Mail Encryption

5.3.4

User's Manual

Index of Contents

0

1 Preface

EgoSecure GmbH shall reserve the right to implement changes with regard to the contents of this document at any time and without any prior notice. Unless specified otherwise, names and details of persons or companies that are used as application examples within the framework of this document shall be completely fictitious. The production of an appropriate number of copies of this document shall be admissible, but for internal use only. This document must neither be copied nor reproduced, neither partially nor completely, neither electronically, mechanically, nor in any other way for other purposes without the explicit written consent of EgoSecure GmbH:

The contents of this document may have been subject to modifications if you did not receive it directly from EgoSecure GmbH: Even if this document has been developed applying the utmost care, Mail Encryption shall not assume any responsibility for possible errors or incompleteness. The application of this document shall comprise the consent to its use as is and without any warranties. Any use of the information mentioned within the framework of this document shall be at one's own risk.

PGP and Pretty Good Privacy are legally protected trademarks of the PGP Corporation, applicable in the USA and other countries. Java and any Java-based brands are trademarks of SUN Microsystems, Inc., applicable in the USA and other countries. UNIX is a registered trademark the rights to which are owned by X/Open Company, applicable in the USA and other countries. Microsoft, Internet Explorer, Windows, Windows NT, Windows 2000, and Windows XP are either registered trademarks or legally protected trademarks of the Microsoft Corporation, applicable in the USA and other countries. Netscape and Netscape Navigator are legally protected trademarks of Netscape Communications Corporation, applicable in the USA and other countries. All possible other trademarks mentioned herein are the property of their respective owners and shall be used herein without the intent of infringement.

OpenSSL is an application marketed under an Apache-similar licence (www.openssl.org).
OpenBSD is an operating system that is distributed under the Berkeley Copyright (www.openbsd.org).
GnuPG is software distributed under GNU Public Licence (www.gnupg.org).
The Apache Webserver and Apache Tomcat are developed under the Apache Software Foundation Copyright (www.apache.org).
Notes making reference to commercial products, procedures, or services, by means of mentioning the product or manufacturer name or any other kind, do not necessarily mean that EgoSecure GmbH approves, recommends, or favours these.

Import, export, and use of these and other encryption products may be subject to statutory limitations.

Views and opinions given by the author within the framework of this document do not necessarily express those of EgoSecure GmbH and must not be used for the purposes of advertising or product recommendation. References to internet addresses were subjected to a thorough examination before the document was printed. However, due to the constant change of the internet contents, EgoSecure GmbH is not able to assume any guarantee for the presence and the contents of the specified sources. Should you find erroneous links within the framework of this manual please let us know stating the corresponding link and the version number of the manual and use the e-mail address info@egosecure.com for the aforementioned.

Printed: April 2014

2 Introduction

Welcome to the secure e-mail solution Mail Encryption

The present manual will support you during Mail Encryption installation and serves as a reference for the individual aspects of the configuration. The manual is divided into the following three parts:

Part I

The first part consists of an introduction to the product. The mode of operation and important product features of the Mail Encryption appliance are described here.

Part II

The second part will provide an explanation on how to commission the secure e-mail gateway Mail Encryption. This comprises the integration of the appliance into your network, as well as the setup of your e-mail and network environments.

Part III

The third and last part contains an overview of the different **configuration options** in the first section. The further chapters describe the configuration and administration steps of the individual menu items in greater detail. For the purposes of easy orientation, the structure of this manual is oriented on the menu structure of the web administration portal.

We would like to wish you much success with the installation.

2.1 Secure e-mail communication through encryption

Mail Encryption uses different standardised encryption procedures and therefore provides the highest security for different communication parameters. This section will provide a description of the procedures used within the framework of the aforementioned.

The secure e-mail gateway appliance Mail Encryption encrypts incoming e-mails. This procedure is completely transparent for the e-mail recipient. The recipient will receive his/her e-mails unencrypted in his/her mailbox and will read these without any additional time required, as has been the case up to now.

Incoming e-mails can be provided with a digital signature. The public S/MIME certificate of the sender is a part of this signature.Incoming e-mails can be provided with a digital signature. In order to minimise the time required for administration assignments, the Mail Encryption appliance will save these S/MIME certificates automatically and will use these for S/MIME e-mail encryption for corresponding communication parameters.

With regard to safe e-mail dispatch, the Mail Encryption appliance will select the method that is most appropriate for the recipient from the following 5 methods:

EgoSecure Mail Encryption (ESWMail)

The EgoSecure Mail Encryption encryption technology is a patented procedure. Within the framework of this procedure, the e-mails are not buffered until they are fetched, as is usual for other webmail procedures, but the e-mails will be delivered completely encrypted to the recipient. There, the e-mails will be stored in the mailbox (e.g. outlook) of the recipient. When using this procedure, e-mails are protected against phishing attacks, because the encrypted e-mail from the mailbox is also required for successful access, along with the password.

An EgoSecure Mail Encryption contains the encrypted message as an attachment. The recipient retrieves the message by opening the encrypted file attachment. In doing so, the message is transferred to the appliance using a secure SSL connection where the message is encrypted and displayed after a password has been entered. The identity of the recipient is authenticated within the framework of each retrieval by entering the password. In contrast to the traditional dispatch of e-mails, e-mail deliveries can be demonstrated on the basis of the correct authentication. The following figure shows an example of an EgoSecure Mail Encryption.

Example for an EgoSecure Mail Encryption (ESWMail) message

Fully automatic domain encryption between all Mail Encryption appliances

The Mail Encryption appliance provides you with the option of encrypting e-mail traffic between several domains on a permanent basis. In doing so, the only condition is that the communication points are equipped with a Mail Encryption appliance in each individual case. All messages will be encrypted and decrypted between the devices automatically. So-called domain keys are used within the framework of this procedure.

S/MIME user encryption

The encryption procedure using S/MIME is based on public and private keys. Public keys are used to encrypt the e-mails and the e-mails can only be subsequently decrypted by means of the appropriate private keys. Thanks to central processing, this procedure works automatically when there are corresponding S/MIME certificates on the appliance. These can be signed on the very Mail Encryption appliance or issued by a public provider of certificates, such as SwissSign.In both cases the certificates can be created automatically. The Mail Encryption appliance supports different interfaces for that purpose.

OpenPGP user encryption

OpenPGP works in accordance with the same basic principle as S/MIME. The OpenPGP keys are

also managed on the Mail Encryption appliance and the e-mails are accordingly automatically encrypted if the key material is present. As opposed to S/MIME, the keys are always generated automatically and are not issued by certification authorities.

TLS/SSL transport encryption

TLS/SSL provides for additional safety and complements the encryption methods described above. The communication between the appliance and other e-mail servers is always established via a TLS/SSL secured channel using a standard configuration, if the destination device supports this. TLS/SSL is also used within the framework of the domain encryption between several Mail Encryption appliances already described above.

2.2 Digital e-mail signatures

When using digital e-mail signatures, binding e-mail communication is ensured by offering the possibility of verifying the authenticity of a message. In this way, it is ensured that a recipient will receive an unaltered message and that the displayed sender will correspond to the actual sender.

The secure e-mail gateway Mail Encryption is able to sign your e-mails either with user or with company certificates. Both procedures will be explained briefly in the following:

Digital e-mail signature by means of user certificate
By signing e-mails with an S/MIME user certificate the recipient will be enabled to verify the authenticity of the e-mail by using his/her e-mail client. This way, it is ensured that the sender is authentic and that the e-mail was not subject to any changes during or after its dispatch. A corresponding S/MIME certificate is required for each e-mail sender address when this method is used.

We recommend using certificates that were issued by a public provider of certificates. You can automate this procedure by using the Mail Encryption integration of the official certification authority SwissSign or of a different certification authority for the aforementioned. The connection of the Mail Encryption appliance to the providers of the certificates will enable you to issue the certificates in a fully automated manner, without any time required for support.

Alternatively, the e-mails may also be signed within the e-mail client of the corresponding sender. The secure e-mail gateway Mail Encryption will only encrypt these e-mails in the case of the aforementioned. Many S/MIME certificates are suitable both for signing and for encryption purposes. Therefore, it may make sense to additionally install the certificates on the Mail Encryption appliance. This way, e-mails with the corresponding certificates can be decrypted automatically.

Digital e-mail signature by means of company certificate
Signing the e-mails by means of an S/MIME company certificate serves the same purpose as signing the e-mails with an S/MIME user certificate. However, only one certificate is required when using this variant.

As S/MIME certificates are only applicable to one e-mail sender address as a matter of principle, all outgoing e-mails are equipped with the same (technical) sender. The recipient receives the e-mails with the identical e-mail address in each case, but with correct name. On the basis of the aforementioned, the automatic collection of contacts and related e-mail addresses no longer works as expected with the recipient. Difficulties must be expected regarding other aspects as well. For example, there is the risk that all your company e-mails will be rejected, if this single sender address was incorrectly classified as spam sender with the recipient

2.3 Central company e-mail disclaimer

The secure e-mail gateway Mail Encryptionis able to complement your e-mails with a company e-mail disclaimer. Disclaimers in text or HTML format are supported.

Utilise the central company disclaimer to attach a uniform text or information such as address and company owner to all e-mails.

Example for text format:

Company AG – Any Street 1, 1234 Any City - www.mycompany.ch

2.4 E-mail content inspection through virus, spam, and phishing protection (VSPP)

Mail Encryption VSPP (virus, spam, and phishing protection) is available as an option and protects you against spam (undesired e-mails), viruses (malicious e-mails), and phishing e-mails (falsified e-mails).

The anti-virus component updates virus definitions and will automatically check your e-mails for viruses.

Spam e-mails are reduced efficiently due to the integrated spam filter that can be easily configured. This filter is based on the combination of different filter techniques such as greylisting, black listing, Bayes's filters, and SMTP protocol checks.

Phishing attacks are prevented by EgoSecure Mail Encryption because the recipient needs both the encrypted message and a password in order to retrieve the message.

Notes on the use together with existing anti-virus systems:

The Mail Encryption appliance can also be used in combination with already existing anti-virus systems. However, please note that Mail Encryption receives/sends the e-mails in an encrypted manner.

In order to check e-mails for viruses, the e-mails must be present in non-encrypted form. Therefore, check your e-mails for viruses after you have decrypted them in your internal network (e.g. on your internal e-mail server), if you wish to continue to use your existing anti-virus product.

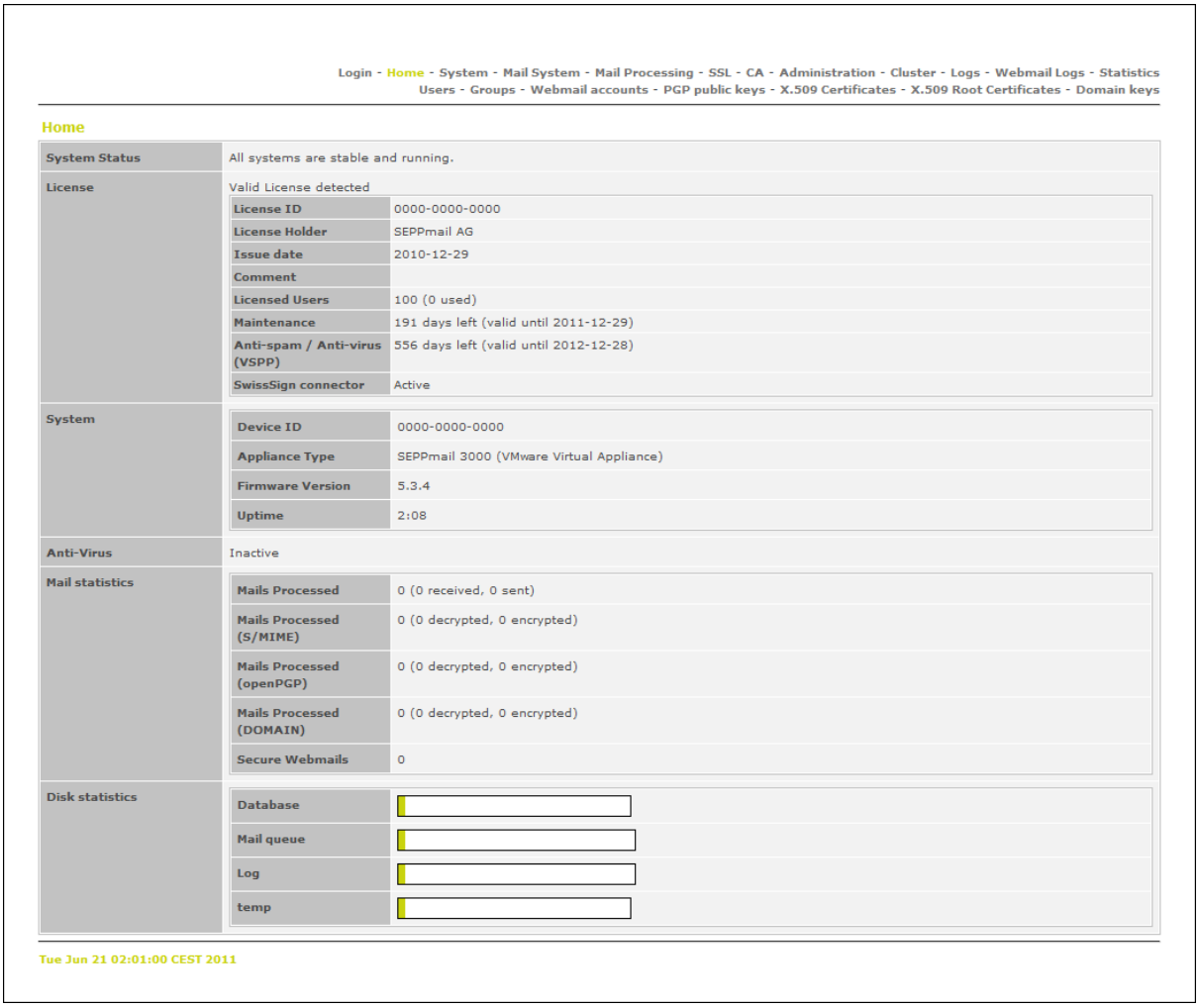
2.5 Compatibility with other secure e-mail systems

On the basis of central e-mail processing and key administration, Mail Encryption can be integrated transparently into your e-mail infrastructure. All acknowledged and secure standard encryption technologies are implemented. In this way, compatibility with the established secure e-mail systems is provided for and there is no need to install any additional client software.

Recipients that do not dispose of any S/MIME or OpenPGP keys may use EgoSecure Mail Encryption to transmit their e-mails in a secure manner.

2.6 Remote administration by means of web portal

All administration options of the Mail Encryption secure e-mail gateway appliance are available within a web browser-based administration portal. Below you can see the overview page and the different administration areas of the administration portal.



Anzeige Display of important appliance information and of the administration areas of the Mail Encryption secure e-mail gateway appliance

3 Commissioning the secure e-mail gateway appliance

3.1 Before you start

Please begin by checking the contents of the packaging for completeness. The delivery will consist of:

Number	Description
1	Mail Encryption hardware appliance respectively Mail Encryption virtual machine appliance for VMware
1	Quick install guide
1	IEC cable (240V)

If your scope of delivery is incomplete or should any problems or questions arise while installing the Mail Encryption system, please contact EgoSecure Mail Encryption or your specialised Mail Encryption dealer.

You will find a list containing the contact details of the corresponding specialised dealers on the website of EgoSecure GmbH - http://www.egosecure.com.

3.2 Integration of the appliance into your e-mail environment (standard configuration)

This section contains the description of a simple scenario where the Mail Encryption appliance directly receives external e-mails and directly sends internal e-mails to external recipients. Depending on the design of your e-mail infrastructure, further e-mail servers or gateways may be present in the e-mail data flow.

In this scenario, the appliance is installed as SMTP gateway between the internet and your e-mail server. The aforementioned will change the e-mail data flow in the following two essential aspects:

- E-mails from the internet are no longer sent to your e-mail server, but to the Mail Encryption appliance.
- Your e-mail server will no longer send the e-mails directly to the internet, but to the Mail Encryption appliance. Therefore, the Mail Encryption appliance will assume a so-called smart-host function.

The e-mail infrastructure for the described design is illustrated in the following figure.

Typical design of an e-mail infrastructure with a Mail Encryption appliance

3.3 Required information for commissioning

It is recommended to collect the following information pertaining to your e-mail environment before you start the commissioning procedure:

Required information	Your details
Public DNS entry or public IP address of the appliance*: This is the name or the IP address your appliance will use to be available from the internet.	
Internal IP address of the appliance: The internal IP address and subnet mask the appliance will use in order to be available within your internal network.	
Host name of the appliance: A host name of your appliance that can be selected freely, e.g. secureemailgateway. This name is normally listed in the DNS server.	
Internal domain the appliance is located in: Examples are: yourcompany.local or yourdomain.de, etc.	
Standard gateway IP address: This is the standard gateway IP address of your firewall or your router which the appliance can use to establish the connection to the internet.	
DNS server: Here you can enter up to three IP addresses of DNS servers. These can be both internal and external DNS servers. Internal servers must forward external queries accordingly.	
Name or IP address of your existing e-mail server: Name or IP address your existing e-mail server uses to be available within the internal network.	
E-mail domains: Enter the domains of the e-mail addresses of your organisation here, e.g. company.ch, company.com.	

Information required for configuring the Mail Encryption appliance

* The Mail Encryption appliance must be available as web server in the internet and therefore requires an IP address available from external sources. This is often the address of the firewall or of a reverse proxy / web application firewall. For simple installations, the IP address your internet router uses to be available for external sources can be used for the aforementioned.

You can obtain this information using the following steps:

1. Open a prompt on a Windows PC and enter `nslookup` followed by Enter.
2. After the ">" character, enter `set querytype=mx` and confirm your entry with Enter.
3. Enter the e-mail domain of your organisation (e.g. yourdomain.ch) and again confirm your entry with Enter.
4. You will receive one or several replies containing the term "mail exchanger ="

Server names after the term "mail exchanger" characterised by the lowest MX preference number have the highest priority with regard to name resolution.

3.4 Connecting the Mail Encryption appliance

In case you have purchased the VM (virtual machine) version of the Mail Encryption appliance, start your virtual appliance.

If you own the hardware version, please connect the appliance as described below:

1. Connect the Ethernet interface of the Mail Encryption appliance identified with “LAN1” to the Ethernet interface of your computer. In order to do this, use a twisted RJ45 patch cable (also known as crossover cable). Alternatively, you can use an Ethernet hub or an Ethernet switch with a normal RJ45 patch cable.

2. Connect the appliance to the mains using the supplied power cord.

3.5 Configuring firewall/router

Define the following rules on your firewall respectively your router in order to ensure secure e-mail communication through Mail Encryption:

Port	Source	Destination	Description	
TCP/22 (SSH)	Appliance	Internet	Allows for the implementation of appliance updates and is used within the framework of support sessions. .	
TCP/22 (SSH)	Appliance	Appliance	Is required during operation with several appliances in cluster group.	**
TCP/25 (SMTP)	E-mail server	Appliance	Is required so that the internal e-mail server is able to send e-mails to the appliance that will be encrypted there.	
TCP/25 (SMTP)	Internet	Appliance	Allows for e-mail traffic between the internet and the appliance.	
TCP/25 (SMTP)	Appliance	Internet	Is required for directly sending e-mails to the internet.	
		E-Mail server	Is required for sending e-mails to an internal e-mail server.	**
UDP/53 (DNS) TCP/53 (DNS)	Appliance	Name server (internal)	Allows for name resolution when internal DNS servers are used.	**
		Name server (external)	Allows for name resolution when internal DNS servers are used.	
		Internet	Allows for name resolution when the setting “built-in DNS Resolver” is being used.	
TCP/80*	Appliance	Internet	Is required for VSPP (virus, spam, and phishing protection) updates.	
TCP/443 (SSL)	Internet	Appliance	Establishes the encrypted communication via SSL (HTTPS) for Mail Encryption.	
UDP/6277*	Appliance	Internet	Is required for VSPP with DCC	
UDP/24441*	Appliance	Internet	Is required for VSPP with Pyzor.	
UDP/123* (NTP)	Appliance	Internet	Allows for time synchronisation	
TCP/8080* (HTTP) und/ oder TCP/8443* (HTTPS)	Admin PC	Appliance	Provides for administrator access within the internal network. It is recommended to only permit the SSL-encrypted connection via port TCP/8443.	**
TCP/5061*	Appliance	Internet	Is used for sending SMS via “aspsms.com”.	

Rules regarding the provision of the network communication of the Mail Encryption appliance

* optional, depending on the configuration of the Mail Encryption appliance

** In simple installations, no firewall will be used between the Mail Encryption appliance and the internal network. In this case, the rules identified with ** are not applicable.

3.6 Network settings and system registration

In the following you will find a description on how you can integrate Mail Encryption appliance into your network and how you can check the network communication. This also comprises the definition of the IP address(es) of your appliance, the DNS settings, the entry of the standard gateway, the assignment of the host name, and the specification of your internal domain.

Ultimately you can check whether the settings have been entered correctly by using the function “Check Update” of the appliance and you can register your system.

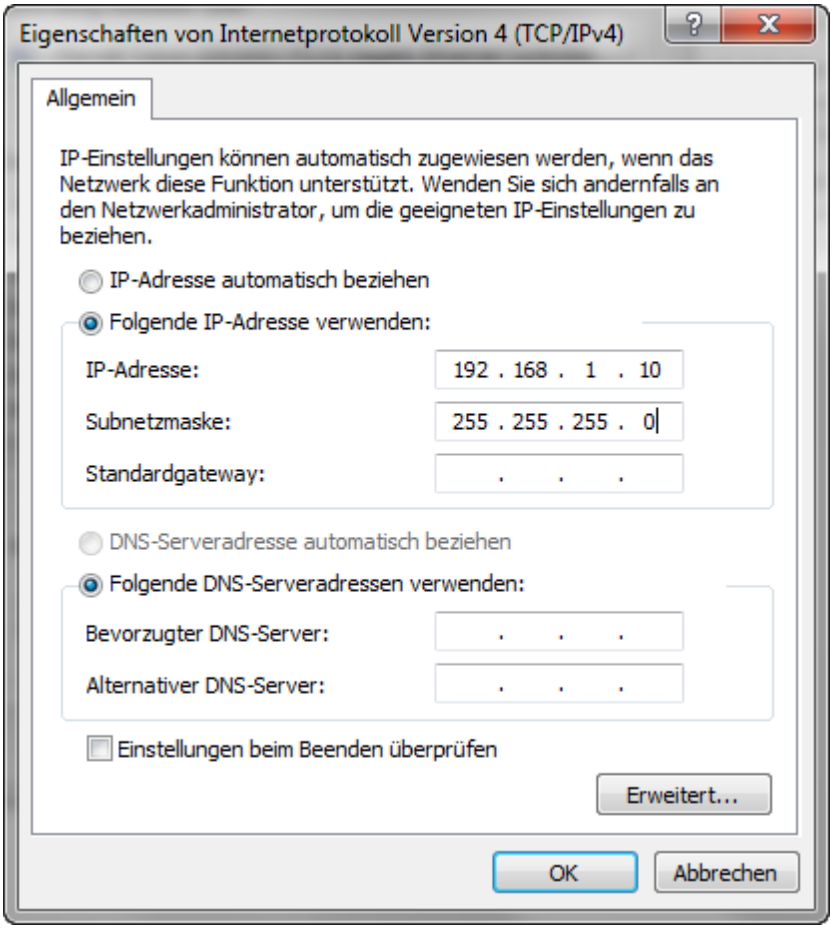
3.6.1 Configuring the installation PC

Regarding the initial configuration of the network parameters of your Mail Encryption appliance, your computer must be in the same network as the appliance. If your computer is not already within the IP range of 192.168.1.x, please change the IP address of your computer to an IP address between 192.168.1.1 and 192.168.1.254.

