spam detection	☐
Enable virus scanning	☐
Enable SSL	☐
Enable STARTTLS	☐
Enable	☐

SMTP Ports

Port	
25	✕

Click on Show status to see whether SMTP is running or stopped and to access the "Locked IPs" table. When a virus or spam is detected, the user's IP is blocked for a certain period of time (1800 seconds). Once that time is up, the user is allowed to use SMTP again. If a source IP reaches the maximum number of connections allowed for a host (40 connections), its IP is also locked. The locked IPs are shown in the "Locked IPs" table.

3.5.2.1 First internal port

SSL internal port. The default value is 4650. Internal ports cannot be repeated.

3.5.2.2 Second internal port

STARTTLS internal port. The default value is 5870. Internal ports cannot be repeated.

3.5.2.3 Third internal port

Internal port. The default value is 2525. Internal ports cannot be repeated.

3.5.2.4 SSL port

SSL port. The default value is 465.

3.5.2.5 STARTTLS port

STARTTLS port. The default value is 587.

3.5.2.6 Max scan size (bytes)

The maximum message size that the antivirus will scan. The default value is 1048576.

3.5.2.7 Max spam size (bytes)

The maximum message size that the anti-spam will scan. The default value is 262144. There will be no spam detection if you set the value to 0.

3.5.2.8 Spam discard score

Treats a message as spam if its score is equal or greater than this value. The default value is 7.

3.5.2.9 Postmaster email

Any virus or spam detected will be notified to this email address.

3.5.2.10 Enable notifications

Allows the postmaster to be notified whenever a virus or spam is detected. The postmaster's email address is set in the previous configuration parameter.

3.5.2.11 Enable spam detection

Check this box to enable spam detection. *The Anti-spam service (see Anti-Spam configuration on page 15) must be enabled to activate spam detection.*

3.5.2.12 Enable virus scanning

Check this box to enable antivirus scanning. *The Antivirus service (see Antivirus configuration: scan web and mail on page 10) must be enabled to activate virus scanning.*

3.5.2.13 Enable SSL

Enables the use of SSL.

3.5.2.14 Enable STARTTLS

Enables the use of STARTTLS.

3.5.2.15 Enable

Enable SMTP.

3.5.2.16 SMTP ports

Emails received on these ports are redirected to internal ports. SSL and STARTTLS ports cannot be added to SMTP ports.

Chapter 4 Text configuration commands

This section describes all the text configuration commands that can be used when configuring the application.

Note

The Security application will only behave properly if the general configuration is correct. Please refer to the appendix titled *General Configuration* on page 33 for information on how to configure the general settings.

Note

Configuration commands must be sent in a single text file to the device through the Atlas i6x management portal.

If a statement does not appear in the configuration text, the engine will use the default value.

4.1 Security configuration

```
security
```

Top level configuration directive

4.1.1 Entities

```
entities
```

Entities configuration section

4.1.1.1 Groups configuration

```
groups
```

Groups configuration section

4.1.1.1.1 Add group

```
add group <value>
```

Add group to the groups table

- *group* : group name

4.1.1.1.2 Individual group configuration

```
group <value>
```

Group name

4.1.1.1.2.1 Add IP address

```
add ip <value>
```

Add IP address

- *ip* : IP address, IP address with CIDR block (e.g., 10.0.0.0/24) or IP range (e.g., 10.0.0.1-10.0.0.32)

4.1.1.2 Categories configuration

```
categories
```

Categories configuration section

4.1.1.2.1 Enable category

```
enable_category <value>
```

Category name (e.g., Spyware). A list of categories can be found in the appendix titled *Categories list* on page 36. More than one *enable_category* command can be added.

4.1.1.3 URL user lists configuration

```
user-lists
```

URL user lists configuration section

4.1.1.3.1 Add URL user list

```
add-list <value>
```

User list name

4.1.1.3.2 Individual URL user list configuration

```
userlist <value>
```

User list name

4.1.1.3.2.1 Add URL to a user list

```
url <value>
```

URL. More than one URL can be added.

