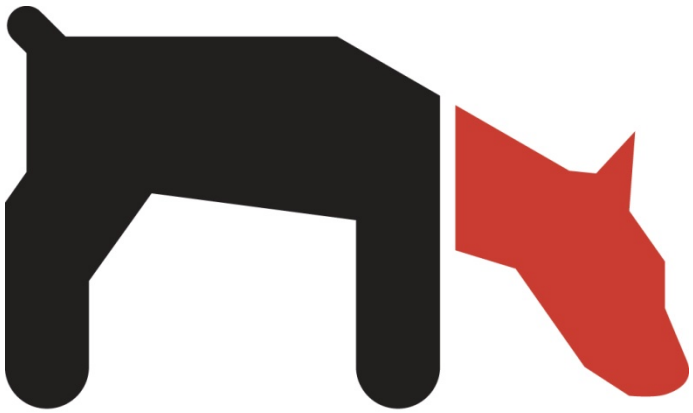

REDDOXX

User Manual

Version 1027

www.reddoxx.com

Copyright

REDDOXX GmbH
Saline 29
D-78628 Rottweil

Fon: +49 (0)741 248 810
Fax: +49 (0)741 248 811

Email: info@reddoxx.com
Internet: http://www.reddoxx.com
Support: http://support.reddoxx.net

Revision number: 1.03

Last alteration: 29.06.2009

Table of contents

1 Login

For safety reasons, the REDDOXX Appliance is only accessible via login. Therefore you have to authenticate yourself as follows with your user name and password.

Purchase of the REDDOXX Appliance with the valid licenses.

1. Double-click on the file rdxuser.exe.
2. The login window appears.

Illustration: Log In window

3. Enter the corresponding host name of your appliance (contact your administrator).
4. Enter your user name.
5. Enter your password.
6. In the field *realm* select the option „local“or the realm which you belong to. The realm is a section similar to a domain in which you have to authenticate yourself.
7. Choose the desired language in the selection list. The selection contains the currently installed languages.