Note:

Please do not use the IP address 192.168.1.60, because this is reserved for the Mail Encryption appliance.

The following figure shows an example of the corresponding network settings:



Network settings of the PC that is used to configure the appliance from

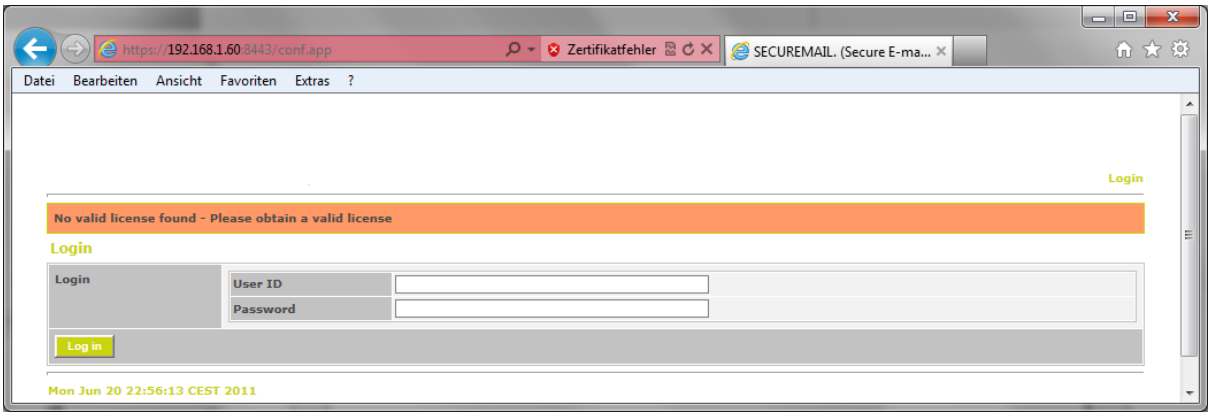
3.6.2 Login as administrator

All administration options of the Mail Encryption secure e-mail gateway appliance are available within a web browser-based administration portal. At the time of delivery you can access the configuration interface by entering the following address:

LAN1 - https://192.168.1.60:8443
LAN2 - https://192.168.2.60:8443

User name	: admin
Password	: admin

Note: In this phase the message "No valid licence found – Please obtain a valid licence" will be displayed in each case, because the Mail Encryption appliance is delivered with a temporary licence. Please follow the further instructions contained in this chapter in order to implement the basic configuration and to register your system. This way, you will be provided with a permanent licence and will be able to use the Mail Encryption secure e-mail gateway appliance to the full extent.

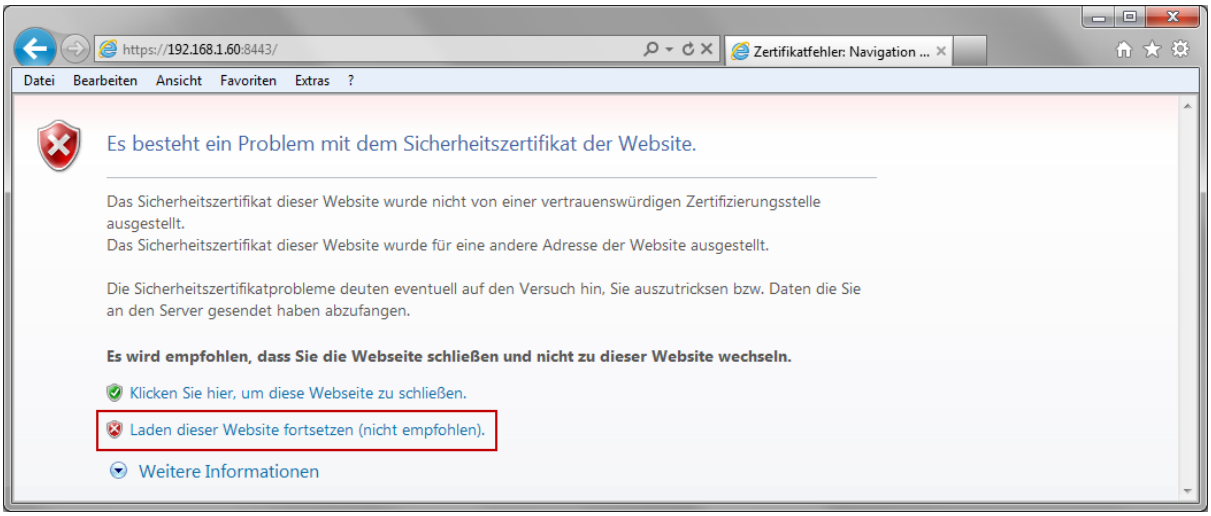


When opening this site you will see an error message containing the note that the SSL certificate of the website is invalid. Please select the option of opening this site nevertheless.

Note: This message will only be displayed at the beginning until a valid SSL certificate is installed (see menu item »SSL« 103).

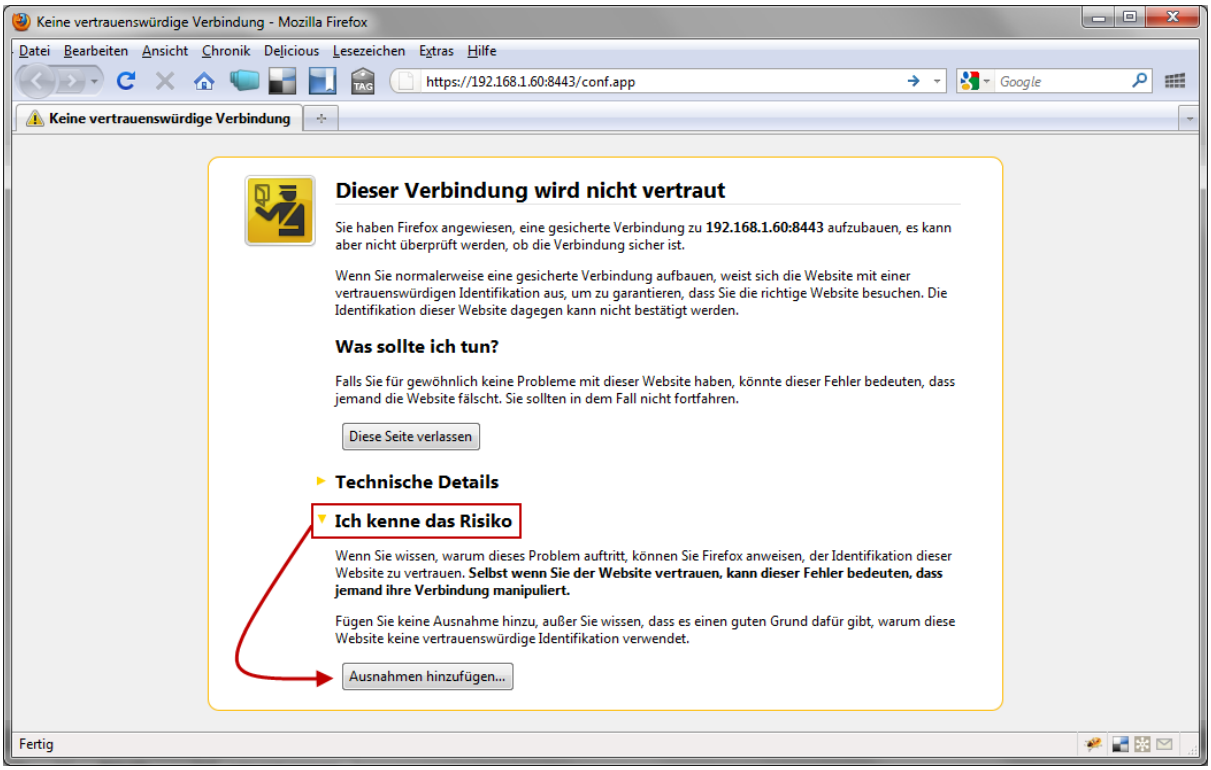
The displayed web browser messages may differ depending on the web browser used. The following figures illustrate the messages for the most commonly used web browsers.

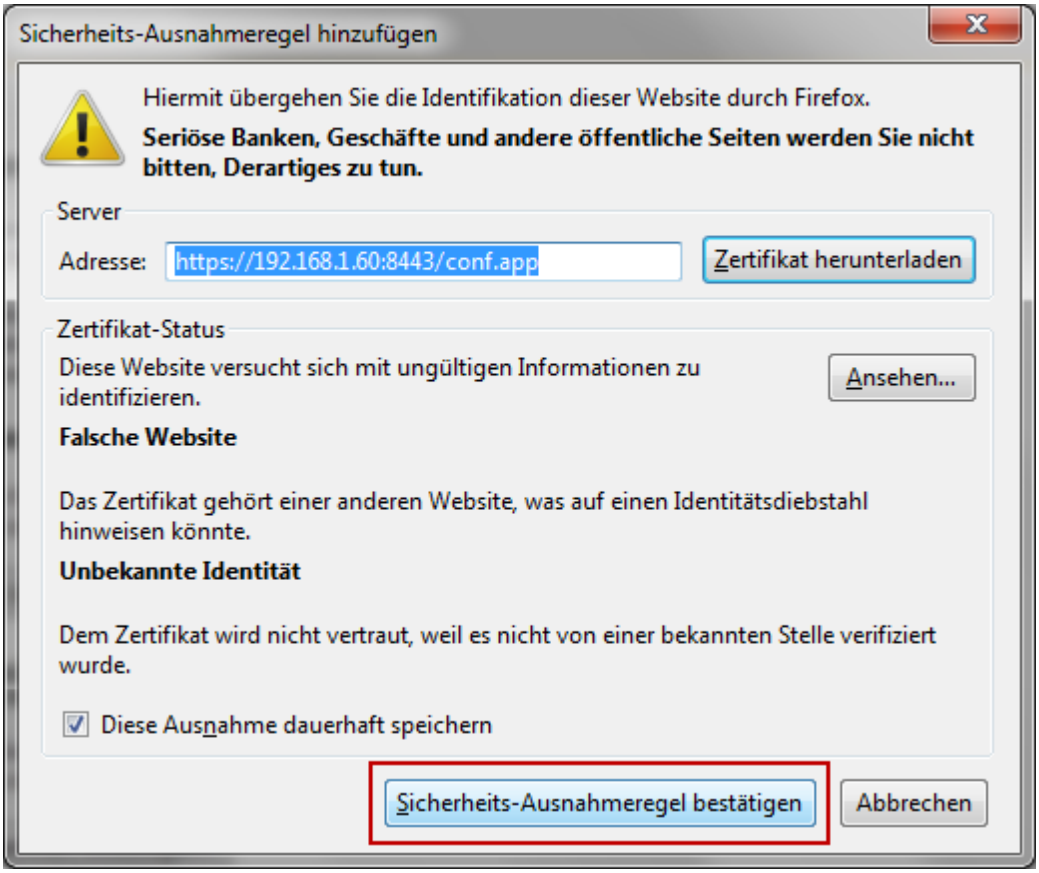
Microsoft Internet Explorer 9



The Internet Explorer web browser will display a security alert when you open the URL for the configuration interface of the Mail Encryption appliance Please select the option “Continue loading this website (not recommended)”. Afterwards, the login site of the configuration interface will be displayed.

Mozilla Firefox 3.6

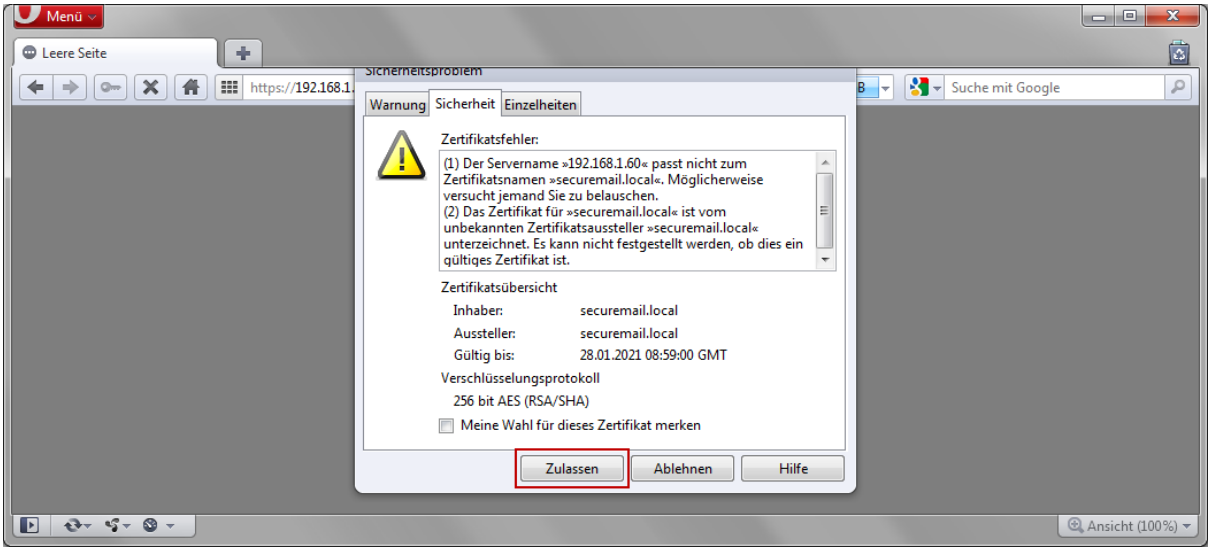




The Firefox web browser will display a window containing a security alert when you open the Mail

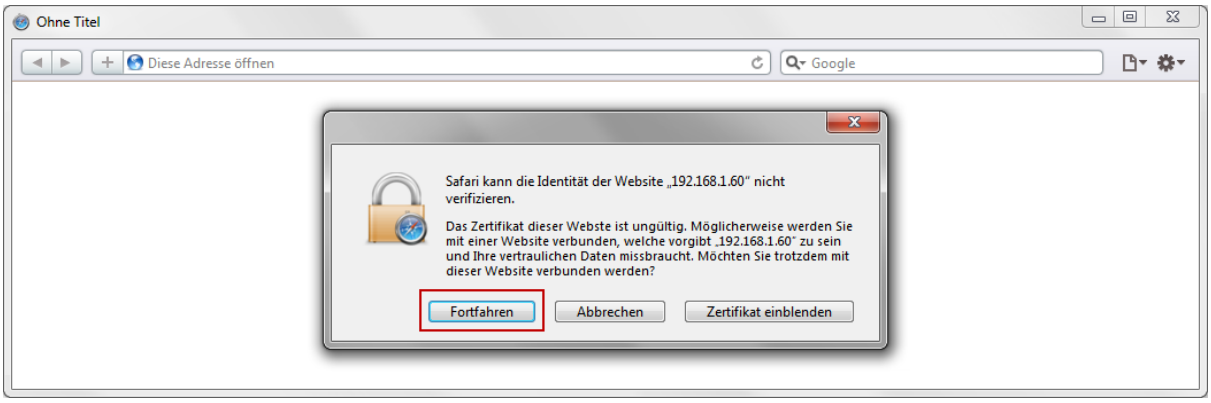
Encryption appliance.Please select the option “I know the risk” highlighted here. You will see another window intended for confirming the exception regulation. Confirm the aforementioned by selecting the “Confirm security exception regulation” button. Afterwards, the login site of the configuration interface will be displayed.

Opera 11.01



The Opera web browser will display a window containing a security alert when you open the Mail Encryption appliance. Please switch to the “Safety” tab in this window and confirm this message by using the “Accept” button. Afterwards, the login site of the configuration interface will be displayed.

Apple Safari



The Safari web browser will display a window containing a security alert when you open the URL for the configuration interface of the Mail Encryption appliance. Please select the “Continue” tab in this window. Afterwards, the login site of the configuration interface will be displayed.

3.6.3 Network settings of the appliance

In order to configure the network settings of your Mail Encryption appliance, you must click the System menu item in the web administration portal.

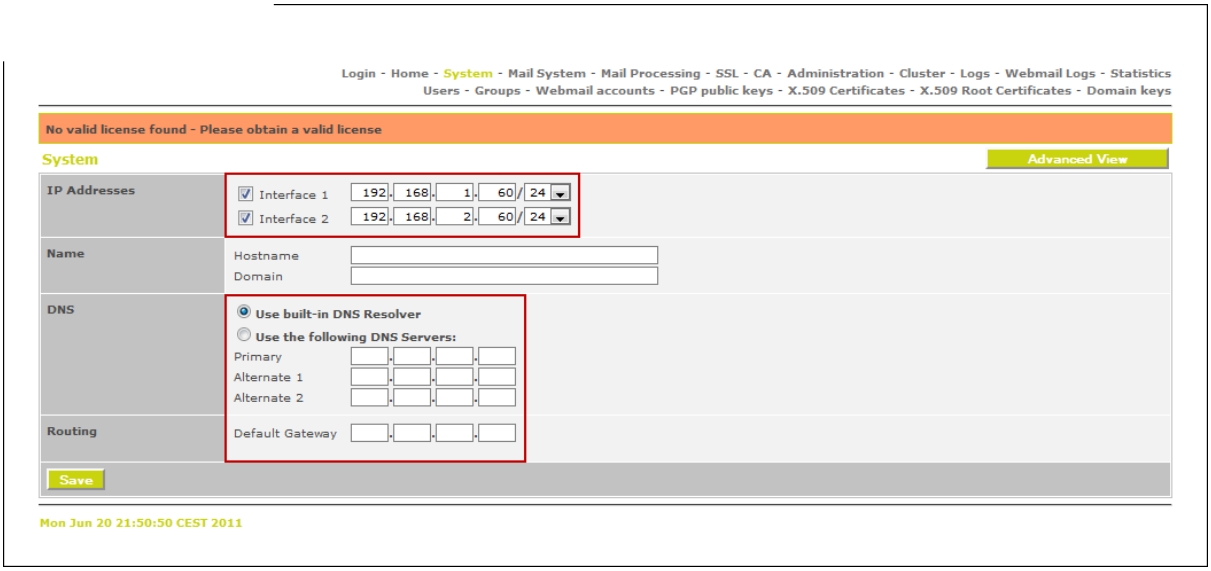
There you must define the following settings:
- Internal IP address of the appliance in the IP Addresses category
- Internal network mask* in the IP Addresses category
- DNS-Server** in the DNS category
- Gateway IP address in the Routing category

* The definition is specified in accordance with the Classless Inter-Domain Routing (CIDR) Notation. For example, the aforementioned corresponds to the following values:
- The network mask 255.255.255.255 corresponds to "/32" (individual IP address)
- The network mask 255.255.255.0 corresponds to "/24" (class C network)
- The network mask 255.255.0.0 corresponds to "/16" (class B network)
- The network mask 255.0.0.0 corresponds to "/8" (class A network)

Depending on which Mail Encryption model you have purchased, you can assign IP addresses of one to three network connections..

** Please ensure that the DNS entries are correct. The entered DNS servers should be able to resolve domain names in the internet. Erroneous entries may result in a very slow responsiveness of the web administration portal so that loading menu items may require several minutes.

Alternatively, you may use the Use built-in DNS Resolver setting. If you decide to use this option, please ensure that your firewall respectively your router is configured in a way that the Mail Encryption secure e-mail gateway appliance is able to implement DNS resolutions via root DNS servers in the internet (cf. section Configuring firewall / router 20).

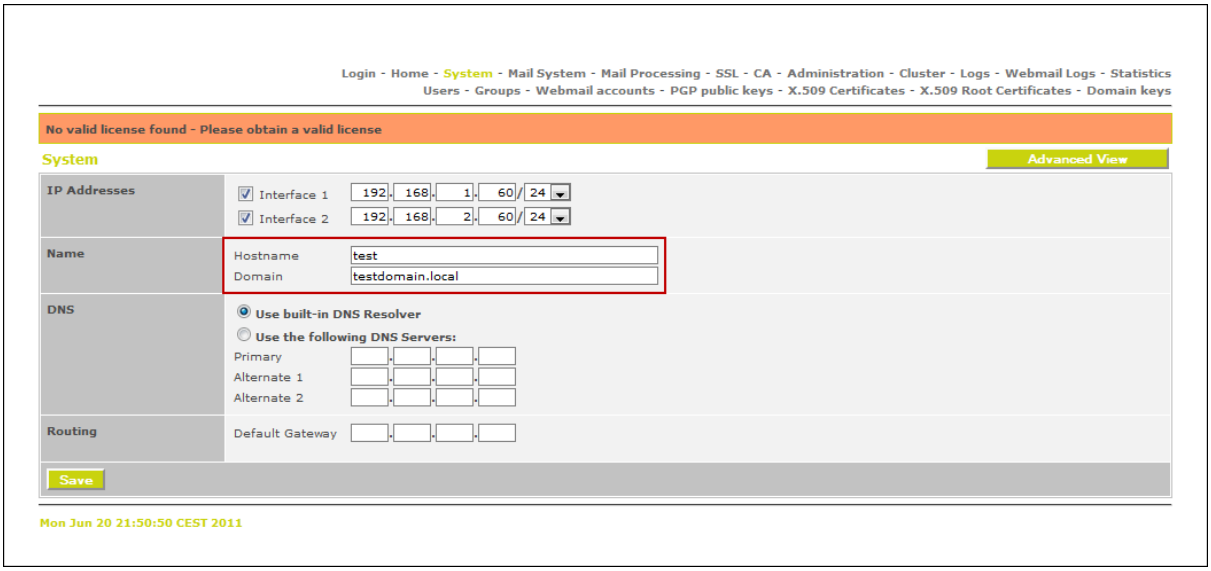


Specification of the network settings

3.6.4 Assigning host and domain names

In order to specify the host and the domain names of your Mail Encryption appliance, please enter the corresponding values for Host name and Domain.

You can select the host name freely, e.g. secure-mailgateway. The domain name corresponds to the DNS domain where the appliance is located (e.g. yourcompany.local or yourdomain.ch). These settings are the internal view, i.e. they must not correspond to the data that would be valid from the internet.



