This manual was prepared with great care. However, SfbIT GmbH and the author cannot assume any legal or other liability for possible errors and their consequences.

No responsibility is taken for the details contained in this manual. Subject to alternation without notice. SfbIT GmbH does not enter into any responsibility in this respect. The hardware and software described in this manual is provided on the basis of a license agreement.

This manual is protected by copyright law. SfbIT GmbH reserves all rights, especially for translation into foreign languages. No part of this manual may be reproduced in any way (photocopies, microfilm or other methods) or transformed into machine-readable language without the prior written permission of SfbIT GmbH. The latter especially applies for data processing systems.

SfbIT GmbH also reserves all communication rights (lectures, radio and television).

The hardware and software names mentioned in this manual are most often the registered trademarks of the respective manufacturers and as such are subject to the statutory regulations. Product and brand names are the property of SfbIT GmbH.

This issue replaces all earlier ones and orients itself on the appliance with respect to naming.
Table of Contents

1 REDDOXX Manual 10
   1.1 Symbolism and Highlights 10
   1.2 General Warning and Safety Notices 11
   1.3 General Function Scope 13

2 The REDDOXX Appliance 14
   2.1 The REDDOXX Appliance - Basic 16
   2.2 The REDDOXX Appliance - Entry 18
   2.3 The REDDOXX Appliance - SMB 20
   2.4 The REDDOXX Appliance - Medium 20
   2.5 Technical Data 21
   2.6 Delivery Scope 22

3 First Steps 23
   3.1 General Information 23
      3.1.1 Function Description 23
      3.1.2 Integration and Commissioning 23
      3.1.3 Firewall - Port List 25
   3.2 Brief Instructions for the Basic Configuration 26
      3.2.1 Connection and Network Configuration 26
      3.2.2 Login 26
      3.2.3 Basic Configuration 28

4 The Administrator Console 35
   4.1 Appliance Configuration 37
      4.1.1 Network Settings 37
         4.1.1.1 Network Settings - General 37
         4.1.1.2 Network Settings - Network 39
         4.1.1.3 Network Settings - Routing 40
         4.1.1.4 Network Settings - Time Server 41
      4.1.2 Settings 42
         4.1.2.1 Settings - General 42
         4.1.2.2 Settings - SMTP 44
         4.1.2.3 Settings - Limits 45
         4.1.2.4 Settings - Queues 47
         4.1.2.5 Settings - Advanced 49
      4.1.3 SMTP Configuration 50
         4.1.3.1 Local Internet Domains 50
         4.1.3.2 Local Networks 56
4.1.3.3 E-mail transport 57
4.1.3.4 Blocked IP Addresses 58

4.1.4 Backup and Restore 59
4.1.4.1 Backup Settings 59
4.1.4.2 Restore Backup 61

4.2 Appliance Administration 62
4.2.1 Mail Queues 62
4.2.1.1 Incoming Mails 62
4.2.1.2 Outgoing Mails 63

4.2.2 User Administration 64
4.2.2.1 Users 64
4.2.2.2 Groups 69
4.2.2.3 E-mail Aliases 71
4.2.2.4 Realm 73
4.2.2.5 Policies – Group Policies 77

4.2.3 Notification 82
4.2.4 Logs 86
4.2.5 Updates 88
4.2.6 Sessions 91
4.2.7 Services 91
4.2.7.1 Overview 91
4.2.7.2 Mail Flow 91
4.2.7.3 SMTP Server Service 92
4.2.7.4 SMTP Client Service 92
4.2.7.5 Control Server Service 92
4.2.7.6 Message Validation Service 92
4.2.7.7 Task Scheduler Service 92
4.2.7.8 Portal Communication Service 93
4.2.7.9 Remote Support Service 93
4.2.7.10 Starting, Stopping and Restarting Services 93

4.3 REDDOXX Spamfinder 94
4.3.1 Spamfinder Queues 94
4.3.2 Filters 97
4.3.2.1 Whitelist Filters 98
4.3.2.2 Blacklist Filters 98
4.3.2.3 Content Filters 99
4.3.2.4 Global Filters 99
4.3.2.5 CISS 100
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.2.6 Filter Settings</td>
<td>102</td>
</tr>
<tr>
<td>4.3.2.7 Filter Profiles</td>
<td>108</td>
</tr>
<tr>
<td>4.3.2.8 Blocking and Admitting</td>
<td>115</td>
</tr>
<tr>
<td><strong>4.4 REDDOXX MailDepot</strong></td>
<td>122</td>
</tr>
<tr>
<td>4.4.1 Archive Configuration</td>
<td>122</td>
</tr>
<tr>
<td>4.4.1.1 MailDepot Archive Data</td>
<td>123</td>
</tr>
<tr>
<td>4.4.1.2 MailDepot Filter Settings</td>
<td>124</td>
</tr>
<tr>
<td>4.4.2 Archive List</td>
<td>125</td>
</tr>
<tr>
<td><strong>4.5 REDDOXX MailSealer Light</strong></td>
<td>127</td>
</tr>
<tr>
<td>4.5.1 Ad-Hoc Encryption</td>
<td>127</td>
</tr>
<tr>
<td>4.5.2 Permanent Encryption</td>
<td>129</td>
</tr>
<tr>
<td>4.5.3 MailSealer Gateways</td>
<td>129</td>
</tr>
<tr>
<td>4.5.4 MailSealer Light Configuration</td>
<td>129</td>
</tr>
<tr>
<td><strong>5 Options in the Menu Bar</strong></td>
<td>131</td>
</tr>
<tr>
<td>5.1 System Login/Logout</td>
<td>131</td>
</tr>
<tr>
<td>5.1.1 Logging in (Connection)</td>
<td>131</td>
</tr>
<tr>
<td>5.1.2 Logging off (disconnect)</td>
<td>132</td>
</tr>
<tr>
<td>5.1.3 Exiting the Program</td>
<td>132</td>
</tr>
<tr>
<td><strong>5.2 View</strong></td>
<td>132</td>
</tr>
<tr>
<td>5.2.1 Search</td>
<td>133</td>
</tr>
<tr>
<td>5.2.2 Log</td>
<td>133</td>
</tr>
<tr>
<td>5.2.3 Status</td>
<td>133</td>
</tr>
<tr>
<td>5.2.4 Statistic</td>
<td>133</td>
</tr>
<tr>
<td>5.2.5 Starting the Log Viewer</td>
<td>135</td>
</tr>
<tr>
<td>5.2.6 CISS Manager</td>
<td>135</td>
</tr>
<tr>
<td>5.2.6.1 Configuring CISS - Creating Themes</td>
<td>135</td>
</tr>
<tr>
<td>5.2.6.2 Configuring CISS - Adding Images</td>
<td>137</td>
</tr>
<tr>
<td>5.2.6.3 Configuring CISS - Adding Languages</td>
<td>137</td>
</tr>
<tr>
<td>5.2.6.4 Configuring CISS - Adding Domains</td>
<td>139</td>
</tr>
<tr>
<td><strong>5.3 Language</strong></td>
<td>139</td>
</tr>
<tr>
<td><strong>5.4 Appliance</strong></td>
<td>140</td>
</tr>
<tr>
<td>5.4.1 Restarting the REDDOXX Appliance</td>
<td>140</td>
</tr>
<tr>
<td>5.4.2 Turning the REDDOXX Appliance off</td>
<td>140</td>
</tr>
<tr>
<td>5.4.3 Setting the Time/Date</td>
<td>141</td>
</tr>
<tr>
<td>5.4.4 Setting the Backup Configuration</td>
<td>141</td>
</tr>
<tr>
<td>5.4.5 Setting &quot;Restore Configuration&quot;</td>
<td>141</td>
</tr>
<tr>
<td><strong>5.5 Info</strong></td>
<td>142</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>5.5.1 License Information</td>
<td>142</td>
</tr>
<tr>
<td><strong>6 The Appliance Console</strong></td>
<td>145</td>
</tr>
<tr>
<td>6.1 Appliance Settings</td>
<td>146</td>
</tr>
<tr>
<td>6.1.1 Network Settings</td>
<td>146</td>
</tr>
<tr>
<td>6.1.2 Time Server Settings</td>
<td>147</td>
</tr>
<tr>
<td>6.1.3 Backup and Restore Settings</td>
<td>147</td>
</tr>
<tr>
<td>6.2 Backup and Restore</td>
<td>148</td>
</tr>
<tr>
<td>6.2.1 Backup and Restore Settings</td>
<td>148</td>
</tr>
<tr>
<td>6.2.2 Start an Appliance Backup</td>
<td>149</td>
</tr>
<tr>
<td>6.2.3 Start an Appliance Restore</td>
<td>149</td>
</tr>
<tr>
<td>6.2.4 Synchronize REDDOXX MailDepot</td>
<td>150</td>
</tr>
<tr>
<td>6.3 Advanced Options</td>
<td>151</td>
</tr>
<tr>
<td>6.3.1 Rebuild the full text index of the Maildepot</td>
<td>152</td>
</tr>
<tr>
<td>6.3.2 Set Appliance Settings to Factory Defaults</td>
<td>153</td>
</tr>
<tr>
<td>6.3.3 Set Spamfinder Settings to Factory Defaults</td>
<td>153</td>
</tr>
<tr>
<td>6.3.4 Re-Create Database</td>
<td>153</td>
</tr>
<tr>
<td>6.3.5 Clear MailDepot</td>
<td>154</td>
</tr>
<tr>
<td>6.4 Start and Stop Services</td>
<td>155</td>
</tr>
<tr>
<td>6.4.1 Start REDDOXX Engine</td>
<td>155</td>
</tr>
<tr>
<td>6.4.2 Start REDDOXX Remote Support</td>
<td>155</td>
</tr>
<tr>
<td>6.4.3 Appliance Reboot</td>
<td>155</td>
</tr>
<tr>
<td>6.4.4 Appliance Shutdown</td>
<td>156</td>
</tr>
<tr>
<td>6.5 Change Admin Password</td>
<td>156</td>
</tr>
<tr>
<td><strong>7 FAQ - Frequently Asked Questions</strong></td>
<td>157</td>
</tr>
<tr>
<td><strong>8 Appendix</strong></td>
<td>159</td>
</tr>
<tr>
<td>8.1 Contact and Support</td>
<td>159</td>
</tr>
<tr>
<td>8.2 Deinstallation and Disposal</td>
<td>159</td>
</tr>
<tr>
<td>8.3 License Agreements</td>
<td>160</td>
</tr>
<tr>
<td><strong>9 Glossary</strong></td>
<td>164</td>
</tr>
<tr>
<td><strong>10 Index</strong></td>
<td>169</td>
</tr>
</tbody>
</table>
1 REDDOXX Manual

1.1 Symbolism and Highlights

This manual is geared towards the administrator of the REDDOXX Appliance. For better legibility, please note that the term "Administrator" refers to both male and female administrators.

Please read the entire manual carefully to ensure professional application of the REDDOXX Appliance. This is the only way we can ease your work with the REDDOXX Appliance.

In the glossary, you will find a compilation of the terminology used in this documentation together with its respective explanations

The typography used in this manual has the following meaning:

<table>
<thead>
<tr>
<th><strong>DANGER/WARNING</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>All warning and safety notices in this manual are marked this way. Always observe the instructions so there will be no damage to persons and/or objects.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>NOTICE</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>A notice or tip points out especially important and helpful information about the REDDOXX Appliance. The REDDOXX Appliance can only function correctly and error-free when it is transported, stored, installed, operated and maintained in line with the manufacturer's instructions.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>HIGHLIGHTE</strong></th>
<th><strong>EXAMPLE</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Tab</td>
<td>&quot;Name of the tab&quot;</td>
</tr>
<tr>
<td>Field name</td>
<td>Name of the field</td>
</tr>
<tr>
<td>Buttons</td>
<td>BUTTON</td>
</tr>
<tr>
<td>Selection list</td>
<td>List entry</td>
</tr>
<tr>
<td>List entry in list view</td>
<td>'Entry'</td>
</tr>
</tbody>
</table>

Also see: Refers to a chapter.

Names

Explanation of the respective name
1.2 General Warning and Safety Notices

This manual contains warning and safety notices, which serve for your own protection but also for the protection of the REDDOXX Appliance. In order not to endanger your safety, you have to observe the following basic conditions for the installation, use and operation of the REDDOXX Appliance.

The notices in this manual are highlighted as follows:

**DANGER**

Omitting precautions and safety measures may lead to severe health damage, injury to persons or even death.

**WARNING**

Only expert personnel is allowed to operate the appliance or remedy possible errors in the hardware. Expert personnel are qualified persons authorized to commission and maintain the device, program the control, operate the hardware according to the safety instructions pursuant to the valid standards and have a corresponding qualification.

**NOTICE**

Observe the settings you perform in the REDDOXX Appliance. All setting you make are saved by the REDDOXX Appliance, not the REDDOXX Console. The Console is only the input mask. You will find these notices exclusively in the content of the manual.

Read the warning and safety instructions carefully before commissioning the REDDOXX Appliance.

**DANGER/WARNING**

Observe all instructions attached to the REDDOXX Appliance and listed in this manual.

Prior to cleaning the REDDOXX Appliance, pull the mains plug. Do not use any liquid cleaning agents or agents containing aerosols. Only use a damp cloth for cleaning.

Do not use the REDDOXX Appliance near water. Do not spill any liquid on or into the REDDOXX Appliance.

Place the REDDOXX Appliance on a stable surface.

There are ventilation openings in the casing. These openings may not be obstructed or covered. Do not place the REDDOXX Appliance next to or on top of a radiator.

Only use the power source stated at the mains connection. If you are not sure about the kind of power source you have, contact your local energy supply company.

Do not walk on the cable and do not put anything on it.

If you are using an extension cord for the REDDOXX Appliance, make sure that the total amperage or all devices connected to this extension cord does not exceed the admissible amperage for the extension cord.
Do not insert any objects into the ventilation slots of the REDDOXX Appliance.

Do not attempt to service your REDDOXX Appliance yourself with the exception of the cases explained in this manual. Only use the controls mentioned in these instructions. If you open covers with the notice "Warranty void if broken", you may expose yourself to high voltage or other risks. Leave the maintenance of these parts up to expert personnel.

In the following cases, pull the mains plug of the REDDOXX Appliance out of the outlet and let expert personnel service the REDDOXX Appliance.
- The cables or the plug are damaged.
- Liquid was poured into the REDDOXX Appliance.

Despite following the instructions, the REDDOXX Appliance does not work properly.
The REDDOXX Appliance was dropped or the casing is damaged.
- The REDDOXX Appliance shows substantial performance changes.

Always transport the REDDOXX Appliance carefully. Impact stress or dropping can also damage the inside of the device. Do not operate damaged devices!
1.3 General Function Scope

Thank you for purchasing the REDDOXX Appliance and the corresponding appliance console. The REDDOXX Appliance is an innovative product for the reliable, active and individual prevention of spam problems and legally conform e-mail archiving. In addition, you can also send critical business data and sensitive information in encrypted form to your business partners, so that unauthorized persons cannot read even intercepted mails. With the REDDOXX Appliance, you protect your company from technical and economic damage as well as image damage.

The REDDOXX Appliance filters undesired mail out right from the start. You save a lot of time, because viruses, worms and Trojans cannot penetrate your active network. The REDDOXX Appliance is simply switched before the e-mail server and geared exactly towards the individual requirements of your company.

Our solution is just as unusual as it is successful:
Contrary to the standard approach "filtering out what is not desired", the REDDOXX Appliance pursues the proactive way: "pre-define what you want!"

The REDDOXX Appliance is an optimally coordinated software and hardware unit, which only selects and forwards desired e-mails immediately. It is installed between the firewall and the e-mail server and therefore only requires a minimum interference with your company's IT.

The REDDOXX Appliance immediately solves four major problems:

1. What's spam for one is a relevant mail for the other. This is why the REDDOXX Appliance selects the desired mails and determines the relevance of the mail with the authorization of the sender in case of doubt.

2. With pre-definition, additional filters and the interactive authorization of the e-mail sender, the REDDOXX Appliance offers the highest chances for success in spam combating and achieves the highest degree of satisfaction for the applicant.

3. Archiving of all e-mails through MailDepot:
   1. Organizational transparency and increased productivity.
   2. Prevention of accidental or intentional deletion of relevant mails.
   3. Increased time resources for administrators and users through user-defined access options to archived e-mails.

4. Encrypted e-mail transmission with MailSealer
2 The REDDOXX Appliance

Information about the REDDOXX Appliances

We offer you the custom-tailored solution for your company. In doing so, we consider your individual requirements ranging from the current number of workplaces up to the further development of your company. The different versions ensure that the REDDOXX Appliance meets all the requirements of small, medium and large-sized companies.

The REDDOXX Appliance has a modular structure: It consists of the products

- REDDOXX Spamfinder
- REDDOXX MailDepot
- REDDOXX MailSealer

The REDDOXX Appliance is available in the following versions:

- Basic
- Entry
- SMB
- Medium

REDDOXX general:

- Simple structure for fast application within minutes; at the same time compatible with all standardized e-mail servers.
- Secure, hardened Linux kernel.
- Powerful virus protection through Norman Sandbox technology

REDDOXX Spamfinder:

- Powerful spam filtering including CISS technology, which provides a spam reduction rate of almost 100%.
- Innovative Advanced Realtime Blacklist Filter, Whitelist Filter as well as additional statistic filters and further content filters as well as Blacklist Filter technologies.
- Possibility to generate automated and external backups.

REDDOXX MailDepot:
2. The REDDOXX Appliance

- Automatic audit and manipulation-proof archiving of all e-mails
- Organizational transparency and increased productivity.

The REDDOXX Appliance is installed between the firewall and the e-mail server and therefore only requires a minimum interference with your company’s IT.

REDDOXX MailSealer:

- Fast encryption and signing of e-mails
- compatible with all standard e-mail programs
- supports S/MIME and PGP
- automatic PKI linkup

**NOTICE**

For the hardware data, refer to the chapter "REDDOXX Appliance - Technical Data" in the documentation of your REDDOXX Appliance.
2.1 The REDDOXX Appliance - Basic

The REDDOXX Appliance Basic is suited for the demands of small and medium-sized companies.

Illustration: REDDOXX Appliance - Basic

Function description of the REDDOXX Appliance's LEDs

<table>
<thead>
<tr>
<th>LED</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. General</td>
<td>Power on/off switch</td>
</tr>
<tr>
<td></td>
<td>operating status</td>
</tr>
<tr>
<td></td>
<td>Hard disk activity</td>
</tr>
</tbody>
</table>

Illustration: LED function description
Connections of the REDDOXX Appliance - Basic

COMPONENTS | HOW TO CONNECT THE REDDOXX APPLIANCE CORRECTLY
---|---
1. REDDOXX Appliance | Connect the REDDOXX Appliance (1) with the mains plug (1).
2. Mains plug | Insert the mains plug (1) into a suitable outlet.
3. Network cable | Plug your network cable into LAN-1(2).

A On/Off switch | Turn the REDDOXX Appliance on. (front side)

B Serial connection | Connection presently not used.

C Monitor connection | Only for maintenance purposes

D USB | Only for maintenance purposes

F Serial connection (COM1) | Connection presently not used.

G Network connections (LAN1-4) | Connection LAN1 presently in use and active. Connection LAN2-4 currently not used.

**ATTENTION**

Observe all warning and safety notices as well as all other relevant information about the proper handling of the REDDOXX Appliance.
2.2 The REDDOXX Appliance - Entry

The REDDOXX Appliance Entry is suited for the demands of small companies.

- 19” rack in 1U form factor, also suited for multi-media racks as the Appliance is a shortrack platform.

Illustration: REDDOXX 19” Rack mount version, models ENTRY, SMB and MEDIUM

Function description of the REDDOXX Appliance's LEDs

<table>
<thead>
<tr>
<th>LED / BUTTON</th>
<th>MEANING</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Button</td>
<td>On/off switch</td>
</tr>
<tr>
<td>2. Button</td>
<td>Reset</td>
</tr>
<tr>
<td>3. General</td>
<td>Operating status</td>
</tr>
<tr>
<td>4. General</td>
<td>Hard disk activity</td>
</tr>
<tr>
<td>5. Network</td>
<td>Network connections</td>
</tr>
<tr>
<td>6. General</td>
<td>Temperature display</td>
</tr>
</tbody>
</table>
Connections of the REDDOXX Appliance

<table>
<thead>
<tr>
<th>COMPONENTS</th>
<th>HOW TO CONNECT THE REDDOXX APPLIANCE CORRECTLY</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. REDDOXX Appliance</td>
<td>Connect the REDDOXX Appliance (1) with the mains plug (2).</td>
</tr>
<tr>
<td>2. Mains plug</td>
<td>Insert the mains plug (2) into a suitable outlet.</td>
</tr>
<tr>
<td>3. Network cable</td>
<td>Plug in the network cable (3)</td>
</tr>
<tr>
<td>A  Network connection</td>
<td>Connect the mains connection (E) with the mains plug (2).</td>
</tr>
<tr>
<td>B  PS2 connection</td>
<td>Connection presently not used.</td>
</tr>
<tr>
<td>C  PS2 connection</td>
<td>Connection presently not used.</td>
</tr>
<tr>
<td>D  USB</td>
<td>Only for maintenance purposes</td>
</tr>
<tr>
<td>E  Parallel connection</td>
<td>Connection presently not used.</td>
</tr>
<tr>
<td>F  Serial connection</td>
<td>Connection presently not used.</td>
</tr>
<tr>
<td>G  Monitor connection</td>
<td>Only for maintenance purposes</td>
</tr>
<tr>
<td>H  Network connections (LAN1-2)</td>
<td>Connection LAN1 presently in use and active. Connection LAN2 presently not used.</td>
</tr>
</tbody>
</table>

**ATTENTION**

Observe all warning and safety notices as well as all other relevant information about the proper handling of the REDDOXX Appliance.
2.3 The REDDOXX Appliance - SMB

We have developed this version to meet the demands of small and medium-sized companies.