4.1.1.3.2.2 Add domain to a user list

```
domain <value>
```

Domain. More than one domain can be added.

4.1.1.3.2.3 Add expression to a user list

```
expression <value>
```

Regular expression. More than one expression can be added.

4.1.1.4 Email lists configuration

```
email-lists
```

Email-lists configuration section

4.1.1.4.1 Add email list

```
add-list <value>
```

Email list name

4.1.1.4.2 Individual email list configuration

```
emaillist <value>
```

Email list name

4.1.1.4.2.1 Add email to an email list

```
email <value>
```

Email address

4.1.2 Antivirus

```
anti-virus
```

Antivirus configuration section

4.1.2.1 Safe URLs and domains

```
safe-url <value>
```

Designate a URL user list as safe. Can be done with as many user lists as necessary. Must be the name of one of the URL user lists entered in the section titled *URL user lists configuration* on page 22.

4.1.2.2 MIME exceptions

```
mime-exception <value>
```

MIME type. More than one MIME exception can be added.

- *image*
- *streamvideo*
- *text*
- *flash*
- *javascript*

4.1.2.3 File extension exceptions

```
file-type-exception <value>
```

File extension (e.g., .zip). More than one exception can be added.

4.1.2.4 Maximum size

```
max-size <value>
```

Maximum allowed file size (in bytes) for virus scanning.

Default value: 500000

4.1.2.5 Enable

```
enable
```

Insert the configuration text *enable* to activate the virus scanning.

4.1.3 URL Filter

```
url-filter
```

URL filter configuration section

4.1.3.1 Postmaster mail

```
postmaster-mail <value>
```

Postmaster email

4.1.3.2 Rules configuration

```
rules
```

Rules configuration section

4.1.3.2.1 Add Rule

```
add rule <value> src-group <value>
```

Add rule

- *rule* : rule name
- *src-group* : source group. Must be one of the groups defined in the section titled *Groups configuration* on page 21 .

4.1.3.2.2 Enable expressions

```
expressionlist
```

Type the command *expressionlist* to allow expressions to be used in users list and categories for the URL filter.

4.1.3.2.3 Individual rule configuration

```
rule <value>
```

Rule name.

4.1.3.2.3.1 Source group

```
src-group <value>
```

Name of the source group. This must be one of the groups defined in the section titled *Groups configuration* on page 21

4.1.3.2.3.2 Permit IP-address URLs

```
ip-address-access
```

Insert in the configuration text *ip-address-access* to allow the use of IP-address URLs.

4.1.3.2.3.3 Default action

```
default-action <value>
```

Action applied by default for the rule:

- *Pass*: allow access.

- *Block*: deny access.

4.1.3.2.3.4 Blacklists

```
black-category <value>
```

Category name. Must be one of the categories defined in the section titled *Categories configuration* on page 22.

4.1.3.2.3.5 White lists

```
white-category <value>
```

Category name. Must be one of the categories defined in the section titled *Categories configuration* on page 22.

4.1.3.2.3.6 Enable

```
enable
```

Insert the text *enable* to activate the rule.

4.1.4 Anti-Spam

```
anti-spam
```

Anti-spam configuration section

4.1.4.1 WhiteList

```
whiteList <value>
```

Email list name. Must be one of the email lists defined in the section titled *Email lists configuration* on page 22.

4.1.4.2 BlackList

```
blackList <value>
```

Email list name. Must be one of the email lists defined in the section titled *Email lists configuration* on page 22.

4.1.4.3 Header subject

```
header-subject <value>
```

String added to the header subject of the emails considered spam

Default value: *****SPAM*****

4.1.4.4 Header subject

```
tag-level <value>
```

Threshold at which a message is considered spam

Default value: 7

4.1.4.5 Stats enable

```
stats-enable
```

Insert *stats-enable* in the text configuration to activate the anti-spam statistics.

4.1.4.6 Enable

```
enable
```

Insert *enable* during text configuration toactivate the anti-spam service.

4.1.5 Email configuration

```
e-mail
```

Email configuration section

4.1.5.1 POP3 Configuration

```
pop3
```

POP3 configuration section

4.1.5.1.1 Ports

```
ports <value>
```

POP3 ports. Add a command for each port.