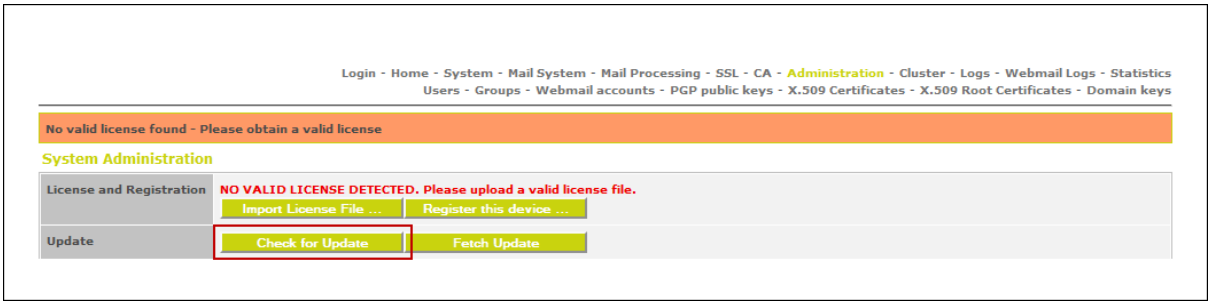
Defining host and domain names

3.6.5 Checking the network configuration

Please implement the following steps in order to ensure that the appliance works with the network settings you implemented:

1. Please click the Administration menu item in the web administration portal.

2. Please click the “Check for Update” button.



"Check for Update" button

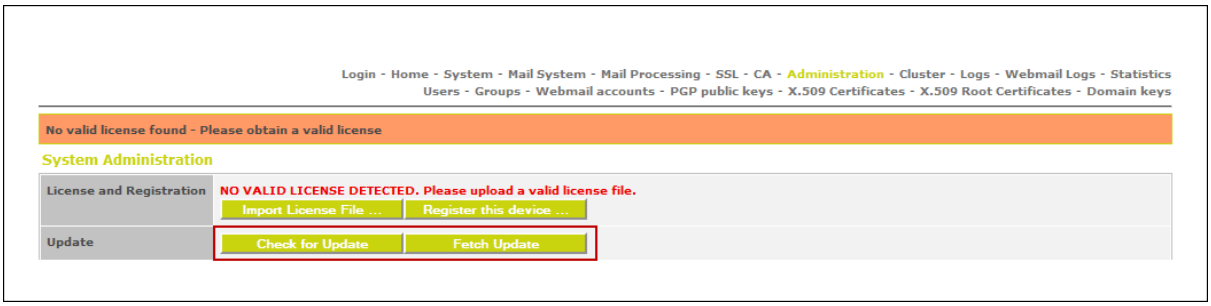
If one of the following messages is displayed, the network configuration was successful::

- You already have the latest version installed
- There is a new version available: Installed version is oldversion, latest version is newversion

Otherwise the message ERROR: unable to connect to update server. Make sure that the device can make connections to the internet on port 22 will be displayed. If this message is displayed, please re-check whether your network settings are correct and whether your firewall respectively your router permits the connection of the appliance to the internet via port TCP/22 (SSH) (cf. section Firewall / Router einrichten 20).

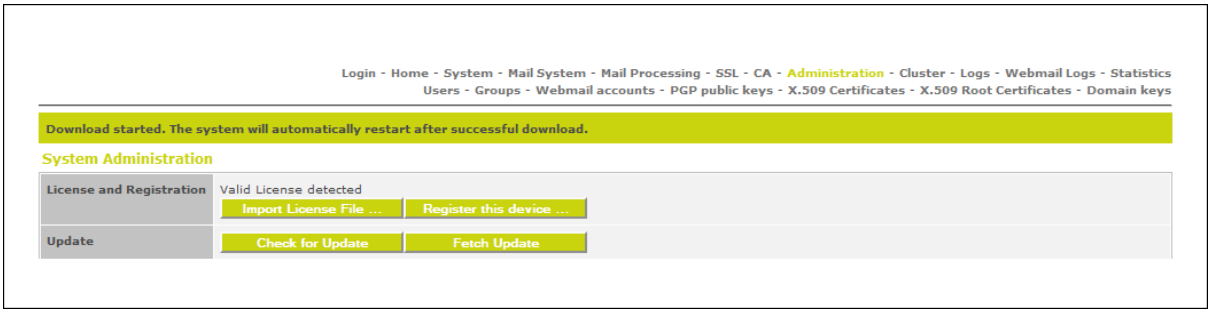
3.6.6 Updating the system

Please click the “Administration” menu item in the web administration portal. Afterwards, please click the “Check for Update” button. If an update is available, please additionally click the “Fetch Update” button. This may be a time-consuming step if the delivered system works with an older firmware and must implement several updates on the basis of the aforementioned.



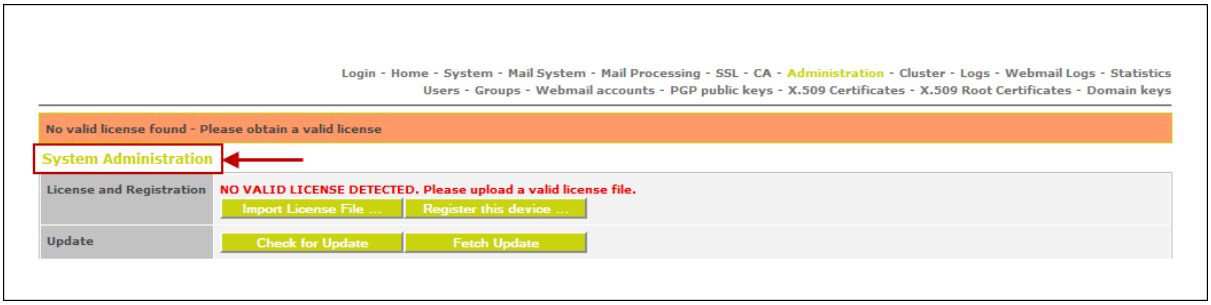
Searching and loading updates

Repeat this step until there are no more updates available. The system will optimise this process so that it is not necessary to make an update for each intermediate version, but only for those involving changes to the data structure.



Confirmation that an update is being loaded

It may happen that you are not provided with any feedback over an extended period of time. If this is the case, please update the display by clicking the System Administration link above the buttons. As long as you were not logged off, the update is not finished.

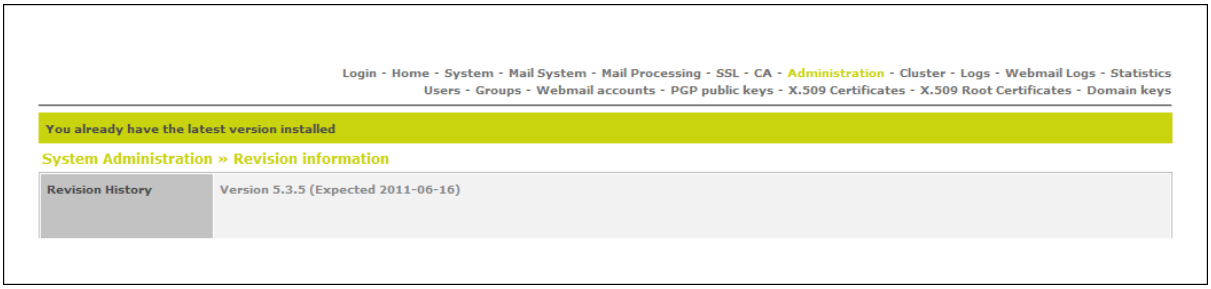


“System Administration” link

After having been updated, the Mail Encryption appliancemust restart and you are required to re-enter your login details. If applicable, please implement this step self-dependently if the system does not provide you with any feedback for an extended period of time, i.e. does not display the login mask.

You can trigger the restart procedure by clicking the “Reboot” button and confirming the security code displayed afterwards. Upon every restart, please re-check whether further updates are available.

If the message You already have the latest version installed is displayed, your Mail Encryption Appliance is up to date.

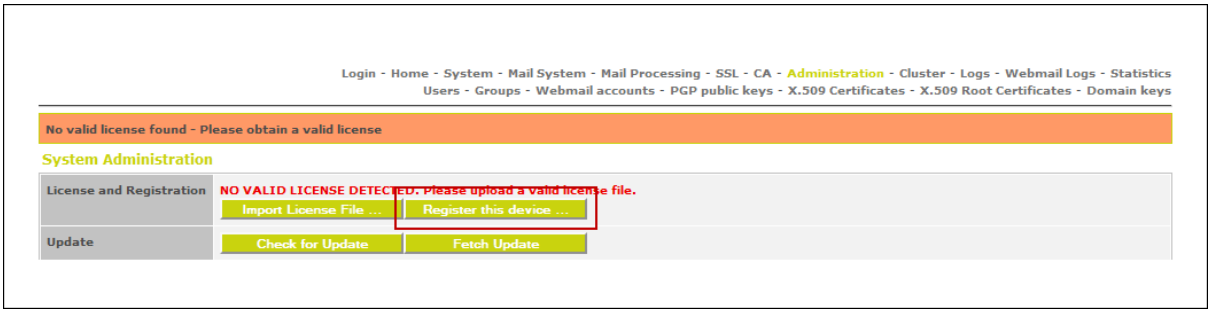


Confirmation that the Mail Encryption appliance is up to date

If further updates are available in the future, this will be displayed automatically upon a restart procedure in each case.

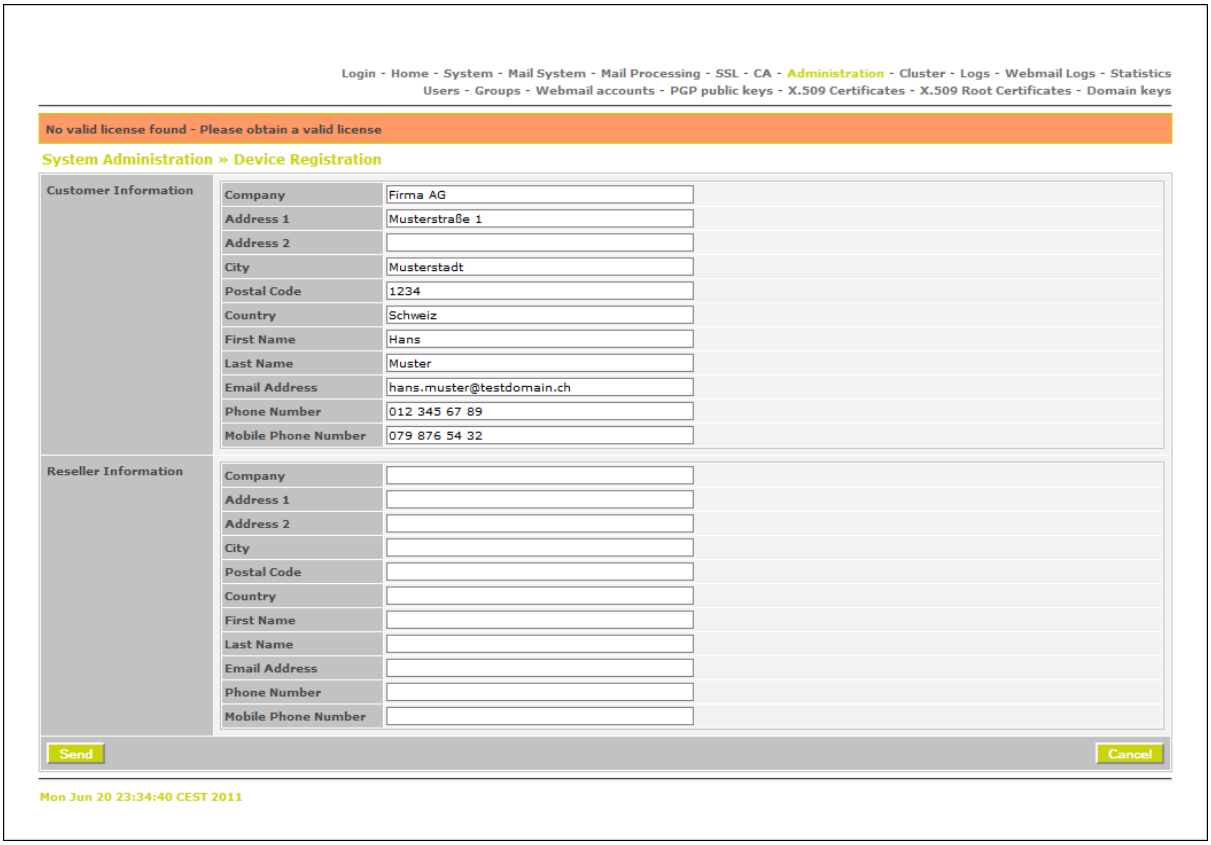
3.6.7 System registration

Register your system so that you are provided with a permanent licence. For this, click the “Register this device...” button.



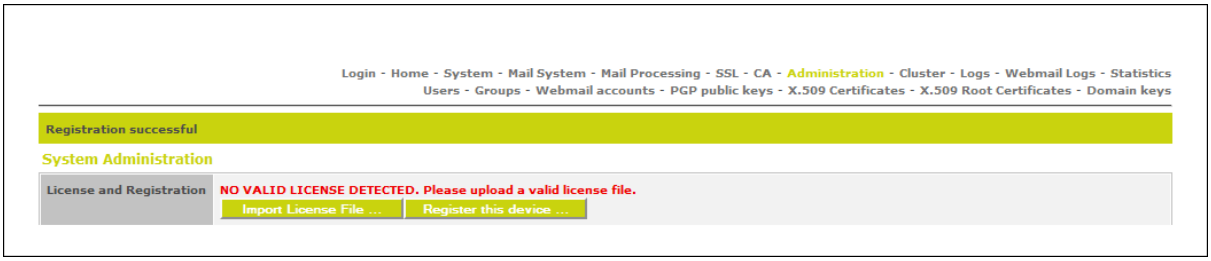
Registering the Mail Encryption appliance

A registration window will be displayed:



Registration window for the collection of your customer information

Please enter your details into the fields of the registration window. Please enter your customer information into the upper half and the details of your reseller into the lower half. Finish your entries by clicking the “Send” button.



Confirmation upon successful registration

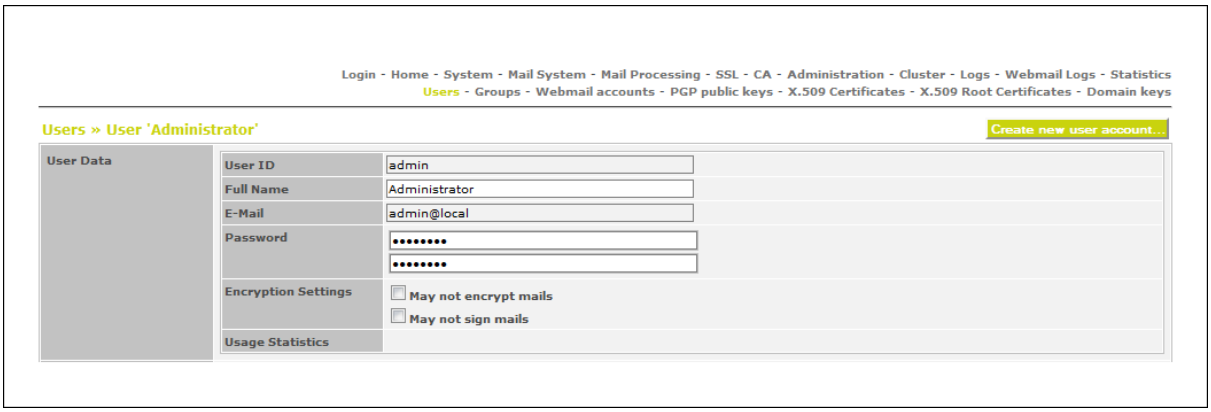
If the message "Registration successful" is displayed, you have completed the registration procedure successfully.

3.7 Important safety precautions

The following sections contain descriptions of the following important safety precautions:

3.7.1 Changing the administrator password

Please ensure that the password of the user “admin” is changed and that a complex password is used. For this, please click “Users” and then “admin” after having logged in with the user “admin”. There you can change the password and, if required, can implement further settings concerning the user “admin”.



Changing the administrator password

3.7.2 Specifying the HTTPS protocol for secure access to the appliance

You will find the “Advanced View” button in the System menu item. Please click this button in order to open further configuration options. The sections GUI Protocol and Webmail Protocol can be used to set whether corresponding accesses to the appliance are to be implemented via HTTP or HTTPS.

For reasons of safety it is recommended to disable the HTTP option and to admit HTTPS only, both for the web administration portal (GUI protocol) and for webmail.

Login - Home - System - Mail System - Mail Processing - SSL - CA - Administration - Cluster - Logs - Webmail Logs - Statistics
Users - Groups - Webmail accounts - PGP public keys - X.509 Certificates - X.509 Root Certificates - Domain keys

System — Normal View

Comment	System Description
IP Addresses	Interface 1: 192.168.1.60/24 Media: (current state: Ethernet autoselect) Interface 2: 192.168.2.60/24 Media: (current state: Ethernet autoselect)
IP ALIAS Addresses	IP Alias 0 / 24 VHID: 1 Interface: Interface 1 Priority: Primary IP Alias 1 / 24 VHID: 1 Interface: Interface 1 Priority: Primary IP Alias 2 / 24 VHID: 1 Interface: Interface 1 Priority: Primary IP Alias 3 / 24 VHID: 1 Interface: Interface 1 Priority: Primary Note: CARP is used for the alias addresses, this means that you can use the same alias addresses on different devices for load balancing / failover. Set the same VHID for two or more equal addresses on same LAN segment ONLY
Name	Hostname Domain
DNS	Use built-in DNS Resolver Use the following DNS Servers: Primary 192.168.1.2 Alternate 1 Alternate 2 Search Domain(s):
Routing	Default Gateway 192.168.1.2 Static Routes Destination / 32 — Gateway
GUI Protocol	HTTP Port 8080 HTTPS Port 8443 Bind to IP or Hostname (use with care!)
Webmail Protocol	HTTP Port 80 HTTPS Port 443 Enable local https proxy, redirect unknown requests to http://
Console Login	Disable console root login Enable PIX workaround (restart device to activate change)
Syslog Settings	Forward maillog to syslog server:
HTTP Proxy Settings	Use proxy for ssh connections Proxy Server Proxy Port Proxy User Proxy Password (Used to update virus signatures and to fetch antispam updates.)
Time zone	(GMT +01:00) Amsterdam, Berlin, Berne, Rome, Stockholm, Paris Automatically adjust GMT offset for DST
Time and Date	Use current setting — Automatically synchronize with an NTP server Server: pool.ntp.org Set date and time manually Date (dd.mm.ccyy) Time (hh:mm:ss)
SNMP Daemon	Enable SNMP

Save

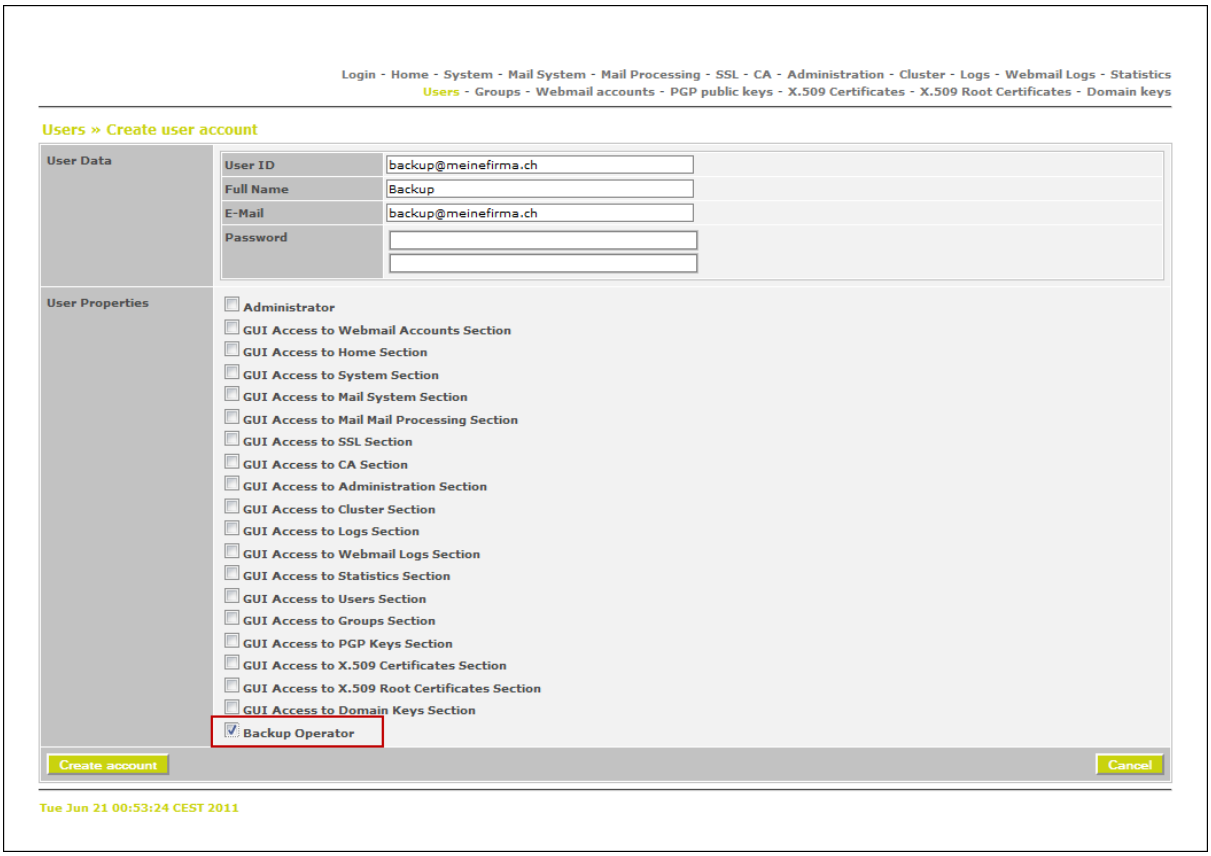
Tue Jun 21 00:48:17 CEST 2011

Definition of the protocols and their ports for the web administration portal and for webmail

3.7.3 Creating a backup user

In order to backup the status of the Mail Encryption appliance at regular intervals, please create a backup user. The backup of the appliance will be sent to the e-mail addresses of all backup users in an encrypted manner on a daily basis.

In order to create a backup user, please click the Users menu item and then click the "Create new user account..." button. Please complete the fields User ID, Full Name, E-Mail, and Password. Please ensure that the e-mail address is valid. Click the Backup Operator checkbox and complete the procedure by clicking the "Create account" button.

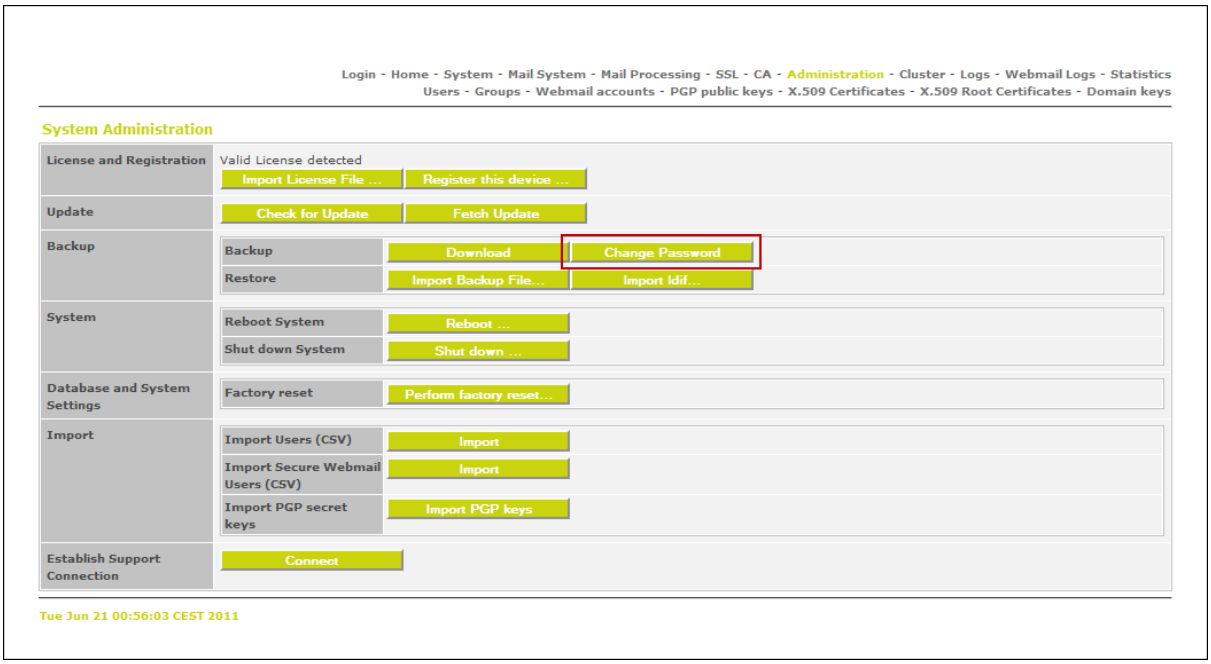


Creation of a backup user

Setting the backup password

In order that backups of the appliance can be implemented, a backup password must be set additionally. Backups of the appliance are encrypted using this password. This password must be entered when the appliance settings are restored by means of importing a backup file.