- 19" rack in 1U form factor, also suited for multi-media racks as the Appliance is a shortrack platform.
- RAID1 for e-mail queues to ensure sophisticated operational safety.

For an image of the REDDOXX SMB as well as the function description of the LEDs and connections, see page 19.

2.4 The REDDOXX Appliance - Medium

Designed for companies in the enterprise sector that require the corresponding performance of such an appliance.

- 19" rack in 1U form factor, also suited for multi-media racks as the Appliance is a shortrack platform.
- RAID1 for e-mail queues to ensure sophisticated operational safety.

For an image of the REDDOXX SMB as well as the function description of the LEDs and connections, see page 19.
## 2.5 Technical Data

<table>
<thead>
<tr>
<th>REDDOXX</th>
<th>Basic</th>
<th>ENTRY</th>
<th>SMB</th>
<th>Medium</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capacity e-mail queues</td>
<td>15 GB</td>
<td>75 GB</td>
<td>75 GB</td>
<td>160 GB</td>
</tr>
<tr>
<td>Standard user number</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Number of recommended users</td>
<td>50</td>
<td>100</td>
<td>250</td>
<td>750</td>
</tr>
<tr>
<td>RAID (Level)</td>
<td>n.a.</td>
<td>n.a.</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Professional virus protection</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Quarantine for each user individually</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Automated update</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Hardened, safe OS</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Compatible with all e-mail servers</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>RAM</td>
<td>256 MB</td>
<td>256 MB</td>
<td>512 MB</td>
<td>2 GB</td>
</tr>
<tr>
<td>Processor</td>
<td>INTEL Celeron 1 GHz</td>
<td>INTEL PENTIUM 4 3 GHz</td>
<td>INTEL PENTIUM 4 3 GHz</td>
<td>INTEL PENTIUM 4 3.4 GHz</td>
</tr>
<tr>
<td>Design</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dimensions (W x H x D)</td>
<td>242 x 60 x 150 mm</td>
<td>485 x 44 x 410 mm</td>
<td>485 x 44 x 410 mm</td>
<td>485 x 44 x 410 mm</td>
</tr>
<tr>
<td>Weight</td>
<td>1.9 kg</td>
<td>6.4 kg</td>
<td>6.5 kg</td>
<td>6.5 kg</td>
</tr>
<tr>
<td>Voltage</td>
<td>100-240 V</td>
<td>100-240 V</td>
<td>100-240 V</td>
<td>100-240 V</td>
</tr>
<tr>
<td>Input current / frequency</td>
<td>5-3A / 50-60 Hz</td>
<td>5-3A / 50-60 Hz</td>
<td>5-3A / 50-60 Hz</td>
<td>5-3A / 50-60 Hz</td>
</tr>
<tr>
<td>Operating temperature</td>
<td>10°-40°C</td>
<td>10°-35°C</td>
<td>10°-35°C</td>
<td>10°-35°C</td>
</tr>
<tr>
<td>Rel. humidity</td>
<td>8-90% non-condensing</td>
<td>8-90% non-condensing</td>
<td>8-90% non-condensing</td>
<td>8-90% non-condensing</td>
</tr>
<tr>
<td>Certification</td>
<td>CE</td>
<td>CE</td>
<td>CE</td>
<td>CE</td>
</tr>
</tbody>
</table>
2.6 Delivery Scope

Prior to the installation, check your delivery for completeness. The delivery contains the following products:

- REDDOXX Appliance
- Software for the REDDOXX consoles on CD
- Administrator console
- User console

**NOTICE**

The latest version of the REDDOXX software as well as the manuals can be downloaded in the support section at http://support.reddoxx.net

Receipt

Check the product for damages upon receipt.

If you notice any apparent damage upon delivery or when unpacking the merchandise, contact your retailer.

**WARNING**

Always transport the device carefully. Impact stress or dropping can also damage the inside of the device. Do not operate damaged devices!
3 First Steps

3.1 General Information

This chapter is supposed to help you with putting the REDDOXX Appliance into operation and contains all steps required to ready the REDDOXX Appliance for operation. First we will show you in a diagram where to install the REDDOXX Appliance. The additional chapters then deal with the connection, registration, basic configuration and operation of your REDDOXX Appliance.

3.1.1 Function Description

The REDDOXX Appliance behaves like a e-mail server vis-à-vis the sender. The first filters already become active while the connection between the sending e-mail server and the REDDOXX Appliance is being established. Depending on the filter settings, the REDDOXX Appliance may already reject e-mails at this stage.

Also see: "Filters"

The REDDOXX Appliance can manage several e-mail domains and forward the respective e-mails to the different e-mail servers in your company.

3.1.2 Integration and Commissioning

The standard system consists of one or several e-mail servers and the REDDOXX Appliance, which is installed between the e-mail servers and your firewall, if available.

Illustration: Function diagram of the REDDOXX Appliance
You only need a few steps to put the REDDOXX Appliance into operation.

- Connect the REDDOXX Appliance with the network,
- assign an IP address and
- adjust the routing of the e-mail traffic in such a way that incoming mails are forwarded to the REDDOXX Appliance as early as possible so that it can then take care of the subsequent forwarding.

For more information, refer to the following brief instructions.

**Tip**

For efficiently combating spam, we recommend installing the REDDOXX Appliance directly behind your firewall as a so-called first mailhop. Then the sender establishes the connection directly with the REDDOXX Appliance.

As the REDDOXX Appliance is capable of learning from your actions, we recommend you also direct the outgoing e-mail traffic through the REDDOXX Appliance.
3. First Steps

3.1.3 Firewall - Port List

These ports must be opened for perfect operation of the REDDOXX Appliance:

**SMTP/25 TCP in/out**
For incoming / outgoing e-mails

**DNS/53 UDP/TCP out**
For domain name service requests to your DNS server.

**HTTP/80 TCP out**
For communication with the REDDOXX portal. This is where the license information is checked. Since version 1019, it is possible to activate a remote access for SfbIT's technical support via the REMOTE SUPPORT SERVICE, port 80 on the REDDOXX switching computer (RDXCALL).

Since version 1019, it is possible to activate a remote access for SfbIT's technical support via the REMOTE SUPPORT SERVICE, port 80 on the REDDOXX switching computer (RDXCALL).

**NTP/123 UDP out**
For time leveling with a time server

**SMB 137/138 UDP out, 139 TCP out, CIFS 445 TCP out**
for backup and archiving (mail depot) on a remote Windows/Samba share.

**LDAP/389 TCP out, LDAP/636 out für SSL**
for user authentication and recipient check via Active Directory, OpenLDAP, Novell eDirectory, Lotus Notes Domino.

**LDAP/3268 TCP out**
for higher-performance LDAP queries against a Global Catalog Server.

**REDDOXX/4010 TCP in**
For the user and administrator console of the REDDOXX Appliance.

**Notice**
You should especially pay attention to these ports when the REDDOXX Appliance is included in another network segment, e.g. a DMZ, and separated from the internal LAN through a firewall.
3.2 Brief Instructions for the Basic Configuration

3.2.1 Connection and Network Configuration

Connecting the REDDOXX Appliance

Proceed as follows to integrate the REDDOXX Appliance into your system.

Requirements: Read the warning and safety instructions.

1. Connect the Spamfinder Appliance to the power supply.
2. Connect a monitor and a keyboard.
3. Turn the REDDOXX Appliance on.
   The IP address is 192.168.0.1.
4. Login as user "admin" with the password "SpamfinderAdmin". The administration menu appears. For further details and screenshots, refer to chapter 6 - Appliance Console.
5. Select the item – Settings
6. Select the item – Network
7. Enter the network data. (host name, domain, IP address, netmask, gateway, 1st DNS, 2nd DNS)
8. Press the TAB key to reach OK and press ENTER. Now the network interface is re-initialized.
9. Select BACK to access the main menu.
10. Select EXIT to exit the console program.
11. Connect a network cable (RJ45) and then connect the appliance with your network.
12. Proceed with the configuration of the admin console as described in the following chapter.

NOTICE

For function descriptions and the exact connections of the REDDOXX Appliance, refer to the main chapter 2 and there to the different model variants.

3.2.2 Login

Performing the 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:

Requirements: Purchase of the REDDOXX Appliance with the valid licenses.
1. Copy the content of the REDDOXX CD onto your computer. The files may be copied to any directory of your choice.

2. Double-click on the file \textit{sfadmin.exe}. The login window opens.

3. Enter the corresponding \textit{hostname}.

4. Enter your \textit{user name}.

5. Enter your \textit{password}.

\textbf{NOTICE}

The following standard values are set upon delivery of the REDDOXX Appliance: \textit{User name: sf-admin} and \textit{password: admin}

6. In realm, select the option "local". A realm is a section similar to a domain where you authenticate yourself.

7. Select the desired \textit{language} in the selection list, which you want to use to display your program. The selection contains the currently installed languages.

8. Click on the button \textit{LOGIN}. The welcome window opens.
3. First Steps

9. Click on the button "Setup assistant" to start the assistant for the first configuration of the REDDOXX Appliance.

**Notice**

Only perform the setup assistant once.

### 3.2.3 Basic Configuration

**Making the Network Settings**

To help you with the basic configuration, the setup assistant takes you through all relevant settings.

**Requirements:** The window for the network settings is active.

**Notice**

If the network settings of the appliance were previously configured via the Appliance Console (chapter 3.2), you can simply take over the data listed there.
3. First Steps

Illustration: Basic configuration – network settings

1. Enter the *hostname*.
2. Enter a/your domain.
3. Enter the IP address of the REDDOXX Appliance.
4. Enter the corresponding *subnet mask*.
5. Enter the standard gateway for the Internet connection.
6. Enter at least one *DNS server*.

**NOTICE**

Ensure that the DNS server is accessible, especially if the REDDOXX Appliance is located in a DMZ.

7. To continue the basic configuration, click on the button **NEXT**. **CANCEL**: Reject changes and exit the basic configuration.

**Adding E-Mail Domains**

Via the e-mail domains, you have the possibility to add all domains for which the REDDOXX Appliance is supposed to receive e-mails.

**Requirements**: Window for the e-mail domains is active.
3. First Steps

1. Enter all domains for which you want to receive e-mails.
2. Click on the button ADD.
   The entered e-mail domains are listed in the field e-mail domains.

   **NOTICE**
   Observe the correct spelling of the e-mail domains. The REDDOXX Appliance cannot receive any e-mails for other domains.

3. To continue the basic configuration, click on the button NEXT.
   BACK: Goes back to the previous window.
   CANCEL: Reject changes and exit the basic configuration.

   **NOTICE**
   In order to delete an added domain again, mark the corresponding entry with a mouse click and delete it with the DEL button on your keyboard. This action cannot be undone.

**Add Local Networks**

Via the local networks, you can add all local networks for which the REDDOXX Appliance is supposed to function as e-mail relay. This way, the REDDOXX Appliance cannot be abused as open e-mail relay when e-mails are sent from the inside to the outside via the REDDOXX Appliance.

**Requirements:** Window for local networks is active.
1. Enter the **IP network** which may send mails to the REDDOXX Appliance.

2. Enter the **subnet mask**. With the subnet mask 255.255.255.255, you enter a single host (e.g. 192.168.0.8).

   **NOTICE**

   Instead of an entire network, you can also state individual IP addresses, e.g. that of your mail server. Individual IP addresses must be masked with 255.255.255.255.

3. Click on the button **ADD**.

   The entered local networks are listed in the field Local Networks.

   If you have several e-mail servers in various IP networks, please also add these networks or hosts.

4. To continue the basic configuration, click on the button **NEXT**.

   **BACK**: Goes back to the previous window.

   **CANCEL**: Reject changes and exit the basic configuration.

   **NOTICE**

   In order to delete an added network again, mark the corresponding entry with a mouse click and delete it with the DEL button on your keyboard. This action cannot be undone.

---

**Configuring E-Mail Forwarding**
Via E-Mail Forwarding, you can state where the REDDOXX Appliance is supposed to forward the e-mails to.

**Requirements:** Window for e-mail forwarding is active.

1. **Outgoing e-mails:**
   Enter the FQDN (host name).
   If necessary, activate the option *Forwarding via DNS* if the e-mails are supposed to be delivered via DNS.

2. Activate the option *Authentication required* if the relay server demands authentication.

3. Enter the *user name* and *password* if you have activated this option in step 3.

4. **Incoming e-mails:**
   If necessary, activate the option *Forwarding via DNS* if the e-mails are supposed to be delivered via DNS.

5. Enter an internal e-mail server at *Internal e-mail server*.

**NOTICE**
If you have several internal e-mail servers, you can configure these later per domain.
7. To continue the basic configuration, click on the button NEXT.
   BACK: Goes back to the previous window.
   CANCEL: Reject changes and exit the basic configuration.

Defining E-Mail Addresses
Here is where the e-mail address of the administrator and the REDDOXX Appliance are managed, which the REDDOXX Appliance requires for the forwarding of system messages. The REDDOXX Appliance uses the administrator's e-mail address to communicate with the administrator. The REDDOXX Appliance's e-mail address is used to communicate with the REDDOXX Portal.

Requirements: Window for e-mail addresses is active.

1. In the field Administrator address enter the administrator's e-mail address.
   The administrator address must exist on one of your e-mail servers. At this address, you receive messages concerning innovations (release notes) and updates of the REDDOXX Appliance.

2. In the field REDDOXX address, enter the e-mail address of the REDDOXX Appliance.
3. To finish the basic configuration, click on the button **DONE**.
**BACK:** Goes back to the previous window.
**CANCEL:** Reject changes and exit the basic configuration.
4 The Administrator Console

Information about the Administrator Console

This chapter explains the exact handling of the administrator console. The administrator console was developed to ease the handling of the REDDOXX Appliance. You can supplement or change all settings of the REDDOXX Appliance via the console at any time. Before you access the actual application window of the REDDOXX Appliance console, you have to log in.

Performing the 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:

Requirements: Purchase of the REDDOXX Appliance with the valid licenses.

1. Copy the content of the REDDOXX CD onto your computer.
   The files may be copied to any directory of your choice.

2. Double-click on the file sfadmin.exe.
   The login window opens.

3. Select the corresponding hostname.

4. Enter your user name.

5. Enter your password.

   NOTICE

   The following standard values are set upon delivery of the REDDOXX Appliance:
   User name: sf-admin and password: admin

6. In realm, select the option "local".

7. Select the desired language in the selection list, which you want to use to display your program.
   The selection contains the currently installed languages.
8. Click on the button LOGIN.
   The application window for the basic configuration is now active.

The following application window contains the sections of the administrator console numbered and named:

Illustration: Application window after login

Legend
1. Menu bar
2. Tree view
3. List view
4. Status view
5. Log view
4.1 Appliance Configuration

4.1.1 Network Settings

Open network settings

Requirements: The REDDOXX Appliance must be connected and in operation.

1. In the navigation tree, double-click on Appliance configuration.
2. In the tree, double-click on the branch Network settings.

ATTENTION

You should make a backup before each change and archive this.
Also see: "Options in the Menu Bar"

4.1.1.1 Network Settings - General

Making the Network Configuration

Via the General Configuration, you can set up the hostname and the DNS servers.

Requirement: Opening the Appliance Configuration

1. Click on the tab "General"

The following fields are displayed:
Illustration: General configuration of the REDDOXX Appliance

2. **Hostname - Hostname:**
Enter any name for the REDDOXX Appliance in the network.
The standard value can be exchanged for any name.

3. **DNS Domain:**
If applicable, enter the name of the domain belonging to the REDDOXX Appliance.

4. **DNS – 1st DNS-Server:**
Enter the corresponding IP address of your network's DNS server.

**NOTICE**
This entry is mandatory! At least one DNS server must be stated.
Ensure that the DNS server is accessible, also if the REDDOXX Appliance is operated in a DMZ.

5. **DNS – 2nd DNS-Server:**
Enter the IP address of another DNS server.

6. For additional configurations, change to the next tab.
**OK:** Saves the settings and closes the Appliance Configuration.
**CANCEL:** Cancels the settings and closes the Appliance Configuration.
4.1.1.2 Network Settings - Network

Making the Network Configuration

You can set up the primary network card via the network configuration. This consists of an IP address and a network mask each. The second network card is currently not yet supported.

Requirement: Opening the Appliance Configuration

1. Click on the tab "Network"
   The following fields are displayed:

   ![Illustration: Network configuration of the REDDOXX Appliance]

2. **LAN 1 – IP address:**
   Enter the IP address of the REDDOXX Appliance.
   The standard values were taken over from the first settings.

3. **LAN 1 – Net mask:**
   Enter the respective network mask of the REDDOXX Appliance.
   The standard values were taken over from the first settings.

4. LAN 2 is presently deactivated and cannot be used.

5. For additional configurations, change to the next tab.
   **OK:** Saves the settings and closes the Appliance Configuration.
   **CANCEL:** Cancels the settings and closes the Appliance Configuration.
4.1.1.3 Network Settings - Routing

Default Gateway and Routing
You can set up the default gateway via the routing configuration.

Requirement: Opening the Appliance Configuration
1. Click on the tab "Routing"
   The following fields are displayed:

   ![Routing configuration of the REDDOXX Appliance]

2. Default gateway:
   Enter the IP address of the default gateway here.

3. If you want to add static routes, you can do so via the button ADD. The following fields
   are displayed:

   ![Routing configuration of the REDDOXX Appliance]
4. Enter a target network, the corresponding subnet mask and a corresponding gateway. Add route by clicking on OK.

5. For additional configurations, change to the next tab.
   OK: Saves the settings and closes the Appliance Configuration.
   CANCEL: Cancels the settings and closes the Appliance Configuration.

4.1.1.4 Network Settings - Time Server

Making the Timeserver Configuration
Via the timeserver configuration, you can enter the timeservers and choose the applicable time zone via the selection list.

Requirement: Opening the Appliance Configuration

1. Click on the tab "Timeserver"
   The following fields are displayed:

   ![Illustration: Timeserver configuration of the REDDOXX Appliance]

2. Timeserver – 1st Timeserver:
   Enter the name of the timeserver to be used.
3. **Timeserver – 2\(^{nd}\) and 3\(^{rd}\) Timeserver**
   If necessary, repeat step 2.

4. **Timezone - Timezone**
   Via the selection list, select the corresponding time zone.
   OK: Saves the settings and closes the Appliance Configuration.
   CANCEL: Cancels the settings and closes the Appliance Configuration.

### 4.1.2 Settings

#### Opening the Settings

**Requirements:** The REDDOXX Appliance must be connected and in operation.

1. In the navigation tree, double-click on **Appliance configuration**.
2. In the tree, double-click on the branch **Settings**.

#### Attention

You should make a backup before each change and archive this.
Also see: "Options in the Menu Bar"

### 4.1.2.1 Settings - General

#### Making General Settings

Via the General Settings, you can enter and administer the hostname and the e-mail addresses of the REDDOXX Appliance. This way, the REDDOXX Appliance can send system messages to itself or the system administrator at any time. To let the Appliance load current updates for the fuzzy filter and current virus updates, it must be able to establish HTTP connections to the Internet. If a proxy server is supposed to be used for this purpose, you can also configure this here.

**Requirement:** Opening the Settings.

1. Click on the tab "General"
   The following fields are displayed:
2. **E-mail addresses – REDDOXX address:**
Enter the e-mail address of the REDDOXX Appliance.

**NOTICE**
The e-mail address of the REDDOXX Appliance must be an e-mail address of a valid e-mail domain and also received by the REDDOXX Appliance. This e-mail address may not be used for other purposes.

3. **E-Mail Addresses – Administrator Address:**
Enter the e-mail address of the administrator.

4. To use an HTTP proxy, activate the checkbox: Using an HTTP proxy.

5. **At "Proxy address, enter the name or IP address of the proxy.**

6. **At Proxy port,** enter the port of the proxy server that enables HTTP communication.

7. For additional configurations, change to the next tab.
   OK: Saves the settings and closes the Appliance Configuration.
   CANCEL: Cancels the settings and closes the Appliance Configuration.
4.1.2.2 Settings - SMTP

Making the Basic SMTP Settings
Via the SMTP settings, you can integrate the REDDOXX Appliance into your network.

**Requirement:** Opening the Settings.

1. Click on the tab "SMTP"
The following fields are displayed:

   ![Illustration: Settings - Network]

2. **Hostname - Hostname:**
Enter the corresponding hostname which the REDDOXX Appliance uses to identify itself in e-mail traffic.
   This hostname consists of the hostname and the domain of the Appliance Configuration.
   
