



mailcleaner

APPLIANCE

QUICK START GUIDE



mailcleaner

© Fastnet SA – 2009 All rights reserved.
Reproduction of this manual in whole or in part
without the permission of Fastnet SA, St-Sulpice,
Switzerland is strictly forbidden. MailCleaner is a
trademark of Fastnet SA. All other brands
mentioned in this manual are trademarks
of their respective owners.

www.mailcleaner.com

PREFACE

The information in this “Quick Start Guide” has been carefully reviewed and is believed to be accurate. The vendor assumes no responsibility for any inaccuracies that may be contained in this document, makes no commitment to update or to keep current the information in this manual, or to notify any person or organization of the updates. **Please Note: For the most up-to-date version of this manual, please see our web site at www.mailcleaner.com.**

MailCleaner (Fastnet SA) reserves the right to make changes to the product described in this manual at any time and without notice. This product, including software, if any, and documentation may not, in whole or in part, be copied, photocopied, reproduced, translated or reduced to any medium or machine without prior written consent.

IN NO EVENT WILL MAILCLEANER BE LIABLE FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, SPECULATIVE OR CONSEQUENTIAL DAMAGES ARISING FROM THE USE OR INABILITY TO USE THIS PRODUCT OR DOCUMENTATION, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN PARTICULAR, MAILCLEANER SHALL NOT HAVE LIABILITY FOR ANY HARDWARE, SOFTWARE, OR DATA STORED OR USED WITH THE PRODUCT, INCLUDING THE COSTS OF REPAIRING, REPLACING, INTEGRATING, INSTALLING OR RECOVERING SUCH HARDWARE, SOFTWARE, OR DATA.

Any disputes arising between manufacturer and customer shall be governed by the laws of Lausanne City in the State of Vaud, SWITZERLAND. The State of Vaud shall be the exclusive venue for the resolution of any such disputes. MailCleaner's total liability for all claims will not exceed the price paid for the hardware product.

WARNING: Handling of lead solder materials used in this product may expose you to lead, a chemical known to the State of California to cause birth defects and other reproductive harm.

1 Introduction	5
2 Unpacking your appliance	6
Package content list.....	6
3 Mounting and plugging in the appliance	7
Mounting appliance in a rack.....	7
Plugging in power and network.....	8
Power on the appliance.....	9
4 Basic MailCleaner configuration	10
Connecting to MailCleaner.....	10
Configuring network.....	11
Configuring a domain.....	12
5 Start filtering	13
Network connectivity verification.....	13
Message routing verification.....	13
Redirecting mail traffic to MailCleaner.....	14
6 Troubleshooting	15
The MailCleaner appliance cannot be reached.....	15
MailCleaner responds but processing is very slow.....	15

1 Introduction

Welcome to a world where the e-mail you get is the e-mail you want..

Thank you for your interest in the MailCleaner MC200 Security Gateway appliance. This document will provide you with a quick and efficient way of securing your e-mail infrastructure within minutes. For more in-depth information, please refer to the MailCleaner User's manual or the MailCleaner Online Administration manual. These manuals are available online, both in the product interfaces and on our website.

MailCleaner is an antivirus and anti-spam system that is extremely powerful and easy to setup. Based on the latest generation of filtering technologies, MailCleaner acts at the highest technical level of the network infrastructure of your company, organization or ISP.

Placed before your mail server in the messaging path, MailCleaner will protect your mailboxes from any potentially dangerous and unwanted content and prevent useless messages from reaching your internal network.

MailCleaner Security Gateway is designed to handle large-scale attacks. Its balance of simplicity and robustness makes it a perfect fit as the main network entry point for your messaging system.



2 Unpacking your appliance

MailCleaner Appliance package content

The MailCleaner MC200 Security Gateway appliance package consists of one main hardware unit, a few accessories and manuals. Please first check that all elements are included in your package and contact your reseller in case of any doubt.

Package content list

- 1- MailCleaner MC200 Security Gateway appliance
- 2- Power cord
- 3- Rack mount screws (4)
- 4- Quick Start Guide
- 5- Settings and registration sheets (2)



3 Mounting and plugging in the appliance

Mounting appliance in a rack

The MailCleaner Security Gateway appliance is a standard 1U 19" chassis which is fully compatible with any standard 19" rack system.