In order to set this password, please click the Administration menu item and then click the "Change Password" button.



Definition of the backup password

3.8 Further steps

You have now created the base for secure e-mail traffic by means of the Mail Encryption appliance.

Please implement the following further steps in order to achieve a minimum configuration for secure e-mail exchange:

- Setting date and time and configuring the NTP synchronisation 57
- Creating e-mail domains to be managed 67
- E-mail relaying settings 72
- Creating an SSL certificate self-dependently 104 (for test operation)
- Requesting an SSL certificate from a certification authority 107 (for productive operation)

The following two items will be described below.

However, please only implement these two steps after you have implemented the steps mentioned above so that the e-mail traffic is not affected adversely.

- Switching over the e-mail data flow 41
- Using e-mail clients 42

3.8.1 Switching over the e-mail data flow

In order to allow for secure e-mail traffic by means of the Mail Encryption appliance, the following changes must be implemented on your existing e-mail server.

- Authorisation of the Mail Encryption appliance for e-mail dispatch by means of e-mail relaying settings
- Defining the Mail Encryption appliance as smart-host

Please ensure that e-mail traffic to external sources by means of the Mail Encryption appliance is possible by configuring your firewall respectively your router as described above (see section Configuring firewall / router 20).

Once you integrate the Mail Encryption appliance into your e-mail data flow in a fixed manner, you must moreover replace the IP address of your existing e-mail server by the IP address of the appliance in your firewall rules.

Once you integrate the Mail Encryption appliance into your e-mail data flow in a fixed manner, you must ensure that the e-mails from external sources are no longer transported to the e-mail server, but to Mail Encryption.This can be configured within the firewall or an upstream spam filter, depending on your network configuration.

According to the default settings, the secure e-mail gateway Mail Encryption will send the e-mails directly to the internet. If e-mail traffic is to be implemented via an SMTP gateway, please configure your appliance accordingly (see Controlling the outgoing e-mail traffic 68).

Authorisation for e-mail dispatch
In order to allow for e-mail dispatch from your Mail Encryption appliance to your existing e-mail server, you must authorise the appliance for the aforementioned. This setting is mostly defined as SMTP e-mail relaying. For this, please enter the internal IP address or the internal host name of the Mail Encryption appliance into the list of authorised e-mail relay computers on your e-mail server

Definition of the Mail Encryption appliance as smart-host
The EgoSecure Mail Encryption appliance will assume the role of an SMTP gateway after it was integrated into your e-mail environment. In this case, your e-mail server will no longer send the e-mails directly to external sources, but to the Mail Encryption appliance.

In order to implement this change, you must define the internal host name respectively the internal IP address of your Mail Encryption appliance as smart-host on your existing e-mail server.

ATTENTION

This change will result in a change to the e-mail communication by integrating the secure e-mail gateway Mail Encryption into the e-mail data flow. All e-mails will be sent to the Mail Encryption**appliance after the change has been implemented.**
Please only implement this change when all other configuration steps of the Mail Encryption appliance are completed. Otherwise, the e-mail traffic may be affected adversely.

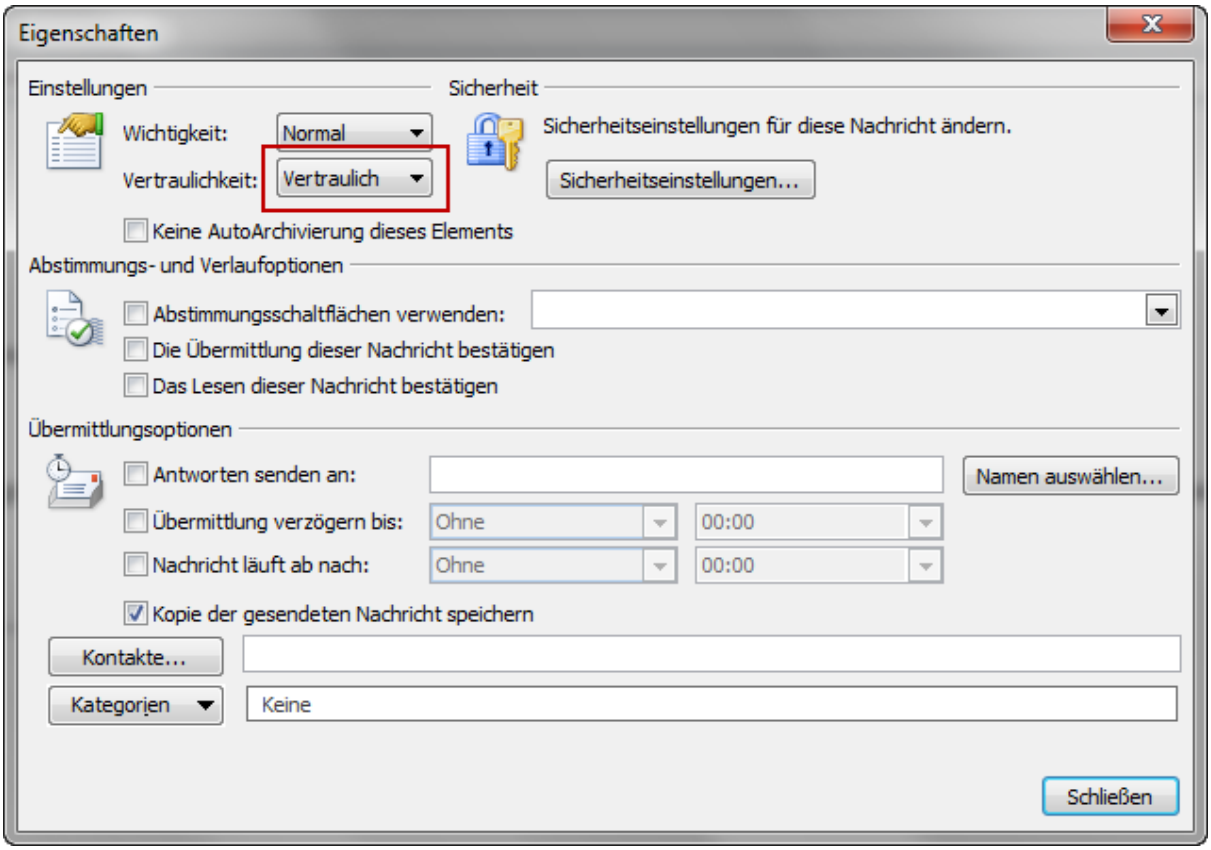
3.8.2 Using e-mail clients

The use of standardised procedures and the central processing by the Mail Encryption appliance provide for the independence of the e-mail client. Therefore, the e-mail client must not be adapted.

Use e-mail clients as follows in order to send e-mails in an encrypted manner:

- Select the message option “Confidential” in MS Outlook.
- Alternatively, enter [secure] into the subject line. This is the term defined by default triggering encrypted e-mail dispatch.

Along with [secure], there are further terms, for signing e-mails for example. You can view and, if necessary, adapt the terms within the framework of the web administration portal in the “Mail Processing” menu in the Ruleset Generator category. For further details, please refer to section Managing the rulset 95.

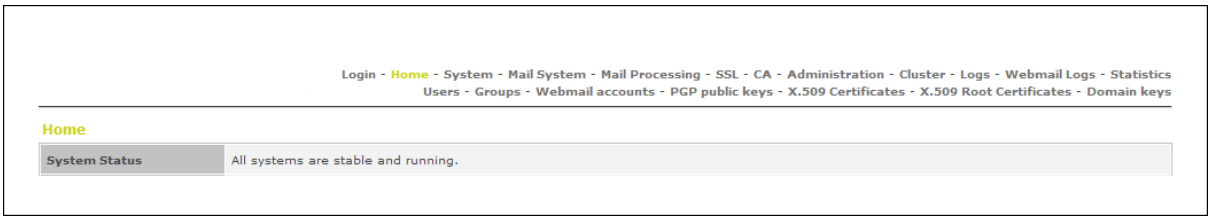


Message option “Confidential” in Outlook

4 Reference of the Menu Items

4.1 Configuration Overview

The administration portal of the Mail Encryption Appliance is divided into the following groups:



Menu structure of the Mail Encryption **secure e-mail gateway appliance**

The following configuration overview contains a short description of all groups. The structure of this part of the manual is oriented on the structure of these groups.

Group	Description
Login	Registration for the configuration interface, changing the personal password for the configuration interface
Home	Display of administrative data, such as system status, system and user licences, current software version, statistical data on the system utilisation, for example
System	Implementation of fundamental network settings, such as IP address, host and domain names, routing, system date and time, for example
Mail System	Configuration of the Mail Encryption e-mail system, e-mail domains, and e-mail routing, e-mail relay server, access control, TLS, anti-spam, blacklists/ whitelists
Mail Processing	Managing/viewing/loading rules on processing e-mails, administration of secure webmail domains, SMS password transfer, disclaimer, e-mail templates, virus scanner and spam protection rules and thresholds, ruleset for e-mail signatures, encryption and decryption
SSL	Configuring and saving the SSL device certificate for the Mail Encryption secure webmail web server
CA	Configuring the proprietary certification authority (CA), configuring the connector to the SwissSign CA, requesting and saving a CA certificate
Administration	Registering Mail Encryption , installing software updates, creating and re-saving data backup, rebooting or shutting down Mail Encryption , resetting Mail Encryption to factory settings, importing existing users or keys, activating the outgoing support connection
Cluster	Creating a cluster with several Mail Encryption systems
Logs	Viewing and managing e-mail log files

Group	Description
Webmail Logs	Viewing and managing secure webmail log files
Statistics	Graphic display of the processed e-mail traffic and of the system utilisation
Users	Creating and managing Mail Encryption user accounts
Groups	Creating and managing Mail Encryption
Webmail accounts	Managing secure webmail accounts
PGP public keys	Importing and managing public PGP keys of communication partners
X.509 Certificates	Importing and managing public S/MIME X.509 certificates of communication partners
X.509 Root Certificates	Importing and managing S/MIME X.509 root CA certificates
Domain keys	Importing and managing PGP and S/MIME domain keys

Reference of the menu items in the Mail Encryption configuration interface

4.2 Menu Item "Login"

Select the “Login” menu item in order to log off from the Mail Encryption configuration interface or to change the password of the proprietary user for the Mail Encryption configuration interface. The individual parameters are described in the following table.

Figure 1 shows the “Login” menu when opening the Mail Encryption configuration interface.

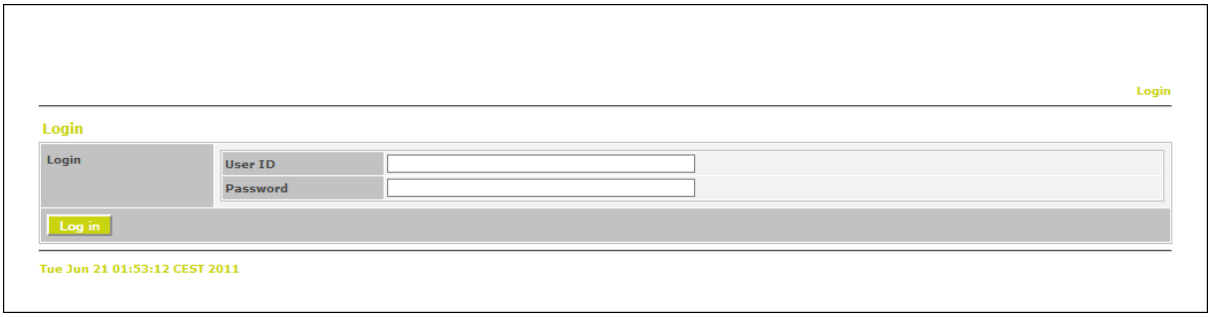


Figure 1 – “Login” menu

Figure 2 shows the “Login” menu when opening it within the Mail Encryption configuration interface.

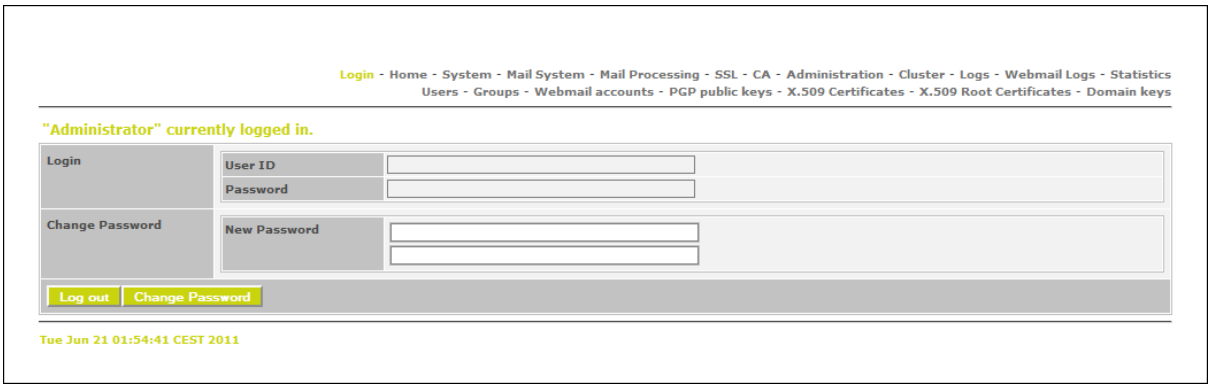


Figure 2 – “Login” menu

Figure 3 shows the “Login” menu after you have logged off from the Mail Encryption configuration interface.

Figure 3 – “Login” menu

Section	Parameter	Description
Login	User ID, Password	Please select the “Log in” button in order to log into the configuration interface.
Log out		Please select the “Log out” button in order to log off from the configuration interface.
Change Password	New Password	You can use this field in order to change the password for the logged in user. When entering the new password a full stop will be displayed as placeholder for every character. In order to avoid typing errors, it is necessary to enter the new password twice. In order to save the new password, please select the “Change Password” button.

Reference of the menu parameters in the “Login” menu

4.3 Menu Item "Home"

Select the “Home” menu item in order to view the administrative system data. The individual parameters are described in the following table.

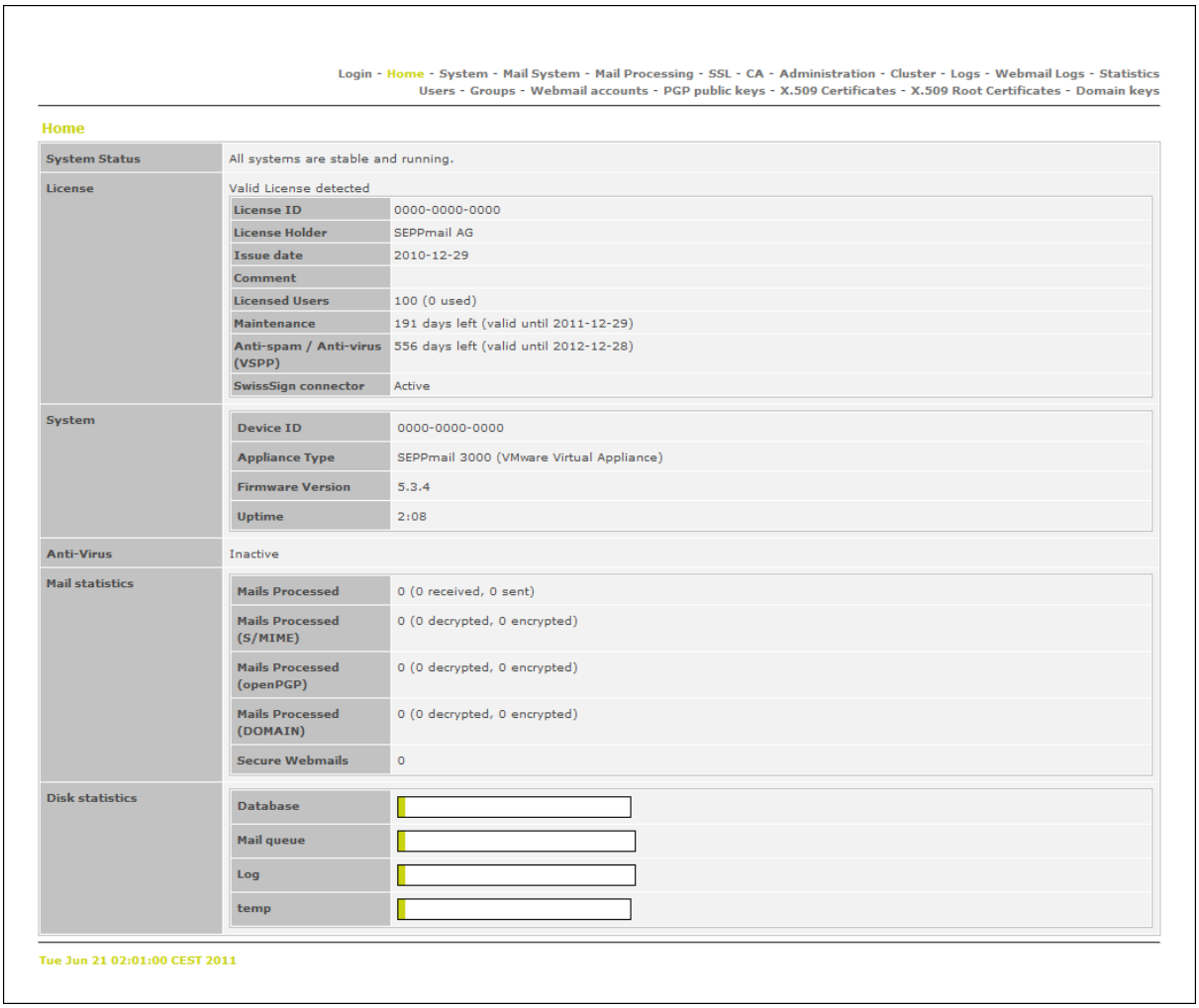


Figure 3 – “Home” menu

Section	Parameter	Description
System Status		The current Mail Encryption system status.
License	License Typ	Information on the system and user licences will be displayed here.
	License ID	Licence number for the Mail Encryption system
	License Holder	Holder of the Mail Encryption licence

Section	Parameter	Description
	Issue date	Issue date of the licence
	Comment	
	Licensed Users	Number of purchased user licences. The number of already used user licences will be displayed in brackets..
	Maintenance	Display of the expiration date of the licence for software updates.
	SPAM / AV (VSPP)	Display of the expiration date of the licence for anti-virus and anti-spam.
System	Device ID	Device licence number
	Firmware Version	Software version currently installed on the System
	Uptime	Runtime of the system since the last reboot
Anti-Virus		Status of the optional virus scanner. This function is only available if you have purchased the software version VSPP (anti-virus, anti-spam, and phishing protection) that is subject to a charge.
Mail statistics	Mails Processed	Number of all e-mails transmitted in total by the system (received, sent)
	Mails Processed (S/MIME)	Number of all e-mails processed via S/MIME (decrypted, encrypted)
	Mails Processed (openPGP)	Number of all e-mails processed via OpenPGP (decrypted, encrypted)
	Mails Processed (DOMAIN)	Number of all e-mails processed via domain encryption (decrypted, encrypted)
	Secure Webmails	Number of all secure webmails sent in total
Disk statistics	Database, Mail queue, Log, temp	Shows the utilisation of individual volumes of the hard disk used within the system, separated according to areas

Reference of the menu parameters in the “Home” menu item

4.4 Menu Item "System"

Select the “System” menu item in order to implement fundamental network settings.

The following processes will be described in the following sections:

4.4.1 Overview Menu Item "System"

You can extend the display of the available parameters by clicking the “Advanced View” button. In order to reduce the advanced representation of the “System” menu item, please click the “Normal View” button in the advanced representation.

This menu can be used to configure the most important parameters of the LAN connection of the Mail Encryption system. The data entered here is also taken as the base settings for many further settings of your Mail Encryption system.

Figure 1 shows the “System” menu in its reduced representation.