   **NOTICE**
   Enter the hostname in FQDN format (Fully Qualified Domain Name). We urgently recommend using a host name which can be resolved via a reverse DNS query (PTR entry), if no smart host (relay) is used.

3. **SMTP – TCP Port:**
   If required, adapt the TCP port for the SMTP connections of the REDDOXX Appliance.
   The default standard value is "25".

4. For additional configurations, change to the next tab.
   **OK:** Saves the settings and closes the Appliance Configuration.
   **CANCEL:** Cancels the settings and closes the Appliance Configuration.
4.1.2.3 Settings - Limits

Making Limit Settings
Via the limit settings, you can set the maximum SMTP connections for incoming and outgoing e-mails. Additional options are timeouts for connection and e-mail sending as well as the maximum e-mail size. You can also set the maximum number of consoles, which may connect to the REDDOXX Appliance at the same time here.

Requirement: Opening the Settings.
1. Click on the tab "Limits"
   The following fields are displayed:

   ![Illustration: Settings - Limits](image)

   - **SMTP - Max. Connections (incoming):** Set the limit value of simultaneously incoming e-mails. This value defines how many incoming SMTP connections are managed and maintained at the same time.
   - **SMTP - Max. Connections (outgoing):** Set the limit value of simultaneously outgoing e-mails.

   **NOTICE**
   For the following settings, take over the respective valid settings in the standard value table as these depend on the variant of the REDDOXX Appliance you have purchased.

   1. **SMTP - Max. Connections (incoming):**
      Set the limit value of simultaneously incoming e-mails.
      This value defines how many incoming SMTP connections are managed and maintained at the same time.

   2. **SMTP - Max. Connections (outgoing):**
      Set the limit value of simultaneously outgoing e-mails.
This value defines how many SMTP connections to other servers are managed and maintained at the same time.

3. **SMTP – Connection Timeout (outgoing):**
   Set the desired connection timeout for outgoing e-mails in seconds. This time defines after how many seconds TCP communication without response the connection is closed.

4. **SMTP – Timeout (outgoing):**
   Set the desired timeout for outgoing e-mails. This time defines after how many seconds outgoing SMTP communication without response the connection is closed.

5. **SMTP – Timeout (incoming):**
   Set the desired timeout for incoming e-mails in seconds. This time defines after how many seconds incoming SMTP communication without response the connection is closed.

6. **SMTP - Max. E-Mail Size (MB):**
   Set the desired e-mail size.

7. **Console - Max. Connections:**
   Set the maximum number of consoles that can connect simultaneously to the REDDOXX Appliance. In this process, admin as well as user connections are counted.

8. For additional configurations, change to the next tab.
   **OK:** Saves the settings and closes the Appliance Configuration.
   **CANCEL:** Cancels the settings and closes the Appliance Configuration.

### Standard Values:

<table>
<thead>
<tr>
<th></th>
<th>Basic</th>
<th>Entry</th>
<th>SMB</th>
<th>Medium</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max. connections (incoming)</td>
<td>30</td>
<td>100</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>Max. connections (outgoing)</td>
<td>50</td>
<td>150</td>
<td>150</td>
<td>150</td>
</tr>
<tr>
<td>Connection timeout (outgoing)</td>
<td>30 sec.</td>
<td>30 sec.</td>
<td>30 sec.</td>
<td>30 sec.</td>
</tr>
<tr>
<td>Timeout (outgoing)</td>
<td>180 sec.</td>
<td>180 sec.</td>
<td>180 sec.</td>
<td>180 sec.</td>
</tr>
<tr>
<td>Timeout (incoming)</td>
<td>180 sec.</td>
<td>180 sec.</td>
<td>180 sec.</td>
<td>180 sec.</td>
</tr>
<tr>
<td>Max. e-mail size</td>
<td>100 MB</td>
<td>100 MB</td>
<td>100 MB</td>
<td>100 MB</td>
</tr>
<tr>
<td>Max. console connections</td>
<td>50</td>
<td>150</td>
<td>150</td>
<td>250</td>
</tr>
</tbody>
</table>

**ATTENTION**

Standard values are already pre-defined in the REDDOXX Appliance. These standard values should not be changed. Only expert personnel or support may make changes here.
4. The Administrator Console

4.1.2.4 Settings - Queues

Making REDDOXX Appliance Settings via Queues

Via the queue settings, you can define the save and forwarding time of the outgoing queues, the CISS queues, the spam queues and the virus queues in days.

**Requirement:** Opening the Settings.

1. Click on the tab "Queues"

The following fields are displayed:

Illustration: Settings - Queues

**NOTICE**

The stated standard values are our recommendations, which you may change at any time.

2. **Outgoing Queue - Max. Delivery Time (Days):**
   Enter the maximum delivery time of the e-mails in the outgoing queues in days. During this time, the system attempts to send the mail. If the mail server that is supposed to receive the mail is still not available after this defined time, REDDOXX sends the sender a corresponding message with SMTP error code and cancels the send process.

3. **CISS - Max. Save Time (Days):**
   Enter the maximum save time of the e-mails in the CISS queues in days.
   If a CISS prompt is not executed after a defined period, the mail is deleted on the appliance and not delivered.
4. **Spam - Max. Save Time (Days):**
Enter the maximum save time of the e-mails in the spam queues in days.
If the mail is not delivered manually until the expiration of the set time, it is deleted.

5. **Virus - Max. Save Time (Days):**
Enter the maximum save time of the e-mails in the virus queues in days.

6. **Queue Report**
If this field is activated, a queue report is generated each day at the defined reporting
time for each user whose spam or CISS queue has increased. In the user console, the user
can define whether this function is desired and in which format this message is to be sent
(html/text).

7. For additional configurations, change to the next tab.
**OK:** Saves the settings and closes the Appliance Configuration.
**CANCEL:** Cancels the settings and closes the Appliance Configuration.

**NOTICE**

Check your entries from time to time and reduce the times if applicable.

**ATTENTION**

After expiration of the set times, the e-mails are deleted irrevocably from the respective
queues.
The parameters set in "Appliance Configuration – Timeserver" are decisive here, above all
the set time zone.
4.1.2.5 Settings - Advanced

Making Advanced Settings
Via the Advanced Settings, you can configure the e-mail relay and the validator.

**NOTICE**
The **mail relay** accepts the outgoing mail traffic. If no relay is entered, the REDDOXX Appliance sends directly via the DNS-MX record of the respective recipient.

**Requirement:** Opening the Settings.

1. Click on the tab "Advanced"
The following fields are displayed:

2. **SMTP - E-Mail Relay:**
Enter the e-mail relay for sending the e-mails.

3. **SMTP – User Name:**
Enter the **user name**.

4. **SMTP – Password:**
Enter the corresponding **password**.
4.1.3 SMTP Configuration

4.1.3.1 Local Internet Domains

Creating new Internet Domains

Via the Local Internet Domains, you can create new internal e-mail domains for which the REDDOXX Appliance is to receive e-mails.

Requirements: Login on the administrator console of the REDDOXX Appliance

1. In the tree view at SMTP Configuration select Local Internet domains.
2. Right-click in the list view.
3. In the selection list, choose the entry Add.
4. Click on the tab "Local Internet domain"
   The following fields are displayed:
5. **Settings - Domain:**
Enter the desired *Domain*.

6. **Settings - Activate anti-spoofing:**

   *Here you can activate or deactivate anti-spoofing for the respective domain.*

   Notice
   
   To activate anti-spoofing, the anti-spoofing filter must be additionally allocated to the respective filter profiles. The function principle and how to edit filters is described in the chapter *Filter profiles*.

7. **REDDOXX Mail Depot – Deactivating archiving:**
   
   If this field is set, no e-mails are archived in the MailDepot.

8. For additional configurations, change to the next tab. LDAP
   
   **OK**: Saves the settings and closes the Appliance Configuration.
   
   **CANCEL**: Cancels the settings and closes the Appliance Configuration.

### LDAP Settings

One of the most essential parts of the REDDOXX filter technology is the recipient check (RVC = Recipient Verify Check). Here you can set whether e-mails are only sent to existing recipient addresses or rejected.

For the authentication method, you can select between a company-wide directory service and the local database of the REDDOXX Appliance.
Requirements: Select local Internet domains and double-click on the domain to be configured.

1. Click on the tab "LDAP"
   The following fields are displayed:

   ![LDAP Settings](image)

   Illustration: Local Internet domains - LDAP

2. **LDAP settings – LDAP server:**
   Enter the IP address of the LDAP server.

   **NOTICE**
   In addition to the IP address, you can also state a port separated by a colon (example: 192.168.0.3:3268). If the LDAP server also has a GLOBAL CATALOG server (e.g. Microsoft Domain Controller), we recommend stating this as preference because it responds up to 10 x faster. The default for the Global Catalog is TCP port 3268.

3. **LDAP settings – LDAP type:**
   Enter the LDAP type. Available for selection are: Active Directory, Exchange 5.5, Lotus Notes Domino and OpenLDAP.

4. **LDAP settings – LDAP Basis:**
   Enter the LDAP basis. Example: dc=company, dc=com

5. **LDAP settings – LDAP user:**
   Enter the user for authentication on the LDAP server.
6. **LDAP settings – LDAP password:**
   Enter the password for authentication on the LDAP server.

7. **Recipient Authentication – Activate Recipient Authentication**
   If this field is activated, the e-mail addresses are checked according to the configured LDAP interface or the locally entered e-mail addresses. This way, the REDDOXX Appliance only accepts mails that are listed in the respective directory (Active Directory, Lotus Domino, etc.) or locally.

<table>
<thead>
<tr>
<th>NOTICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>After the recipient check was activated, the service &quot;SMTP server&quot; must be restarted on the REDDOXX Appliance. The service is located in the directory tree under &quot;Appliance administration&quot;.</td>
</tr>
<tr>
<td>Further information about the LDAP configuration is available at the REDDOXX Support Center at <a href="http://support.reddoxx.net">http://support.reddoxx.net</a> in the column Download Center/Build1020.</td>
</tr>
</tbody>
</table>

8. **Recipient authentication - test method:**
   You can select either LDAP or LOCAL as test method.

9. **Automatically create user:**
   If this field is activated, users are automatically created upon the first receipt of an e-mail. Here the system first checks whether a user is available in LDAP for the e-mail address of the recipient. If this user exists in the LDAP, it is automatically created on the Appliance with all assigned e-mail addresses. Each e-mail address automatically receives the default filter profile in this process.

10. **Automatically create user - Realm:**
    Select the realm to be used for user authentication. You define the realm in the user administration at "Login configuration".

**CISS Signature**

This optional signature is attached to the automatic e-mail, which the REDDOXX Appliance sends for notification. This signature must be entered separately for each domain.

**Requirements:** Select local Internet domains and double-click on the domain to be configured.

1. Click on the tab "CISS"
   The following fields are displayed:
2. Enter any domain-specific signature.
   This optional signature is attached to the message text which the REDDOXX Appliance sends to
   the sender in case of a CISS challenge. It can be entered separately for each domain.

   **NOTICE**
   Also see: For further information about automatically generated e-mails, please refer to
   the chapter "Notifications".

3. Click on Ok to save the configuration and exit.
   CANCEL: Reject changes and exit the configuration.

**Editing Local Internet Domains**

Proceed as follows to edit an existing Internet domain.

**Requirements:** Internet domain is available in the list view.

1. In the tree view at **SMTP Configuration** select **Local Internet domains**.
2. Double-click on the domain to be edited.
   The configuration window opens.
3. Make the desired changes.
4. Click on Ok to save the configuration and exit.
   CANCEL: Reject changes and exit the configuration.
Delete Local Internet Domain

Proceed as follows to delete an existing Internet domain.

Requirements: Internet domain is available in the list view.

1. In the tree view at *SMTP Configuration* select *Local Internet domains*.
2. Right-click on the list entry to be deleted.
3. In the selection list, choose the entry *Delete*.
4. Confirm the prompting message with *Yes* to delete the Internet domain.
   No: Realm is not deleted.

* NOTICE – INFORMATION ABOUT RECIPIENT AUTHENTICATION

With the recipient authentication, the REDDOXX Appliance tries to determine whether the recipient of the mail is being serviced by the internal e-mail server, already before forwarding the mail.

At present, the following e-mail systems are supported for this function:

Microsoft Exchange 5.5, Microsoft Exchange 2000, Microsoft Exchange 2003, Lotus Notes Domino Server

Configuration:

<table>
<thead>
<tr>
<th>Backend Type</th>
<th>Exchange 5.5</th>
<th>Exchange 2000 and 2003</th>
<th>Lotus Notes</th>
<th>OpenLDAP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test method</td>
<td>LDAP</td>
<td>LDAP</td>
<td>LDAP</td>
<td>LDAP</td>
</tr>
<tr>
<td>LDAP Server</td>
<td>IP/hostname of the exchange server</td>
<td>IP/hostname of a domain controller</td>
<td>IP/hostname of a domain controller</td>
<td>IP/hostname of a domain controller</td>
</tr>
<tr>
<td>LDAP type</td>
<td>Exchange 5.5</td>
<td>Active Directory</td>
<td>Lotus Domino</td>
<td>OpenLDAP</td>
</tr>
<tr>
<td>LDAP basis</td>
<td>dc=company, dc=com (Example)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LDAP user</td>
<td>UPN of the LDAP user</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LDAP password</td>
<td>Password of the LDAP user</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

UPN = User Principal Name

e.g.  ldap-proxy@company.com

The user is used for the Active Directory or Lotus Domino query and must be authorized to read the attributes of the e-mail address.

**IMPORTANT**

**Exchange 5.5**

Neither the basis nor the user are entered here (anonymous login).

E-mail addresses must be published in the address book.
4.1.3.2 Local Networks

Creating new Local Networks
Via the local networks you define from which host or networks e-mails may be sent via the REDDOXX Appliance.

Requirements: Login on the administrator console of the REDDOXX Appliance

1. In the tree view at SMTP Configuration select Local Networks.
2. Right-click in the list view.
3. In the selection list, choose the entry New.
   The following fields are displayed:

   ![Illustration: Local networks – local network]

4. Enter the local network or a single host.
5. Single hosts, e.g. the internal mail server, require the mask 255.255.255.255.
6. Click on Ok to save the configuration and exit.
   CANCEL: Reject changes and exit the configuration.

**NOTICE**
If there is a mail relay or a firewall with an SMTP server service or a POP3 collector service before your REDDOXX Appliance, which receives the e-mails first, this may NOT be listed in the local networks.

Edit Local Networks
Proceed as follows to edit existing networks.

Requirements: Entries are available in the list view.

1. In the tree view at SMTP Configuration select Local Networks.
2. Double-click on the network to be edited.
   The configuration window opens.
3. Make the desired changes.
4. Click on Ok to save the configuration and exit. 
   CANCEL: Reject changes and exit the configuration.

Deleting local networks
Proceed as follows to delete existing networks.

Requirements: Networks are available in the list view.
1. In the tree view at SMTP Configuration select Local Networks.
2. Right-click on the list entry to be deleted.
3. In the selection list, choose the entry Delete.
4. Confirm the prompting message with Yes to delete the profile.
   No: Profile is not deleted.

**NOTICE**
Changes to the local networks require the restart of the SMPT server service.
The restart of a service is described in this document in Appliance Administration/Services.

4.1.3.3 E-mail transport

Creating new E-Mail Transport
Via the e-mail transport, you can define to e-mail server the e-mails of the registered domain are to be forwarded.

Requirements: Login on the administrator console of the REDDOXX Appliance
1. In the tree view at SMTP Configuration select E-Mail Transport.
2. Right-click in the list view.
3. In the selection list, choose the entry New.
   The following fields are displayed:

   Illustration: E-mail transport

4. Enter the desired Domain.
5. Enter the corresponding target server.
6. Click on OK to save the configuration and exit. 
   CANCEL: Reject changes and exit the configuration.

**NOTICE**

If the domain of an e-mail is not registered here, the target server is determined via a DNS lookup on the DNS server entered in the configuration.

---

**Edit E-Mail Transport**

Proceed as follows to edit existing e-mail transports.

**Requirements:** E-mail transport is available in the list view.

1. In the tree view at **SMTP Configuration** select **E-Mail Transport**.
2. Double-click the e-mail transport to be edited. 
The configuration window opens.
3. Make the desired changes.
4. Click on OK to save the configuration and exit. 
   CANCEL: Reject changes and exit the configuration.

---

**Delete E-Mail Transport**

Proceed as follows to delete existing networks.

**Requirements:** E-mail transports are available in the list view.

1. In the tree view at **SMTP Configuration** select **E-Mail Transport**.
2. Right-click on the list entry to be deleted.
3. In the selection list, choose the entry **Delete**.
4. Confirm the prompting message with **YES** to delete the profile. 
   **No:** Profile is not deleted.

---

**4.1.3.4 Blocked IP Addresses**

To explicitly prohibit the establishment of SMTP connections for IP addresses or complete network sections, you can define these sections here.

**Creating blocked IP Addresses**

**Requirements:** Login on the administrator console of the REDDOXX Appliance

1. In the tree view, select **SMTP configuration - Blocked IP addresses**.
2. Right-click in the list view.
3. In the selection list, choose the entry **Add**.
   The following fields are displayed:
4. Enter the network to be blocked.
5. Enter the corresponding subnet mask.
6. Optionally, you can enter the reason for blocking in the field "Description".
7. Click on OK to save the configuration and exit.
   CANCEL: Reject changes and exit the configuration.

4.1.4 Backup and Restore

Backup Information
The backup function offers the possibility to save the complete data of the appliance automatically. In this process, all queues and configurations of the REDDOXX Appliance are backed up.

4.1.4.1 Backup Settings

Setting the Network Permission
Via the permission, you can state the network path and its parameters in which the backup is supposed to be saved.

Requirement: Login on the administrator console of the REDDOXX Appliance

1. In the tree view, select **Backup and restore – Backup settings**.
2. Right-click on **Backup settings**
3. In the selection list, choose the entry Edit.
The following fields are displayed:
4. **Network permission - Permission:**
Enter the UNC path.

**NOTICE**
The path is stated in UNC (Uniform Naming Convention) format:
\servername\foldername
You may not state any subdirectories.
The backup may not be saved together with another directory (e.g. Archive).

5. **Network permission – user name:**
Enter the user name.

6. **Network permission - Password:**
Enter the password.
   **The password may not be longer than 16 characters!**

7. **Network permission - Domain:**
Enter the name of the domain if applicable.

**Setting a Schedule**
Here you can enter the weekdays, the time at which the backup is supposed to be started and the name of the backup file. The backup is only saved at the stated time in the previously configured UNC path if the checkbox for the weekday is activated.

**Requirement:** Login on the administrator console of the REDDOXX Appliance
8. In the tree view, select **Backup and restore – Backup settings**.
9. Right-click on **"Backup settings"**
10. In the selection list, choose the entry **Edit**.
11. Click on the tab "Schedule"

The following fields are displayed:

![Backup configuration - schedule](image)

**NOTICE**
You can test the connection to the server permission by clicking on RESTORE. No error message may appear in the log view in this case.

### 4.1.4.2 Restore Backup

The table lists the backups written so far. To restore, please select the desired backup.

**NOTICE**
With the Appliance version 1021, the restore can only still be performed via the Appliance Console. Also see chapter 6.2 – Appliance console - backup and restore

**Requirement:** Backups are available in the list view.
1. Select the desired backup in the list view.
2. With a right-click on the desired backup, you open a selection list in which you can restore the backup.

<table>
<thead>
<tr>
<th>Name</th>
<th>Size</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>sbackupdi</td>
<td>5.14 MB</td>
<td>04.04.2006 01:04:12</td>
</tr>
<tr>
<td>sbackupdo</td>
<td>5.06 MB</td>
<td>30.03.2006 01:04:11</td>
</tr>
<tr>
<td>sbackupfr</td>
<td>4.90 MB</td>
<td>24.03.2006 01:04:07</td>
</tr>
<tr>
<td>sbackupmi</td>
<td>5.04 MB</td>
<td>29.03.2006 02:25:07</td>
</tr>
<tr>
<td>sbackupmo</td>
<td>5.14 MB</td>
<td>03.04.2006 11:39:08</td>
</tr>
<tr>
<td>sbackupsa</td>
<td>5.00 MB</td>
<td>01.04.2006 01:04:10</td>
</tr>
<tr>
<td>sbackupso</td>
<td>5.08 MB</td>
<td>02.04.2006 01:04:11</td>
</tr>
<tr>
<td>sconfig</td>
<td>5.86 KB</td>
<td>06.03.2006 11:40:16</td>
</tr>
</tbody>
</table>

Illustration: Backup and restore – restore

**NOTICE**

You can only restore backups if the firmware version has not changed in the time between backup and restore.

### 4.2 Appliance Administration

#### 4.2.1 Mail Queues

**Information about Queues**

In the queues, the e-mails wait for further processing by the REDDOXX Appliance.

**Mode of Function**

*Also see:* "Information about the services in chapter 4.2.7".