8. The following application window contains the section of the user console.

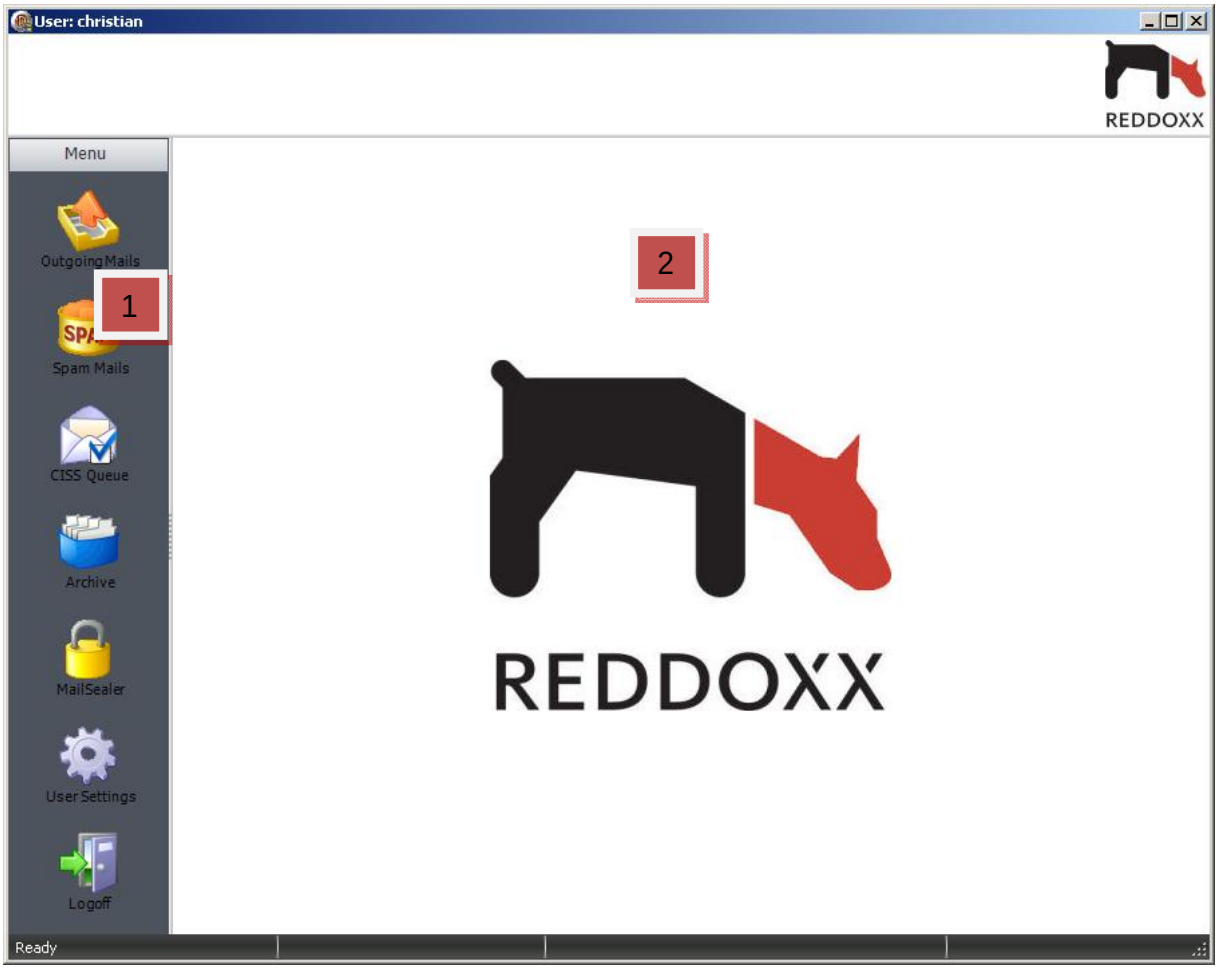

Illustration: Application window after login

Legend:

1. Menu bar.
2. Display window.

2 Options in the menu bar

The main menu consists of the Outgoing mails, Spam, CISS queue, Archive, Mail Sealer, User settings and Logout.

Illustration: Menu bar

Outgoing Mails

Here you get all emails listed that the user is sending to the internet.

Spam Mails

Here are listed all mails that were sent to the user but were detected as spam.

CISS Queue

The CISS Queue contains all emails which has been kept back and has not been released yet by the sender or by the recipient.

Archive

In the Mail Depot you will find all the emails which have been archived by the appliance.

Mail Sealer

The Mail Sealer (Light) offers you the possibility to send your email encrypted with a password.

User Settings

The user settings allow you to change your general setting. You can maintain your email addresses here.

Logoff

You log off from your personal user GUI.

2.1 Outgoing Mails

In addition to the displayed email list you also have the possibility to search for certain emails.

Illustration: Search outgoing messages

The search is basically a full-text search. You can determine whether to search for incoming or outgoing emails in the SMTP or POP3 queue.

2.2 Spammails

All emails which the Reddoxx Appliance has identified as spam will be listed here. Also you have the possibility to search for certain emails.

Illustration: Search Spammails

The search is basically a full-text search. You can also choose a deputy.

2.2.1 Spammail options

Various manual options are available for the individual processing of those messages. By clicking the right mouse button on the display the following options appears.

Illustration: Options Spammails

Deliver:	The email is sent to the recipient.
Deliver (Whitelist address):	The email is sent to the recipient and the sender's address will be added to the local whitelist.
Deliver (Whitelist Domain):	The email is sent to the recipient and the sender's domain is added to local whitelist.
Delete:	The email is deleted from the queue.
Preview:	The contents of the email will be displayed in a separate window.

2.3 CISS queue

When using the CISS filter the sender receives an email which must be acknowledged, so that his email to you will be sent. The mail remains in the CISS queue until it will be confirmed. You can browse the CISS queue if you wait for a certain mail.

Illustration: Search CISS queue

The search, send, and preview options are consistent with those of the spam mails.

Emails, which the sender has not been confirmed, the recipient can deliver manually (e.g.: newsletter, publicity).

2.4 Archive

In the Mail Depot is a possibility to display all archived emails of the logged on user. Furthermore, this menu uses an advanced search.

The number of displayed emails is dependent on the parameterization in the user settings.

2.4.1 Simple search

Illustration: Search MailDepot

The search options are consistent with those of the spam mails.

2.4.2 Advanced search

The advanced search provides additional search criteria.