4.1.5.1.2 Internal port

```
internal-port <value>
```

Internal port that receives the redirected traffic from the POP3 ports.

Default value: 8110

4.1.5.1.3 SSL port

```
ssl-port <value>
```

SSL port

Default value: 995

4.1.5.1.4 Delete messages

```
delete-msgs
```

Insert *delete-msgs* in the configuration text to activate virus/spam message deletion.

4.1.5.1.5 Maximum SPAM size

```
spam-size-max
```

Maximum message size (in bytes) allowed for spam detection.

Default value: 262144

4.1.5.1.6 Enable anti-spam

```
enable-antispam
```

Insert *enable-antispam* in the configuration text to activate anti-spam detection.

4.1.5.1.7 Enable antivirus

```
enable-antivirus
```

Insert *enable-antivirus* in the configuration text to activate virus scanning.

4.1.5.1.8 Enable ssl

```
enable-ssl
```

Insert *enable-ssl* in the configuration text to activate SSL.

4.1.5.1.9 Enable pop3

```
enable-pop3
```

Insert *enable-pop3* in the configuration text to activate POP3.

4.1.5.2 SMTP Configuration

```
smtp
```

SMTP configuration section.

4.1.5.2.1 Ports

```
ports <value>
```

SMTP ports. Insert a command for each port.

4.1.5.2.2 First internal port

```
internal-ssl-port <value>
```

Internal port that receives the redirected traffic from the SSL port.

Default value: 4650

4.1.5.2.3 Second internal port

```
internal-starttls-port <value>
```

Internal port that receives the redirected traffic from the STARTTLS port.

Default value: 5870

4.1.5.2.4 Third internal port

```
internal-port <value>
```

Internal port that receives the redirected traffic from the SMTP ports.

Default value: 2525

4.1.5.2.5 SSL port

```
ssl-port <value>
```

SSL port

Default value: 465

4.1.5.2.6 STARTTLS port

```
starttls-port <value>
```

STARTTLS port

Default value: 587

4.1.5.2.7 Maximum scan size (bytes)

```
scan-size-max <value>
```

Maximum size of messages to be scanned for viruses.

Default value: 1048576

4.1.5.2.8 Maximum spam size (bytes)

```
spam-size-max <value>
```

Maximum size of messages to be analyzed for spam.

Default value: 262144

4.1.5.2.9 Spam discard score

```
spam-threshold <value>
```

Threshold for treating a message as spam.

Default value: 7

4.1.5.2.10 Postmaster email

```
postmaster-mail <value>
```

Email address to which the virus/spam notifications are sent.

4.1.5.2.11 Enable notifications

```
enable-notify
```

Insert *enable-notify* in the configuration text to allow notifications to be sent to the postmaster.

4.1.5.2.12 Enable spam detection

```
enable-antispam
```

Insert *enable-antispam* in the configuration text to activate spam detection

4.1.5.2.13 Enable virus scanning

```
enable-antivirus
```

Insert *enable-antivirus* in the configuration text to activate virus scanning.

4.1.5.2.14 Enable SSL

```
enable-ssl
```

Insert *enable-ssl* in the configuration text to activate SSL.

4.1.5.2.15 Enable STARTTLS

```
enable-starttls
```

Insert *enable-starttls* in the configuration text to activate STARTTLS.

4.1.5.2.16 Enable SMTP

```
enable-smtp
```

Insert *enable-smtp* in the configuration text to activate SMTP.

4.1.6 Monitoring update period (seconds)

```
monitoring-update-period <value>
```

The period between updates of the numerical status information.

Default value: 0

Chapter 5 Examples of use

In this section, several use cases are presented to serve as a practical guide on how to navigate through the application web and have a well-configured system that is ready to use.