The Incoming and Outgoing Messages are the basic queues of the REDDOXX Appliance.

#### 4.2.1.1 Incoming Mails

E-mails accepted by the SMTP server of the REDDOXX Appliance sent internally or externally are temporarily saved in the Incoming Messages queue. Here the REDDOXX Appliance checks the e-mails and places them in the queues Spam, CISS, Virus or Outgoing Messages, depending on the result of the check.
You can look for e-mails manually in this queue and delete them. The list view shows the ID, the time received, the sender and the recipient, the size of the e-mails, the forwarding time as well as the result of the e-mails. Sorting via e-mail attributes is also possible here.

4.2.1.2 Outgoing Mails

All e-mails sent internally or externally by the SMTP client of the REDDOXX Appliance are placed in the queue Outgoing Messages.

For further information, see **Incoming queues**.

Searching for E-mails

You can search for e-mails in the respective queues.

**Restrictions:** None, searching for e-mails is possible in all queues.

1. Select with a double-click in the tree view Mail queues or Spamfinder queues.
2. Select the desired queue.
3. In the menu view, click on the icon with the magnifying glass.
4. The following fields are displayed above the list:

6. In Search term, Sender and Recipient enter the data you know.
7. Sorting via e-mail attributes is also possible here. To do so, click on the column header. Another click reverses the direction.
8. Click Search to start the search.

Deleting E-Mails

You can delete e-mails in the respective queues.

**Restrictions:** None. Deleting e-mails is possible in all queues.

1. In the tree view, select **Queues** with a double-click.
2. Select the desired queue.
3. Right-click on the e-mail to be deleted.
4. In the selection list, choose the entry **Delete**.
5. Confirm the prompting message with YES to delete the profile. No: Profile is not deleted.
4.2.2 User Administration

Information about User Administration
In the user administration, you can manage users, local e-mail addresses, the login configuration as well as groups and policies.

4.2.2.1 Users
In the column USER, you can add, edit, delete, search and import users, as well as assign or revoke licenses and change the password.

The list view offers the following data at a glance:

- List with names of the created users
- Primary e-mail address
- Realm
- Spamfinder licenses
- MailDepot licenses
Adding Users

1. In the selection list, choose the entry Add.
   The following fields are displayed:

   ![User Administration - User data](Image)

   Illustration: User Administration - User data

   2. Enter the desired user name.
   3. Enter a password.
   4. Click on Ok to save the configuration and exit.
      CANCEL: Reject changes and exit the configuration.

Edit Users

Proceed as follows to import an existing user.

1. Double-click on the user to be edited.
   The configuration window opens.

2. Make the desired changes.
3. Click on **Ok** to save the configuration and exit.
   **CANCEL**: Reject changes and exit the configuration.

**Delete Users**

Proceed as follows to delete an existing user.

1. Right-click on the user to be deleted.
2. In the selection list, choose the entry **Delete**.
3. Confirm the prompt with Yes to delete the selected user. No: User is not deleted.

**Adjusting the Password**

To change the password of a user do the following steps.

1. Right-click on a user from the selection list.
2. Choose the option: **Set Password**.
   
The following windows appears:

3. **insert** the new password.
4. **confirm** the new password.
5. Click on **OK**. The new password is set and the dialogue is closed. Select **Cancel** if you do not wish to change the password.

**Assign License**

To assign a license to a user, do the following:

1. Mark in the selection list one or more user, click right and choose „Assign License“. 
   
The following window appears:
2. Select from the drop down list the option „Spamfinder license“ or „Archive license“ and click OK. The license is assigned and the window gets closed. This change is immediately effective without a restart.

Remove License
To remove a license from a user, do the same steps as before, but select in the context menu “remove license”. You can also use multi user selection.

NOTICE
Licenses gets automatically assigned if the Spamfinder or the Maildepot is used inside the user console. Since version 1021 all licenses gets validated. If licenses has been assigned versions before, it may happen, that you run out of valid licenses after a firmware version update. You will get an error message showing „Invalid license count“ or „no valid license“. (see also the FAQ). Here you can remove already assigned licenses.

Import User
Proceed as follows to import a user from a list.

1. Right-click in the list view.
2. In the selection list, choose the entry User import.
The following window appears:
3. In the menu Import, select the option **Read user from file**.

4. Select the import file and click on **Open**. Then the following list appears.

   ![User import list](image)

   **NOTICE**
   The import file must have the following structure:

   **User name,password.realm,e-mail address1,e-mail addressN ...**

   If you do not see any user on the list, check out this contrains:
   - Fields must be separated by a comma .
   - All fields must not be empty.
   - User must be unique.

5. In the menu Import, select **Save user**.
   The following dialog appears:

   ![User import filter selection](image)

6. Select the realm and the profile to be used for the users to be imported.

7. Once the users were successfully imported, you can close the window. The users appear in the list view.
4. The Administrator Console

4.2.2.2 Groups

Groups are required to control user policies. One or several users are assigned to a group. In the list view, you see the columns *Group name* and *Description*. You can add, edit and delete groups.

Illustration: User administration – groups

**Adding Groups**

1. In the selection list, choose the entry **Add**. The following dialog appears:

   Illustration: User administration – add groups

2. Enter a group name.
3. Enter a description.
Click on ADD to assign users to this group. The following dialog appears:

![User administration – add users to groups](image)

4. Select one or several users from the list.
5. Click on OK to apply the user group assignment.
6. Now click on OK to establish the group.

**Edit Group**
1. Double-click on the group to be edited.
2. Make the desired changes.
3. Click on Ok.

**Delete Group**
1. Right-click on the group to be deleted.
2. In the selection list, choose the entry **Delete**.
   Confirm the prompt with Yes to delete the selected group. No: The group is not deleted.
4.2.2.3 E-mail Aliases

E-mail aliases are assigned to a user. You can add, edit or delete e-mail aliases, change the filter profile and deactivate archiving for several e-mail aliases at the same time.

In the list view, you see the columns E-mail address, filter profile, user and disable archiving.

Illustration: User administration - e-mail aliases

Adding E-mail Aliases

7. In the selection list, choose the entry Add.
   The following fields are displayed:

   ![Illustration: User administration - add e-mail alias]

8. Enter the desired e-mail address.
9. Select the user allowed to manage this address.
10. Select the desired filter profile.
11. activate the checkbox Disable archiving if you want to avoid archiving those emails
12. Now click on OK to create the e-mail alias.

Editing E-mail Aliases

4. Double-click the e-mail address to be edited.
   The following dialog appears:
5. Make the desired changes.
6. Click on Ok to save the configuration and exit.
   CANCEL: Reject changes and exit the configuration.

Deleting E-mail Aliases
3. Right-click on the e-mail alias to be deleted.
4. In the selection list, choose the entry Delete.
5. Confirm the prompting message with Yes to delete the selected e-mail address. No: The e-mail alias is not deleted.

Changing Filter Profiles
1. Mark all e-mail addresses for which you want to change the filter profile simultaneously.
2. Click on the list selection (right). The following dialog opens:
   3. Select the desired filter profile.
   4. OK: All previously selected e-mail aliases receive the newly entered filter profile.
4.2.2.4 Realm

The Realm defines, which user database is used to authenticate the users. You can define several realms to enable users to login from different systems.

The standard realm "local" uses the local user database of the REDDOXX Appliance. It cannot be changed or deleted.

You can add, edit and delete realms.

In the list view, you see the columns Name and Authentication type.

Illustration: User administration – realm

Creating a new Realm
Illustration: User Administration - Realm

4. Enter the realm name.

5. Via the selection list, select the authentication type. The authentication type "local" refers to the local user database of the REDDOXX Appliance.

6. Enter the authentication server. The following are supported: local, Windows2000, Windows2003, Netware5, Netware6 Active Directory, Lotus Domino, OpenLDAP.

7. Enter the TCP port. The default port for LDAP is 389. You must enter a valid value here.

8. If desired, activate the option Secure transmission SSL. Please note that the default port for LDAP via SSL is 636.

9. Enter the active directory domain.

10. Enter the BaseDN.

11. Importing e-mail addresses
    If necessary, activate the option Import e-mail addresses in order to match the e-mail addresses for the user with the authentication server at each login.

12. Setting primary e-mail addresses
    If necessary, activate the option Set primary address in order to match the primary e-mail addresses for the user with the authentication server at each login.

13. Click on OK to save the configuration and exit.
    CANCEL: Reject changes and exit the configuration.

Edit Realm

1. Double-click on the REALM to be edited. The configuration window opens.

2. Make the desired changes.

3. Click on OK to save the configuration and exit.
    CANCEL: Reject changes and exit the configuration.

Delete Realm

1. Right-click on the realm to be deleted.

2. In the selection list, choose the entry Delete.

3. Confirm the prompt with Yes to delete the selected realm. No: Realm is not deleted.
### NOTICE – INFORMATION ABOUT REALMS

The Realm defines, which user database is used to authenticate the users.

The following table indicates the supported systems and the respective function scope:

<table>
<thead>
<tr>
<th>LDAP Server</th>
<th>User Authentication</th>
<th>Recipient Check</th>
<th>User Auto Creation</th>
<th>E-mail Address Import</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Active Directory</td>
<td>Yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>with Exchange 2000+</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exchange 5.5</td>
<td>No</td>
<td>yes</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>Lotus Notes Domino 6+</td>
<td>Yes</td>
<td>yes²</td>
<td>yes</td>
<td>yes²</td>
</tr>
<tr>
<td>Novell eDirectory</td>
<td>Yes</td>
<td>no</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td>OpenLDAP</td>
<td>Yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
</tbody>
</table>

² The following restrictions apply for Lotus Notes Domino:

Only the following e-mail addresses are rated as valid:

- Internet address
- Shortname/UserID
- User name

The stated addresses must be clear in Lotus Domino! Double entries lead to the rejection of the mail!

With shortname/UserID, you can skip the Internet domain. Then all Internet domains defined in the Domino server are accepted.

When importing during user login, at first only the Internet address is created as e-mail alias in the REDDOXX Appliance. The additional e-mail addresses are then generated upon e-mail receipt.
**Configuration:**

<table>
<thead>
<tr>
<th></th>
<th><strong>WINdows 2000</strong></th>
<th><strong>WINdows 2003</strong></th>
<th><strong>NETware 5.x</strong></th>
<th><strong>NETware 6.x</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication type</td>
<td>Windows 2000</td>
<td>Windows 2003</td>
<td>Netware 5</td>
<td>Netware 6</td>
</tr>
<tr>
<td>Authentication server</td>
<td>IP/hostname of a Windows domain controller</td>
<td>IP/hostname of a Netware server with LDAP service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCP port</td>
<td>TCP port of the LDAP service, standard: 389 OR for Secure LDAP: 636</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Secure transmission</td>
<td>Activate Secure LDAP here if your system supports Secure LDAP.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory Domain</td>
<td>AD domain e.g. company.com</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BaseDN</td>
<td>dc=company, dc=com</td>
<td></td>
<td>e.g. o=context</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th><strong>LOTUS DOMINO</strong></th>
<th><strong>OPENLDAP</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication type</td>
<td>Windows 2000</td>
<td>Windows 2003</td>
</tr>
<tr>
<td>Authentication server</td>
<td>IP/hostname of the server with LDAP service</td>
<td></td>
</tr>
<tr>
<td>TCP port</td>
<td>389 / SecureLDAP 636</td>
<td></td>
</tr>
<tr>
<td>Secure transmission</td>
<td>Activate Secure LDAP here if your system supports Secure LDAP.</td>
<td></td>
</tr>
<tr>
<td>Active Directory Domain</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BaseDN</td>
<td>o=REDDOXX,dc=company, dc=com</td>
<td></td>
</tr>
</tbody>
</table>

**NOTICE**

For LDAP linkup to Novell Netware, it must be possible to read the following user attributes with an **anonymous LDAP bind**: dn, cn, objectClass.

Further LDAP settings are available at the REDDOXX Support Center at http://support.reddoxx.net in the column Download Center/Build1020.
4. The Administrator Console

4.2.2.5 Policies – Group Policies

Function Overview and Terminology

The policies help you to create rules that define the function scope of the user console. Rules are always applies on groups. This is why you must have already assigned users to groups (see chapter 4.2.2.2).

The policies define whether select functions are allowed or prohibited for one or several groups. Examples:

- Add/delete whitelist entries
- Delete e-mails from queues

A policy contains so-called rule sets, a summary of individual functions to an umbrella term.

Rule Sets

The following rule sets are available:

- General rules
- Spamfinder rules
- Spamfinder filter list rules
- MailDepot rules
- MailSealer rules
- Deputy groups
A rule set can have 3 different statuses:
1. Not configured
2. Deactivated
3. Activated

To 1.) This set of rules is not evaluated. It is ignored in this policy. The status of the individual functions remain unchanged.

To 2.) All functions of this rule set are deactivated. The following policies are no longer considered for this rule set.

To 3.) The functions of the rule set are considered individually. The following policies are no longer considered for this rule set.

**Operation Sequence**
If there are no policies yet or if all rule sets are *not configured*, the default of the options applies initially and no deputies are defined.

When a user logs on to the user console, all available policies are processed in sequence from top to bottom.

If a user is included in the group that was assigned to the policy, the rule set is no longer considered on the following policies, unless the rule set previously had the status *not configured*.

You can set the sequence of the policies via the context menu (higher, lower).

**Configuration of the Rule Sets**

1. Open the window for processing the configuration by right-clicking on a policy in the tree menu. The following window appears:

   The following window appears:
2. Select the desired rule set and activate it.
3. Select the option you wish to activate.

**Group Assignment**

4. Assign this policy to a group.

**NOTICE**

Policies only always apply for the users contained in the user groups stated here.
5. The checkbox *Apply policy* to all users assigns this policy to all users. This omits the configuration and administration of a group containing all users.

**Input Section Apply Policy to:**
6. *ADD adds a group from a group selection list* (see chapter 4.2.2.2). The rule set of this policy is applied to users contained in this group.

7. *DELETE removes a marked group from this policy.*

**Input Section Reject Policy to:**
ADD adds a group to the group exemption list. The rule set of this policy is NOT applied to users contained in this group.

8. Click on OK to save the settings.

**NOTICE**
Example: A rule set of a policy applies to all users (*Apply policy to all users*) with the exception of the group of administrators (*reject Policy for*).
Deputies

A peculiarity of the rule sets is the deputy group rule set.
Here, the administrator can assign *deputies* for users on holiday, for example. This gives the deputy access to the e-mails of the user he is supposed to substitute.

In the rule set *Deputy groups*, you define, which e-mail addresses can be deputized.

<table>
<thead>
<tr>
<th>NOTICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deputy groups merely serve for clarity and are not connected to the user groups.</td>
</tr>
</tbody>
</table>

In the user group assignment of the policy, you define who may represent this e-mail address (*deputy groups*).

Configuration of the Deputy Groups

Illustration: Deputy configuration

1. Right-click on the deputy groups.
2. Select *Add deputy group*.
3. Assign a name to the new deputy group.

   With a right mouse click on the new deputy group, you can:
   3.1 *Delete* deputy group again.
   3.2 *Renaming* the deputy group.
   3.3 Adding a deputy e-mail address.

   By right-clicking on the e-mail address, you can delete it from the group again.
4. The Administrator Console

**NOTICE - EXCEPTION TO OTHER RULE SETS**

The list of all e-mail addresses a user may represent is compiled from ALL policies for the user group the user is assigned to.

---

4.2.3 Notification

**Information about Notifications**

Via Notifications, you can edit the standard texts of the e-mails sent in the respective situation.

**The following standard texts can be configured:**

- CISS
- Address verification
- Virus warning to the administrator
- Virus warning to the recipient
- Virus warning to the sender

**Edit CISS Notifications**

With CISS notifications, you can adapt the language, the subject and the content of the e-mail.

**Restrictions:** None.

1. Select *Messages* in the tree view.
2. In the list view, right-click on 'CISS'.
3. In the selection list, choose the entry *Edit*.
   
The following fields are displayed:
4. Via the selection list, select the desired language.
   The standard setting contain the e-mail text in German and English.

5. Activate the option Field to activate the language.

6. Change the e-mail at wish.

   **NOTICE**
   The texts with the percent signs are wildcards and may not be changed or deleted.

7. Click on OK to save the configuration and exit.
   CANCEL: Reject changes and exit the configuration.

### CISS Message Wildcards:

<table>
<thead>
<tr>
<th>WILDCARD</th>
<th>EXPLANATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>%SUBJECT%</td>
<td>Subject of the received e-mail</td>
</tr>
<tr>
<td>%CHALLENGE_URL%</td>
<td>URL to the REDDOXX portal</td>
</tr>
</tbody>
</table>

**Edit Messages for Address Verification**

With address verification messages, you can adapt the subject and the content of the e-mail.

**Restrictions:** None.

1. Select *Messages* in the tree view.
2. In the list view, right-click on 'Address Verification'.
3. In the selection list, choose the entry *Edit*.

   The following fields are displayed:
4. Change the e-mail at wish.

**NOTICE**
The texts in percent signs are wildcards.

5. Click on OK to save the configuration and exit.
   CANCEL: Reject changes and exit the configuration.

**Wildcards for Address Verification Messages:**

<table>
<thead>
<tr>
<th>WILDCARD</th>
<th>EXPLANATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>%VerifyMail%</td>
<td>E-mail address to be verified</td>
</tr>
<tr>
<td>%VerifyID%</td>
<td>ID (number) that has to be entered for verification of the e-mail address.</td>
</tr>
</tbody>
</table>

**Edit Virus Alarm Messages**

With virus alarm messages, you can adapt the subject and the content of the e-mail. You can send these messages to the administrator, the recipient and the sender.

**Restrictions:** None.

1. Select *Messages* in the tree view.
2. In the list view, right-click on 'Virus alarm to administrator'.
3. In the selection list, choose the entry *Edit*.

   The following fields are displayed:
4. Change the e-mail at wish.

**NOTICE**
The texts in percent signs are wildcards.

5. Click on OK to save the configuration and exit.
**CANCEL**: Reject changes and exit the configuration.

**NOTICE**
Proceed the same way with messages to the recipient and the sender.

**Wildcards for virus alarm messages:**

<table>
<thead>
<tr>
<th>Wildcard</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>%VIRUSNAME%</td>
<td>Name of the detected virus</td>
</tr>
<tr>
<td>%SENDER%</td>
<td>Sender of the e-mail</td>
</tr>
<tr>
<td>%RECIPIENTS%</td>
<td>Recipient of the e-mail</td>
</tr>
<tr>
<td>%SUBJECT%</td>
<td>E-mail subject</td>
</tr>
</tbody>
</table>
4.2.4 Logs

The REDDOXX Appliance generates a log file for each day. These are displayed in the list view **Logs** in the menu tree. These have the following file name format:

Spamfinder-yyyy-mm-dd HH:MM.log (yyyy=year, mm=month, dd=day, HH=hour, MM=minute).

If the log exceeds a file size of 50 MB, a new log file is generated.

The logs can be displayed and analyzed with a special log analysis.

There are the following options to analyze logs:

- Entire log in the viewer
- Filter acc. to process ID
- Smart Filter
- Save log in local system

**Entire Log**

To view the log of a specific day with the viewer, click on "Logs" in the tree view and then double-click on the desired log in the list. The following log viewer appears:
ProcessID

It is possible to filter the log information of a certain process. To do so, you have to select a specific ProcessID in the viewer. The ProcessID is indicated by square brackets.

Smart Filter

Due to the fact that it is often desired to filter the progress of an associated action, e.g. the mail flow of an e-mail, but this passes through different processes, you can filter the process with the help of the SmartID. The SmartID is enclosed in round brackets.

Function of the Filtering Process (Process/Smart)

1. In the Log Viewer, right-click on a desired ID (Smart or ProcessID).
2. The following menu appears:

```
Clear filter
Filter process ID: [18759689]
Smart filters
Loglevel
```

3. Select the desired filter type.

4. Now the Log Viewer only displays the corresponding data.

5. To deactivate filtering, right-click on the option "Delete filters".

### 4.2.5 Updates

**Requesting Updates**

We will inform you via email about new available updates with our release notes. The email gets send to the address you have specified under SETTINGS. You can request yourself an update by clicking on *Request updates*.

**Requirements:** none.

1. Select *Updates* in the tree view.

2. Right-click in the list view.

   The following view appears:

```
   REDDOXX - Build: 1022
```

   3. Select the entry *Request updates*.

   The update should appear in the list view after a few minutes. You can update the list view by pressing F5.
4. The Administrator Console

**NOTICE**

If you cannot see the option "REQUEST UPDATES" you probably use an old version of the console software. Download the latest one and request the update again.

4. Wählen Sie den Eintrag **Updates anfordern**

Folgende Ansicht wird angezeigt:

![Download of 1 file(s) started.](image)

Depending on your bandwidth, the update should be finished after a few seconds or minutes, and appears in the list area.

You will see following screen:

![Update downloads finished successfully.](image)

**NOTICE**

The anti-virus protection and anti-spam filter is updated automatically! Check whether there are enough valid licenses. The AV version should not be older than 1 to 2 days.

**Installing Updates**

Via the menu point "Updates", you can install updates.