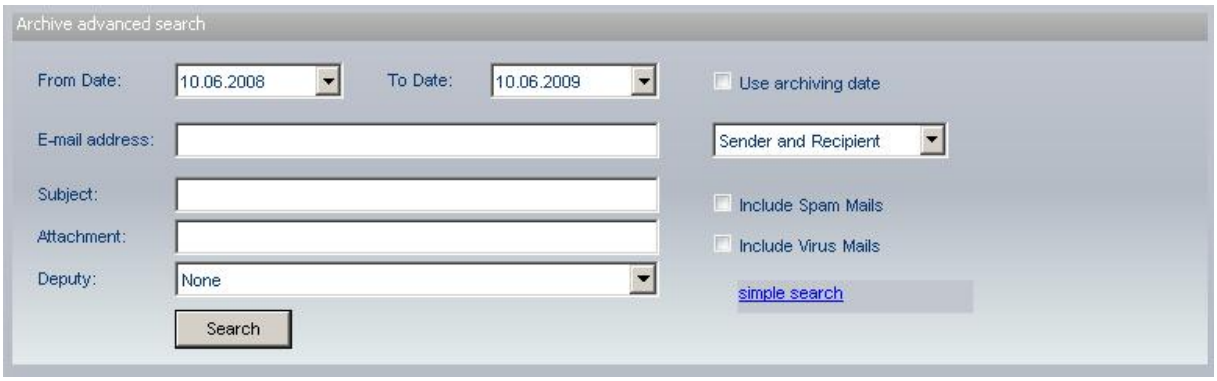

Illustration: advanced search MailDepot

From - To:	The search will be limited by a date entry.
Email address:	The email address of the sender or recipient can be entered. (Sender or recipient, or both are selectable).
Subject:	Only in subject will be searched.
Attachment:	Only in attachment will be searched.
Deputy:	Only in mails of the deputy will be searched.
Use archiving date:	It will only be searched for mails at the specified archive date.
Include Spam/ Include Virus:	Spam and virus emails can be included to the search.

2.4.3 Advanced full text search

The full text Advanced Search describes a search for all available criteria.

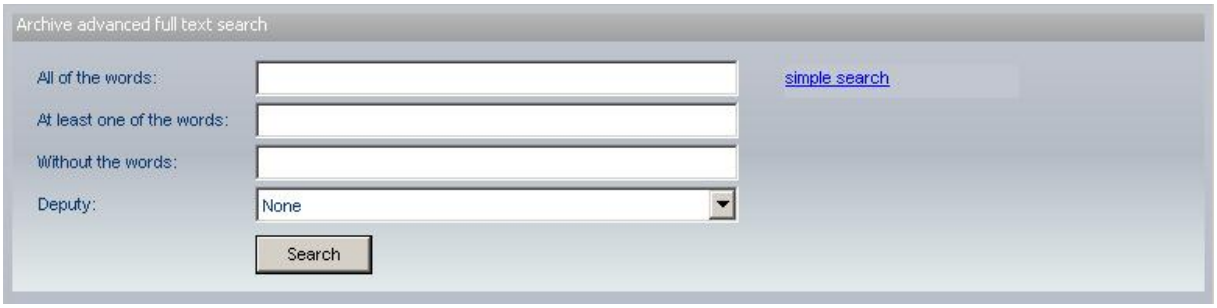

Illustration: full text advanced search option MailDepot

All of the words:	For all the entered words will be searched.
At least one of the words:	At least one of the words will be searched
Without the words:	Without the words will be searched.
Deputy:	Only in to the mails of the deputy will be searched.

2.4.4 Archive options

Various manual options are in the individual processing of those messages available. By clicking the right mouse button on the display the following options appears.

Illustration: Options MailDepot

Preview: The contents of the email will be displayed in a separate window. For example:

Illustration: Preview

If the message has an attachment, so you can open and save that. By clicking the right mouse button, these options are offered.

Deliver:	The email is sent to the recipient.
Save message:	The message will be stored in *.eml format on a free chosen path of the hard disk.

More options in the preview window can be found in the menu bar.

Illustration: View options

Message Header:	Shows the header of the email.
Message Source:	Shows the complete source code of the email.

2.5 Mailsealer

In Mailsealer light you have the option to send your emails with a freely selectable password protection. The password must have no criteria. By clicking the right mouse button on the display the following options appears.

Illustration: Options Mailsealer

Add passphrase:	A recipient address including encryption record is added.
Edit passphrase:	An existing set of encryption can be changed.
Delete passphrase:	An actual encryption may be deleted.