5.1 URL filter

Imagine a school where students come in with their laptops. They connect to the Internet through an Atlas i6x that has Teldat Security application installed. You want the students to surf the Web but you also want to block certain content that you consider inappropriate. The Security application allows you to do this by following the steps here:

- (a) Enter the Security application's Configuration web.
- (b) Create a group with the students IP addresses. You may skip this if you have already created the group.
    - (a) Click on the “Entities” tag in the left-hand menu. This displays the different menu entities.
    - (b) Click on “Groups” to access the Groups configuration section.
    - (c) Enter a name for your group (e.g., students), and click the ↑+ button.
    - (d) Click on the new tag with the name of your group (e.g., students) in the left-hand menu. This takes you to the individual group configuration section.
    - (e) Enter the IP range of the students (e.g., 10.0.0.20-10.0.0.50) and click the ↑+ button. The group may now be used.
- (c) Enable the categories you want to restrict. This will allow the Security application to download and update the URLs and domain lists associated with each category.
    - (a) Click on “Entities” in the left-hand menu. This displays the different menu entities.
    - (b) Click on “Categories” to access the Categories configuration section.
    - (c) Select the categories (e.g., drugs, guns, porn, virusinfected, warez, etc.,) you want to enable and add them using the ↑+ button.
- (d) Create a rule for the group forbidding access to inappropriate content.
    - (a) Click on the URL filter tag to access the URL Filter configuration section.
    - (b) Click on “Rules” in the left-hand menu.
    - (c) In the rules table, select the group that you have previously created as source group (e.g., students), enter a name for the rule (e.g., rule1) and click the ↑+ button. You will see a new rule in the table and in the left-hand menu.
    - (d) Click on the new rule name in the left-hand menu to access the configuration window for that rule.
    - (e) In the *black list* table, select the categories you want to restrict one by one (only the categories you have previously enabled in the entities section may be selected) and add them by clicking the ↑+ button.
    - (f) Set the default action to *Pass* to allow access to all web sites except those blacklisted.
    - (g) Check the enable box to enable the use of the rule.
    - (h) Click on the Modify button.
- (e) Enable URL filtering.
    - (a) Click on the URL filter tag to access the URL Filter configuration section and check the enable box to activate URL filtering.
    - (b) Click on the Modify button.

If you want to apply the rule to other previously registered IP groups:

- (a) Enter said rule's configuration section by clicking on its name in the left-hand menu.
- (b) In the rule configuration window, click on the source group and select the new predefined group.
- (c) Click on the Modify button. The rule will apply to the new group instead of the old one.

Now, imagine that you want to allow access to one domain only (the one with the educational content) and deny access to all other sites.

(a) Instead of using categories, define your own URL user list.

  (a) Click on “Entities” from the left-hand menu. This displays the different menu entities.

  (b) Click on “URL user lists” to access the URL user lists configuration section.

  (c) Create a new user list entering a name for the list (e.g., eduList) and clicking the + button. A tag with the list name will appear in the left-hand menu.

  (d) Click on the list name in the left-hand menu and access the list configuration web.

  (e) You will see three tables: URLs, domains and expressions. In this example, you would enter the domain you want users to be able to access (e.g., education.net) in the domains table and click on the + button.

(b) Create a rule for the group so that users can only access a specific domain.

  (a) Click on the URL filter tag to access the URL Filter configuration section.

  (b) Click on “Rules” in the left-hand menu.

  (c) Once in the rules table, select the group you previously created as source gorup (e.g., students), enter a name for the rule (e.g. rule2) and click on the + button. A new rule will appear in the table and on the left-hand menu.

  (d) Click on the new rule name in the left-hand menu to access the configuration window for that rule.

  (e) In the *white list* table, select the URL user list you have previously created (e.g., eduList) and add it using the + button.

  (f) Select *Deny* as the default action to deny access to all web sites except the one that has been whitelisted.

(c) Check the enable box so that the rule is active.

(d) Click on the Modify button.

5.2 Anti-spam

Imagine that some of your providers keep sending you a lot of promo and advertising emails. You don't want to stay in touch with these providers and you want all their emails to be tagged as spam so that your employees stop having to deal with them. Here are the steops you have to follow to configure the Security application accordingly:

(a) Create an email list.