**Requirements:** Updates available in the list.

1. Select **Updates** in the tree view.
2. Right-click in the list view.
3. Choose the update you want to install out from the list view and click right.

**NOTICE**

Updates must be installed version after version in ascending order.
After that the update starts and the new firmware gets installed. Usually this is done in 1 – 2 minutes. When it's done, you will see the update protocol. Have a look onto the last line if it shows that the update was finished successful. If not, refer to the FAQ section of the REDDOXX support area. (http://support.reddoxx.net)

Illustration: Protocol of a firmware-Update.

Delete Updates
Usually the update gets removed after it was installed. You can delete it by clicking right on it and choose “DELETE”.
4.2.6 Sessions

Information about Sessions

Via the sessions, you can view all users logged into the REDDOXX Appliance.

Illustration: Sessions

4.2.7 Services

4.2.7.1 Overview

Via the services administration, you can view and control the individual services.

Illustration: Services

4.2.7.2 Mail Flow

The following diagram shows the mail flow of an e-mail:

Mail reception (SMTP server) - validation (Validator) - delivery (SMTP client):
4.2.7.3 SMTP Server Service

The SMTP server receives e-mails from other e-mail servers and saves the e-mails in the queue "Incoming Messages". The phase 1 filters are checked before the mails are accepted.

4.2.7.4 SMTP Client Service

The SMTP Client Service sends e-mails waiting for forwarding in the queue "Outgoing Messages".

4.2.7.5 Control Server Service

The Control Server services the connections of the administrator consoles as well as of the user console and serves to configure and administer the REDDOXX Appliance.

4.2.7.6 Message Validation Service

The Message Validation Service checks all e-mails in the queue "Incoming Messages". Here the e-mails are checked with the phase 2 filters and for viruses. Depending on the result of the verification, the e-mails are then moved to one of the following queues: viruses, spam or CISS.

4.2.7.7 Task Scheduler Service

The Task Scheduler Service starts cyclic processes, e.g. the cleanup of the queues.
4.2.7.8 Portal Communication Service
The Portal Communication Service processes e-mails sent by the REDDOXX portal, e.g. CISS. By encoding or decoding the e-mails, it takes care of safe communication with the REDDOXX portal.

4.2.7.9 Remote Support Service
The REDDOXX Remote Support Service enables better remote maintenance for the REDDOXX support without you having to change your firewall rules. The REDDOXX Remote Support Service is always deactivated and should only be started after consulting a REDDOXX support member.

4.2.7.10 Starting, Stopping and Restarting Services

Start Service
Via Services, you can start a service that is not running.

Requirements: Current status 'false'.
1. Select Services in the tree view.
2. Right-click on the service to be started.
3. In the selection list, choose the entry Start.

End Service
Via Services, you can stop a running service.

Requirements: Current status 'true'.
1. Select Services in the tree view.
2. Right-click on the service to be stopped.
3. In the selection list, choose the entry Stop.

Restart Service
Via Services, you can restart a running service.
4. The Administrator Console

Requirements: Current status ‘true’.

1. Select Services in the tree view.
2. Right-click on the service you want to restart.
3. In the selection list, choose the entry Restart.

4.3 REDDOXX Spamfinder

In the Spamfinder section, you make the presets for managing filter settings and the spam queues.

4.3.1 Spamfinder Queues

You will find e-mails that were not sent yet in one of the following queues. In all queues, you can send or delete one of the mails listed there by right-clicking. To sort the list entries, click on the desired column header. Another click reverses the sorting direction. The content of an e-mail cannot be viewed due to legal regulations. Also keep in mind that e-mails, which you cannot find here, are already in the outgoing queue.

Spam queue

E-mails listed in the Spam queue were classified as spam by the REDDOXX Appliance. In the 7th column "Filter", you see which anti-spam filter kicked in.

<table>
<thead>
<tr>
<th>ID</th>
<th>Received</th>
<th>Sender</th>
<th>Recipient</th>
<th>Size</th>
<th>Subject</th>
<th>Filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>375G0C69BEF8</td>
<td>16:10:20 07.21.12</td>
<td><a href="mailto:brian@brianahoo.net">brian@brianahoo.net</a></td>
<td><a href="mailto:info@email24.net">info@email24.net</a></td>
<td>2.28 KB</td>
<td>Brian Watchdog</td>
<td>RBL-Filter</td>
</tr>
<tr>
<td>43ETF7FAAD0D</td>
<td>16:10:20 07.21.12</td>
<td><a href="mailto:com@seniortime.creative.co.uk">com@seniortime.creative.co.uk</a></td>
<td><a href="mailto:info@email24.net">info@email24.net</a></td>
<td>1.17 KB</td>
<td>Ruben Buy your loved one Red</td>
<td>Fuzzy-Filter</td>
</tr>
<tr>
<td>5609F589F4D7</td>
<td>16:10:20 07.21.12</td>
<td>susan@<a href="mailto:first@your-shopping.net">first@your-shopping.net</a></td>
<td><a href="mailto:info@email24.net">info@email24.net</a></td>
<td>4.47 KB</td>
<td>Anything else?</td>
<td>RBL-Filter</td>
</tr>
<tr>
<td>68E10ED5F8F3</td>
<td>16:10:20 07.21.12</td>
<td><a href="mailto:selltheendogas@eurolitephilly.com">selltheendogas@eurolitephilly.com</a></td>
<td><a href="mailto:info@email24.net">info@email24.net</a></td>
<td>24.91 KB</td>
<td>Still upset about it</td>
<td>RBL-Filter</td>
</tr>
<tr>
<td>889438F7111D</td>
<td>16:10:20 07.21.12</td>
<td>disneyprincess@disneystep...</td>
<td><a href="mailto:info@email24.net">info@email24.net</a></td>
<td>1.99 KB</td>
<td>eledegv</td>
<td>Fuzzy-Filter</td>
</tr>
<tr>
<td>117211C4487E</td>
<td>16:10:20 07.21.12</td>
<td><a href="mailto:balforshonoh@seniorcollege.edu">balforshonoh@seniorcollege.edu</a></td>
<td><a href="mailto:info@email24.net">info@email24.net</a></td>
<td>3.32 KB</td>
<td>Leave your problems with people like...</td>
<td>RBL-Filter</td>
</tr>
<tr>
<td>42672F43075C</td>
<td>16:10:20 07.21.12</td>
<td><a href="mailto:leiforsay587@uobmail.ly.com">leiforsay587@uobmail.ly.com</a></td>
<td><a href="mailto:info@email24.net">info@email24.net</a></td>
<td>2.21 KB</td>
<td>yourmail</td>
<td>Fuzzy-Filter</td>
</tr>
<tr>
<td>554AB03D740D</td>
<td>16:10:20 07.21.12</td>
<td><a href="mailto:barbara@seniorcollege.edu">barbara@seniorcollege.edu</a></td>
<td><a href="mailto:info@email24.net">info@email24.net</a></td>
<td>1.49 KB</td>
<td>Your 2009 Order #099999</td>
<td>Fuzzy-Filter</td>
</tr>
<tr>
<td>7BC6CF0F09D7</td>
<td>16:10:20 07.21.12</td>
<td><a href="mailto:inthone@inthecloud.com">inthone@inthecloud.com</a></td>
<td><a href="mailto:info@email24.net">info@email24.net</a></td>
<td>2.33 KB</td>
<td>Prepare yourself for your new site...</td>
<td>RBL-Filter</td>
</tr>
<tr>
<td>7C879BC2D000</td>
<td>16:10:20 07.21.12</td>
<td><a href="mailto:clark@seniorcollege.com">clark@seniorcollege.com</a></td>
<td><a href="mailto:info@email24.net">info@email24.net</a></td>
<td>5.34 KB</td>
<td>October 71% OFF</td>
<td>Fuzzy-Filter</td>
</tr>
<tr>
<td>7F8ED63C507B</td>
<td>16:10:20 07.21.12</td>
<td><a href="mailto:leiforsay557@uobmail.ly.com">leiforsay557@uobmail.ly.com</a></td>
<td><a href="mailto:info@email24.net">info@email24.net</a></td>
<td>7.09 KB</td>
<td>Congratulations Online Marketing Co.</td>
<td>RBL-Filter</td>
</tr>
</tbody>
</table>

NOTICE

The e-mail is only listed in the spam queue if the action "QUARANTENE" is set for the filter.

CISS Queue

E-mails whose senders are still unknown to the Spamfinder ( ⇒ not yet entered in the address or domain whitelist), are set to the CISS queue with activated CISS filter.

NOTICE
Make sure that OVERSTEERING of the negative filter CISS is activated for the filters AWL and DWL. For more details about the CISS filter technology, refer to the chapter 4.3.2.5 Filter - CISS.

Viruses and prohibited File Extensions

E-mails with viruses in attachments or attachments with prohibited file extensions are sent to the virus queue. Zipped file extensions are also checked for viruses if they are not encrypted.

**NOTICE**

Only the administrator can view and manage the virus queue.

The queues can be searched and deleted.

**Also see:** "Appliance Administration - Mail Queues".

Send E-Mail

You can send e-mails to the recipient in the respective queues.

**Restrictions:** E-mail forwarding is only possible in the queues Spam, CISS and Viruses.

1. In the tree view, select *Queues* with a double-click.
2. Select the desired queue.
3. Right-click on the e-mail to be sent.
4. In the selection list, choose the entry *Send*.

Send E-Mail (Whitelist)

In the respective queues, you can send e-mails to the recipient and enter him in the Whitelist at the same time.

**Restrictions:** E-mail forwarding is only possible in the queues Spam and CISS.

1. In the tree view, select *Queues* with a double-click.
2. Select the desired queue.
3. Right-click on the e-mail to be sent.
4. In the selection list, choose the entry *Send (whitelist)*.

Sorting E-Mails

In the respective queues, you can sort e-mails via the column head in the list view.

**Requirement:** E-mails available in the list.

1. In the tree view, select *Queues* with a double-click.
2. Select the desired queue.
3. Double-click on the column head according to which you wish to sort your e-mails. Sorting takes place alphabetically.
4. The Administrator Console

4.3.2 Filters

Information about Filters
Contrary to concentrating on what's not desired, the REDDOXX Appliance filters out the e-mails the user wants to receive. Therefore the technology is based on the most modern and innovative filter techniques.

The sequence of different filter technologies can be configured individually and also be made available individually to the users via different profiles.

How E-Mails are Filtered

![Filter scheme](image)

Illustration: Filter scheme
4.3.2.1 Whitelist Filters

Whitelists are so-called friendly lists, and inasmuch as certain criteria are fulfilled, the e-mails are forwarded directly without delay. These lists vary from individual e-mail addresses up to general domain addresses. They may contain individual IP addresses or IP address ranges or simply certain subject contents that classify an e-mail as "desired". In the REDDOXX Spamfinder, these lists were implemented as follows:

- AWL: Addresses Whitelist
- DWL: Domain Whitelist
- NWL: Network Whitelist
- SWL: Subject Whitelist

These filter lists are available to all users of a system on a general basis but also for individual users in order to perfect the accuracy of the REDDOXX Spamfinder.

Whitelist Auto-Add Adjustment

The whitelists are automatically supplemented as soon as a user sends an e-mail. This happens so that the answers to these e-mails are classified as "desired" and therefore forwarded.

**NOTICE**

To use the auto whitelist function, the outgoing mail traffic must also be routed via the REDDOXX Appliance.

4.3.2.2 Blacklist Filters

E-mails from certain domains, IP ranges, e-mail addresses or with certain subject content can be filtered out by the integrated Blacklist technologies. The administrator can create these lists company-wide and users can additionally maintain them.

However, the Blacklist filters of the REDDOXX Spamfinder are also based on external, public lists. A general problem of these filter techniques is the risk of wrong detection (so-called false positives).

The integrated user quarantine function of the REDDOXX Spamfinder reduces the risk of false-positives, because each user has the possibility to access his quarantine section and make sure that it does not contain e-mails, which don't belong there.

This also reduces the administrators' efforts to look for important e-mails among the spam.

The Blacklist filters integrated in the REDDOXX Spamfinder are:

- ABL (address blacklist): Checking the sender's address against an address blacklist maintained in the REDDOXX Spamfinder
- DBL (domain blacklist): Checking the sender's domain against an address blacklist maintained in the REDDOXX Spamfinder
4. The Administrator Console

- **NBL (network blacklist):**
  Checking the IP address of a sending e-mail server against a network blacklist maintained in the REDDOXX Spamfinder.

- **SBL (subject blacklist):**
  Checking the e-mail's subject line against a subject blacklist maintained in the REDDOXX Spamfinder.

**On the basis of external servers, the following filters are also available:**

- **RBL (realtime blacklist):**
  Realtime check of the sending mail server against public blacklist servers.

- **ABL (advanced realtime blacklist):**
  The advanced realtime blacklist filter checks the last mail server in the mail flow, meaning the one who sends the e-mail to the Spamfinder. If you obtain your e-mails via an own relay, this must be excluded in the configuration.

- **Fuzzy filter:**
  Filter developed by REDDOXX, which compares the content of the e-mail with already identified spam mails.

- **SRC (sender receive check):**
  The sender receive check filter is used to determine whether an e-mail is sent from an existing e-mail account. This e-mail account would then in turn accept a response to the corresponding e-mail. If not, the SRC filter kicks in. In order to prevent that e-mails without a valid sender, e.g. some newsletters or order systems, are not delivered by accident, we recommend setting the filter action with the SRC to MARK. In addition, you can maintain your desired newsletters in the whitelists.

### 4.3.2.3 Content Filters

**SWL: Subject Whitelist, SBL: Subject Blacklist and Bayes Filter**

Content filters like the Bayes Filter are adapted to each user and also adapt to changes in spam. In order to detect e-mails as spam, these filters use Bayesian check sums to check the words and sentences of an e-mail with respect to their frequency for spam probability. Previous e-mails serve as comparison (spam and desired mails). The architecture of the REDDOXX Spamfinder's content filters refers to the CISS method, which first takes over the information of the content filters into the database when the CISS was passed successfully.

### 4.3.2.4 Global Filters

**Norman Antivirus Filter**

As a comprehensive security system for e-mails, the REDDOXX Spamfinder Appliance also contains an integrated virus protection for your e-mail server. In order to highlight the quality standards of the filters, we use the virus protection by Norman Defense, based on the sandbox technology.
4. The Administrator Console

4.3.2.5 CISS

The Innovation of the REDDOXX Spamfinder Appliance is called CISS

CISS (Confirmation Interactive Site Server), is a unique, several stage control process, which ensures the permanent exchange of wanted mails between sender and recipient.

**Stage 1:** E-mail receipt, check for viruses through anti-spam filter and temporary saving. Dispatch of a response e-mail to the sender with the request for authentication at the stated link.

**Stage 2:** Request to perform a certain action on the Internet page, which can only be performed by a person, not by spam robots.

**Stage 3:** Feedback from the portal to the REDDOXX Spamfinder about the successful authorization and automatic forwarding of the e-mail to the recipient.

**How does CISS work?**
Known sender sends e-mail:
1. A customer or business partner sends you an e-mail.
2. The REDDOXX Appliance checks this e-mail with respect to viruses, worms, Trojans and of course, also whether this is a spam mail.
3. After this check, the e-mail is forwarded to you immediately.

Unknown sender sends e-mail:
1. An unknown person writes you an e-mail.
2. The REDDOXX Appliance checks this e-mail with respect to viruses, worms, Trojans and of course, also whether this is a spam mail. Because the sender is unknown, the e-mail is saved temporarily. The Spamfinder generates an e-mail to the sender with the request for the one-off authentication at the stated link.
3. On this Internet page, the sender is asked to perform a certain action, e.g. click on a certain part of an image.
4. Such actions can only be performed by persons and not automatically.
5. This action generates a reply to the REDDOXX Appliance about the successful authentication of the sender.
6. The saved e-mail is directly sent to you and now there is nothing in the way of your new business transaction!
4.3.2.6 Filter Settings

You can configure the individual filters via the filter configuration.

Realtime Blacklist Filter Configuration

The Realtime Blacklist Filter is a DNS Blacklist Filter. The Advanced Realtime Blacklist Filter is an Extended DNS Blacklist Filter. You can configure the Advanced Realtime Blacklist Filter as follows.

In the tree view, double-click on **Filters - Filter settings**

The following fields are displayed:
4. The Administrator Console

1. Enter a blacklist which the corresponding filter is supposed to query.
2. With the button Add, add the blacklist to the list.
3. With the button Add, add the relays you trust within your mail flow. You can obtain the name of the relay e.g. from the header of a mail (e.g. mail.company.net).
4. Click on Ok to save the configuration and exit.
   CANCEL: Reject changes and exit the configuration.

Auto Whitelist Adjustment Configuration
This filter adds the recipient of the outgoing e-mails to the sender’s Address Whitelist.

1. Select the tab – **Auto whitelist adjustment**.
   The following fields are displayed:
   
   ![Filter configuration – Auto white list adjustment](image)
   
   Illustration: Filter configuration – Auto white list adjustment

3. If required, activate this filter.

4. Enter the desired validity in days.

   **NOTICE**
   
   Whitelists should be valid for at least 90 days.
   
5. To prevent that the sender address of a spam sender is entered in the white list due to an automatic response of your mailbox, you can deny the whitelisting of any subjects, e.g. holiday, absence (out of office), etc. To do so, enter a part or the entire subject into the subject exclusion field. This setting applies globally for all users.

   **NOTICE**
   
   The recipient of the outgoing e-mails cannot be configured for AutoResponder; use the exception function for this purpose.

6. With the button ADD, add the exception to the list.
   With the button DEL, you can delete any exception already entered again.

7. Click on **OK** to save the configuration and exit.
   **CANCEL:** Reject changes and exit the configuration.

**Virus Scanner Configuration**
In the configuration of the virus scanner, you can set to whom the notifications are sent. Here you can also state file extensions for attachments that are not allowed to pass.

**Restrictions:** Only the Virus Scanner can be configured the following way.

2. Select the tab **Virus scanner**.
   The following fields are displayed:

   ![Illustration: Filter configuration – Virus Scanner](image)

3. Activate the target person(s) that are supposed to receive a notification.
4. Enter the file extension to be blocked (e.g. .exe) and click on **Add**.
5. Click on **OK** to save the configuration and exit.

   **CANCEL:** Reject changes and exit the configuration.

   **NOTICE**
   Please make sure that the entry of the file extension starts with a dot (.)

---

**CISS Filter Configuration**

With the CISS filter configuration, you can set the validity of the whitelist in days and the maximum challenges per sender. Challenges are the attempts of the sender to send an e-mail to the recipient for the xth time (here: 3 times) without receiving a response from the recipient.

**Restrictions:** Only the CISS Filter can be configured the following way.
1. Select the tab **CISS filter**.
   The following fields are displayed:

   ![Illustration: Filter configuration – CISS Filter](image)

2. State the desired validity of the CISS Filter whitelist in days.
3. Enter the maximum challenges per sender.
4. Click on Ok to save the configuration and exit.
   CANCEL: Reject changes and exit the configuration.
Bayes Filter

In the Bayes filter configuration, you can delete the Bayes database and activate/deactivate the automatic training of the filter

1. Select the tab **Bayes filter**.
   The following fields are displayed:

   ![Filter configuration – Bayes filter](image)

   - **Status**
     - Number of spam messages: 773676
     - Number of good messages: 3383
     - Database size: 524,32 MB

   - **Settings**
     - Enable automatic bayes training
     - Reset bayes database

   Illustration: Filter configuration – Bayes filter

2. The status contains the number of mails that serve as basis for the Bayes filter. The system distinguishes between spam and undesired mails. The physical size of these mails is additionally displayed in the database.

3. **Activate automatic training:**
   Before you apply the Bayes filter, you should train it for approx. 1 week first. In doing so, the filter learns, which mails are desired or undesired by using whitelists and blacklists and constructs its database accordingly using the contents.

   For details about the functioning of the Bayes filter, see the chapter "Filter settings".

4. **Emptying the Bayes database:**
   Due to initial configuration errors of the REDDOXX Appliance or wrong entries in the blacklists and whitelists, it may happen that the Bayes filter classifies contents as SPAM and takes them over into its database and therefore reports desired mails as spam or does not detect undesired e-mails. In this case, you should check the
configuration of the REDDOXX and the blacklists/whitelists. Then you can empty the database and re-establish it (= training).

NOTICE

After one week of training the Bayes filter, both values for the spam e-mails or the number of desired mails should show positive figures. The larger the two values are, the more exact the filter is going to work. Should the database become too large at one point (depends on the hardware equipment of your REDDOXX Appliance), this may impair the processing speed. In such a case, you can empty the database and retrain it.

4.3.2.7 Filter Profiles

The core of the Spamfinder is its filter profiles. Here you can enter filter rules according to your spam frequency.

You can also create new profiles, change available profiles, copy and also delete them.

Here you define, which filters are allocated to a profile and which profiles are to be available to the user for selection. Both the administrator as well as the user (if authorized) can add filter profiles to e-mail aliases.

Illustration: Filter Profiles

Pre-defined Filter Profiles

The REDDOXX has 4 pre-defined filter profiles. In the basic configuration, they always contain the positive filters DWL, AWL and SWL.