2.5.1 Add passphrase

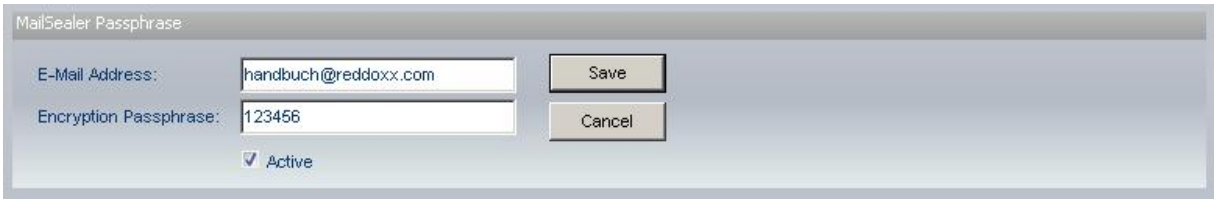

Illustration: Add encryption

Email address:	Here you enter the email address of the recipient
Encryption passphrase:	Here, the password must be set.
Active:	To activate the encryption, the mark must be set.

2.6 User settings

In the user settings, you can set the profile, email addresses, and the filter lists.

2.6.1 Profile

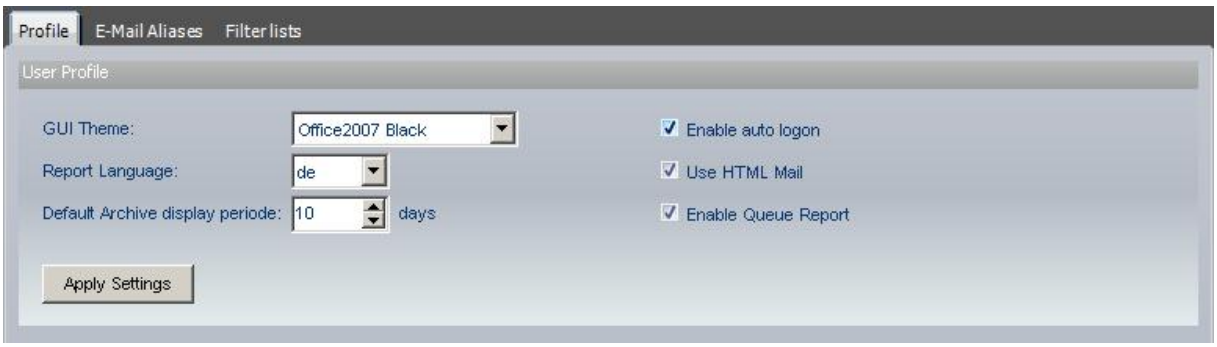

Illustration: User settings profile

GUI theme:	The view of the GUI can be adjusted by selecting different themes.
GUI language:	The language of the GUI can be adapted accordingly. There are German, English, Dutch, and Italian to choose from.
Default archive display Period:	The number of days determines which last filing period is displayed.
Enable auto logon:	The automatic login is enabled. The user only needs the first time his login data. After this the log on happens with this data automatically.
Use HTML mail:	The quarantine report will be sent in HTML format.
Enable queue report:	The queue report is activated.

2.6.2 Email aliases

Email aliases are the different email addresses, which are assigned to a user. In this area the opportunity is to add, edit or delete aliases.

Illustration: Options email alias

Add: With this option other email aliases can be added. You will need a Request ID, which you will receive by the associated user.

Illustration: Add alias

Email address: Enter the new email address. Then you will receive a notification to this address, which must be confirmed by the request ID.

Request ID: Enter the request ID. The Request ID protects against abuse, so that unauthorized persons cannot assign the queue of others.

Please note the correct spelling of the email address, otherwise the request ID can not be delivered.

Edit: The filter profile and the Deputy Director for spam and archive management can be changed and adjusted.