  (a) Click on “Entities” in the left-hand menu. This displays the different menu entities.

  (b) Click on “Email lists” to access the configuration section.

  (c) Enter a name for your email list (e.g., notWelcome) and click the + button to create it.

  (d) Click on the new tag with the name of your email list (e.g., notWelcome) from the left-hand menu. This takes you to the individual email list configuration section.

  (e) Here you can add all the email addresses you need. Enter each address and then click on the + button.

(b) Configure the Anti-spam service.

  (a) Click on “Anti-Spam” to access the Anti-spam configuration section.

  (b) Add the email list (e.g., notWelcome) to the black list by selecting it from the lists available in the black list table. The list should be available once you have registered it in the "Entities" configuration section (previous step). Then click the + button.

  (c) Check the enable box to start the spam detection service.

  (d) Click on Modify so that the anti-spam configuration changes take effect.

(c) You must now configure the email to allow the anti-spam detector to analyze the emails.

  (a) Click on “email” in the left-hand menu to access the “Email” configuration window.

  (b) Two options will appear in the left-hand menu under the "Email": POP3 and SMTP. Click on POP3 to configure it.

  (c) Check the “enable anti-spam” box (if you want email antivirus scanning, check “enable antivirus” as well). You cannot activate spam detection until you have enabled the anti-spam service, as described in step 2. Similarly, the antivirus scanning option needs the antivirus to be enabled in the antivirus configuration section.

(d) Check the box to enable anti-spam for POP3 traffic (see the section titled *POP3* on page 17 for more information on all the configuration options).

(e) Click on Modify so that the configuration changes take effect.

(f) Now click SMTP in the left-hand menu to configure the SMTP section.

(g) In the SMTP configuration window, check the “enable anti-spam” box (if you want email antivirus scanning, check “enable antivirus” as well). You will not be able to activate spam detection until you have enabled the anti-spam service, as described in step 2. Similarly, the antivirus scanning option needs the antivirus to be enabled in the antivirus configuration section.

(h) Check the box to enable the anti-spam for SMTP traffic (see the section titled *SMTP* on page 18 for more information on all the configuration options).

(i) Click on Modify so that the configuration changes take effect.

Appendix A General Configuration

To be able to run, the Security application needs the CIT to be configured in a certain way. There are two ways to do it: by using the Atlas i6x configuration web or configuring the CIT manually. The web option allows Atlas i6x applications to access the CIT. The Security application will configure automatically. If you choose to do it manually, you have to access the CIT and divert traffic from the CIT to the applications by means of an access list.

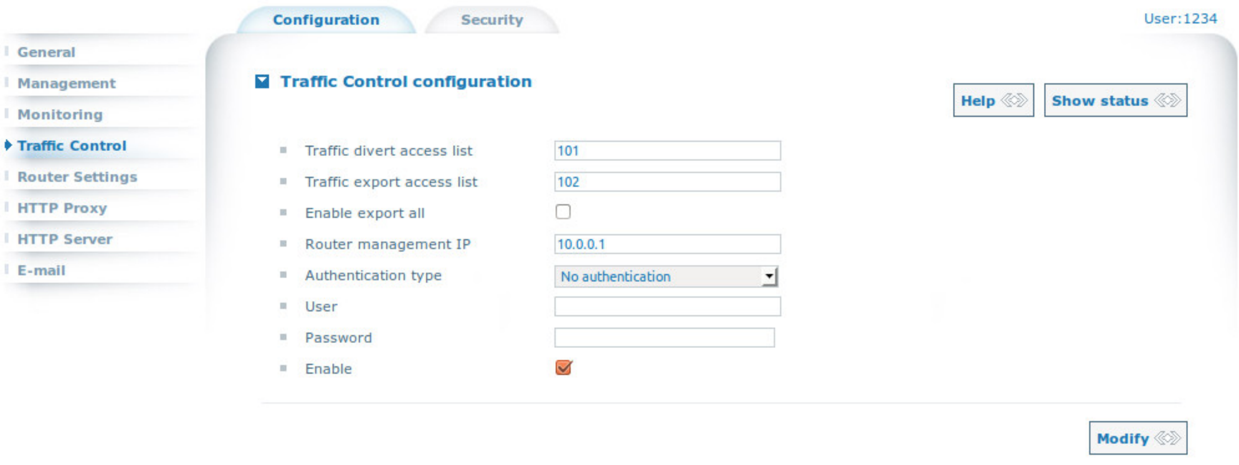
A.1 Enabling CIT access for the applications in the configuration web.