Default Filter Profile

Initially, the default profile contains the filters FUZZY, RBL, ARBL, DBL, ABL, SBL, SRC.

With automatic user and e-mail alias creation, the default profile is always assigned first. Set this profile in such a way that it meets the requirements of most users in your company. The
automatic e-mail alias generation with automatic assignment to the default filter profile significantly reduces the administration extent.

**Quarantine Filter Profile**

Initially, the quarantine profile contains the filters FUZZY, RBL, ARBL, DBL, ABL, SBL, SRC and BAYES. You can adapt this profile in such a way that it corresponds to the requirements deviating from the default profile.

The actions of most of these filters are set to quarantine. Bayes and SRC are set to "Mark".

**Strong Filter Profile**

The strong filter profile contains the filters FUZZY, RBL, ARBL, DBL, ABL, SBL, SRC and CISS. This profile is intended for users that want an immediate and reliable spam protection. This is ensured by the CISS filter.

**Built-In Profile**

The *built-in profile* is used if no filter profile was assigned to the e-mail alias yet. Prerequisite is the general activation of the profile (see chapter 4.1.2.5.). It cannot be changed. It signals the administrator that the REDDOXX is in operation but not sufficiently configured, or that there are generally no licenses or not for this user. The built-in profile only contains the filters RBL, ARBL and FUZZY. Detected SPAM e-mails are marked with the tag [REDDOXX Spamfinder], a deviating tag is not possible.

**Creating a new Filter Profile**

**Requirement:** None.

1. Select *Filter Profiles* in the tree view.
2. Right-click in the list view.
3. In the selection list, choose the entry **Add**.

The following fields are displayed:
4. Enter the name of the profile in the profile options.

5. Activate the option Available to user, if you also want to make the filter profile available to the users. Then the users can select this filter profile for their e-mail addresses in the user console.

6. Import or export filter profiles, if applicable.

   Export your desired filter profiles to be able to import it to another REDDOXX Appliance (e.g. at a subsidiary).

**Filters**

Different filters can be selected and compiled according to priority.

**Requirement:** None.

1. Click on the tab "Filter"

   The following fields are displayed:
2. **Positive filter - Selected:**
   All active positive filters are listed in the field *Selected*. You can change the sequence of the filters with the vertical arrows. To do so, mark the desired filter and click on the corresponding button. You can change the sequence of the filters with the vertical arrows. Sequence: from top to bottom, top first.

3. **Positive filter - available:**
   All available positive filters are listed in the field *Available*. Via the horizontal arrows, you can add the available filters to the list of selected filters and vice versa. To do so, mark the desired filter and click on the corresponding button. You can change the sequence of the filters with the vertical arrows. Sequence: from top to bottom, top first.

4. **Negative Filters:**
   The same as for the positive filters (point 2-3) applies for the fields "Selected" and "Available". In addition, you can assign 3 different actions to the individual negative filters. To assign or change an action, double-click on a filter. The following window appears:
5. **Tag**: A tag is a text that is prefixed to an e-mail in the subject field if the desired action MARK is selected. Other actions do not change the subject.

6. **Action**: In this selection list, you can choose between 3 actions:
   1. **Mark**: Marks the e-mail in the subject field with the entered tag. The tag is prefixed to the subject and the e-mail is sent.
   2. **Quarantine**: The e-mail is shifted to the protected quarantine directory and not sent to the recipient. All e-mails in quarantine are located in the Spamfinder queues.
   3. **Reject**: The e-mail is rejected and not sent to the recipient. The sender receives a bounce e-mail.

**Notice**

If several negative filters kick in, the action with the strongest weighting is triggered.

Weighting sequence: MARK (light) - QUARANTINE (medium) - REJECT (strong).

With the anti-spoofing filter, make sure that the marking is not set to REJECT. Otherwise a bounce e-mail is generated that may be sent to you because your address was stated as sender.

**Filter Sequence**

The filter sequence is defined by the performance relevance and the false positive rate of the filter.

The selected negative filters are applied from top to bottom. If the action REJECT is triggered with a filter, no other filters are processed:

<table>
<thead>
<tr>
<th>Filters</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti-spoofing</td>
<td>Quarantine</td>
</tr>
<tr>
<td>Fuzzy</td>
<td>Quarantine</td>
</tr>
<tr>
<td>RBL</td>
<td>Quarantine</td>
</tr>
<tr>
<td>Advanced RBL</td>
<td>Quarantine</td>
</tr>
<tr>
<td>SBL</td>
<td>Mark</td>
</tr>
<tr>
<td>ABL</td>
<td>Mark</td>
</tr>
<tr>
<td>DBL</td>
<td>Mark</td>
</tr>
<tr>
<td>SRC</td>
<td>Mark</td>
</tr>
</tbody>
</table>
Oversteering Filters

If expressively desired e-mails (whitelist entry) are to be forwarded without further checking for SPAM relevance, the negative filters must be oversteered by the respective positive filters (DWL, AWL, SWL). The ANTISPOOFING filter is an exception here.

**Requirement:** None.

1. Select *Filter Profiles* in the tree view.
2. Right-click on a profile in the list view.
3. Click on the tab "Oversteer"
   The following fields are displayed:

   ![Illustration: Filter profiles – Tab "Oversteer"](image)

4. Select, which positive filters oversteer the negative filters. If a negative filter is oversteered by a positive filter, the negative filter no longer has any relevance.

   **NOTICE**

   Especially with the CISS filter, the AWL filter MUST oversteer the negative filter CISS, otherwise the CISS challenge is generated each time.
5. Click on Ok to save the configuration and exit.
   CANCEL: Reject changes and exit the configuration.

**Edit Filter Profile**
Here you can edit already created filter profiles.

**Requirement:** Created filter profile is available.
1. Select *Filter Profiles* in the tree view.
2. Right-click on the filter profile to be deleted.
3. In the selection list, choose the entry *Edit.*
4. Make the desired changes.
5. Click on Ok to save the configuration and exit.
   CANCEL: Reject changes and exit the configuration.

**Copy Filter Profile**
Here you can copy already created filter profiles.

**Requirement:** Created filter profile is available.
1. Select *Filter Profiles* in the tree view.
2. Right-click on the filter profile to be copied.
3. In the selection list, choose the entry *Copy.*
4. Double-click on the filter profile with the addition (copy).
5. In the profile options, enter the name of the new filter profile.
6. Click on Ok to save the configuration and exit.
   CANCEL: Reject changes and exit the configuration.

**Delete Filter Profile**
Here you can delete already created filter profiles.

**Requirement:** Created filter profile is available.
1. Select *Filter Profiles* in the tree view.
2. Right-click on the filter profile to be deleted.
3. In the selection list, choose the entry *Delete.*
4. Confirm the prompting message with *Yes* to delete the profile.
   No: Profile is not deleted.
4.3.2.8 Blocking and Admitting

Blocking and Admitting (Blacklists and whitelists)
The following points apply for all lists described below:

- **Global or user-related:**
The settings for the black and whitelist entries in the administrator console apply globally, meaning for all users. If there are applicable black/whitelist entries for the user as well, these take precedence over the global settings. Therefore it may be that a global block is on REJECT, but the user has set the block to MARK. Fact is: The user always wins!
The following applies for all blacklists: The action selected for a block applies. The setting in the filter profile itself is of no relevance.

- **Validity date:**
Make sure to select a valid date in the future, otherwise the entry will not apply. At present, there are no progress reports. The default date is TODAY + 365 days.

- **Large/Small Caps:**
E-mail addresses, domain names and subject lines are not case sensitive.

- **Umlauts:**
Umlauts in subject lines are supported since version 1022.

**NOTICE**
IP-based blacklists are located in "SMTP settings - Blocked IP addresses. These apply system-wide and are profile-neutral.

Creating a new DWL Domain Whitelist
You can create new Domain Whitelists via the filter lists.

**Requirement:** None.

1. In the tree view, select **Blocking and admitting - DWL domain whitelist**.
2. Right-click in the list view.
3. In the selection list, choose the entry **New**.
   The following fields are displayed:
4. Enter a *Domain*.

5. State the validity period of the filter.
   Click on the calendar page if you need a calendar for the date selection.

6. If required, enter a comment to this filter.

7. Click on OK to save the configuration and exit.
   CANCEL: Reject changes and exit the configuration.

---

**Creating a new DBL Domain Blacklist**

You can create new Domain Blacklists via the filter lists.

**Requirement:** None.

1. In the tree view, select Blocking *and admitting - DBL domain blacklist*.
2. Right-click in the list view.
3. In the selection list, choose the entry *New*.
   The following fields are displayed:

4. Enter a *Domain*.

5. State the validity period of the filter.
   Click on the calendar page if you need a calendar for the date selection.

6. Select the *action* for the filter via the selection list.
   The possible settings are mark, quarantine and reject.
7. If required, enter a comment to this filter.
8. Click on OK to save the configuration and exit.  
   CANCEL: Reject changes and exit the configuration.

Creating a new AWL Address Whitelist
You can create new Address Whitelists via the filter lists.

**Requirement:** None.

1. In the tree view, select **Blocking and admitting - AWL address whitelist**.
2. Right-click in the list view.
3. In the selection list, choose the entry **New**.  
The following fields are displayed:

![Image of REDDOXX configuration window]

Illustration: Blocking and admitting - AWL address whitelist

4. Enter the desired **e-mail address**.
5. State the validity period of the filter.  
   Click on the calendar page if you need a calendar for the date selection.
6. If required, enter a comment to this filter.
7. Click on **OK** to save the configuration and exit.  
   **CANCEL:** Reject changes and exit the configuration.
Importing ABL Address Whitelist

Serves to import e-mail addresses to the address whitelist.

1. In the tree view, select **Blocking and admitting - AWL address whitelist**.
2. Right-click in the list view.
3. In the selection list, choose the entry **Import addresses**.
   The following fields are displayed:

4. Select "Read addresses from file".
5. Select the file to be imported in the dialog field - File selection.
   Format: one e-mail address per line. The address must be valid (@ sign). The line must be
   terminated with a CR line feed, also the last line. Invalid addresses, e.g. comments, are
   skipped.
   The following list is displayed:

6. Select in the menu "Import - Save addresses". Now the addresses are imported to the
   whitelist. You receive a control message stating how many addresses were imported.

Creating a new ABL Address Blacklist
You can create new address blacklists via the filter lists.

**Requirement:** None.

1. In the tree view, select *Blocking and admitting - ABL address blacklist*.
2. Right-click in the list view.
3. In the selection list, choose the entry **New**.
   The following fields are displayed:

![Illustration: Blocking and admitting - ABL address blacklist]

7. Enter the desired **e-mail address**.
8. State the validity period of the filter.
   Click on the calendar page if you need a calendar for the date selection.
9. Select the **action** for the filter via the selection list.
   The possible settings are mark, quarantine and reject.
7. If required, enter a comment to this filter.
8. Click on **Ok** to save the configuration and exit.
   **CANCEL:** Reject changes and exit the configuration.

**Create a new SWL Subject Whitelist**

You can create new Subject Whitelists via the filter lists.

**Requirement:** None.

1. In the tree view, select *Blocking and admitting - SWL subject whitelist*.
2. Right-click in the list view.
3. In the selection list, choose the entry **New**.
   The following fields are displayed:
4. Enter a character string.

5. State the validity period of the filter.
   The default is: Today + 365 days.
   Click on the selection list Valid until if you require a calendar for selecting the date.

6. If required, enter a comment to this filter.

7. Click on Ok to save the configuration and exit.
   CANCEL: Reject changes and exit the configuration.

Creating a new SBL Subject Blacklist

You can create new Subject Blacklists via the filter lists.

**Requirement:** None.

1. In the tree view, select **Blocking and admitting - SBL subject blacklist**.

2. Right-click in the list view.

3. In the selection list, choose the entry **New**.
   The following fields are displayed:

   4. Enter a character string.
5. State the validity period of the filter.
   The default is: Today + 365 days.
   Click on the selection list *Valid until* if you require a calendar for selecting the date.

6. Select the *action* for the filter via the selection list.
   The possible settings are mark, quarantine and reject.

7. If required, enter a comment to this filter.

8. Click on *Ok* to save the configuration and exit.
   *CANCEL*: Reject changes and exit the configuration.

---

**Edit Filters**

Proceed as follows to edit an existing filter.

**Requirements:** Filter is available in the list view.

1. In the tree view at *Block and admit*, select the respective filter list.
2. Double-click on the filter to be edited.
   The configuration window opens.
3. Make the desired changes.
4. Click on *Ok* to save the configuration and exit.
   *CANCEL*: Reject changes and exit the configuration.

---

**Delete Filter**

Proceed as follows to delete an existing filter.

**Requirements:** Filter is available in the list view.

1. In the tree view at *Block and admit*, select the respective filter list.
2. Right-click on the filter to be deleted.
3. In the selection list, choose the entry *Delete*.
4. Confirm the prompting message with *Yes* to delete the Internet domain.
   *No*: Realm is not deleted.
4. The Administrator Console

4.4 REDDOXX MailDepot

Illustration: Navigation tree REDDOXX MailDepot

4.4.1 Archive Configuration

Making General MailDepot Settings

Via the general settings, you can activate e-mail archiving, select the location for saving (= archive type), and configure the access to a network remote share.

Requirement: Opening the Settings.

1. In the tree view, click on REDDOXX MailDepot.
2. In the tree, double-click on the branch Archive configuration.

The following fields are displayed:

![General Archive data Filter settings]

- E-mail archiving:
  - Enable archiving: check box
  - Archive type: drop-down menu

- Network share:
  - Share type: drop-down menu
  - Share: text field
  - Username: text field
  - Password: text field
  - Domain: text field

- Indexer:
  - Enable full text indexer: check box
  - Indexing time: text field

[OK Cancel]
3. **E-mail archiving – Activate archiving:**
   Turns archiving on or off.

4. **E-mail archiving – Archive type:**
   The archive type defines whether the e-mails are saved locally on the REDDOXX Appliance or in a network access.

5. **Network permission - Permission type:**
   Defines the permission type. Only Windows permissions are supported at present.

6. **Network permission - Permission:**
Enter the UNC path

<table>
<thead>
<tr>
<th>NOTICE</th>
</tr>
</thead>
</table>
| The path is stated in UNC (Uniform Naming Convention) format:  
\servername\foldername  
Please do not state any subdirectories and final backslashes.  
The path for the MailDepot may not be the same one as the permission that was configured for the backup. |

7. **Network permission – user name:**
Enter the **user name**. For security reasons, we recommend not using the administrator for archiving but instead a separate user (e.g. reddoxx)

8. **Network permission - Password:**
Enter the corresponding **password**.  
**The password may not be longer than 16 characters!**

9. **Network permission - Domain:**
   If applicable, enter the name of the domain belonging to the permission.

10. **Enable the full text indexer**- enables that the daily incremental indexer indexes the mails which have been coming in during the day.

11. **Time point when the daily incremental indexers starts**

12. For additional configurations, change to the next tab.  
   **OK:** Saves the settings and closes the Appliance Configuration.  
   **CANCEL:** Cancels the settings and closes the Appliance Configuration.

### 4.4.1.1 MailDepot Archive Data

#### Defining Archive Data

You can switch e-mail archiving from local to decentralized archiving or vice-versa.

Data transfer starts immediately after clicking on one of the two buttons. Check the log display for possible error messages.

**Requirement:** Opening the Settings.

1. Click on the tab "Archive data"
   The following fields are displayed:
4. The Administrator Console

2. Button **Switch MailDepot to decentralized archiving:**
   The archive data is transferred from the local hard drive of the REDDOXX Appliance to the UNC path.

3. Button **Switch MailDepot to local archiving:**
   The archive data is transferred from the UNC path to the local hard drive of the REDDOXX Appliance.

4. For additional configurations, change to the next tab.
   **OK:** Saves the settings and closes the Appliance Configuration.
   **CANCEL:** Cancels the settings and closes the Appliance Configuration.

### 4.4.1.2 MailDepot Filter Settings

**Defining Filter Settings**

Via the filter settings, you can define the archiving volume. Here you can state whether e-mails, which were declared as spam by a certain spam filter, are to be excluded from archiving.

**Requirement:** Opening the Settings.
1. Click on the tab "Filter settings"
   The following fields are displayed:
   
   ![Illustration: REDDOXX MailDepot general]

   2. Preventing archiving: Mark all filters that are supposed to prevent archiving.

   3. For additional configurations, change to the next tab.
      OK: Saves the settings and closes the Appliance Configuration.
      CANCEL: Cancels the settings and closes the Appliance Configuration.

### 4.4.2 Archive List

**The MailDepot Archive List**

In the archive list, you see all e-mails archived by the MailDepot with exception of the spam (incl. CISS) and virus e-mails. You can have this displayed by activating the respective checkboxes in Advanced search.

On the initial listing you get the first 1000 mails. To get all the mails enter a "@" into the search field. The initial listing can be adjusted and more limited under APPLIANCE ADMINISTRATION – SETTINGS – ADVANCED (siehe chapter 4.1.2.4)

**Requirement:** MailDepot is active.

1. In the navigation tree, click on **Archive list**.
   The following view is displayed:
2. **Search term**: Enter the criterion for which you want to search.

3. **Search in**: Select the desired field type in the selection list. The default is "Sender and receiver". Other available selections are: sender, recipient, subject, attachments.

4. **Search**: Click on Search to start the standard search.

5. **Advanced**: Click on **ADVANCED** to open the option window for the advanced search. The following window appears:

![Image of REDDOXX MailDepot archive list - Advanced search]

6. Fill in the fields as you wish and click on Search.
   A click on Cancel closes the window.

**NOTICE**

E-mails that were deposited in the CISS queue were also already archived. And that independent of whether the challenge was answered or the e-mail sent from the queue.
4.5 REDDOXX MailSealer Light

With the MailSealer Light, you can encrypt e-mails for sending. Here you can choose between the ad-hoc and the permanent method.

4.5.1 Ad-Hoc Encryption

Encryption with a pass phrase in the subject line.

To send an e-mail encrypted once, enter your pass phrase in the subject line. The pass phrase is delimited by previously defined characters. The default is (* .... *).

Application example:

Illustration: Subject with statement of a pass phrase for ad-hoc encryption

Upon sending, the e-mail first reaches the REDDOXX and is encrypted with the pass phrase here. The pass phrase is removed from the subject line in this process and the text MailSealer: is prefixed to the subject. Then the e-mail is sent. The recipient receives the following notice in the message text:

Illustration: E-mail indication of an encrypted mail

The sender has this email encrypted with the REDDOXX MailSealer Light, because it contains confidentially informations.

To read this email you need the free of cost REDDOXX MailSealer Light Reader which you can download here.

Url: http://mailsealer.reddoxx.net

The required passphrase you will get from the sender.
The encrypted e-mail is enclosed as attachment „message.rdxmsl“. When double-clicking on the attachment, the reader opens and demands the pass phrase.

After successful entry, the reader displays the encrypted e-mail in plain text.

**NOTICE**
If the recipient receives an encrypted mail from REDDOXX for the first time, he must download the MailSealer READER once from the stated hyperlink and link this program with the file extension .rdxmsl.
4.5.2 Permanent Encryption

With permanent encryption, the user deposits the pass phrase for each e-mail address to which he wants to send encrypted e-mails in the user console.

![Illustration: Pass phrase setting in the user console](image)

4.5.3 MailSealer Light - Gateways

Automatic encryption and decoding of e-mails.

If the user also has a REDDOXX, he can deposit the pass phrase for decoding the e-mails in the user console. The e-mail is automatically decoded when received and placed in the mailbox. This procedure is totally transparent and does not require any user interaction.

4.5.4 MailSealer Light Configuration

![Illustration: Navigation tree REDDOXX MailSealer](image)
1. Double-click on the branch *MailSealer configuration*. The following dialog appears:

![Illustration: Navigation tree REDDOXX MailSealer light - configuration]

Illustration: Navigation tree REDDOXX MailSealer light - configuration

2. Activate the MailSealer Light by ticking the checkbox.
3. Open tag: Enter a character string here, which you use to mark the start of a pass phrase in the subject line.
4. Close tag: Enter a character string here, which you use to mark the end of a pass phrase in the subject line.
5. Click Ok to finish the configuration
5 Options in the Menu Bar

The main menu consists of the sections File, View, Language, Appliance and Info.

5.1 File: System Login/Logout

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

5.1.1 Logging in (Connect)

Requirements: The administrator console (the program sf-admin.exe) must be started. There is no current connection to the system (logged out).

In the main menu File, click on Connect.

The following dialog is displayed:

Illustration: Login window
3. *Host name:* Enter the host name to which you want to connect or select it from a list. The list contains the entries you already made so far.

4. *User name:* Enter sf-admin.

5. Enter the password.

**NOTICE**

The following standard values are set upon delivery of the REDDOXX Appliance:
*User name:* sf-admin and *password:* admin

6. In realm, select the option "local".

7. Select the desired *language* in the selection list, which you want to use to display your program.
   The selection contains the currently installed languages.

8. Click on the button **LOGIN**.
   The application window for the basic configuration is now active.

### 5.1.2 Logging off (disconnect)

If you want to login to another REDDOXX Appliance, you first have to disconnect the current connection.