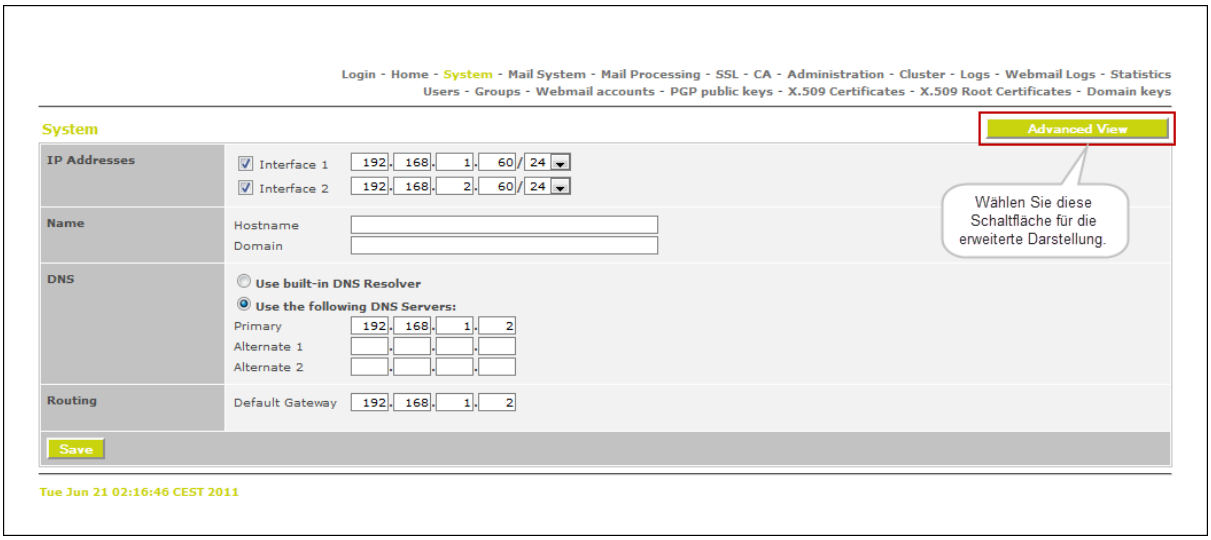


Figure 1 – “System” menu

Section	Parameter	Description
Comment	**System Description**	Please enter a denomination identifying the Mail Encryption system here.. For example, this parameter can be used as subject during automatic data backup; otherwise, it serves for description purposes only.
IP Addresses	**Interface 1**	Please enter the IP address, including subnet mask, and the media type of the physical network interface “eth0” here. By default, you can leave the media type set to the “autoselect” value. One interface configuration will be displayed for each physically existing network interface in each case. The interface number displayed here corresponds to the following network interface: **Interface 1 - eth0**

Section	Parameter	Description
	Interface 2	Please enter the IP address, including subnet mask, and the media type of the physical network interface “eth1” here. By default, you can leave the media type set to the “autoselect” value. One interface configuration will be displayed for each physically existing network interface in each case. The interface number displayed here corresponds to the following network interface: **Interface 2 – eth1**
	Custom host file entries:	Please enter a combination of IP-Adresses to execute a local resolution of DNS names. Format: 10.0.0.1 host.domain.com
IP ALIAS Addresses	**IP Alias 0**	• additional alias IP address of the interface • network mask of the additional alias IP address • VHID (Virtual Host Identification) of the interface • interface – interface the additional alias IP address is to be assigned to • priority – priority of the interface within the cluster
	IP Alias 1	• additional alias IP address of the interface • network mask of the additional alias IP address • VHID (Virtual Host Identification) of the interface • interface – interface the additional alias IP address is to be assigned to • priority – priority of the interface within the cluster
	IP Alias 2	• additional alias IP address of the interface • network mask of the additional alias IP address • VHID (Virtual Host Identification) of the interface • interface – interface the additional alias IP address is to be assigned to • priority – priority of the interface within the cluster
	IP Alias 3	• additional alias IP address of the interface • network mask of the additional alias IP address • VHID (Virtual Host Identification) of the interface • interface – interface the additional alias IP address is to be assigned to • priority – priority of the interface within the cluster
Name	**Hostname**	Please enter the host name of the Mail Encryption system here, e.g. mailencryption
	Domain	Please enter the domain name of the Mail Encryption system here, e.g. egosecure.com **Note:** The name of the system consists of the host name and the

Section	Parameter	Description
		domain name, e.g. mailencryption.egosecure.com
DNS	**Use built-in DNS Resolver**	Regarding this parameter, the system will always attempt to resolve the name with the help of the DNS root name servers on the internet. If you select this parameter, the resolution of DNS names may require large amounts of time and the response of the Mail Encryption system may be delayed on the basis of the aforementioned.
	Use the following DNS Servers:	DNS queries for addresses Mail Encryption is not responsible for itself will be forwarded to superior DNS name servers. For this, Mail Encryption should initially forward the DNS query to an internal DNS server within the proprietary network of the DNS servers of your internet provider you can specify here.
	Primary	Please enter the first DNS name server here which Mail Encryption will forward DNS queries to.
	Alternate 1	If the primary DNS name server is not available or if it does not answer, you can enter an alternative DNS name server here the DNS queries will then be forwarded to.
	Alternate 2	If the primary and the first alternative DNS name servers are not available or if they do not answer, you can enter a further alternative DNS name server here the DNS queries will then be forwarded to. Please ensure that a DNS name server specified here is available, because the function of Mail Encryption may be affected adversely otherwise.
	Search Domain (s):	Please enter a search list containing domain names here that will be queried successively in the event of a DNS query.
	local zone:	Domain name: Enter a pseudo-domainname for which you want to resolve locally in the IP adress of the responsable e-mail server (MX-Record), e.g. pseudo.local.
		host: Hostname, e.g. mail mx: Preference, e.g. 10 ip: IP-adress of the e-mail server, e.g. 10.0.0.1 The responsable e-mail server for the domain pseudo.local will now be resolved to mail.pseudo.local with the IP adress 10.0.0.1 and Preference 10. Local zones can be used, if they can't execute the resolution of the MX record for a domain through a local DNS server and several alternative e-mail servers are needed as a failover for a domain.
Routing	**Default Gateway**	Please enter the IP address of the default router in your network segment here. All data packages that cannot be delivered directly within the local network segment will be forwarded to this IP router.

Section	Parameter	Description
	Static Routes	Along with the use of a default router, you can also specify static IP routes within the Mail Encryption system.These IP routes will be prioritised regarding the use of the default router.
GUI Protocol	**HTTP Port**	Enable this parameter in order to allow for non-encrypted access to the configuration interface by means of HTTP protocol. In order to this, enter a corresponding TCP/port. This option is activated by default and uses the port TCP/8080 in order to gain access to the Mail Encryption configuration interface.
	HTTPS Port	Enable this parameter in order to allow for non-encrypted access to the configuration interface by means of HTTPS protocol. For this, enter a corresponding TCP/port. This option is activated by default and uses the port TCP/8443 in order to gain access to the Mail Encryption configuration interface. **Note:** If, on the basis of an error, the configuration interface no longer responds via HTTPS, a fallback will be activated automatically allowing for access to the configuration interface by means of HTTP to port TCP/8080. This will work even if the use of HTTP regarding the access to the configuration interface was disabled.
	Bind to IP or Hostname	Please enter the host name or the IP address the access to the configuration interface is assigned to. **Note:** In this case, you will only be able to access the system by using the host name respectively the IP address specified here that are also configured within the Mail Encryption system. An erroneous configuration may result in you being locked out from the configuration interface.
Webmail Protocol	**HTTP Port**	Enable this parameter in order to allow for non-encrypted access to the webmail interface of the Mail Encryption system by means of HTTP protocol. For this, enter a corresponding TCP/port. The default HTTP port is TCP/80. **Note:** Please do not use the HTTP protocol for accessing the webmail interface from the internet or from another insecure network. This way, you will allow the logging of web browser connections to the webmail interface of Mail Encryption.
	HTTPS Port	Enable this parameter in order to allow for encrypted access to the webmail interface of the Mail Encryption system by means of HTTPS protocol. For this, enter a corresponding TCP/port. The default HTTPS port is TCP/443.

Section	Parameter	Description
	Enable local https proxy, redirect unknown requests to http://	Reverse Proxy - Activate this parameter, to activate the access for the webmail subsystem not directly, but through the local Mail Encryption reverse proxy. You can also use the Mail Encryption reverse proxy for the access to an internal OWA-server (Outlook Web Acess). HTTP has to be activated on the OWA-interface of the internal MS Exchange server. The reverse proxy forwards all not Mail Encryption relevant requests to intern, e.g. to a special landing-page on the company website or to a OWA-server. ActiveSync connections will also be forwarded to the internal MS Exchange server.
Console Login	**Disable console root login**	If you enable this parameter, the console login on the Mail Encryption system will be blocked.. **Note:** When enabling this parameter, please note that the desired access to the system will no longer be possible in the event of an error in this case either.
	Enable PIX workaround	Enable this parameter if you are using a Cisco PIX firewall and the system is accessed via SSH by means of this firewall.
Syslog Settings	**Forward maillog to syslog server:**	Host name or IP address of the Syslog server within the LAN. The Mail Encryption system logging will be sent additionally to thespecified Syslog server. UDP/514 will be used as destination port.
Proxy Settings	**Proxy Server**	Host name or IP address of the web proxy servers
	Proxy Port	Destination port of the web proxy server, e.g. destination port 8080 or 8081.
	Proxy User	User name for logging in to the web proxy server
	Proxy Password	Password for logging in to the web proxy server
	Use direct connection on port 22 outgoing (preferred)	Activate this option, if a direct SSH connection to the internet is possible without going through a proxy server. The SSH connection uses the protocol TCP with port 22 (TCP/22).
	Connect through SOCKS 4 proxy	Activate this option, to tunnel SSH connections through a generic SOCKS proxy. This option can be used if the direct access via SSH to the internet is regulated, but it's possible for the Mail Encryption system to connect through a SOCKS proxy (version 4) to the internet.
	Connect through SOCKS 5 proxy	Activate this option, to tunnel SSH connections through a generic SOCKS proxy. This option can be used if the direct access via SSH to the internet is regulated, but it's possible for the Mail Encryption system to connect through a SOCKS proxy (version 5) to the internet

Section	Parameter	Description
	Connect through HTTP proxy	Activate this option, to tunnel SSH connections through a HTTP proxy. This option can be used if the direct access via SSH to the internet is regulated, but it's possible for the Mail Encryption system to connect through an HTTP proxy to the internet.
	Connect through Telnet proxy	Activate this option, to tunnel SSH connections through a Telnet proxy. This option can be used if the direct access via SSH to the internet is regulated, but it's possible for the Mail Encryption system to connect through a Telnet proxy to the internet.
	Use port 80 instead of 22	Activate this option if a direct HTTP connection to the internet is possible. The SSH connection then uses the TCP port 80 (HTTP) instead of TCP with port 22 (SSH TCP/22).
Time zone	**Auswahl der Zeitzone**	Use the drop-down menu to select the time zone applicable to the location of the Mail Encryption system.
Time and Date	**Use current setting**	Regarding this option, the current data and the current time of the internal system clock will be used.
	Automatically synchronize with an NTP server	Regarding this option, date and time are synchronised with a specified time server by means of the NTP protocol, destination port TCP/123.
	Server	Host name or IP address of a time server within the network
	Set date and time manually	You can specify the values for the current data and the current time manually here.
	Date	current date in format: dd.mm.ccyy
	Time	current time in format: hh:mm:ss
SNMP Daemon	**Enable SNMP**	Activate Enable SNMP and disable the SNMP daemon on the Mail Encryption system. After having activated the SNMP protocol, you can retrieve information of your Mail Encryption system by means of SNMP tools, such as snmpwalk. Further information on the SNMP support of the Mail Encryption system can be found in chapter »SNMP« 58.
	Listen Adress	
	Read-only Community	Password for the read-only access of the SNMP data.
	Read-write Community	Password for the write-only access of the SNMP data.
	Download MIBs	click this link to download the MIB of the Mail Encryption system as a zip file.

Reference of the menu parameters in the “System” menu item

4.4.2 Forwarding e-mail logs to a central Syslog server

In order to send the e-mail log files of your Mail Encryption appliance to a central Syslog server, please click the "System" menu item in the web administration portal, followed by the "Advanced View" button.

Please enter the name or the IP address the Mail Encryption appliance can use to reach your Syslog server into the Syslog Settings category.

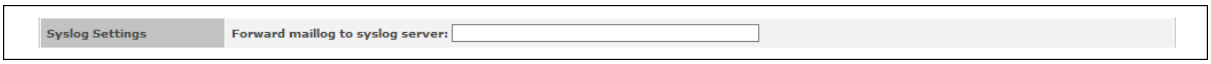


Figure 1 – Forwarding e-mail log data to a central Syslog server

4.4.3 Setting date and time and configuring the NTP synchronisation

In order to set the date and the time or to configure the automatic synchronisation of your Mail Encryption appliance with the network time protocol (NTP) server, please click the "System" menu item and then the "Advanced View" button in the web administration portal.

Use the Time zone and Time and Date categories in order to define your time zone and in order to manually set the date and time or to implement the automatic synchronisation with an NTP server

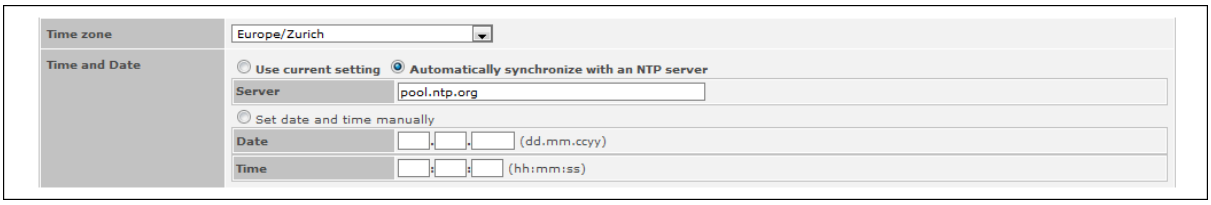


Figure 1 – Setting date and time and configuring the NTP synchronisation

4.4.4 Activating SNMP

In order to control the use of the Simple Network Management Protocol (SNMP), please click the "System" menu item and then the "Advanced View" button in the web administration portal. In order to enable SNMP, please enable the "Enable SNMP" checkbox in the SNMP Daemon category.

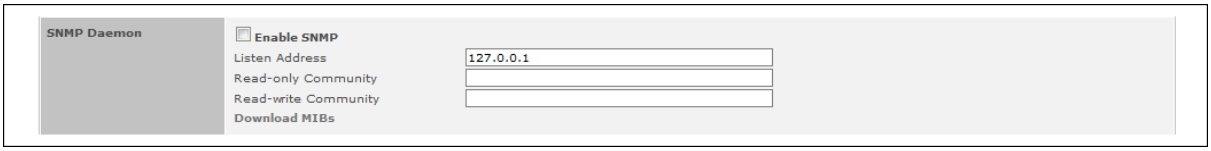
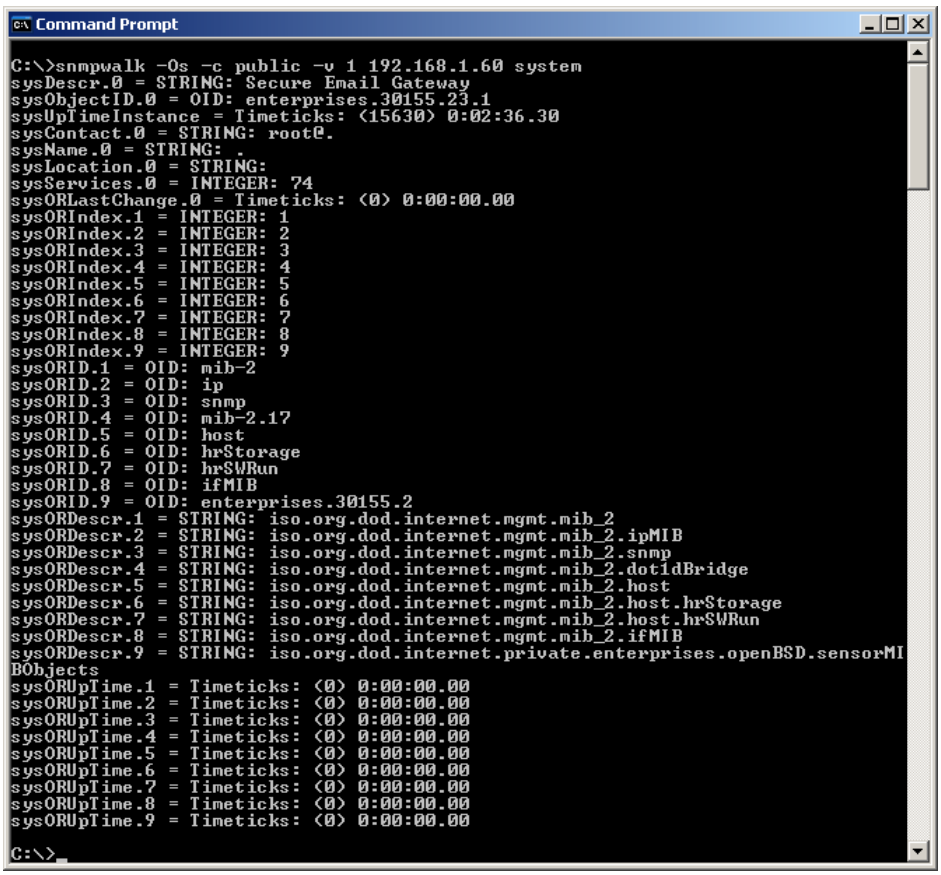


Figure 1 – Enabling SNMP

After having activated SNMP, you can retrieve information of your Mail Encryption appliance by means of SNMP tools, such as snmpwalk. Figure 2 contains an example for the aforementioned.



```
Command Prompt
C:\>snmpwalk -Os -c public -v 1 192.168.1.60 system
sysDescr.0 = STRING: Secure Email Gateway
sysObjectID.0 = OID: enterprises.30155.23.1
sysUpTimeInstance = Timeticks: (15630) 0:02:36.30
sysContact.0 = STRING: root@.
sysName.0 = STRING: .
sysLocation.0 = STRING:
sysServices.0 = INTEGER: 74
sysORLastChange.0 = Timeticks: (0) 0:00:00.00
sysORIndex.1 = INTEGER: 1
sysORIndex.2 = INTEGER: 2
sysORIndex.3 = INTEGER: 3
sysORIndex.4 = INTEGER: 4
sysORIndex.5 = INTEGER: 5
sysORIndex.6 = INTEGER: 6
sysORIndex.7 = INTEGER: 7
sysORIndex.8 = INTEGER: 8
sysORIndex.9 = INTEGER: 9
sysORID.1 = OID: mib-2
sysORID.2 = OID: ip
sysORID.3 = OID: snmp
sysORID.4 = OID: mib-2.17
sysORID.5 = OID: host
sysORID.6 = OID: hrStorage
sysORID.7 = OID: hrSWRun
sysORID.8 = OID: ifMIB
sysORID.9 = OID: enterprises.30155.2
sysORDescr.1 = STRING: iso.org.dod.internet.mgmt.mib_2
sysORDescr.2 = STRING: iso.org.dod.internet.mgmt.mib_2.ipMIB
sysORDescr.3 = STRING: iso.org.dod.internet.mgmt.mib_2.snmp
sysORDescr.4 = STRING: iso.org.dod.internet.mgmt.mib_2.dot1dBridge
sysORDescr.5 = STRING: iso.org.dod.internet.mgmt.mib_2.host
sysORDescr.6 = STRING: iso.org.dod.internet.mgmt.mib_2.host.hrStorage
sysORDescr.7 = STRING: iso.org.dod.internet.mgmt.mib_2.host.hrSWRun
sysORDescr.8 = STRING: iso.org.dod.internet.mgmt.mib_2.ifMIB
sysORDescr.9 = STRING: iso.org.dod.internet.private.enterprises.openBSD.sensorMI
BObjects
sysORUpTime.1 = Timeticks: (0) 0:00:00.00
sysORUpTime.2 = Timeticks: (0) 0:00:00.00
sysORUpTime.3 = Timeticks: (0) 0:00:00.00
sysORUpTime.4 = Timeticks: (0) 0:00:00.00
sysORUpTime.5 = Timeticks: (0) 0:00:00.00
sysORUpTime.6 = Timeticks: (0) 0:00:00.00
sysORUpTime.7 = Timeticks: (0) 0:00:00.00
sysORUpTime.8 = Timeticks: (0) 0:00:00.00
sysORUpTime.9 = Timeticks: (0) 0:00:00.00

C:\>_
```

Abbildung 2 - Abruf von SNMP-Informationen der Mail Encryption appliance

4.5 Menu Item "Mail System"

Select the "Mail System" menu item in order to implement fundamental settings of the Mail Encryption e-mail system.

The following processes will be described in the following sections:

4.5.1 Overview Menu Item "Mail System"

Figure 1 – "Mail System" menu

Section	Parameter	Description
Managed Domains	**Domain Name**	List of all e-mail domains created on the Mail Encryption system for e-mail encryption and e-mail routing.

Section	Parameter	Description
	Server IP Address	List of the e-mail server IP addresses for forwarding the e-mails to the created e-mail servers of the e-mail domains.
	Server Port	List of the e-mail server TCP ports the destination e-mail servers use to accept e-mails for the created e-mail domains.
	Secure Webmail Settings	Shows the secure webmail profile that has been specified for this e-mail domain.
	Disclaimer Settings	Indicates which disclaimer is to be attached to outgoing e-mails of the corresponding e-mail domain
	TLS level	Indicates which type of TLS transport encryption should be used by the Mail Encryption appliance for the corresponding e-mail domain towards the specified e-mail server.
	“Add Domain...” button	Click this button in order to add further e-mail domains. These e-mail domains must match the e-mail addresses of your company. You will find further information on managing e-mail domains in the chapter »Creating e-mail domains to be managed« 67.
	Automatically create and publish S/MIME domain keys for all domains	This parameter causes that a self-dependently signed X.509 S/MIME domain key is created automatically for all e-mail domains newly added using the “Add Domain...” button and that this key is transmitted to a central update service. This newly generated S/MIME domain key for your e-mail domain will be distributed automatically to all Mail Encryption systems afterwards so that all companies operating a ein Mail Encryption system can exchange encrypted e-mails between each other without any more efforts. **Note:** If you do not wish to use this option, please disable this parameter before creating any new e-mail domains. The S/MIME domain key will then not be generated automatically. This procedure can be implemented manually afterwards using the “Generate new S/MIME Certificate” button after the creation within the settings of the e-mail domain. The S/MIME certificate newly created as described above will not be transmitted to the central update service. This parameter is enabled by default.

Section	Parameter	Description
	Fetch Mail from remote POP3 server	This parameter causes that the POP3 account created within the user account is fetched in a time interval by Mail Encryption. This interval is 3 minutes. The e-mails fetched as described above are forwarded to the loca Mail Encryption system. This parameter is disabled by default.
	Verify recipient addresses using SMTP-Lookups	This parameter results in the e-mail address of the recipient being checked in advance with the e-mail server created for the e-mail domain where the e-mails are forwarded to. If the examination of the recipient's e-mail address is not successful, the Mail Encryption system will reject the acceptance of the e-mail.
Outgoing Server	**Use built-in mail transport agent**	This parameter causes that outgoing e-mails towards the internet are delivered directly to the destination e-mail server of the e-mail recipient by the Mail Encryption system.
	Use the following SMTP server:	If you do not want to directly deliver outgoing e-mails towards the internet, it is recommendable to use an e-mail relay server with your provider. All outgoing e-mails will be transmitted to this e-mail relay server, whereby this server will then forward your e-mails to the recipient. Alternatively, you can also use an existing internal e-mail server for dispatch purposes.
	Server name	Please enter the host name or the IP address of the e-mail relay server of your provider or of the existing internal e-mail server here. **Note:** If possible, use a host name, because IP addresses for e-mail relay servers may be subject to change more often and, thus, additional efforts in order to configure the system can be avoided. If you are using an existing internal e-mail server, you can use the IP address of this server, because the IP addresses of internal systems do not change that frequently.
	Server requires authentication:	E-mail relay servers with your provider or existing internal e-mail servers mostly require authentication in order that you are enabled to transfer e-mails to these servers. Please use the corresponding login details for the aforementioned.
	User ID	Please enter the user name for login purposes here.
	Password	Please enter the password for login purposes here.