(a) Access the Atlas i6x “Configuration” web section by clicking on the “Configuration” icon or the “Configuration” tab (at the top). The left-hand menu will display several options.

(b) By clicking on “Traffic Control”, you will access the “Traffic Control” configuration screen.

(c) Here you will find a check-box with the word “Enable”. Check the box and press the “modify” button to enable traffic control and allow applications (like Security) to access CIT configuration.

Fig. A.1. Traffic Control configuration

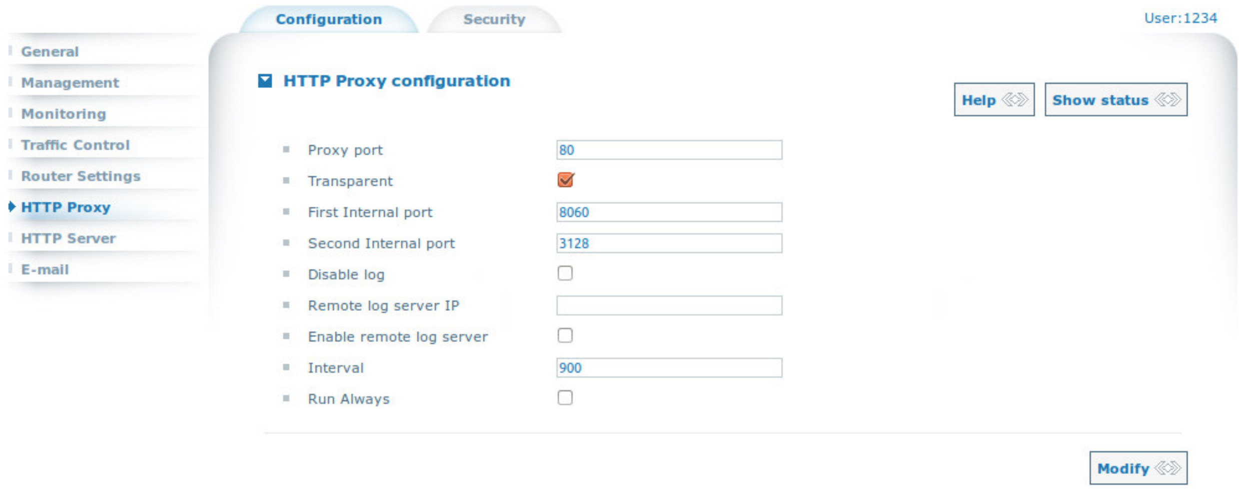


Traffic Control configuration

- Traffic divert access list: 101
- Traffic export access list: 102
- Enable export all: ☐
- Router management IP: 10.0.0.1
- Authentication type: No authentication
- User:
- Password:
- Enable: ☑

When you enable the antivirus and/or the URL filter services while the "Traffic Control" function is active, an access list will configure the CIT so that it diverts web traffic to the Linux. The port where the traffic is received can be configured in the "HTTP Proxy" section of the "Configuration" web, under the "Proxy port" field. It is usually port 80. In the figure below, you can see the "HTTP Proxy" configuration window.

Fig. A.2. HTTP Proxy configuration



HTTP Proxy configuration

- Proxy port: 80
- Transparent: ☑
- First Internal port: 8060
- Second Internal port: 3128
- Disable log: ☐
- Remote log server IP:
- Enable remote log server: ☐
- Interval: 900
- Run Always: ☐

A.2 Configuring CIT manually for traffic divert

If you have not enabled "Traffic Control", you must configure the CIT manually.