1. In the menu bar, click on Disconnect.
2. Close the application (exit) or login again.

### 5.1.3 Exiting the Program (exit)

To exit the administrator console, select the menu point Exit. Any connections that are still established are closed as well.

### 5.2 View

![Illustration: Menu View](Image)
5. Options in the Menu Bar

5.2.1 Search

With the option SEARCH, you show or hide the search field in the top right part of the window. This way, you can search the entries in all queues according to sender or receiver.

**Requirement:** The content of a queue or the archive list is displayed.

![Illustration: Search entry field]

1. **Search term:** Enter the criterion for which you want to search.

   **NOTICE**
   Per default the view is limited up to 1000 entries. Fill in a „@“ if you want to see all entries.

2. **Search in:** Select the desired field type in the selection list. You can select between "Sender" (preselection) and "Recipient".

3. **Search:** Click Search to start the search.

5.2.2 Log

Via the option Log (also F7 key), you can turn the live log on or off. In deactivated mode, you therefore have more room for the above list view.

5.2.3 Status

Via the option Status (also F8 key), you can turn the appliance status display on the bottom left of the window on and off. In deactivated mode, you therefore have more room for the above navigation tree.

5.2.4 Statistic

Via "Statistic", you can create diagrams about the filter behavior of the REDDOXX Appliance, print and save them.

**Requirement:** Logs must be available.

4. In the menu bar, click on View.

5. In the selection list open the context menu with a right-click

   The following view appears:
3. **ADD Series** adds a new graph onto the diagram.

The following view appears:

4. **Make your desired selections**

5. **Add the desired statistic by clicking on OK.**

Following view appears:
6. Right click on a graph to open the context menu.
7. **Change Color** of the selected graph
8. **Remove** the selected graph from the chart.

### 5.2.5 Starting the Log Viewer

The Log Viewer lets you view logs. This corresponds to the same function as described in chapter 4.2.4, but you can also view logs that were already saved locally or logs of other REDDOXX Appliances (e.g. subsidiaries). To do so, open the dialog file and load the desired log file.

### 5.2.6 CISS Manager

#### 5.2.6.1 Configuring CISS - Creating Themes

Here you define the appearance (layout) of your CISS portal page. If you wish to have different layouts for separate domains, you need to create multiple themes and then assign a domain to your prepared themes.
5. Options in the Menu Bar

1. In the tree, right-click on *CISS themes*.
2. In the selection list, click on **Add theme** and assign a name of your choice.
3. Select a desired layout for your CISS page. 5 different layouts are available.
4. Then select the individual areas to define the corresponding layout.
5. In order to integrate a logo, click on the button **LOAD** in the Logo preview. The supported image formats are GIF and JPG.

**NOTICE**

Image size: 400px width. Larger images are automatically scaled down, smaller images are not enlarged.

6. In order to integrate a background image, click on the button **LOAD** in *Background image*. The supported image formats are GIF and JPG.

**NOTICE**

You can constantly see a preview of your generated CISS page. To do so, click on the button **Preview**.
5.2.6.2 Configuring CISS - Adding Images

Here you can add and configure images for use by CISS.

1. In the tree, click on your created theme and then right-click on Images. Then click on Add image and select the desired image.

The following view appears:

Illustration: CISS manager - images

2. Select the grid size for generating the interaction fields via the option Grid size. Now define the interaction fields by clicking on the desired image area.

**NOTICE**

Interactive fields are shaded. Clicking again on a shaded field cancels the interaction again.

3. To be able to configure click instructions, you first have to add languages.

5.2.6.3 Configuring CISS - Adding Languages

Here you can add and configure different languages for use by CISS.
5. Options in the Menu Bar

1. In the CISS navigation tree, click on your created theme and then right-click on Languages. Then click on Add language in the selection list and select the desired language. The following view appears:

![Illustration: CISS manager - languages]

2. For each language, you can now define separate text versions for the parameters "error page, thank you page, top text, back button and close window".

3. To define these texts, double-click on the corresponding parameters (e.g. error page). The text editor is displayed:

![Illustration: CISS manager - languages - text editor]

4. You can define your own texts in the text editor.

**NOTICE**
5. Options in the Menu Bar

You can obtain a selection of German and English sample texts from the REDDOXX Support Center at: http://support.reddoxx.net in the column REDDOXX Spamfinder – CISS - Text samples.

5.2.6.4 Configuring CISS - Adding Domains

Here you can assign a theme to an e-mail domain, which is then active for the use of CISS.

**Requirement:** A local Internet domain must already be configured.

1. In the tree, click on your created theme and then right-click on *Domains*. Then click on *Add domain* in the selection list and select the desired domain.

   The following view appears:

   ![Illustration: CISS manager - domains](image)

   **NOTICE**

   All e-mail domains entered in *Domains* are activated for use by CISS. However, in order for CISS to kick in, the CISS filter must be assigned for the respective filter profile.

2. click OK to add the domain to the theme.

3. To save the entire CISS configuration, click on *Save*.

   With a click on *CANCEL*, you close the CISS Manager and cancel the configuration.

5.3 Language

At present, you can select between 3 different languages. English, German and Italian.
5. Options in the Menu Bar

In the menu LANGUAGE, select the desired language. All views are immediately displayed in the new language.

Illustration: Menu item "Language"

5.4 Appliance

In the Appliance section, you can restart and turn the REDDOXX Appliance off, set the time and date as well as save and restore the configuration.

Illustration: Menu item Appliance

5.4.1 Restarting the REDDOXX Appliance

You can comfortably restart the REDDOXX Appliance via the REDDOXX console.

Requirement: Login to the REDDOXX Appliance.

1. In the menu bar, click on Appliance.
2. In the selection list, choose the entry Restart. The REDDOXX is ready for operation again in approx. 1 minute.

5.4.2 Turning the REDDOXX Appliance off

You can comfortably turn the REDDOXX Appliance off via the REDDOXX console.
5. Options in the Menu Bar

Requirement: Login to the REDDOXX Appliance.
1. In the menu bar, click on Appliance.
2. In the selection list, choose the entry **Shutdown**.

### 5.4.3 Setting the Time/Date

Here you can match the date and the time of the REDDOXX Appliance with the current settings of the computer.

Requirement: Right settings on the computer (BIOS).
1. In the menu bar, click on Appliance.
2. In the selection list, choose the entry **Set date / time**.

### 5.4.4 Setting the Backup Configuration

Once the REDDOXX Appliance was correctly set up, you can save all settings of the REDDOXX Appliance in a file. This way, you can restore the saved configuration status at any time.

Requirement: Login to the REDDOXX Appliance.
1. In the menu bar, click on Appliance.
2. In the selection list, choose the entry **Backup configuration**.
   Due to the fact that all configurations must be read out to save the settings, you briefly have to terminate all services. You have to confirm this in a dialog. The services are restarted again immediately after readout. No data is lost during this process.
3. Select the desired location for saving and save the configuration settings.

**NOTICE**

With activated data backup (see the chapter "Backup and Restore"), the configuration of the REDDOXX Appliance is also backed up.

### 5.4.5 Setting "Restore Configuration"

Already backed up configurations are reloaded in the restore configuration. To do so, select the already saved configuration file and open it. Afterwards the system tells you whether the configuration was successfully loaded.
5. Options in the Menu Bar

5.5 Info

5.5.1 License Information

Adapting the License Information

Here you can manage the licenses for the REDDOXX Appliance.

Requirement: Purchase of the REDDOXX Appliance.

1. In the menu bar, click on Info.
2. In the selection list, choose the entry License information.

The following view appears:

Illustration: License Information - license summary

3. In the selection In the license summary, you obtain information about the licensee, the number of licenses and the expiration of the subscription. By clicking on Update license, the license summary is updated.

Customer Address

Here you can manage and update your address data.

Requirement: Purchase of the REDDOXX Appliance.

1. In the menu bar, click on Info.
2. In the selection list, choose the entry License information.
3. Click on the tab "Customer address"
   The following fields are displayed:

   Illustration: License Information - customer address

4. Fill in all fields properly and click on Update address

5. **CLOSE** the window

**License Numbers**

This is where your REDDOXX licenses and subscriptions are managed.

1. Click on the tab "License numbers"
   The following fields are displayed:
2. You see an overview of all entered licenses with activation and expiration information. To enter a new license number, enter the number of the purchased license in the field **License number**.

3. To register the entered license number on the REDDOXX Appliance, click on the button **ADD LICENSE**.
6 The Appliance Console

General
The appliance console is used to make system closed configuration and administration tasks as for e.g. network settings, backup and restore settings and starting and stopping services.

How to connect to the appliance console
You get a appliance console on a directly plugged terminal, or via ssh protocol (port 22) with the putty-application on a Windows PC.
Login as user “admin” with initial password “SpamfinderAdmin”.

Overview
The Appliance console contains the following functions:
• initial network settings for immediate accessibility in the network;
• system and data backup (backup and restore);
• resetting the appliance to the original (factory) settings;
• Clear the MailDepot and rebuild the full text index of the mailarchive;
• starting and stopping the remote support services and the appliance;
• adapting the admin password for this appliance console.
6.1 Appliance Settings
Here you adjust the network and the backup settings for a Restore.

6.1.1 Network Settings
Adjust the appliance with hostname, Domain, IP-Address, Netmask, Gateway and two DNS-Servers.
6.1.2 Time Server Settings
Setup the time servers. Note, that you have opened UDP Port 123 on the firewall.

6.1.3 Backup and Restore Settings
Please refer to chapter 6.2.1.
6.2 Backup and Restore

6.2.1 Backup and Restore Settings
Setup the settings for backup and restore of the appliance.
Select a UNC-Share name without subdirectories.
Choose Username and password and a domain name for authentication against a domain controller if present.
6.2.2 Start an Appliance Backup

If you want to migrate the appliance to another hardware, you need a constant state. Stop the REDDOXX engine with **YES** to ensure this. The operation of the REDDOXX is stopped. **NO**: The operation of the REDDOXX is not interrupted. The backup runs in the background.

6.2.3 Start an Appliance Restore

With the cursor buttons, select the desired backup and activate it for restore with the SPACE bar. Then the marking shows an asterisk (*).
Confirm the prompt with YES. The RESTORE starts.

6.2.4 Synchronize REDDOXX MailDepot

You must synchronize the MailDepot directly after a RESTORE.

In this process, the e-mails still written to the Remote Share in the time between BACKUP and RESTORE are matched with the internal REDDOXX database.
6.3 Advanced Options

In the ADVANCED OPTIONS you can reset the appliance to factory default settings. Furthermore you can delete the whole MailDepot or rebuild the full text search index.

**WARNING**

Resetting the appliance to factory default settings will destroy all data. You are not able to restore the data until you have a successfully done BACKUP.
6.3.1 Rebuild the full text index of the Maildepot

Choose YES to start the rebuild of the full text search index.

On the screen appears as follows:

At this point the indexer is waiting until the next incoming email which is to be archived. This is necessary to mark the endpoint for the full text indexer and the starting point for the daily incremental indexer.

Please note that the Option „full text indexing“ in the MailDepot configuration is activated. If not set, the indexer is waiting until infinitely. If the option was not already enabled, you can enable now without interrupting the indexer. The indexer will recognize immediately after enabling this option.

After receiving the next mail into the archive the indexer starts and counts the amount of mails to be indexed and shows an estimated time how long it will take.

At the end the dialogue goes back to the main menu.

The full text indexer needs for ~ 500.000 emails on a MEDIUM appliance up to 24 hours. We recommend starting the full text indexing over the weekend.
6.3.2 Set Appliance Settings to Factory Defaults

Use this to reset the network configuration to the original state. Before resetting, you will be asked once again whether you really want to do this. Cancel with NO if you do not want to reset the appliance after all.

6.3.3 Set Spamfinder Settings to Factory Defaults

Serves to reset the Spamfinder settings to the original state. Before resetting, you will be asked once again whether you really want to do this. Cancel with NO if you do not want to reset the Spamfinder settings after all.

6.3.4 Re-Create Database

Serves to delete all e-mails, filter lists and user data. Before resetting, you will be asked once again whether you really want to do this. Cancel with NO if you do not want to reset the database after all.
6.3.5 Clear MailDepot

Here you can delete all data inside the MailDepot. The internal database will be cleaned and the local files will be deleted. File on a remote network share must be deleted by the administrator himself.
6.4 Start and Stop Services

6.4.1 Start REDDOXX Engine
Serves to stop and restart the REDDOXX Engine.

6.4.2 Start REDDOXX Remote Support
By starting the remote support services, you enable the support staff of sfbIT to access your REDDOXX Appliance.
Stop this services after checking with the REDDOXX support.

6.4.3 Appliance Reboot
Serves to restart the appliance. A prompt appears beforehand.
6.4.4 Appliance Shutdown
Serves to shut down the appliance. A prompt appears beforehand.

![Warning dialog]

6.5 Change Admin Password
Here you can change the password for the user admin for access to the appliance console. If you want to cancel the dialog, press CTRL-C.

![Password changing dialog]
7  FAQ - Frequently Asked Questions

The most frequently asked questions about the REDDOXX Appliance and the corresponding answers.

NOTICE
A complete list of all FAQs is located in the REDDOXX Support Center at http://support.reddoxx.net

Question:
What to do in case of a hardware failure?

Answer:
If you have purchased the option Next Business Day (NBD) - 24 hour response time - please contact technical support directly at:

Phone: +49(0) 741 248 / 816
e-mail: support@reddoxx.net

Important! - If you do not have this option, please contact your retailer.

Question:
Which rules apply for the subject, white and blacklists (SBL / SWL) and what are the filtering criteria?

Answer:
1. The partial string search applies. The entire expression must appear in the subject. This also applies for several words. A blank character is treated the same as any other character.
2. The characters are not case-sensitive.
3. There are no wildcards or regular expressions.
4. Umlauts and special characters are not yet considered.

Question:
How can the admin access the e-mails of employees?

Answer:
In case it is necessary to check the e-mails or if an urgent mail is expected and the employee is on holiday, it is possible to create access to his mail account. However, to do so, the employee must have appointed a deputy beforehand (e.g. the administrator or the supervisor).

Question:
Why do newly created users in the Active Directory not appear in the Spamfinder user administration?

Answer:
The Spamfinder only accesses the Active Directory when the recipient check is activated. Please check these settings at ==> Appliance configuration - SMTP settings – Local Internet domain - Tab LDAP - Recipient check
The user is first created in the Spamfinder when
- he first registers on the user console or
- sends or receives an e-mail via the Spamfinder for the first time.

In addition, it may be that the replication of the controller is not completed yet.
Check the log file for possible error messages.

**Question:**
What can I do when the Bayes filter does not function? RC 3 is stated in the log file.

**Answer:**
RC 3 means: general IO error in the internal database. This occurs very rarely. It may be caused by crashes, e.g. in case of a power failure. As a rule, however, the internal database can compensate such failures.

Deleting the Bayes database via the admin console (in the filter settings) solves the problem.

**Question:**
Does the virus scanner also scan ZIP archives?

**Answer:**
Yes. Zip archives are of course also scanned by the Norman Virus Engine. However, if the archive is encrypted or password-protected, a virus scanner cannot scan the archive.
You can test this e.g. with the test virus called EICAR.
8 Appendix

8.1 Contact and Support

Contact
If you have any questions, suggestions, praise or criticism concerning your REDDOXX Appliance, please contact us by e-mail or phone.

SfbIT GmbH
Saline 29
D-78628 Rottweil
Fon: +49 (0)741 248 810
Fax: +49 (0)741 248 811
E-mail: info@SfbIT.com
Internet: www.SfbIT.com

Support
The support team at SfbIT does everything in its power to satisfy customer demands and ensure customer satisfaction. This is why we offer extensive support options for all REDDOXX Appliances, which are available to our customers in a portal. Here is where you can find them: http://support.reddoxx.net

8.2 Deinstallation and Disposal

Deinstalling the REDDOXX Consoles
The following steps describe the deinstallation of the administrator and the user console.

Requirements: REDDOXX is no longer required.
1. Delete the files sfadmin.exe and sfuser.exe from your computer.
2. Reset your e-mail routing.
3. Separate the REDDOXX Appliance from all connections.

Disposing of the REDDOXX Appliance
Dispose of the appliance and the corresponding components in line with all national laws and regulations.
EAR no.: DE 86380757
8.3 License Agreements

General Terms and Conditions of SfbIT GmbH, Rottweil, for the Product REDDOXX

1. General section
2. Scope of application
   1. The Terms and Conditions of SfbIT GmbH, Saline 29, 78628 Rottweil (hereinafter referred to as „SfbIT“) for the Spamfinder Appliance (hereinafter referred to as „Spamfinder“) shall apply exclusively. Any terms set by SfbIT´s contractual partner (hereinafter referred to as “Customer”) at variance with the following Terms and Conditions and not expressly agreed in writing by SfbIT are not binding and are effectively contradicted. These Terms and Conditions shall also apply if SfbIT has unreservedly effected delivery to the Customer in full knowledge of the Customer's terms contradicting or at variance with the following Terms and Conditions.

2. These Terms and Conditions shall also apply to all future business dealings with the Customer.

3. These Terms and Conditions shall only apply to corporate clients.

2. Proprietary rights
   1. All software and hardware as well as all pictures, drawings, calculations and other documents shall be supplied subject to SfbIT’s ownership and proprietary rights.
   2. The Customer hereby agrees inter partes to hold SfbIT harmless of any proprietary rights claims as a result of deliveries being effected on the basis of the Customer's drawings or any other information infringing third-party proprietary rights.

3. Set-off right and right of retention
   1. The Customer shall only be entitled to set-off if and insofar as his counterclaims are legally valid, undisputable or agreed in writing by SfbIT. The Customer’s right of retention is limited to claims arising from the contractual relationship.
   2. The Customer may only withhold payment on the grounds of defects only to the extent of the defect and only if the existence of the defect can documented beyond all doubt.

4. Reservation of title
   1. SfbIT shall reserve the right of ownership of all delivered items until all payments pertaining to the delivery, including any dues as shall arise in the future, have been effected in full. In case of breach of the contract by the Customer, especially if the Customer falls into arrears, SfbIT reserves the right to take back the object of sale.
   2. The Customer agrees to handle the delivered items with care and to insure them at original value against any kind of loss at his own expense during the period of retention of title. SfbIT further reserves the right to insure the product itself at the Customer's expense.
   3. The Customer shall also bear all maintenance and inspection costs during the period of retention of title, even if the works are executed by SfbIT.
   4. The Customer shall notify SfbIT in writing without delay in case of seizure or any third-party intervention, so SfbIT can initiate a third-party action against execution. The Customer shall be liable to bear any legal and extrajudicial costs arising in connection with such claim insofar as the third party is not in a position to reimburse them.

5. Shipment, passing of risk
   1. Shipment shall be carried out at the Customer's risk. The risk shall pass to the Customer at the latest with the product being dispatched, even if further services are performed by SfbIT.
   2. Shipment is delayed due to circumstances beyond SfbIT’s control, the risk shall pass to the Customer from the day of readiness for shipment. SfbIT can insure the shipment against breakage, damage in transit as well as any damage caused by fire and water upon written request of the Customer and at his expense.
   3. In accordance with the Packaging Regulations, transport and all other packaging shall not be taken back. The Customer is obliged to dispose of the packaging at his own expense.

6. Perturbations affecting supply of services
   1. Should SfbIT not be in position to meet the agreed deadlines (“Perturbation”) for reasons beyond SfbIT’s control, including but not limited to strike or lockout, the deadlines shall be postponed by the duration of perturbation, including a reasonable reboot period if necessary. The contractual partner shall notify the other party without delay of the cause of the perturbation in his area and of the duration of the delay.
   2. In case of increased costs as a result of perturbation, SfbIT may also request compensation for these additional costs, insofar as the Customer is not responsible for the fault and its cause lies outside his area of responsibility.
   3. Should the Customer be able to or claim to be in a position to withdraw from the contract due to SfbIT failing to deliver the agreed services and/or to claim for damages in lieu of the service to be performed, the Customer shall upon SfbIT’s request confirm in writing within a reasonable deadline, whether he would like to assert his rights or further wishes the service to be performed. In case of withdrawal, the Customer shall reimburse SfbIT the value for previously existing possible use; the same applies to deteriorations as a result of proper use.

7. General liability of SfbIT
   1. SfbIT shall be liable towards the Customer
   2. for any damage caused wilfully or through acts of gross negligence by itself, its legal representatives or its agents, according to the Product Liability Act and
   3. for any damage causing injury to life, body or health, for which SfbIT, its legal representatives or its agents are responsible.
   2. SfbIT shall not be liable in case of ordinary negligence, except insofar as it is in breach of a major contractual obligation (cardinal obligation). For property damage, this liability shall be limited to the typical contractual predictable damage. This also applies to loss of profits and non-realised savings. Liability for any other more remote consequential damage is excluded. For a single claim, liability...
shall be limited to the contractual value, if fees are currently being paid, to the amount of the fees per contractual year, however no less than € 50,000. This section shall not affect liability under 7.1.