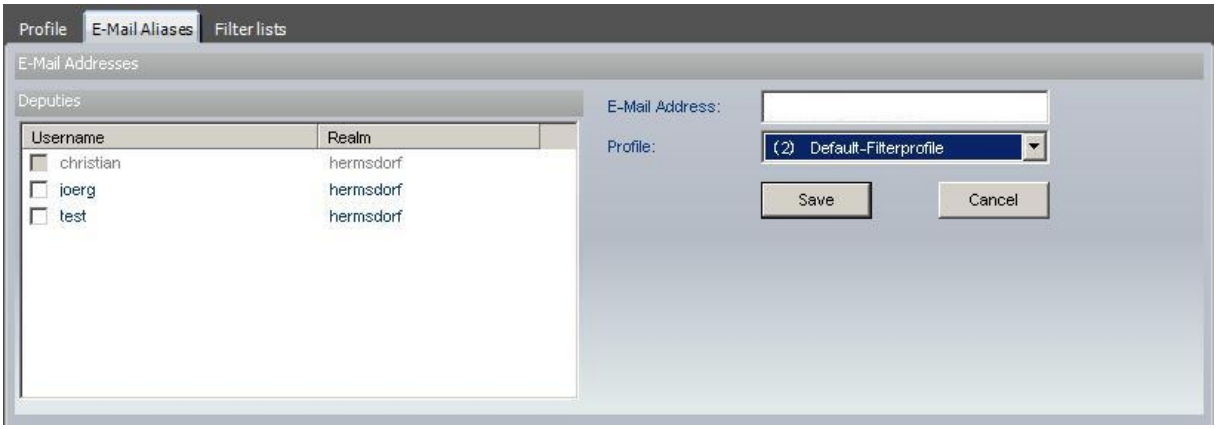

Illustration: edit alias

Delete: The selected alias can be deleted. An additional request is to prevent accidental erasure.

Illustration: delete alias

Set primary address: The selected email address is used as a primary set.

2.6.3 Filter lists

In the filter lists it is possible to set addresses, domains, and subject to trusted and untrustworthy.

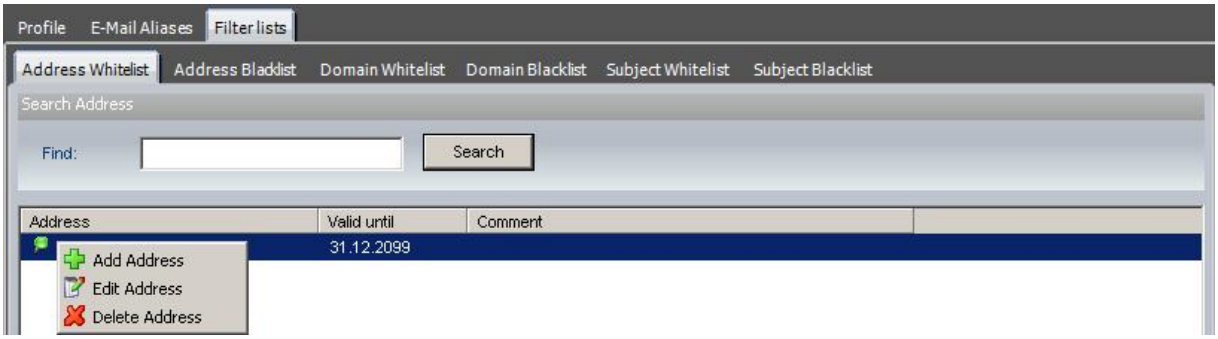

Illustration: Filter lists

The filter lists are divided into the following areas:

> The approach of adding on domains and subject is the same.

Address Whitelist:	email address is trusted.
Address Blacklist:	email address is untrustworthy.
Domain Whitelist:	email domain is trusted.
Domain Blacklist:	email domain is untrustworthy.
Subject Whitelist:	emails with this subject are trusted.
Subject Blacklist:	emails with this subject are untrustworthy.

There are the possibilities to add, edit and delete whitelist- and blacklist entries.

Add whitelist

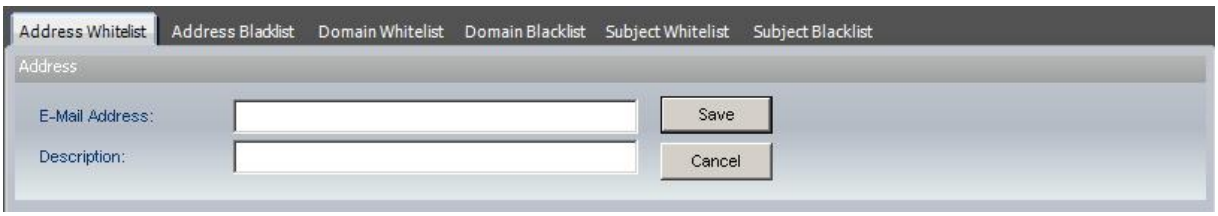

Illustration: Add whitelist

Email address:	Add the email address of a trusted sender.
Description:	A description can be given.