Although it is highly recommended for production, this step is optional.

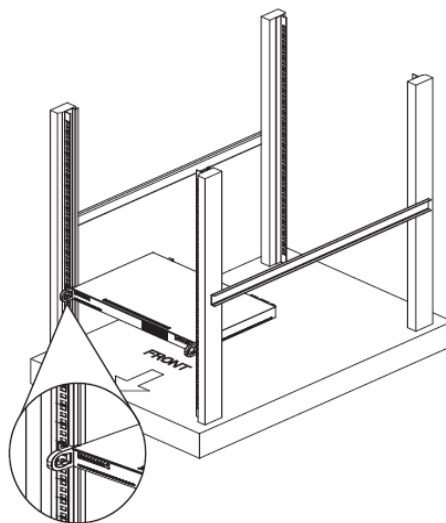
Important: This document only includes basic instructions. The chassis is based on SuperMicro's chassis SC510-200B, so we recommend that you also read the following document for more information about requirements and general precautions:

<http://www.supermicro.com/manuals/chassis/1U/SC510.pdf>

Rack Mounting Instructions:

- Decide on a suitable location for the rack unit that will house that appliance. It should be in a clean, dust-free area that is well ventilated. Avoid areas where heat, electrical noise and electromagnetic fields are generated.
- Confirm that the appliance includes the four mounting screws required to mount the appliance into a rack.
- Align the screw holes of the chassis with the screw holes of the rack.

Insert the mounting screws into the screw holes in the front of the chassis and through the screw holes in the rack.



Plugging in power and network

The MailCleaner Security Gateway appliance only requires the power cord and a network cable to be plugged in order to be fully operational. No screen, keyboard or mouse is required. The unit can be fully managed through the network and its web-based interfaces. See the picture below for power supply and network connections. Both plugs are on the rear panel of the unit.

Figure 3-1 Power supply

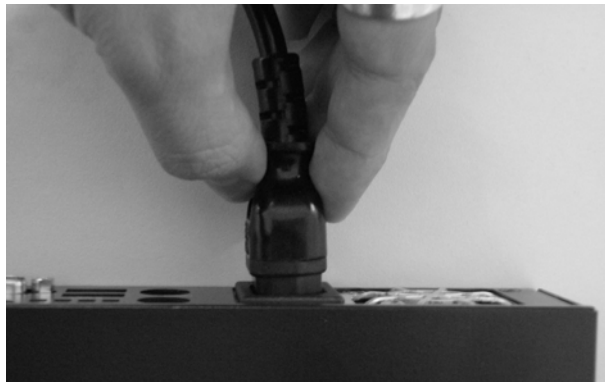


Figure 3-2 Network cable

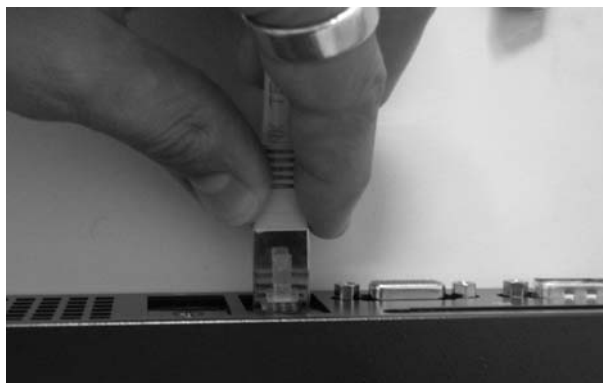


Figure 3-3 Final rear panel view



Power on the appliance

Once your MailCleaner unit has been correctly mounted and plugged in, you can power it on. Press the power switch on the unit front panel. The power led should first be red and then turn green as the system is booting. The appliance may take a couple of minutes to finish booting and be ready.

Figure 3-4 Front panel with power led and switch



4 Basic MailCleaner configuration

This section guides you to the few remaining steps before your MailCleaner can start filtering.