Section	Parameter	Description
TLS settings	**“Add TLS Domain...” button**	Please select the “Add TLS Domain...” button in order to manage the TLS settings. You will find further information on managing TLS e-mail domains in the chapter »“Configuring TLS encryption per domain« 69.
SMTP settings	**max. message size (kb)**	Please enter the maximum size of an e-mail in kilobyte that the Mail Encryption system is allowed to transfer into this field. E-mails exceeding this size will be rejected.
	Postmaster address	Please enter the e-mail address of the local administrator of the Mail Encryption system. All status messages generated by Mail Encryption will be sent to this e-mail address.
	SMTP bind address (use with care!)	Specification of the IP address of a network interface that is used to receive all e-mails (normally not required).
	openPGP key creation options	
	automatically send new public keys to users	This parameter causes that the public keys generated by OpenPGP are sent automatically to the internal users within the company network via e-mail
Relaying	**Relaying allowed: .../**	Please enter the IP address of the e-mail server the Mail Encryption system may receive e-mails from here. You can also enter an entire IP network here.
	Relaying allowed: .../	If you dispose of a second e-mail server e-mails are to be accepted from, please enter the IP address of this server here additionally. The Mail Encryption system will now also receive e-mails coming from this system. You can also enter an entire IP network here.
	Add Relaying for:	Any further additional e-mail servers or IP networks from which the Mail Encryption system is allowed to receive incoming e-mails can be specified here.
Antispam	**Recommended Settings:**	If you have purchased the optional software option VSPP, anti-virus, and spam protection, the options for configuring these optional components will be available to you. This software option is only available in the case of corresponding licensing.
	Use Greylisting	This parameter causes the “Greylisting” function to be enabled within the e-mail system. Incoming external e-mails will no longer be accepted immediately, but in a delayed manner. This results in the methods used by spam senders regarding the

Section	Parameter		Description
			direct dispatch of e-mails remain without success. You can use this function to significantly reduce the occurrence of spam e-mails. The reception of desired e-mails will not be prevented by this function, but only delayed. The e-mail server of the sender will attempt a second delivery after a short period of time. The e-mail will then be accepted. The term “external e-mails” comprises all e-mails that were not sent from an e-mail server specified in the “Relaying” section. Note: This function is only applicable if the Mail Encryption system directly receives incoming e-mails from the internet. Spam e-mails that were already received and forwarded by another e-mail server cannot be avoided by this function. **Note on “Greylisting”** Greylisting is a method for fighting spam e-mails. Regarding this function, it is assumed that e-mail servers and e-mail clients observe the RFC standard for SMTP. Spam senders often do not use any RFC-compliant software in order to send spam e-mails. The temporary rejection of the e-mail to be sent by the recipient is not analysed and there will be no further delivery attempt. This way, viruses distributing self-dependently via e-mail are rejected, because they do not make any second delivery attempt either. It is recommended to use the option »Greylist learning only (no mail rejection)« for approx. one month before enabling the “Use Greylisting” option. By using the »Greylist learning only (no e-mail rejection)« option the Mail Encryption appliance enters into a learning mode with regard to the greylisting function and temporarily does not reject any e-mails.
		Use Antispam Engine (Note: remember to activate in ruleset)	This parameter causes that the spam filter on the Mail Encryption system is enabled. The configuration of the spam filter is implemented in the ruleset generator in the »Mail Processing« 76 menu.
		Use Antivirus Engine (Note: remember to activate in ruleset)	This parameter causes that the virus scanner on the Mail Encryption system is enabled. The configuration of the virus scanner is implemented in the ruleset

Section	Parameter		Description
			generator in the »Mail Processing« 76 menu
		Require HELO command	This parameter results in an examination of whether the sending e-mail server uses the HELO command when establishing the connection with Mail Encryption is implemented. If this is not the case, no e-mails will be accepted when this parameter is enabled.
		PTR check (reverse DNS lookup)	Spam senders frequently use e-mail servers that are not registered in the DNS. If this option is enabled, no e-mails from e-mail servers that do not dispose of an entry in the DNS will be accepted.
		Check if sender domain is valid	Using this option you can enable the examination of the domain part of the sender e-mail address of each e-mail coming in from external sources. If there is no entry for this domain within the DNS, the e-mail will be rejected.
		Require valid hostname in HELO command	Enable this option if e-mails are only to be accepted from those e-mail servers that report with a valid host name. If there is no entry for this host name within the DNS, the e-mail will be rejected.
		Require fully qualified hostname in HELO command	Enable this option if e-mails are only to be accepted from those e-mail servers that identify themselves with a complete host name (FQDN = Fully qualified domain name).
	optional Settings		
		Greylist learning only (no mail rejection)	This parameter will activate the greylisting learning mode. In this, the database containing the information required for the greylisting mode will be built. Please use this option for approx. one month before enabling and using the active greylisting mode “Use Greylisting”.
		Strict PTR check (reserse DNS lookup)	When using this option, it is assumed for the acceptance of e-mails that the IP address of the sending e-mail server can be resolved to its host name within the DNS (PTR) and that the host name indicates the corresponding IP address again (A record).
Blacklists	**Add Blacklist (RBL):**		On the basis of spam activities, e-mail servers are added to blacklists. These lists are maintained by different providers on the internet. In order to reject e-mails sent from such e-mail servers, you must enter the name of the corresponding Realtime Blackhole Lists (RBL) into this input field.

Section	Parameter	Description
Manual Blacklisting / Whitelisting	**add acccess entry**	You can use this menu item to block or explicitly permit IP networks from which an e-mail server attempts to send an e-mail to the Mail Encryption system. For this, please enter the IP network, the action, and a comment into the corresponding input fields. network : <IP network or IP host address> action : <action> comment : <comment on the entry> The “action” parameter may assume the following values: accept | reject accept : permit explicitly reject : block **Example:** In order to reject all e-mails that are sent from the IP network range 186.56.148.x, please enter the IP network part 186.56.148 and define the action “reject”. However, networks for which you explicitly wish to permit the acceptance of sent e-mails must be declared with the action “accept”.

Reference of the menu parameters in the “Mail System” menu item

4.5.2 Creating e-mail domains to be managed

In order to configure e-mail domains you wish to manage using your Mail Encryption appliance, please click the "Mail System" menu item and then the "Add Domain..." button in the web administration portal.

Enter the e-mail domain name or the e-mail domain names you wish to manage using your appliance into the Domain Name category. This is your domain respectively these are your domains, matching the e-mail address of your organisation. If you enter several names, please separate each name with a space character.

Enter the IP address or the host name of the e-mail server responsible for the e-mail domain into the Server IP or MX name category. Please ensure that the Mail Encryption secure e-mail gateway is able to reach the corresponding e-mail server using the specified IP address or the host name, if required. The appliance will decrypt incoming e-mails of the defined domain(s) and will forward this/ these to the corresponding e-mail server.

Selfsigned S/MIME certificates, that have been issued by Mail Encryption, can be used as well as externally signed certificates in In the category S/MIME Domain Encryption.

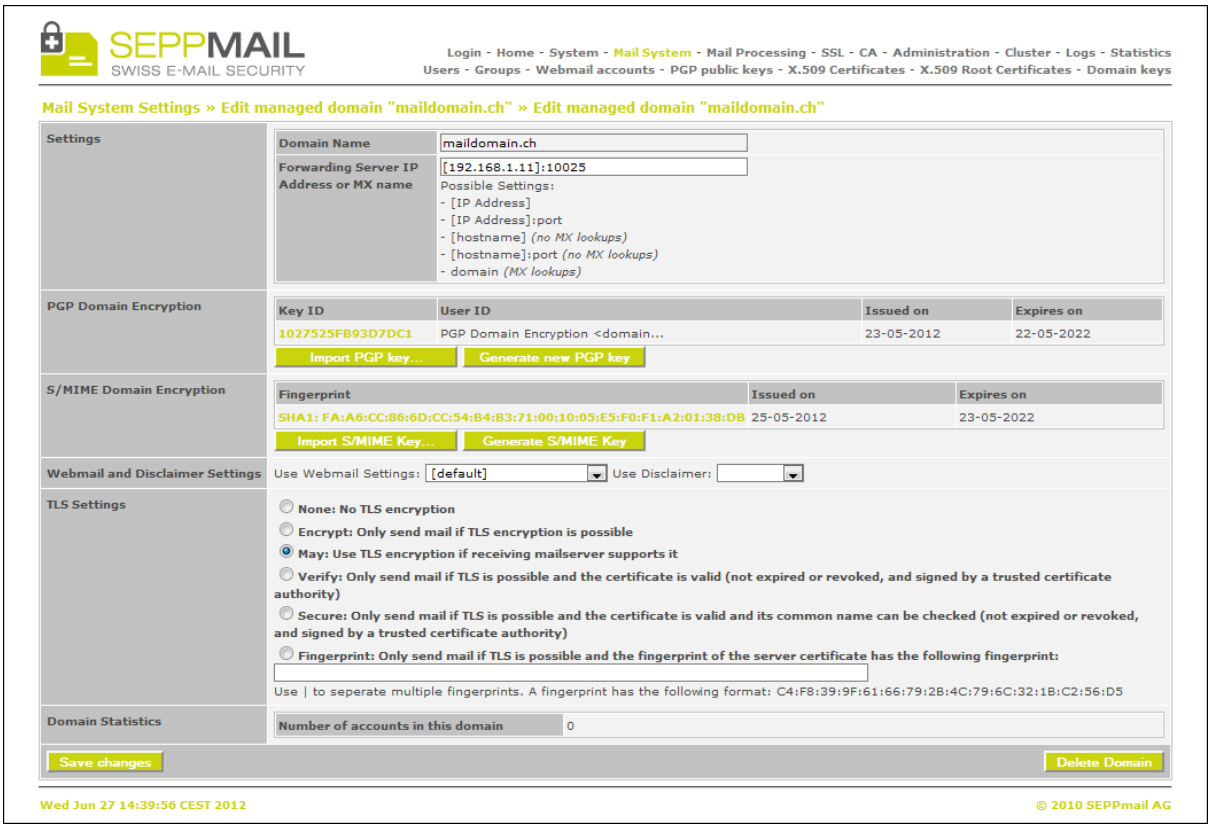


Figure 1 – Adding an e-mail domain

4.5.3 Controlling the outgoing e-mail traffic

In order to define how outgoing e-mails are processed, please click the "Mail System" menu item in the configuration interface.

If Mail Encryption is supposed to send the e-mails directly to external e-mail recipients, please select the "Use built-in mail transport agent" option. If external dispatch is to be implemented by means of an existing e-mail server, please define the corresponding server in the Outgoing Server category next to "Server Name". If the e-mail server requires any authentication, please enter the user name and the password for "User ID" and "Password".

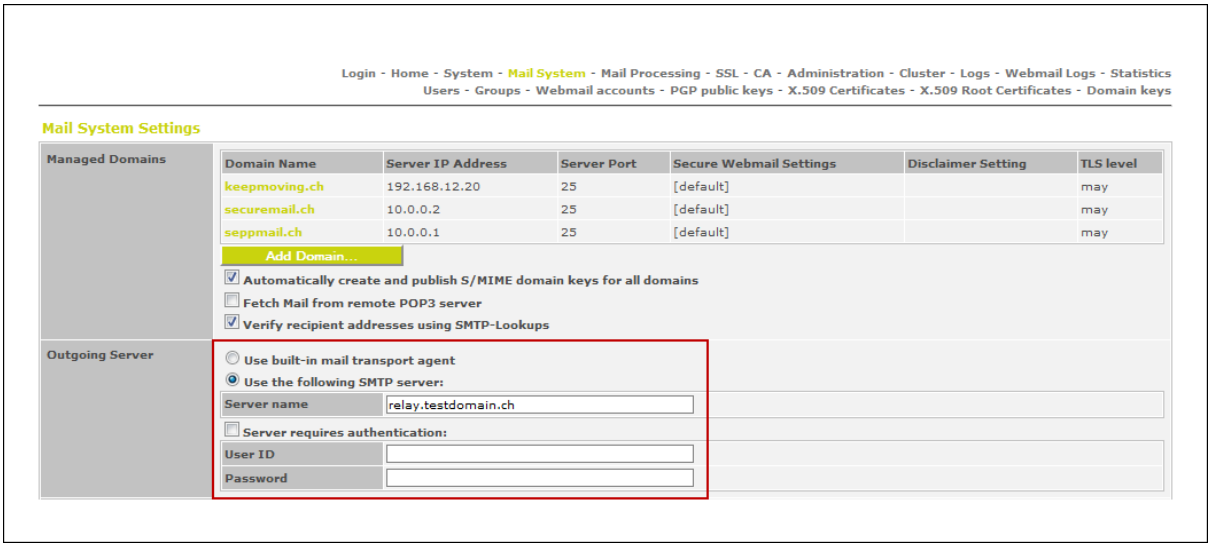


Figure 1 – Definition of the outgoing e-mail server

4.5.4 Configuring TLS encryption per domain

In order to manage TLS settings, please click the “Mail System” menu item and then the “Add TLS Domain...” button in the configuration interface.

You can define the level of TLS encryption for different e-mail domains the Mail Encryption appliance sends e-mails to.

Please define the parameters as follows:

- Domain Name: name of the domain Mail Encryption sends e-mails to
- Optional Server Address: IP address of the e-mail server responsible for the domain (optional)
- Server Port: port of the main server responsible for the domain (normally port 25)

Please define the level of TLS encryption in the TLS Settings category by selecting one of the following options:

TLS setting	Description
None	No TLS encryption.
May	E-mails will be sent using a TLS-encrypted channel, if the receiving e-mail server supports TLS encryption.
Encrypt	E-mails will only be sent if dispatch via TLS encryption is possible.
Verify	E-mails will only be sent if dispatch via TLS encryption is possible and if the SSL certificate of the receiving e-mail server is valid.
Secure	E-mails will only be sent if dispatch via TLS encryption is possible, if the SSL certificate of the receiving e-mail server is valid, and if the name of the e-mail server can be checked successfully in accordance with the certificate.
Fingerprint	E-mails will only be sent if dispatch via TLS encryption is possible and if the SSL certificate of the receiving e-mail server corresponds to the defined fingerprint. SHA1 is supported as fingerprint.

Levels of TLS encryption

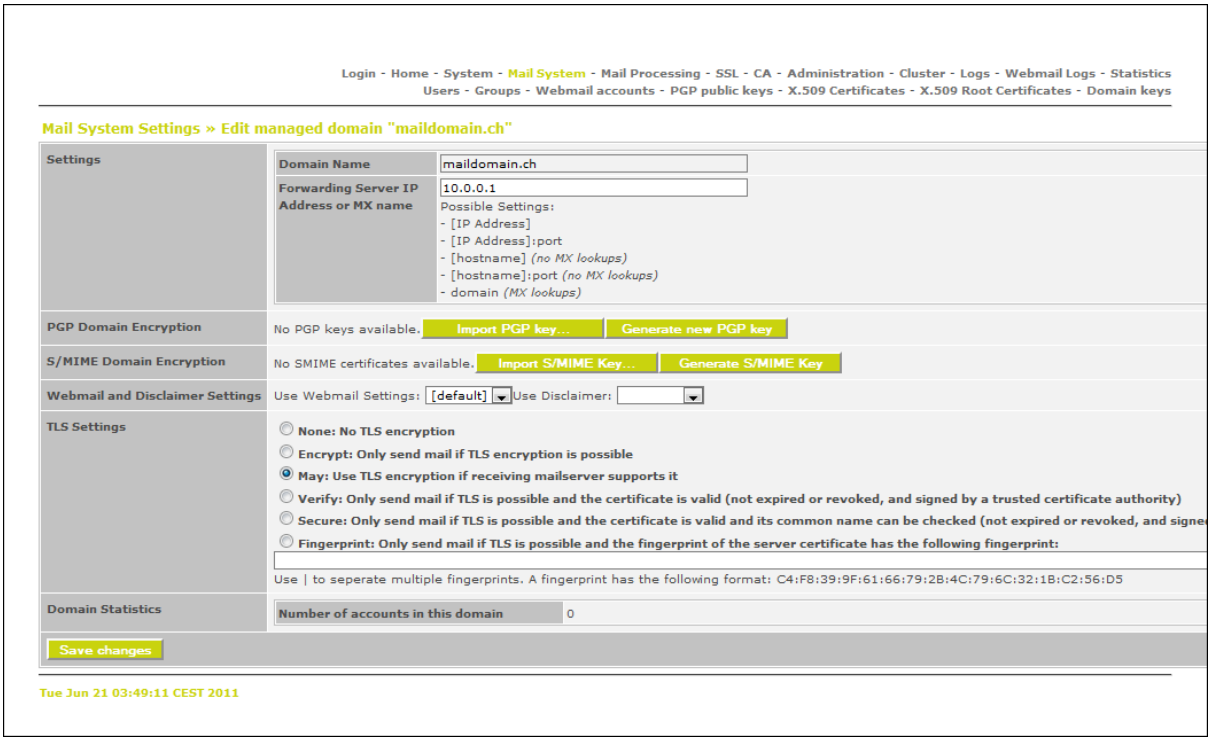


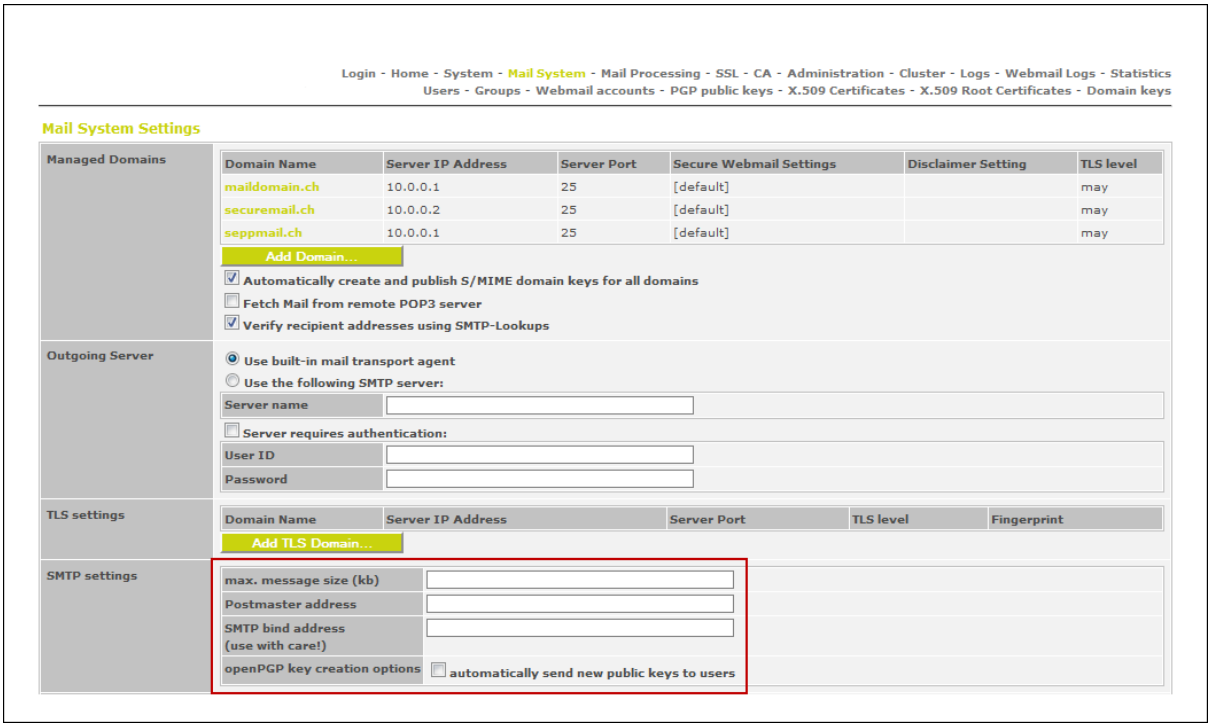
Figure 1 – Definition of the TLS encryption for an e-mail domain

4.5.5 SMTP Settings

In order to define the SMTP settings of your Mail Encryption appliance, you must click the Mail System menu item in the web administration portal.

You can specify the following parameters:

- max. message size (kb): maximum size of an e-mail message
- Postmaster address: e-mail address of the postmaster
- SMTP bind address (use with care!): specification of the IP address of a network interface that is used to receive all e-mails (normally not required)
- OpenPGP key creation options, automatically send new public keys to users: If this option is enabled, the public keys generated by OpenPGP will be sent automatically to the users



SMTP settings

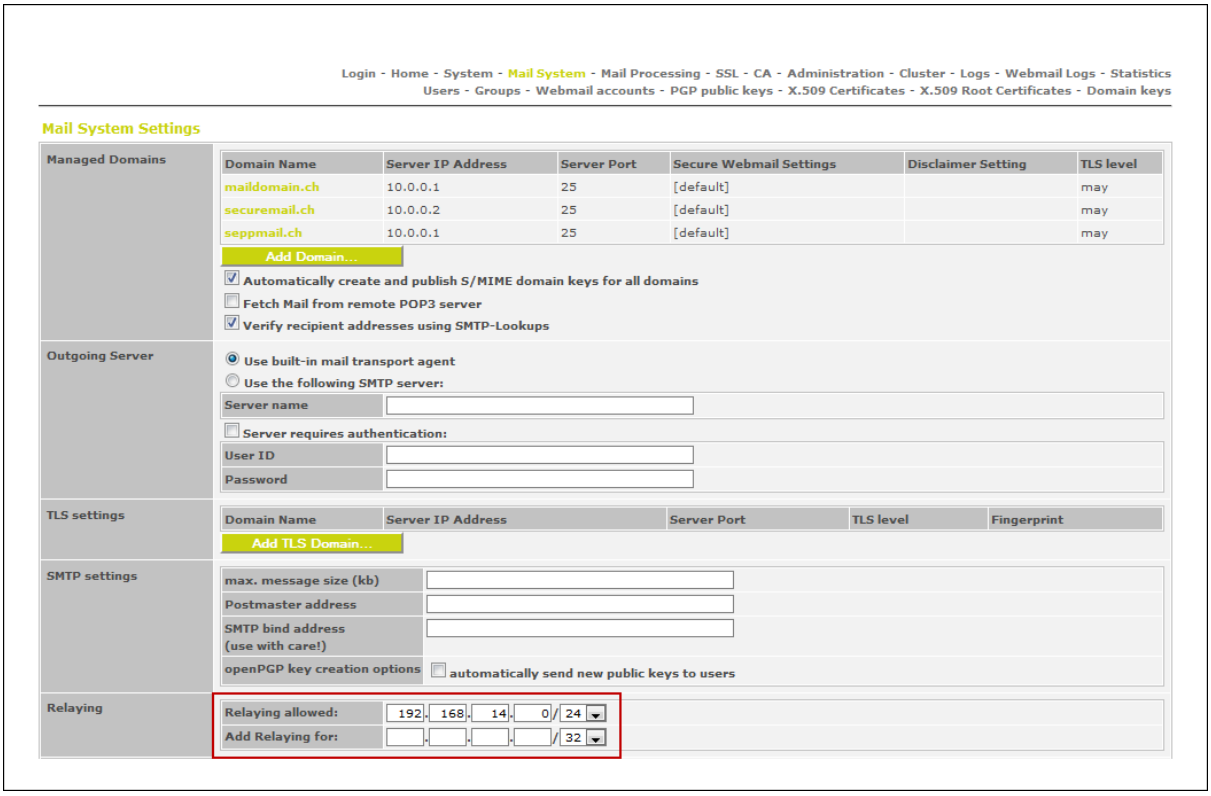
4.5.6 Mail Relaying

In order to define the e-mail relaying settings of your Mail Encryption appliance, you must click the Mail System menu item in the web administration portal.

You can use the Relaying category to define which networks or IP addresses can be used to send e-mails via the Mail Encryption appliance from. Please ensure that only internal networks respectively IP addresses are listed that can be found in your administration. This way, you will prevent the incorrect dispatch of e-mails via your Mail Encryption appliance.