For email related services (antivirus email scanning and spam detection), the Linux has to be able to access the mail traffic received by the CIT. This is possible by configuring the ports designated to receive mail so that they divert traffic to the Linux. We will use an access list to divert only the desired traffic.

For web services (antivirus web scanning and URL filtering), we need to divert the traffic received on port 80.

If you don't make the right traffic available to the applications, they will not work even if they are running. Here are the steps to configure the CIT:

(a) Telnet to the CIT IP address.

```
telnet <CIT-address>
```

(b) Access dynamic configuration mode.

```
p 5
```

(c) Configure an access list (either by modifying an existing access list or by creating a new one). This depends on whether or not the configuration already has an access list for traffic export defined. First, access the access lists menu.

```
feature access-lists
```

- *Create a new access list.* The following example shows the structure that the access list must have:

```
      access-list 101
         description vli_traffic_divert
;
         entry 1 description httpproxy_pre
         entry 1 default
         entry 1 permit
         entry 1 destination port-range 80 80
         entry 1 protocol tcp
;
         entry 2 description smtp_25
         entry 2 default
         entry 2 permit
         entry 2 destination port-range 25 25
         entry 2 protocol tcp
;
         entry 3 description ssmtp_465
         entry 3 default
         entry 3 permit
         entry 3 destination port-range 465 465
         entry 3 protocol tcp
;
         entry 4 description ssmtp_starttls_587
         entry 4 default
         entry 4 permit
         entry 4 destination port-range 587 587
         entry 4 protocol tcp
;
         entry 5 default
         entry 5 deny
;
      exit
```

In the example we define the ports whose traffic we want to divert to the applications. These ports are port 80 for http traffic and the external ports that you entered in the email configuration (see *POP3* on page 17 and *SMTP* on page 18). If you have enabled SSL or STARTTLS, you must add these ports as well.

Each access list entry contains:

(a) *description <info>*: information tag

(b) *default*: set default values for a new entry

(c) *permit*: what we are going to do with the traffic

(d) *destination port-range <port> <port>*the destination port, the start and end of the range will be the same if we are inserting one port

(e) *protocol tcp*: the protocol

A final entry denying any traffic not specified beforehand, must be added to the end of the access list. The order of the entries is relevant: traffic will be checked in the order that they are listed. If it matches one entry, the other will not be checked.

(a) *default*: set default values for a new entry

(b) *deny*: what we are going to do with the traffic

Once you know which ports will receive the diverted traffic, create your own access list and copy it to the CIT configuration here, in the access-list menu.

- *Modify an existing access list.* If an access list is being used to divert traffic, it must be added to the existing configuration entries for your ports (as described in the section on how to create an access-list). You can copy it in the access lists menu as if it were a new access-list.

(d) Exit the access-lists menu.

```
exit
```

(e) Enter the VLI menu.

```
feature vli
```

(f) Enable traffic divert if it is not yet enabled. Insert your access list number.

```
application traffic-divert access-list <access-list-number>
```

(g) Exit the VLI menu.

```
exit
```

(h) Exit dynamic configuration mode.

```
ctrl + p
```

(i) Exit telnet.

```
logout
```

Appendix B Categories list

The following list shows the categories that can be used as category entities. This list was produced using a service that collects URLs from the Web and classifies them. Although this is called a 'blacklist', the categories can also be used as white lists. These are just lists of sites and do not imply the expression of any opinion whatsoever on the part of Teldat. The categorized list does not include all existing web sites since that would be impossible.

Some category names may change over time, creating more specific categories or grouping several categories in one. However, most will remain unchanged.