By default, your MailCleaner Security Gateway Appliance comes with comprehensive and well suited settings for the most common implementations. However, you are still required to provide some specific information, such as network parameters and the mail domains to be filtered. These two brief steps require network access with a recent browser to connect to your MailCleaner Security Gateway Appliance.

Connecting to MailCleaner

By default, MailCleaner comes pre-configured with the IPv4 address **192.168.1.101** and both the user and administration interfaces use the HTTPS protocol on port **443**. To reach MailCleaner's administration interface, open your favorite browser and type in the following URL:

<https://192.168.1.101/admin/>

Note: Depending on your network infrastructure, you may have to adapt it or your current workstation to be able to reach the 192.168.1.0/24 network. Please consult your network administrator for more information. You will be able to change the network configuration of MailCleaner to adapt to your network topology.

Warning: the web-based interface uses SSL encryption for maximum security, but the default certificate may not be fully trusted by your browser. You should either accept it temporarily or create a permanent exception in order to allow your browser to connect to the MailCleaner web-based interface.

Once connected to the web-based administration interface, you should see a login panel, as in figure 4-1. Enter the username **admin**, and the password **1234**, then click “login”.

Figure 4-1 Administration web based interface, login panel

Upon successful login, the main administration panel will appear. On the left, you can see the main navigation menu that provides you access to the different MailCleaner configuration options. For now, only two of these options will be used.

Network configuration

Depending on the current configuration of your network, one of the first steps may be to change the default network settings, since they may not be adapted to your network topology. Note that if the default settings are appropriate, this step can be skipped.

From the main administration menu, click on the “Base system” entry, under the “Configuration” section, as shown in figure 4-2.

Figure 4-2 Network configuration menu entry

On figure 4-3, you will see the network configuration panel. Enter the different parameters that match your network topology and then click on “Submit” button to activate your changes. You can optionally configure the second physical network interface available on the unit as well.

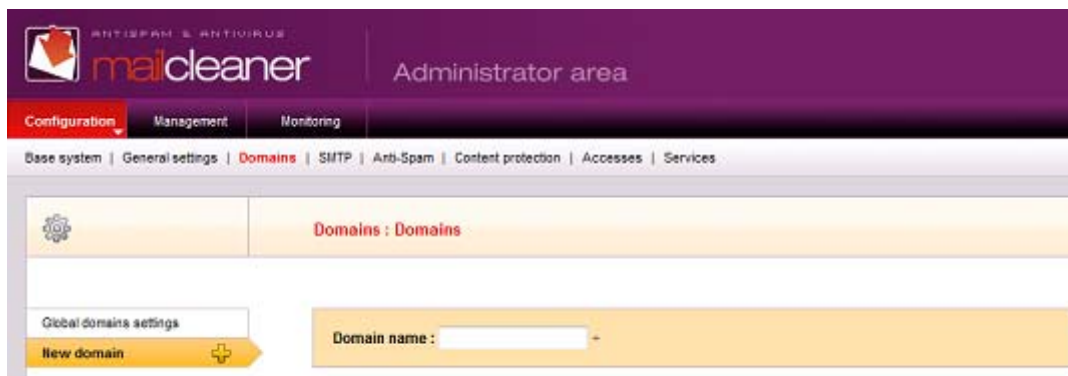
Important: You may be disconnected after applying network changes. If so, reconnect your browser to the new IP address in order to return to the MailCleaner administration web-based interface.

Figure 4-3 Network configuration panel

Configuring a domain

The second important step before your MailCleaner can start filtering mail is to provide the list of mail domains it will be accepting, filtering and the relaying mail for. Click on the “Configuration” entry under the domain section in the main navigation menu, as shown in figure 4-4.

Figure 4-4 Domain configuration menu entry with “New domain”



Click on the “New domain” link to open the new domain panel on the right. Two values are required: the domain name and the destination servers.

The domain name is the actual mail domain you wish to filter (i.e., the domain part after the @ of your email addresses).

The destination server is the fully qualified name or IP address of the server to which MailCleaner should send clean messages for final mailbox delivery.

Click on “Submit” to add the domain.

Although this is all that is required to allow MailCleaner to start filtering messages for your domain(s), you are strongly advised to have a look at the other settings and refer to the online documentation for more information.