Add blacklist

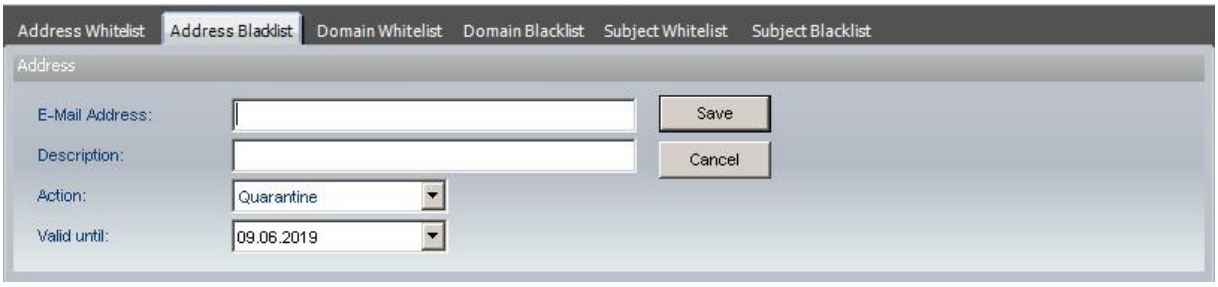

Illustration: Add blacklist

Email address:	Add the email address of the sender you want to block.
Description:	A description can be given for this entry.

If automatic login is enabled and an employee wants to login as a different user, the employee must after the auto-subscribe unsubscribe to arrive the registration menu.

Action:	Which action should be performed if the above given address matches.

There are 3 types:

Quarantine:	The email will be postponed to the quarantine list.
Tag:	The email will be delivered to the recipient with a mark in the subject.
Decline:	The email will not be accepted from Reddoxx.

Valid until:	The validity of this entry is determined.

2.7 Logout

The user will be logged out from the user-GUI.

3 Glossary

A

ABL Filter:

Address blacklist filter – checking the sender address against a list maintained in the Spamfinder. The entries can be made both user-related as well as company-wide. The lists are maintained manually by the administrator or the user.

Advanced RBL Filter:

Advanced Realtime Blacklist Filter - All email servers involved in the transport of the incoming mail are checked against public blacklist servers. We do not assume any guarantee for the function of the selected blacklist servers as well as the absence of errors in the list entries on the blacklist servers.

Appliance:

The appliance is the hardware component of the Spamfinder - the REDDOXX Appliance. There are three variants of the REDDOXX Appliance. This ensures that the demands of all sizes of companies and email traffic are covered optimally. Observe the warning and safety notices!

AWL Filter:

Domain whitelist filter – checking the sender address against a list maintained in the Spamfinder. The entries can be made both user-related as well as company-wide. Some filters establish this list automatically. The lists are further maintained manually by the administrator or the user.

B

Bayes Filter:

Via the content check, the Bayes filter determines the spam probability. Spamfinder automatically establishes the word lists. We do not assume any liability for wrong detection.

C

CISS:

Confirmation Interactive Site Server, in short CISS, is a unique, several stage control process, which ensures the permanent exchange of wanted mails between sender and receiver. Intelligent authorization of the sender by means of CISS (registered for patent), a unique challenge/response-functionality.

CISS Filter:

Confirmation Interactive Site Filter – This method ensures that the sender is a natural person. For this purpose, a corresponding Internet page is provided via the Spamfinder portal, which is accessible in the Internet. The availability of the Spamfinder portal is at least 98.5% per year.

Cluster:

A cluster denotes a number of networked computers. These networked computers are available for parallel processing. Partial tasks belonging to a task are processed. Contrary to parallel computers, the load distribution takes place on the level of individual processes

started on one or several machines in the cluster. You therefore do not require parallel software or special operating systems but instead a scheduler that assigns the partial tasks to the individual computers. Alternatively, clusters are also used to increase the availability of systems.

Console:

Software component the REDDOXX Appliance is controlled by.

D

DBL Filter:

Domain blacklist filter – checking the sender domain against a list maintained in the Spamfinder. The entries can be made both user-related as well as company-wide. The lists are maintained manually by the administrator or the user.

DMZ:

A DMZ means demilitarized zone. A DMZ is an intermediate network that is formed at network interfaces but does not belong to either of the networks. It represents an inherent network that is not as heavily secured as the network that is actually to be protected. With simple security gateways, DMZ is usually generated at a third interface of the package filter. If the security gateway consists of a package filter - application level gateway - package filter, another interface of the application level gateway (ALG) usually serves as DMZ interface. If package filters or ALG have more than three interfaces, additional DMZ can be formed.