- *Abortion*: Information on abortion (except those related to religion)
- *Ads*: Advert servers and banned URLs
- *Adult*: Sites containing adult material, such as swearing (but not porn)
- *Aggressive*: Similar to violence, but more promoting than depicting
- *Alcohol*: Sites with alcohol-related content
- *Antispyware*: Sites that remove spyware
- *Arjel*: List of sites approved by the Regulatory authority for online games
- *Artnudes*: Art sites containing artistic nudity
- *Astrology*: Astrology websites
- *Audio-video*: Sites that offer audios and videos
- *Banking*: Banking websites
- *Beerliquorinfo*: Sites with information only on beer or liquors
- *Beerliquorsale*: Sites with beer or liquors for sale
- *Blog*: Journal/Diary websites
- *Books*: Sites that provides books
- *Celebrity*: Sites with information about celebrities
- *Cellphones*: Sites with information on mobile/cell phones
- *Chat*: Sites with chat rooms, etc.
- *Child*: Sites for children
- *Childcare*: Sites to do with childcare
- *Cleaning*: Sites to do with cleaning
- *Clothing*: Fashion-related sites and those that sell clothes
- *Contraception*: Information on contraception
- *Cooking*: Sites about cooking et al
- *Culinary*: Sites about cooking et al
- *Dating*: Dating sites
- *Desktopsillies*: Sites containing screen savers, backgrounds, cursors, pointers, desktop themes and similar time-wasting and potentially dangerous content
- *Dialers*: Sites with dialers, like those used in porn web sites or by trojans
- *Drugs*: Drug-related sites
- *Ecommerce*: Sites to shop online shopping
- *Entertainment*: Sites on movies, books, magazines, humor
- *Filehosting*: Sites to do with file hosting
- *Filesharing*: File sharing sites
- *Financial*: Financial information
- *Frencheducation*: Sites to do with French education
- *Gambling*: Gambling sites (including stocks and shares)
- *Games*: Game-related sites

- *Gardening*: Gardening sites
- *Government*: Military, schools, etc.
- *Guns*: Sites with guns
- *Hacking*: Hacking/cracking information
- *Homerepair*: Sites on home repair
- *Humor*: Humor sites
- *Hunting*: Sites on hunting, fishing, etc.
- *Hygiene*: Sites on hygiene and personal grooming
- *Instantmessaging*: Sites containing messenger client download and web-based messaging sites
- *Jewelry*: Sites that sell and discuss jewelry
- *Jobsearch*: Job-hunting sites
- *Kidstimewasting*: Sites kids often waste time on
- *Lingerie*: Sites about lingerie
- *Magazines*: Magazine sites
- *Mail*: Webmail and email sites
- *Malware*: Sites with malware
- *Manga*: Manga sites
- *Marketingware*: Sites on marketing products
- *Medical*: Medical websites
- *Mixed_adult*: Mixed adult content sites
- *Mobile-Phone*: Mobile phone sites
- *Naturism*: Sites that contain nude pictures and/or promote a nude lifestyle
- *News*: News sites
- *Onlineauctions*: Online auctions
- *Onlinegames*: Online gaming sites
- *Onlinepayment*: Online payment sites
- *Personalfinance*: Personal finance sites
- *Pets*: Pet sites
- *Phishing*: Sites that try to trick people into giving out private information.
- *Porn*: Pornography
- *Press*: Press
- *Proxy*: Sites with proxies to bypass filters
- *Radio*: Non-news-related radio and television
- *Reaffected*: Sites that have changed ownership and, therefore, content
- *Religion*: Religious sites
- *Remote-Control*: Sites about remote control devices
- *Ringtones*: Sites containing ring tones, games, pictures, etc.
- *Searchengines*: Search engines such as google
- *Sect*: Sites about religious groups
- *Sexuality*: Sites dedicated to sexuality, possibly including adult material but excluding educational material
- *Shopping*: Shopping sites
- *Socialnetworking*: Social networking websites
- *Social_Networks*: Social networking websites
- *Sportnews*: Sports news sites
- *Sports*: All sports sites
- *Spyware*: Sites that run or use spyware software to download

- *Tobacco*: Sites on tobacco
- *Updatesites*: Sites that allow software updates to be downloaded, including virus sigs
- *Vacation*: Sites on holiday plans
- *Verisign*: Verisign
- *Violence*: Sites containing violence
- *Virusinfected*: Sites that host virus-infected files
- *Warez*: Sites with illegal pirate software
- *Weapons*: Sites detailing or selling weapons
- *Weather*: Weather-related web sites
- *Webmail*: Just webmail sites
- *Whitelist*: Sites that are 100% suitable for kids