5 Start filtering

This section guides you through the final step to prepare your MailCleaner for production.

Before redirecting your mail traffic to the MailCleaner appliance, it is strongly advised that you take a few minutes to check basic connectivity and routing.

Network connectivity verification

Basic network connectivity can be checked by standard tools such as ping and telnet. By default, MailCleaner will listen on ports TCP 25 for SMTP and 443 for HTTPS. Responses to ping requests should not show any packet loss and should come in a timely manner. The HTTPS web-based interface should be accessible and pages should load quickly and smoothly. Using the command in listing 5-1 on any Unix or Windows command prompt should produce the output shown in listing 5-2.

Listing 5-1 SMTP network connectivity check command

```
> telnet 192.168.1.101 25
(replacing 192.168.1.101 with the actual ip address you set up for your MailCleaner appliance)
```

Listing 5-2 SMTP network connectivity check output

```
Trying 192.168.1.101...
Connected to mailcleaner.localhost.
Escape character is '^]'.
220 mailcleaner.localhost ESMTP Exim 4.69 Thu, 10 Apr 2009 11:15:23 +0200
Some data may slightly change, but the 220 reply should appear quickly.
```

Generally, if any of these checks seems slow, you should first verify the DNS settings. If anything else doesn't work as expected, please check the network settings and your network infrastructure.

Message routing verification

Message routing through MailCleaner can be verified by simply sending messages directly to it. You can either configure your mail client to use MailCleaner as the outgoing SMTP server, or manually send messages on port TCP 25 using a tool such as telnet.

Messages should be delivered to the destination mail server within a few seconds. If you have just changed the network settings, it could possibly take up to one minute the first time. Repeat the process and messages should pass through MailCleaner in a few seconds.

If the message is refused by MailCleaner, you should check the domain configuration. If the delivery is slow, you should check your DNS settings and/or your network connectivity. If messages do not reach your mailbox, you should check the quarantine on the MailCleaner appliance to be confirm that it wasn't detected as spam. (This can happen when sending messages manually, e.g., via Telnet). Please refer to the MailCleaner user manual for more information on the user quarantine. If the problem persists, consult the different logs available in the administration web-based interface and on your destination mail server, and consult the online administration manual for troubleshooting procedures.

Redirecting mail traffic to MailCleaner

Once your MailCleaner appliance is configured and all tests confirm that it works properly, you can redirect all of your mail traffic to the MailCleaner Security Gateway appliance to start eliminating unwanted and dangerous messages.

Usually, the MailCleaner Security Gateway is placed as the mail entry point of your network, using the MX record of your domain's DNS configuration. Simply configure the MX value to the MailCleaner IP address. If your network topology requires some other gateway to be placed before MailCleaner, you can redirect the mail traffic by reconfiguring that gateway.

At this point, your MailCleaner Security Gateway appliance should start receiving and processing real-world messages, blocking unwanted messages and content, and delivering valid messages to your mailboxes.

In case of any problem, you should check the different status displays in the MailCleaner web-based administration interface, provided the different logs are available. If your problems cannot be resolved, please contact your reseller for further help.

6 Troubleshooting

The MailCleaner appliance cannot be reached

If your MailCleaner cannot be reached via the network, make sure that all cables are properly connected and that the network infrastructure is functioning. Try to connect to your system with the default IP address (192.168.1.101).

MailCleaner responds but processing is very slow

If the web-based interface is very slow to load and message delivery takes more than two minutes, you should check DNS settings in the network configuration panel and verify MailCleaner can resolve addresses correctly using the DNS server.

Refer to page 4 of the following document for information on which ports should be opened in your firewall to allow MailCleaner to correctly use all of its algorithms:
<http://www.mailcleaner.net/downloads/MailCleaner-installation.pdf>

You should also check the current load of the system. Maybe your mail traffic is currently too high for a single appliance. Generally, one MailCleaner MC200 Security Gateway appliance can handle up to 200,000 accepted messages per day.

Make sure the SMTP callout feature is activated and working correctly for each domain. Consult the online administration interface for more information on this subject.