DNS:

The Domain Name System (DNS) is one of the most important services in the Internet. The DNS is a distributed database that manages the name space in the Internet.

Domain:

A domain is a coherent section of the hierarchic DNS name space. Starting from its domain name, a domain always comprises the entire subordinate tree structure.

DWL Filter:

Domain whitelist filter – authorizing the sender domain against a list maintained in the Spamfinder. The entries can be made both user-related as well as company-wide. The lists are maintained manually by the administrator or the user.

F

Failover:

A failover denotes a technology in the IT sector that serves to keep data and services highly available.

H

Host name:

The host name of the REDDOXX Appliance in the network.

L

LDAP:

LDAP (Lightweight Directory Access Protocol) is a network protocol applied for so-called directories. It handles the communication between the LDAP client (e.g. with a mail server or a digital address book) and the directory server. It offers all log-specific functions required for such communication: registration on the server, the search query and data modification.

M

Mail Hop:

Mail hop is when an email is transferred from one server to another. Each of these servers is regarded as a mail hop.

N

NBL Filter:

Network blacklist filter - Checking the IP address of the email server against a list maintained in the Spamfinder. The entries can be made both user-related as well as company-wide. The lists are maintained manually by the administrator or the user.

NWL Filter:

Network whitelist filter - Authorization of the IP address of the email server against a list maintained in the Spamfinder. The entries can be made both user-related as well as company-wide. The lists are maintained manually by the administrator or the user.

O

OS:

Operating System.

Q

Quarantine:

For all authorized users, the REDDOXX Appliance contains quarantine mailboxes, which can be set up individually. Together with the achieved false positive rates, this feature enables you to achieve the conformity with the valid laws.

R

RAID:

A RAID system (Redundant Array of Inexpensive Disks, often also Redundant Array of Independent Disks) serves to organize several physical hard disks of a computer to form a powerful and safe logical drive.

RBL Filter:

Realtime Blacklist Filter - The sending email servers are checked against public blacklist servers. We do not assume any guarantee for the function of the selected blacklist servers as well as the absence of errors in the list entries on the blacklist servers.

Realm:

A realm is a section similar to a domain where you authenticate yourself. (Also see the chapter: "User Administration - Login Configuration")

RVC Filter:

Recipient Verify Check Filter - To protect the local email server from "spam floods", the recipient address is checked by asking the respective email server, whether the recipient is known. This function is currently available for Microsoft Exchange Server as of version 5.5.

S

SBL Filter:

Subject Blacklist Filter – Checking the email subject against a list maintained in the Spamfinder. The entries can be made both user-related as well as company-wide. The lists are maintained manually by the administrator or the user.

SMTP:

Simple Mail Transfer Protocol. This protocol enables you to fit out an email with a bit more than just sending it "as is"! The protocol has several function options. On the one hand, SMTP lets your emails go straight to the receiver and on the other hand SMTP enables routing your emails via different servers, so-called MTA, to the recipient. Almost all email clients use this protocol to send electronic mail.

SRC Filter:

Sender Receive Check Filter - Checks whether the sender would also accept an email. Wrong detection, e.g. with newsletters or other automatically generated emails, cannot be ruled out, but prevented by making the respective entries in the positive lists.

SWL Filter:

Subject Whitelist Filter – Authorization of the email subject against a list maintained in the Spamfinder. The entries can be made both user-related as well as company-wide. The lists are maintained manually by the administrator or the user.

T

TCP/IP:

Transmission Control Protocol / Internet Protocol. TCP/IP is the protocol that controls the connections/data exchange between computers in the Internet. When transmitting information, TCP divides the sent data into small packages, gives them a check sum (transmission safety) and numbers them consecutively (to ensure that the packages are reassembled again in the correct sequence). The TCP packages also contain the addresses of sender and receiver (IP addresses).

V

Virus Scanner:

The virus scanner checks the attachments of all emails for viruses. Packed files are temporarily unpacked and checked. Emails in which a virus was detected are saved in a quarantine section. Only the administrator has access to this section. Your Spamfinder obtains the virus signatures directly from the scanner manufacturer (ClamAV). We do not assume any guarantee for the topicality of the signature files as well as the availability of the signature server. We do not assume any liability for damage caused by undetected viruses.