3. SfbIT shall only be liable to pay damages arising from a guarantee-undertaking, if this has been specified explicitly in the warranty. This liability is subject to limitations under 7.2 in case of ordinary negligence.

4. In case of data loss, SfbIT shall only be liable to the amount necessary for the restoration of the data subject to proper data storage by the Customer. In case of ordinary negligence, SfbIT shall only be liable if the Customer carried out proper data storage just before the measure responsible for data loss.

5. 7.1 to 7.4. shall apply to any claims for reimbursement of expenses and other liability claims of the Customer against SfbIT.

8. Obligation to maintain secrecy

1. The parties mutually commit themselves to maintain complete secrecy towards third parties regarding all business processes becoming known to them within the frame of their cooperation, especially business and industrial secrets. The obligation to maintain secrecy shall also endure after termination of the contract.

2. All business correspondence and documentation exchanged by the parties is to be kept carefully in the parties’ respective offices and to be protected from unauthorised inspection.

9. Covenant not to assign

1. No Customer claims against SfbIT from the contractual relationship may be assigned.

10. Product liability

1. The Customer shall only use Spamfinder in accordance with the intended use and must ensure that Spamfinder is only sold to persons familiar with the product risks.

2. The Customer shall fulfill its warning obligation when using Spamfinder as raw material and partial element of its own products upon bringing the final product into circulation, also with respect to the product delivered by SfbIT. The Customer shall inter partes hold SfbIT harmless of any claims arising as a result of a breach of this obligation upon first request.

11. Place of performance, place of jurisdiction, operative law, USA legal provisions

1. The place of performance is Rottweil.

2. The place of jurisdiction for all disputes arising from this contract is Rottweil. However, SfbIT reserves the right to bring an action against the Customer at the latter’s principal or secondary place of business.

3. Only German law shall apply. The application of UN purchase rights is excluded.

4. The Customer shall on his own authority observe all import and export regulations applicable to deliveries or services, especially US regulations. The Customer shall bear all customs duties, fees and other charges applicable to cross-border deliveries or services. The Customer shall on his own authority deal with all legal or official procedures in connection with cross-border deliveries or services, unless otherwise expressly agreed.

2. Rules for the purchase of Spamfinder

I. Subject-matter of the contract

I. Spamfinder’s nature and scope of performance as well as the environment for which it was released can be derived from the product description.

II. Spamfinder is supplied with operating instructions (user documentation or online-help) and installation instructions. Both operation instructions and installation instructions can also be supplied to the Customer electronically.

III. Spamfinder can be installed by the Customer.

II. Rights of use and protection against unauthorised use

I. SfbIT shall grant the Customer the right to use Spamfinder to the extent specified in the contract upon full payment of the fees due. In the absence of an agreement to that effect, the Customer shall be granted a simple non-exclusive right of use for permanent use, which only entitles the Customer to use Spamfinder on one computer with one single user at a time. The right of use granted to the Customer shall be for internal purposes only. Any extended use requires prior agreement before it can be implemented. Fees are based on the scope of the right of use.

II. The Customer may only copy the Spamfinder software insofar as it is necessary for use in conformity with the contract. Copyright notices in the software may neither be changed nor deleted.

III. SfbIT reserves the right to take adequate technical protective measures against any software use which is not in conformity with the contract. This may not significantly impair the use of Spamfinder in an alternative or subsequent configuration.

IV. SfbIT shall reserve the right of ownership of the surrendered reproduced versions until full payment of the fees owed, prior to which any rights of use are only temporary and may only be granted by SfbIT subject to revocation.

V. SfbIT may revoke the Customer’s right of use if the latter significantly contravenes any restrictions on use or any other regulations ensuring protection against unauthorized use, prior to which SfbIT may set a final deadline for remedy. SfbIT may issue a revocation without setting a final deadline in case of repeated infringements or in specific circumstances justifying immediate revocation upon consideration of the parties’ mutual interests. The Customer is to confirm any suspension of use in writing following revocation.

III. Obligations of the Customer

I. The Customer is to appoint a responsible contact person who is in a position to make or immediately initiate binding decisions for the Customer, and who can provide SfbIT with any necessary information.

II. The Customer shall ensure that qualified staff is available to use Spamfinder at the latest at the time of delivery.

III. The Customer shall notify SfbIT without delay of any changes in the operating environment.

IV. The Customer shall notify SfbIT in writing of any defects, in a comprehensible and detailed format, upon indication of all information necessary for fault recognition and analysis. He shall especially specify any working steps that caused a particular defect as well as the manifestation and effects of the same.

V. The Customer shall assist SfbIT with eliminating the defects if necessary; especially he shall provide SfbIT with working appliances upon request.
VI. The Customer hereby acknowledges that any future versions of Spamfinder as well as any operating instructions and other documents will also be copyrighted. This particularly applies to source programmes that constitute SfbIT industrial secrets. The Customer shall ensure at all times that source programmes cannot be accessed by third parties without SfbIT’s prior approval.

VII. The Customer may not undertake anything that may facilitate unauthorized use, like for instance attempting to decompile the programmes. The Customer shall notify SfbIT without delay of any imminent or already occurred unauthorized access in his area as soon as he has been informed.

IV. Customer’s warranty claims

I. The Customer shall not be entitled to warranty claims for material defects in case of only minor deviations of SfbIT’s services from the agreed quality or usability of the product. Likewise, the Customer shall not be entitled to warranty claims in case of excessive or improper use, natural wear and tear, failure of components in the system environment, non-reproducible or other software defects as can be identified by the Customer, or in case of damage caused by specific external influences that are not governed by the contract. This also applies in case of subsequent alterations or repair by the Customer or third parties, provided this does not impede analysis and elimination of a material defect. 1 7 shall additionally apply to all damage claims and claims for reimbursement of expenses.

II. Claims for material defects become statute-barred within one year from beginning of the statutory period of limitation. Statutory periods for claims under a right of recourse in accordance with § 478 BGB (German Civil Code) shall remain unaffected. The same applies in case of intentional or gross breach of duty on the part of the Customer, malicious non-disclosure of a defect, as well as in case of injury to life, body or health.

III. SfbIT’s processing of a claim for material defects of the Customer shall only result in a suspension of the Statute of Limitations insofar as all relevant statutory requirements are met. This does not entail a new beginning of the statutory period of limitation.

IV. Supplementary performance (new delivery or remedy) may only affect the statutory period of limitation of the defect requiring supplementary performance.

V. The Customer may only claim for material defects if the notified defects are reproducible or otherwise detectable. Notification of defects is especially subject to II 3.4.

VI. Should the Customer be entitled to warranty claims, he shall first only be entitled to supplementary performance within a reasonable period. Supplementary performance also includes, at SfbIT’s discretion, either remedy or delivery of replacement software. SfbIT shall take all Customers’ reasonable interests into account when making a decision.

VII. Should supplementary performance fail or if it cannot be realized for any other reasons, the Customer may, as per applicable legislation, reduce the fees, withdraw from the contract or assert a damage claim or claim for reimbursement of expenses. The Customer shall make use of his right to assert his warranty claims within a reasonable period, as a rule within 14 calendar days.

VIII. SfbIT may demand payment of its fees, insofar as

I. it took action following notification in the absence of a visible defect, unless the Customer was not in a position, with reasonable effort, to realise that there was no defect,

II. a notified fault is not reproducible or otherwise cannot be identified by the Customer, or additional expenses arise due to improper discharge of the Customer’s duties (also see II 3).

V. Legal imperfections in title

I. SfbIT shall only be liable for infringing third party rights through the delivery of its service insofar as the service is used in conformity with the contract and especially in the operating environment prescribed in the contract.

II. SfbIT shall only be liable for infringing third-party rights within the European Union and European Economic Area as well as the operating site of the service as prescribed in the contract.

III. The Customer shall notify SfbIT without delay of any third-party claims according to which SfbIT infringed their rights through the delivery of its service. SfbIT and, if applicable, its suppliers shall have the right, however shall not be obliged, to dismiss the asserted claims at their expense.

IV. In case of infringement of third-party rights as a result of SfbIT’s delivered service, SfbIT shall at its discretion and its own expense, procure the right of using the service to the Customer, or provide the service without infringing any rights, or withdraw provision of the service upon reimbursement of the fees paid by the Customer (minus an adequate compensation for use), if SfbIT cannot grant any other relief with reasonable effort. SfbIT shall take all Customer’s reasonable interests into account when making a decision.

6. Purchase price payment

1. The purchase price shall be due immediately.

2. SfbIT shall grant the Customer a payment term of 4 weeks from the date of shipment of Spamfinder.

7. Spamfinder malfunctions

1. It should be expressly pointed out that a defective configuration, classification and administration of Spamfinder, for which the Customer is responsible, may cause malfunctions. Configuration, classification and administration are entirely the Customer’s responsibility.

3. Virus protection

1. Spamfinder uses the Norman software virus protection. Licence Terms, Maintenance Terms as well as Terms and Conditions of Norman Data Defense Systems GmbH, Kieler Str. 15, 42697 shall apply to the virus protection module of Spamfinder. The Licence Terms can be downloaded from the following Web site: http://www.spamfinder.com/index.php?id=56&L=1

4. Rules for Spamfinder’s software maintenance

1. Subject-matter of the contract

1. Under the provisions of this contract, SfbIT shall provide the following maintenance services only for the current version of the Spamfinder object of maintenance upon payment of the agreed fees.

2. SfbIT shall provide the following maintenance services:

1. Fault management: SfbIT shall acknowledge and classify according to the agreed fault categories any fault notifications of the Customer, and based on this classification, perform the agreed fault analysis and elimination measures. Fault management does not
include services in connection with the use of Spamfinder in non-released environments or with modifications of Spamfinder by the Customer or third parties.

2. Receipt of fault notifications of the Customer: SfbIT shall receive and classify all orderly fault notifications of the Customer during its usual business hours. SfbIT shall confirm receipt of a Customer’s fault notification upon request of the Customer upon notification of the granted identification.

3. Implementation of measures for fault elimination: In case of serious faults and other types of faults being notified, SfbIT shall initiate any appropriate measures considering the circumstances notified by the Customer in order to first localise the origin of the fault. SfbIT shall notify the Customer without delay should the notified fault appear not to have been caused by Spamfinder following first analysis, failing which SfbIT shall initiate any relevant measures for more a detailed analysis and elimination of the notified fault. SfbIT shall provide the Customer without delay with Spamfinder instructions for use or corrections in case of existing measures to avoid or eliminate a Spamfinder fault. The Customer shall apply such measures to avoid or eliminate faults without delay and notify SfbIT of any remaining faults during implementation of the same.

4. Delivery of new versions: SfbIT shall provide the Customer with the new versions of Spamfinder in an effort to bring the product up to date and to prevent faults. SfbIT shall make the new versions available to the Customer's mailbox, who will then perform the installation himself from there.

5. SfbIT shall provide the Customer with Spamfinder updates including modifications and improvements as well as minor functional adds-on and improvements. Furthermore, SfbIT shall provide the Customer with correction patches for Spamfinder and with any other measures with a view to preventing possible faults. The new Spamfinder versions shall be jointly be known as “new versions”. The maintenance services do not include the delivery of upgrades with major functional adds-on or of new products or undertakings to develop Spamfinder, unless otherwise expressly agreed.

6. The Customer shall examine the new versions without delay and notify SfbIT of any identifiable defects in accordance with § 377 HGB (German Commercial Code). Insofar as SfbIT provided the Customer with a new version, it shall also continue to ensure maintenance of the previous version for a reasonable transitional period, which, as a rule, should not exceed three months. The Customer may only claim for material defects of the new versions if the notified defects are reproducible or otherwise detectable.

7. Customer care centre (Hotline): SfbIT shall set up a customer care centre for the Customer (Hotline). This centre shall process the Customer’s queries pertaining to technical operating requirements and conditions of Spamfinder as well as any other individual functional aspects. The hotline shall not answer queries in connection with the use of Spamfinder in non-released environments or with modifications of Spamfinder by the Customer or third parties. The Hotline shall be available to answer queries from Monday to Friday, from 8:00 a.m. to 5:00 p.m. except on statutory bank holidays. SfbIT’s primary location shall be decisive in determining statutory bank holidays. The Customer shall assign to SfbIT only competent and technically qualified personnel that are familiar with processing internal Spamfinder user queries on his premises. Only this SfbIT-assigned personnel may contact the hotline for queries and fill in the SfbIT enquiry form. The hotline will accept such enquiries by e-mail, telefax and telephone during SfbIT’s usual business hours. The hotline shall answer all duly formulated queries during the normal course of business if possible. The hotline may answer a particular query by referring to the documentation and other Spamfinder training methods already available to the Customer. Insofar as the hotline cannot provide a relevant answer, SfbIT shall pass on the query to a competent partner, especially queries concerning hardware or software which it did not deliver. Any additional services by the hotline, like other response times and deadlines, as well as readiness to call back or SfbIT on-site intervention at the Customer’s offices, are to be expressly agreed beforehand.

8. Additional services: SfbIT shall not be liable to provide any services outside the scope described in 1.2.1 to 1.2.5. Any such services shall require separate agreements and are to be remunerated separately.

9. Exchange of Spamfinder: in case of exchange of Spamfinder, the Customer shall ensure that no confidential information can be found in Spamfinder. The Customer shall also ensure that during the exchange, all electronic mails can be duly delivered safely.

2. Term of contract
1. The contractual relationship shall be entered into for a period of one year from the date of conclusion of contract.
2. The Customer may conclude a new agreement within 30 days after expiry of the term at the then applicable conditions.

3. Right of use
1. The Customer’s right to use the new versions and other Spamfinder corrections shall be equivalent to the rights to use the previous version of Spamfinder. The rights to use the new version and other corrections shall replace the rights to use the previous versions and other corrections after a reasonable transitional period – which, as a rule, should not exceed one month. The Customer may archive a reproduced version.

4. Obligations of the Customer
1. The Customer shall appoint a responsible contact person who is in a position to make or immediately initiate binding decisions for the Customer and who can provide SfbIT with any necessary information.

2. The Customer shall notify SfbIT without delay of any changes in the operating environment. In addition, the Customer shall ensure that Spamfinder is used only in a released environment supported by Spamfinder.

3. The Customer shall notify SfbIT in writing of any defects, in a comprehensible and detailed format, upon indication of all information necessary for fault recognition and analysis. He shall especially specify any working steps that caused a particular defect as well as the manifestation and effects of the same.

4. The Customer shall ensure that competent personnel are available to assist SfbIT.

5. The Customer shall assist SfbIT if necessary and create all necessary conditions for proper order execution in his operating environment, especially a remote access to the Customer’s system, as well as provide any other analysis material. In addition, the Customer shall at no cost provide enough workstations and working appliances upon SfbIT’s request.

6. Unless otherwise agreed, the Customer shall additionally keep all documents, information and data provided to SfbIT in such a way that they can be reproduced in case of damage or loss of data carriers.

7. The Customer shall grant SfbIT access to the software through telecommunications. For this purpose, the Customer shall establish all necessary connections upon SfbIT’s instructions.

8. SfbIT may request payment of additional fees insofar as
1. it took action following notification in the absence of a visible defect, unless the Customer was not in a position, with reasonable effort, to realise that there was no defect,
2. a notified fault is not reproducible or otherwise cannot be identified by the Customer, or additional
9. Glossary

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 e-mail 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 e-mail 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.

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.

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 a 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.

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: 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 are 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.

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

**Host name:** The name of the REDDOXX Appliance in the network.

**Console:** Software component with which the REDDOXX Appliance is controlled.

**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.

**Mail Hop:** Mail hop is when an e-mail is transferred from one server to another. Each of these servers is regarded as a mail hop.

**NBL Filter:** Network blacklist filter - Checking the IP address of the e-mail 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 e-mail 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.

**OS:** Operating system.

**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 e-mail 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 e-mail servers from "spam floods", the recipient address is checked by asking the respective e-mail 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 e-mail 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 e-mail with a bit more than just sending it "as is"! The protocol has several function options. On the one hand, SMTP lets your e-mails go straight to the receiver and on the other hand SMTP enables routing your e-mails via different servers, so-called MTA, to the recipient. Almost all e-mail clients use this protocol to send electronic mail.

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

SWL Filter: Subject Whitelist Filter – Authorization of the e-mail 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: Norman Sandbox - The virus scanner checks the attachments of all e-mails for viruses. Packed files are temporarily unpacked and checked. E-mails in which a virus was detected are saved on Spamfinder in a quarantine section. Only the administrator has access to this section. Your Spamfinder obtains the virus signatures directly from the
manufacturer (Norman ASA). 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.
10 Index

A
Administrator console MERGEFORMAT ... 34
Appliance configuration - general
MERGEFORMAT ........................................ 36
Appliance configuration - network
MERGEFORMAT ........................................ 38
Appliance configuration - routing
MERGEFORMAT ........................................ 39
Appliance configuration - time server
MERGEFORMAT ........................................ 40
Appliance configuration MERGEFORMAT36, 38, 39, 40
Appliance MERGEFORMAT ................... 133, 134
Application window MERGEFORMAT ...... 34

B
Basic configuration MERGEFORMAT .......... 26
Basic MERGEFORMAT .............................. 14
Blacklist MERGEFORMAT ................... 91, 108
Brief instructions MERGEFORMAT .......... 26

C
Careful MERGEFORMAT ...................... 11
CISS MERGEFORMAT ............................. 91
CISS queues MERGEFORMAT ................. 61
CISS scheme MERGEFORMAT ................. 13
Connection MERGEFORMAT ............... 26
Connections MERGEFORMAT .......... 20
Contact MERGEFORMAT .................... 149
Content filter MERGEFORMAT ............. 91
Copyright MERGEFORMAT .................. 3

D
Deinstallation MERGEFORMAT ............ 149
Disposal MERGEFORMAT .................. 149
Download Service MERGEFORMAT ...... 147

E
E-mail transport MERGEFORMAT ....... 56, 57

F
Filter configuration MERGEFORMAT ....... 96
Filter diagram MERGEFORMAT ............... 91
Filter lists MERGEFORMAT ................... 108
Filter profiles MERGEFORMAT .............. 102
Filter technologies MERGEFORMAT ....... 91
Filters MERGEFORMAT ............................ 91, 96, 102, 108
First steps MERGEFORMAT ............... 23, 26
Function diagram MERGEFORMAT ......... 23

G
General information MERGEFORMAT ....... 10
General Terms and Conditions
MERGEFORMAT ........................................... 150
Global filters MERGEFORMAT ................ 91
Glossary MERGEFORMAT ..................... 10

I
Incoming mails MERGEFORMAT .............. 61

L
LEDs MERGEFORMAT .............................. 20
License agreements MERGEFORMAT ....... 150
Local e-mail address MERGEFORMAT ...... 63
Local e-mail addresses MERGEFORMAT .. 63, 66, 67
Local Internet domain MERGEFORMAT .... 49
Local networks MERGEFORMAT ............ 55
Login configuration MERGEFORMAT 63, 69, 74
Login MERGEFORMAT ....................... 26, 34

M
Mailhop MERGEFORMAT ..................... 23
Medium MERGEFORMAT ..................... 14

N
Negative filters MERGEFORMAT ........... 102
Norman Antivirus MERGEFORMAT ....... 91
Notices MERGEFORMAT .................................. 11
Notifications MERGEFORMAT ......................... 79
Outgoing mails MERGEFORMAT ...................... 61
Oversteering MERGEFORMAT .................... 102
Phases MERGEFORMAT .................................. 102
Positive filter MERGEFORMAT ................. 102
Problem MERGEFORMAT ...................... 34
Queues MERGEFORMAT .................................. 61
Realm MERGEFORMAT ............................ 69, 74
Revision number MERGEFORMAT ............ 3
Risk warnings MERGEFORMAT ............... 11
Safety instructions MERGEFORMAT .......... 11
Services MERGEFORMAT ...................... 86, 88
Settings - advanced MERGEFORMAT .......... 46, 48
Settings - general MERGEFORMAT .......... 41, 115, 123
Settings - limits MERGEFORMAT .......... 44
Settings - network MERGEFORMAT .......... 43
Settings MERGEFORMAT .................. 41, 43, 44, 46, 48, 115, 123
Settings queues MERGEFORMAT ............ 46
SfbIT GmbH MERGEFORMAT .................. 3, 149
SMB MERGEFORMAT .................................. 14, 20
SMTP configuration MERGEFORMAT 49, 55, 56, 57
Spam MERGEFORMAT ............................... 13, 91
Spam queues MERGEFORMAT .............. 61
Spamfinder Appliance MERGEFORMAT .... 11, 14, 20, 133, 134
Spamfinder MERGEFORMAT .... 3, 10, 11, 13
Spamfinder Portal MERGEFORMAT .......... 147
Support MERGEFORMAT ..................... 149
Thread MERGEFORMAT ...................... 46, 48
Typography MERGEFORMAT .................. 10
User administration MERGEFORMAT 63, 66, 67, 69, 74
User data MERGEFORMAT .................... 63
Variants MERGEFORMAT ..................... 14
Virus protection MERGEFORMAT .......... 91
Virus queues MERGEFORMAT ............ 61
Warning notice MERGEFORMAT ............ 11
Whitelist MERGEFORMAT .................. 91, 108