The definition of the networks is specified in accordance with the Classless Inter-Domain Routing (CIDR) Notation. For example, the aforementioned corresponds to the following values:

- The network mask 255.255.255.255 corresponds to "/32" (individual IP address)
- The network mask 255.255.255.0 corresponds to "/24" (class C network)
- The network mask 255.255.0.0 corresponds to "/16" (class B network)
- The network mask 255.0.0.0 corresponds to "/8" (class A network)

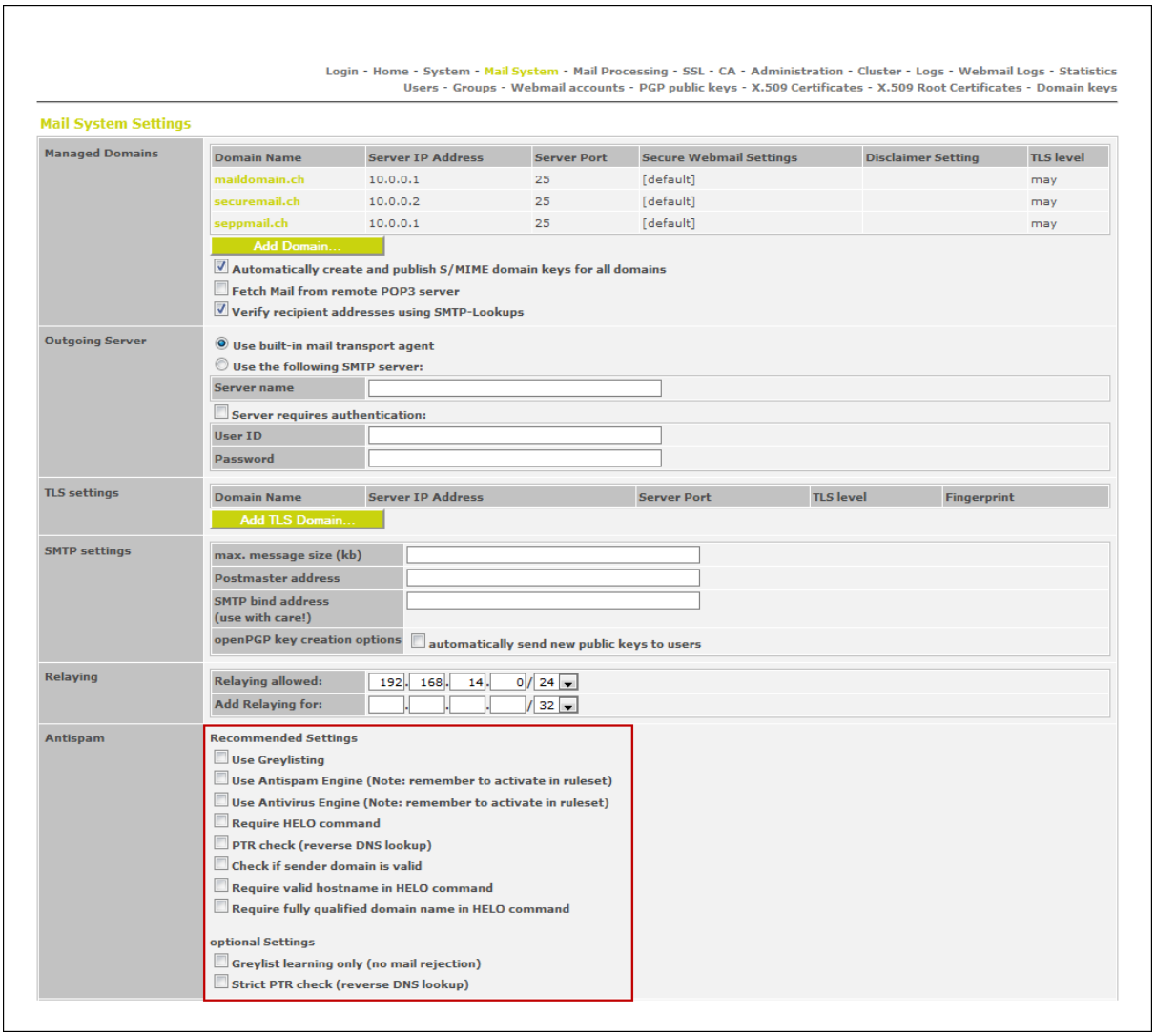


E-mail relaying settings

4.5.7 Anti-spam settings

In order to define the anti-spam settings of your Mail Encryption appliance, you must click the “Mail System” menu item in the web administration portal.

You will only be able to use the anti-spam functionality if you have licensed VSPP (virus, spam, and phishing protection).



Anti-spam settings

The following options are available in the category Antispam:

Use Greylisting
Greylisting is a method for fighting spam e-mails. Within the framework of the aforementioned, e-mails coming from unknown addresses are not accepted immediately, but are initially rejected. For legitimate e-mails, the sending e-mail server will hold the e-mails pendent and will re-transmit the e-mails at a later point in time. The e-mails will then be accepted during the second delivery attempt.

Regarding this mechanism, it is assumed that e-mail servers and clients adhere to the RFC standard

for SMTP. Spam senders often do not use any RFC-compliant software for the sending of spam e-mails. They are not able to deal with the error and are not able to remember that they must try again at a later point in time.

Viruses distributing self-dependently are rejected in so doing, because they do not implement any second delivery attempt either.

It is recommended to use the Greylist learning only (no e-mail rejection) option for approx. one month before enabling the “Use Greylisting” option. By using the Greylist learning only (no e-mail rejection) option, the appliance enters into a learning mode with regard to the greylisting function and does not temporarily reject any e-mails.

Use Antispam Engine
Enable this option in order to use the VSPP anti-spam feature

Require HELO command
It is checked whether the sending e-mail server uses the HELO command. If this is not the case, no e-mails will be accepted when this option is enabled..

PTR check (reverse DNS lookup)
Spam sender often use e-mail servers that are not entered within the DNS. When this option is enabled, no e-mails from corresponding e-mail servers will be accepted.

Check if sender domain is valid
If this option is used, only e-mails will be accepted if the e-mail exchanger host specified by the e-mail server indicates the corresponding IP address.

Require valid hostname in HELO command
When this option is enabled, e-mails are only accepted if the e-mail server identifies with a valid host name.

Require fully qualified domain name in HELO command
Enable this option if e-mails are only to be accepted from those e-mail servers that identify themselves with a complete host name (FQDN = Fully qualified domain name).

Greylist learning only (no e-mail rejection)
This option will activate the greylisting learning mode. In this, the database containing the information required for the greylisting mode will be built. Please use this option for approx. one month before using the active greylisting mode Use Greylisting.

Strict PTR check (reverse DNS lookup)
When using this option, it is assumed for the acceptance of e-mails that the host address of the sending e-mail server can be resolved via its IP address within the DNS (PTR) and that the name entry indicates the corresponding IP address again (A record).

4.5.8 Managing blacklists / whitelists

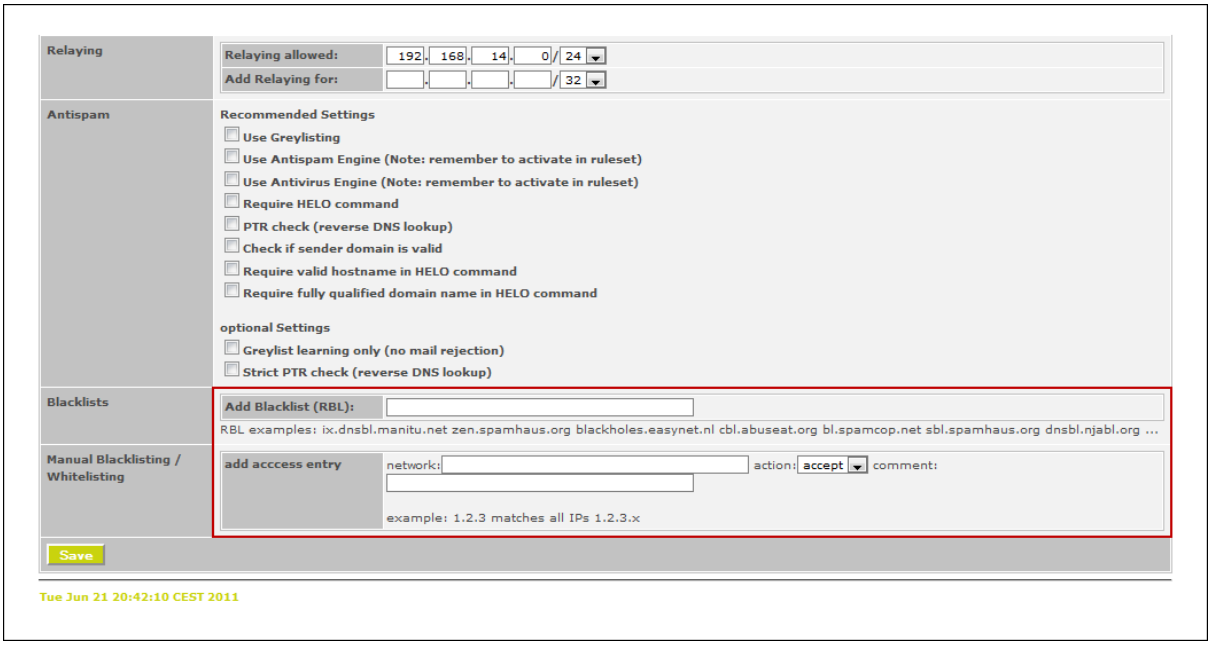
In order to define blacklists and whitelists, you must click the “Mail System” menu item in the web administration portal.

Mail servers are added to blacklists on the basis of spamming activities. These lists are maintained by different providers on the internet. In order to reject e-mails coming from such servers, please

enter the corresponding Realtime Blackhole Lists (RBL) into the Blacklists category.

If you wish to manually block or explicitly permit networks, please enter these into the Manual Blacklisting / Whitelisting category.

For example, in order to reject all e-mails coming from the network 186.56.148.x, you must enter 186.56.148 and define the action reject. However, networks for which you explicitly wish to permit the acceptance of e-mails must be declared with the action accept.



Managing blacklists / whitelists

4.6 Menu Item "Mail Processing"

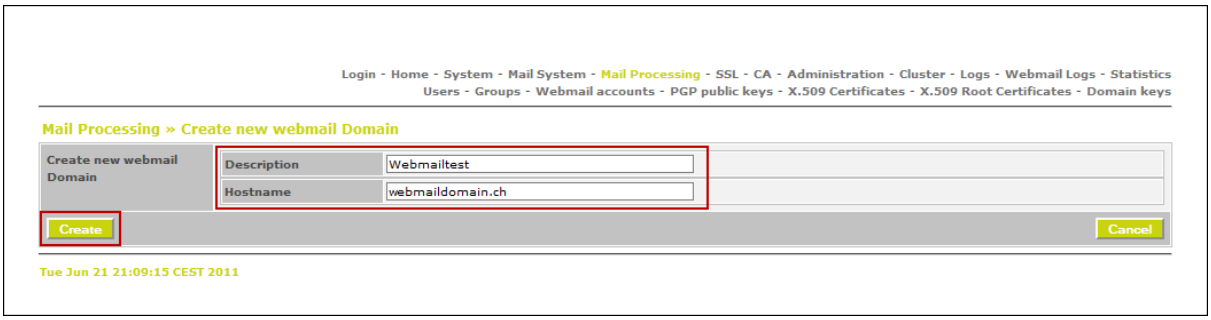
This chapter describes the process of managing the e-mail ruleset.

The following processes will be described in the following sections:

4.6.1 Creating webmail domains

In order to create a new webmail domain, please click the "Create new webmail domain..." button in the Webmail domains category.

Please enter the following values:
• Description: a description of the new webmail domain
• Host name: name of the host of the new webmail domain. This name is part of the URL that is used to retrieve webmails, e.g. https://appliancehostname.ch/webmaildomain.ch

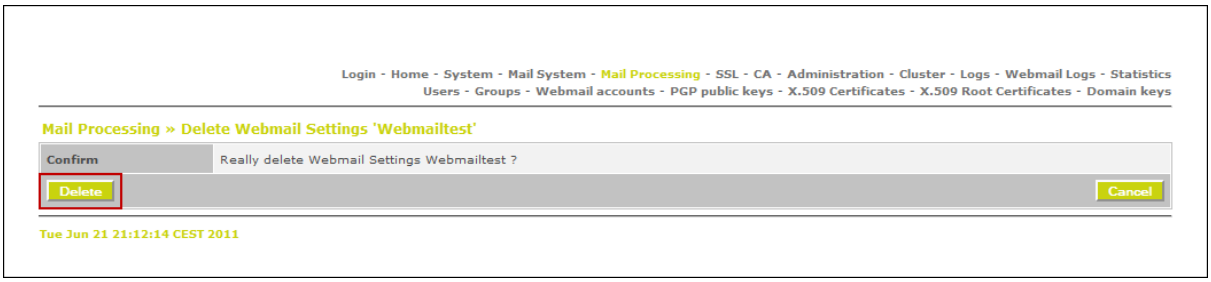


Creating a new webmail domain

Confirm the creation of a new webmail domain by clicking the "Create" button.

4.6.2 Deleting webmail domains

In order to delete a webmail domain, please select the webmail domain to be deleted in the Webmail domains category and click the “Delete...” button.



Confirmation of the deletion of a webmail domain

Confirm the deletion of a webmail domain by clicking the "Delete" button.

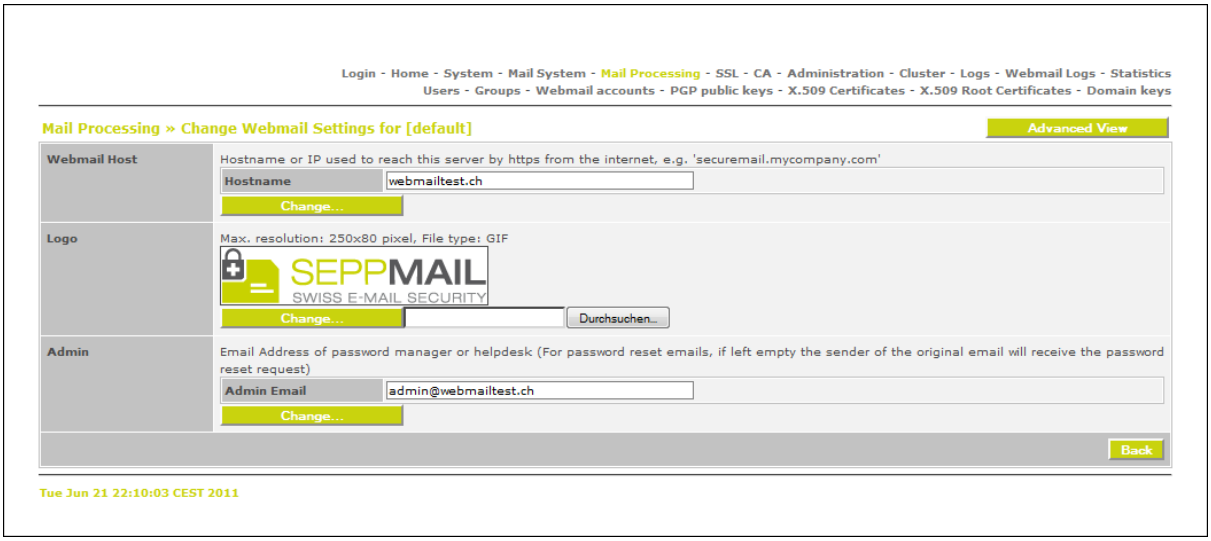
4.6.3 Managing webmail domains

In order to manage webmail domains, you must click the “Mail Processing” menu item in the web administration portal.

You can edit webmail settings by selecting the corresponding webmail domain in the Webmail domains category and then clicking the “Edit...” button. The standard webmail domain is called [default].

You can manage the following parameters:

- Hostname: name of the host of the new webmail domain. This name is part of the URL that is used to retrieve webmails, e.g. https://appliancehostname.ch/webmaildomain.ch
- Logo: image displayed to recipients when retrieving EgoSecure Mail Encryption (ESWMail) messages.
- Admin Email: e-mail address of the responsible administrator

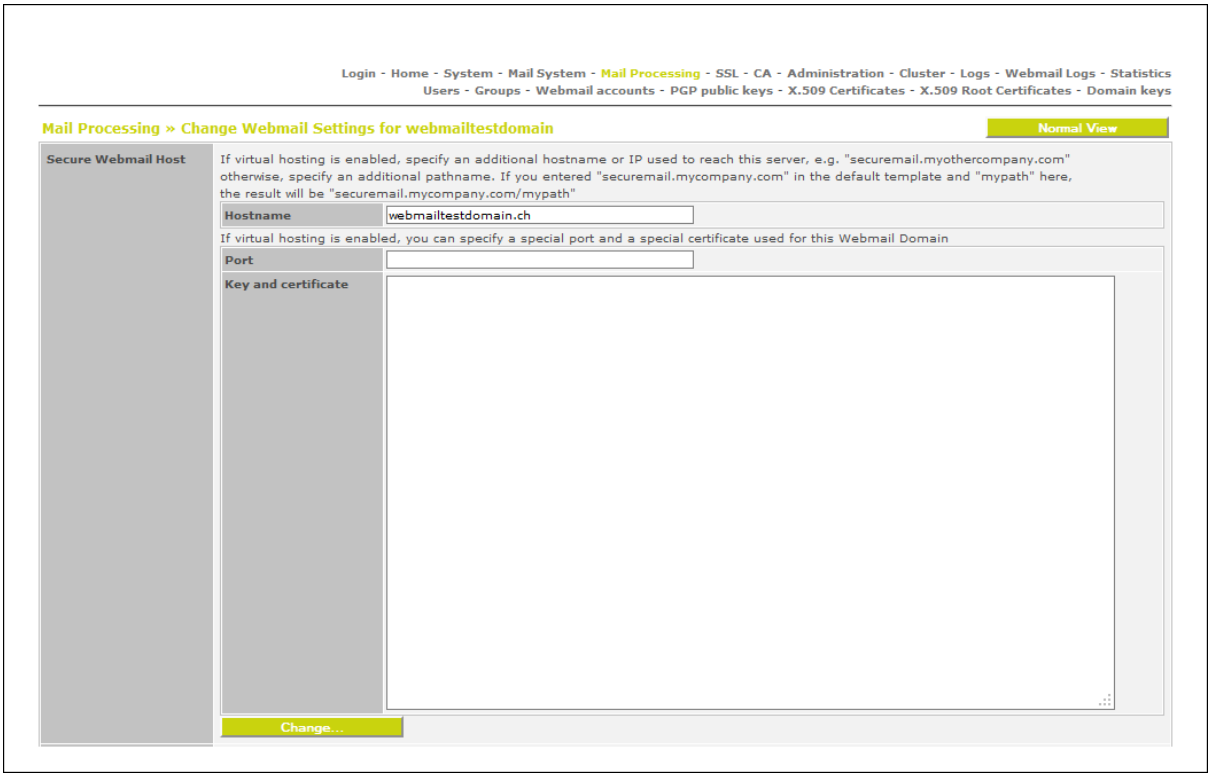


Managing the settings of an existing webmail domain

In case you wish to implement further settings, please click the “Advanced View” button. Along with the standard settings described above, you can implement modifications within the following categories there:

These sections are explained in detail in the following.

"Advanced View" - »Secure Webmail Port« - »Secure Webmail Key and certificate«

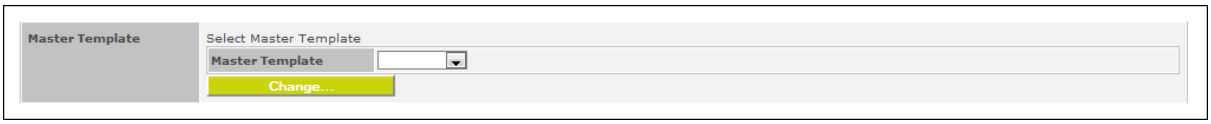


Category port, key and certificate at "Advanced View"

Using the Port, Key, and certificate section you can enter a proprietary port and you can store a

proprietary SSL certificate for the webmail domain.

"Advanced View" - Master Template

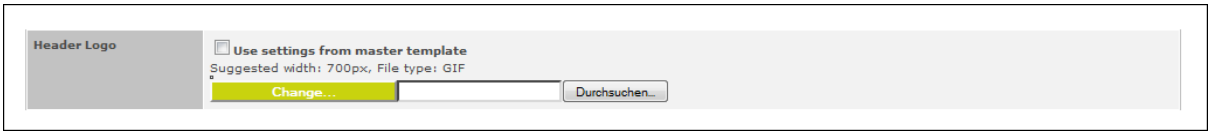


Category Master Template at Advanced View

You can use the Master Template section to select a webmail domain the settings of which can be transferred. This will facilitate the process of managing options that are to be applicable to several webmail domains.

If the standard webmail domain [default] is selected, the aforementioned is used as a template for transferring settings. To which extent settings will be transferred can be specified within the framework of the individual categories that are explained in detail below.

"Advanced View" - Header Logo

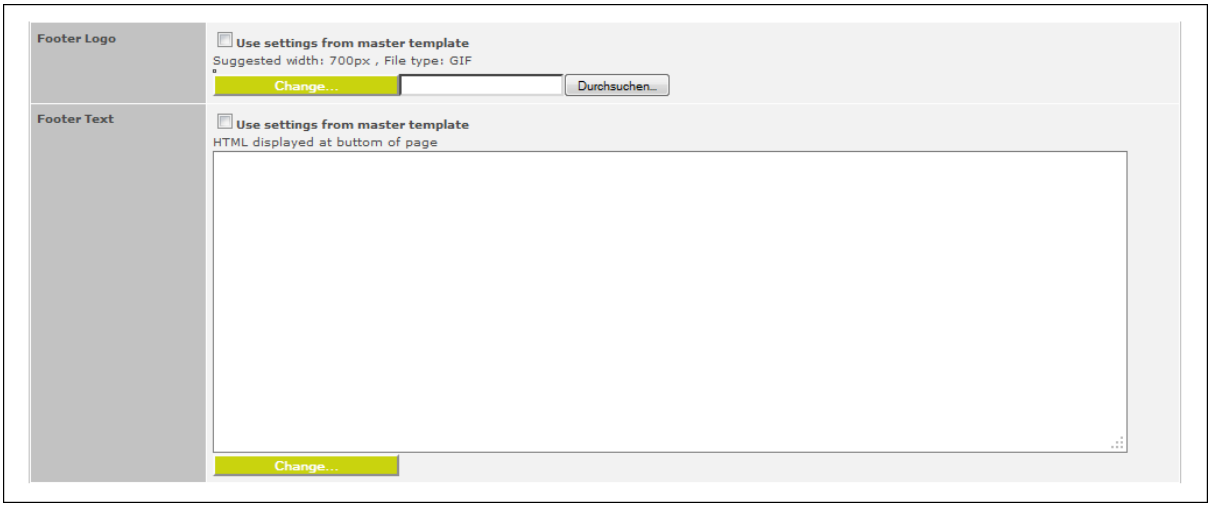


Category Header Logo at Advanced View

You can use the Header Logo section to specify an image recipients will see when they retrieve EgoSecure Mail Encryption (ESWMail) messages in the area of the header.

If you wish to transfer the header image from the master template, please enable the Use settings from master template checkbox.

"Advanced View" - Footer Logo und Footer Text

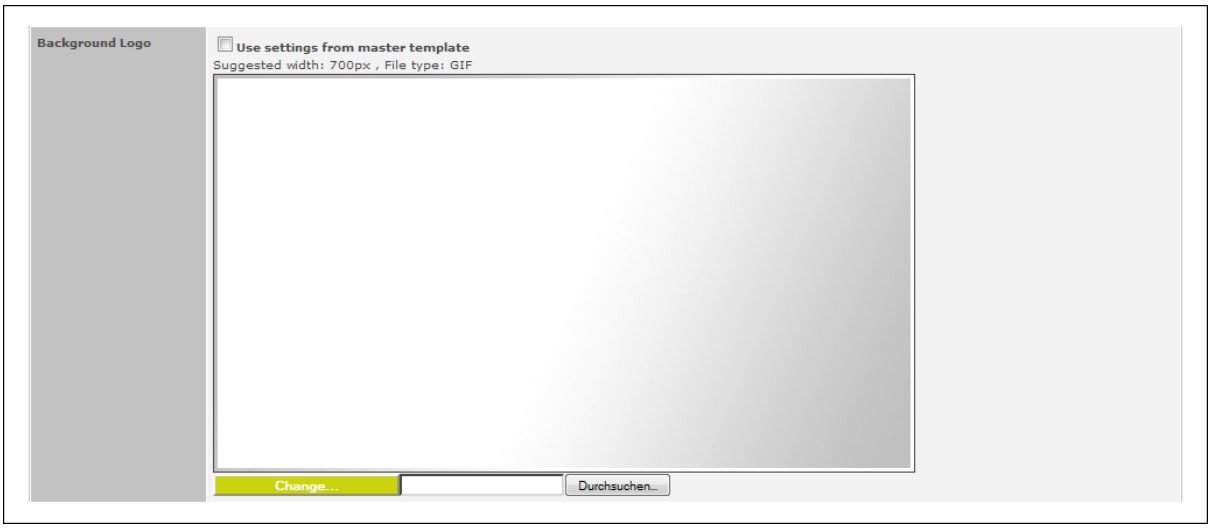


Category – Footer Logo and Footer Text at Advanced View

You can use the Footer Logo and Footer Text sections to specify an image and a text the recipients will see when retrieving EgoSecure Mail Encryption (ESWMail) messages in the area of the footer.

If you wish to transfer the footer image respectively the footer text from the master template, please enable the Use settings from master template checkbox next to Footer Logo respectively next to Footer Text.

"Advanced View" - Background Logo

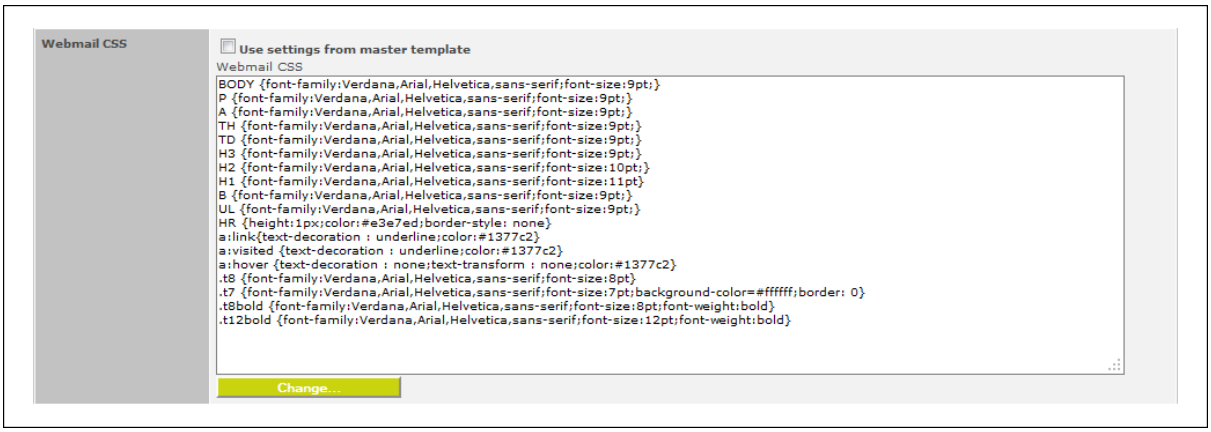


Category Background Logo at Advanced View

You can use the Background Logo section to specify a background image recipients will see when they retrieve EgoSecure Mail Encryption (ESWMail) messages.

If you wish to transfer the background image from the master template, please enable the Use settings from master template checkbox.

"Advanced View" - Webmail CSS

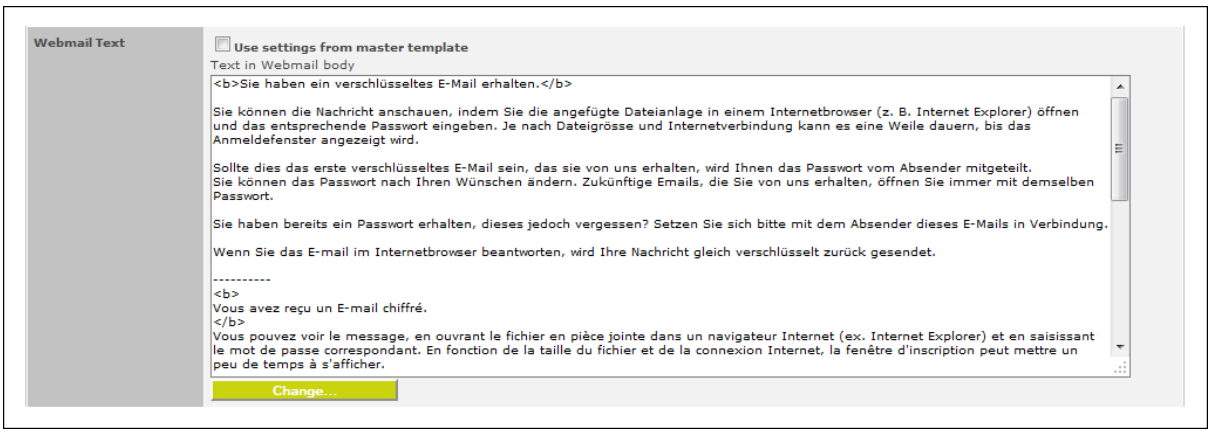


Category Webmail CSS at Advanced View

You can use the Webmail CSS section to specify the Cascading Style Sheet (CSS) definitions. These control the properties of text elements, such as the font type and the font size of the webmail message text, the representation of links, etc..

If you wish to transfer the CSS properties from the master template, please click the Use settings from master template checkbox.

"Advanced View" - Webmail Text

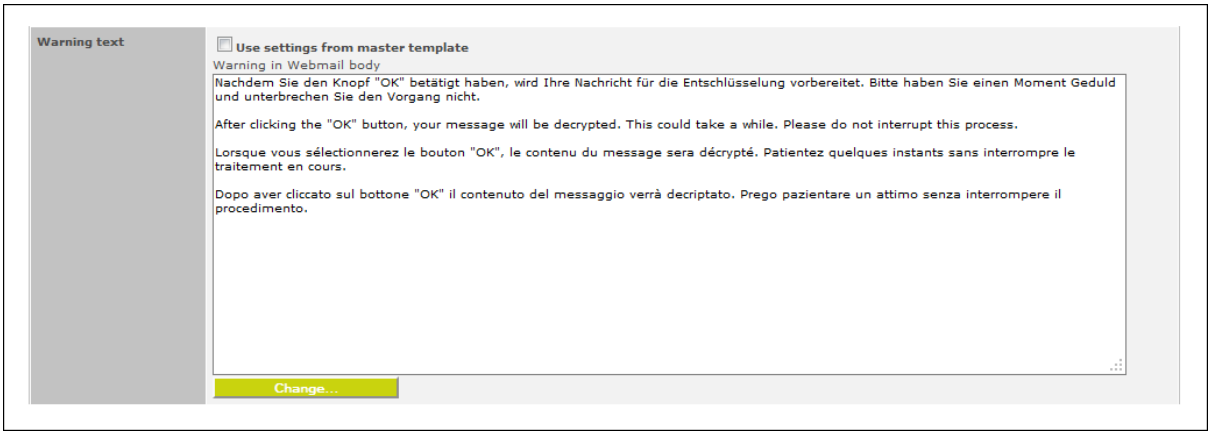


Category Webmail Text at Advanced View

You can use the Webmail Text section to specify the standard webmail text. This text will be displayed to webmail recipients when a new EgoSecure Mail Encryption (ESWMail) is delivered.

If you wish to transfer the text from the master template, please enable the Use settings from master template checkbox.

"Advanced View" - Warning Text

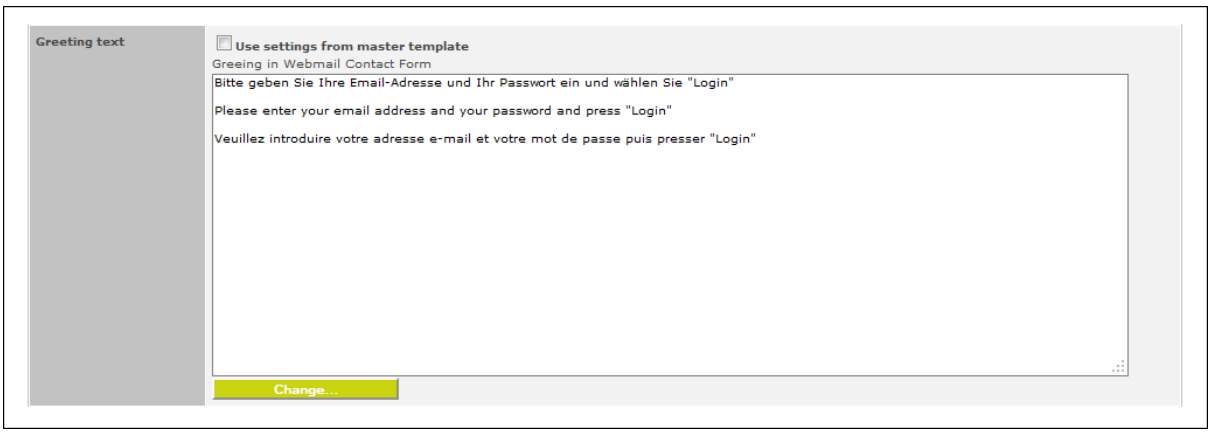


Category Warning Text at Advanced View

You can use the Warning Text section to specify the text that will be displayed to webmail recipients immediately before an EgoSecure Mail Encryption (ESWMail) message is decrypted.

If you wish to transfer the text from the master template, please enable the Use settings from master template checkbox.

Greeting Text

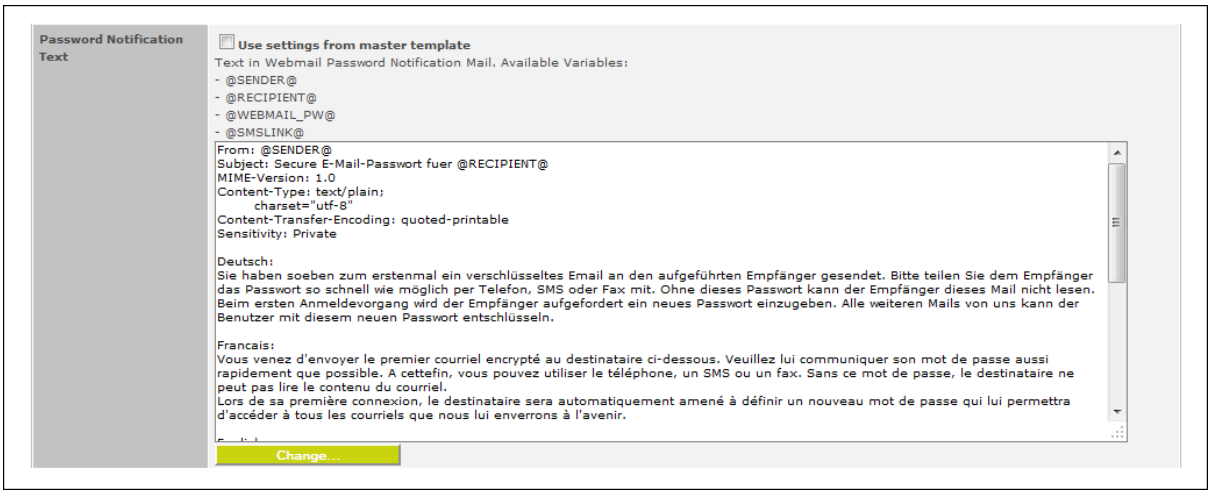


Category Greeting Text at Advanced View

You can use the Greeting Text section to specify the text that will be displayed in the EgoSecure Mail Encryption (ESWMail) interface if a registration regarding a webmail occurs.

If you wish to transfer the text from the master template, please enable the Use settings from master template checkbox.

"Advanced View" - Password Notification Text



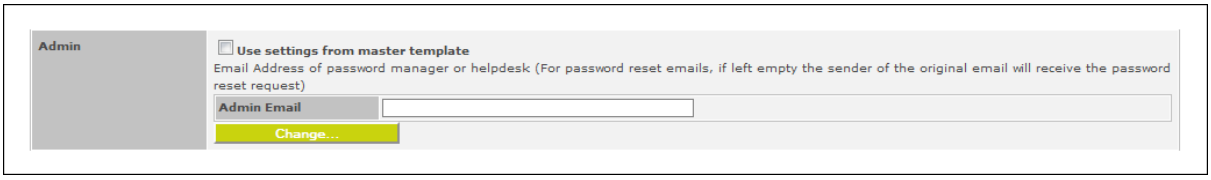
Category Password Notification Text at Advanced View

You can use the Password Notification Text section to specify the text webmail senders will receive as e-mail notification if they send an EgoSecure Mail Encryption (ESWMail) to a new webmail recipient for the first time.

The following variables can be used within this text:
- @SENDER@: e-mail address of the sender
- @RECIPIENT@: e-mail address of the recipient
- @WEBMAIL_PW@: automatically generated initial password of the recipient
- @SMSLINK@: link to the application for automatic SMS transmission (if applicable)

If you wish to transfer the text from the master template, please enable the Use settings from master template checkbox.

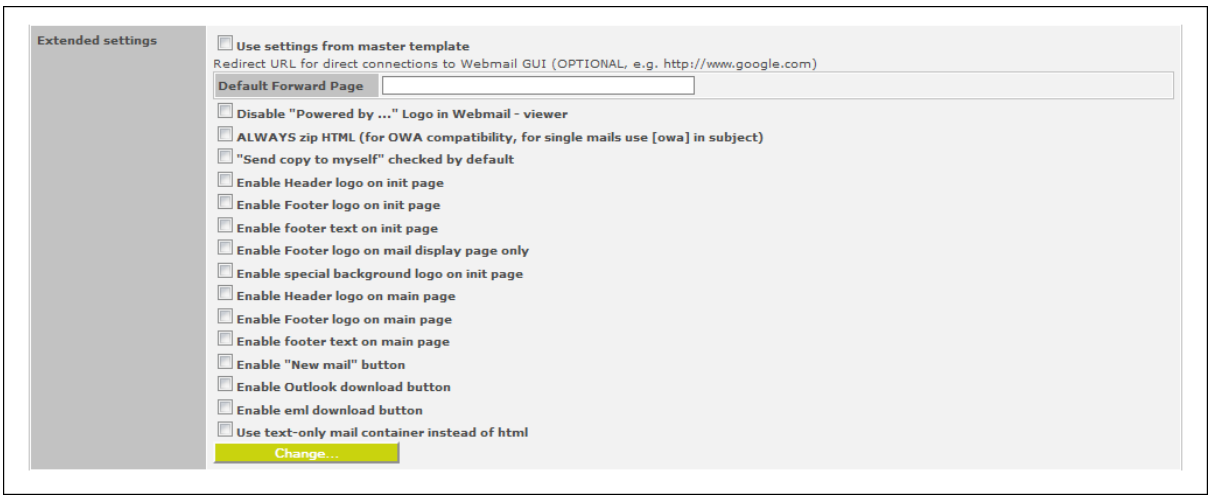
"Advanced View" - Admin



Category Admin at Advanced View

You can use the Admin section to enter the e-mail address of an administrator who will be provided with an e-mail notification if a webmail recipient wishes to have his/her password reset. For this, the security level must be set to Reset by hotline.

"Advanced View" - Extended Settings



Category Extended Settings at Advanced View

You can use the Extended Settings section to implement the following settings:

- Use settings from master template: enable this checkbox if you wish to transfer the settings from the master template.
- Default Forward Page: URL that is used if the webmail site is retrieved directly instead of from an EgoSecure Mail Encryption (ESWMail) message (optional).
- Disable "Powered by ..." Logo in Webmail-viewer: when this option is enabled, the text “Powered by Mail Encryption” will not be displayed when an EgoSecure Mail Encryption (ESWMail) is retrieved.
- ALWAYS zip HTML (for OWA compatibility, for single mails use [owa] in subject): Use these settings if the encrypted e-mail part of an EgoSecure Mail Encryption (ESWMail) is to be attached in ZIP format instead of using the HTML format. This setting is required if the recipient uses Outlook Web Access (OWA), because webmails in HTML format cannot be decrypted from OWA. In order to use this setting for individual e-mails only, the term [owa] can be used in the subject line. If an EgoSecure Mail Encryption in HTML format should arrive at an OWA recipient, the appliance will detect this. Afterwards, the sender will be requested to send the e-mail again. Simultaneously, the recipient will be set to “ZIP” and will be able to read the new e-mail.
- "Send copy to myself" checked by default: This setting causes that the option “Send copy to myself” (sending a copy of the outgoing mail to oneself) is activated by default for webmail users.
- Enable Header logo on init page: Enable this setting if the header image is already to be displayed on the webmail initial page. The webmail initial page is the page where the webmail recipient will be requested to enter his/her password.
- Enable Footer logo on init page: Enable this option if the footer image is to be displayed on the webmail initial page.
- Enable footer text on init page: Enable this option if the footer text is to be displayed on the webmail initial page.
- Enable Footer logo on mail display page only: Enable this option if the footer image is only to be displayed on the webmail display page.
- Enable special background logo on init page: Enable this setting if the background image is to be displayed on the webmail initial page.
- Enable Header logo on main page: Use this setting if the header image is to be displayed on the webmail main page.
- Enable Footer logo on main page: This setting can be used to display the footer image on the

webmailmain page.

- Enable footer text on main page: Enable this setting if the footer text is to be displayed on the webmail main page.
- Enable "New mail" button: Enable this setting if the “New mail” button is to be displayed in the webmail frontend.
- Enable Outlook download button: Enable this setting if the “Outlook” button is to be displayed in the webmail frontend.
- Enable eml download button: Enable this setting if the “Save message” button is to be displayed in the webmail frontend.
- Use text-only mail container instead of html: The short information for the webmail recipient is only executed as a text message and not as a HTML message.

"Advanced View" - Language Settings

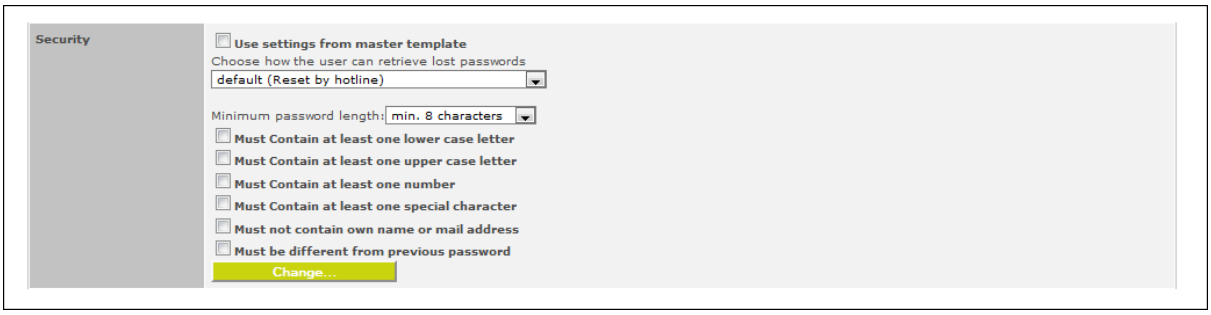
Category Language Settings at Advanced View

You can use the Language Settings section to define the available languages and the default language for EgoSecure Mail Encryption (ESWMail).

Define the default language by using the drop-down list next to Default language and define the available languages using the checkbox below Available Languages.

If you wish to transfer the settings from the master template, please click the Use settings from master template checkbox.

"Advanced View" - Security



Category Security at Advanced View

Use the Security section in order to define the security settings for EgoSecure Mail Encryption (ESWMail).

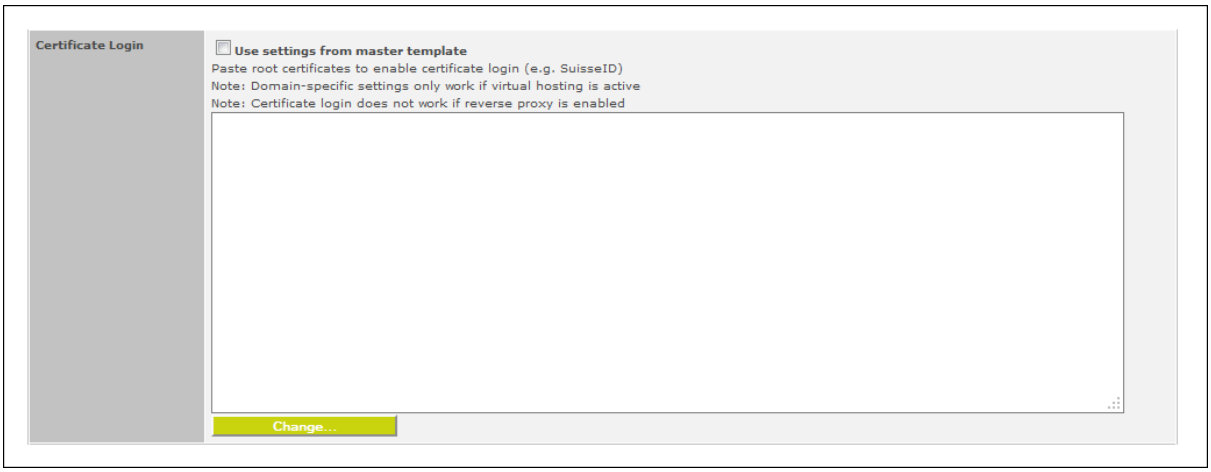
If a webmail user forgets his/her password, he/she can click the link called “Forgot password” when retrieving a webmail. If you select the Reset by e-mail setting below Choose how the user can retrieve lost passwords, the recipient subsequently will be provided with a new password via e-mail automatically. If you select Reset by hotline, the responsible webmail administrator will be provided with a corresponding e-mail notification (this corresponds to default setting default). If you select Reset by hotline, no reminder question/answer, the webmail recipient must not enter any security question and answer when logging into his/her webmail account for the first time.

You can define the password criteria with the following options:

- Minimum password length: minimum password length (default: 8 characters)
- Must Contain at least one lower case letter: The password must contain at least one lower case letter.
- Must Contain at least one upper case letter: The password must contain at least one upper case letter.
- Must Contain at least one number: The password must contain at least one numerical character.
- Must Contain at least one special character: The password must contain at least one special character.
- Must not contain own name or mail address: The password must not contain the own name or the own e-mail address.
- Must be different from previous password: The password must not match the one used before.

If you wish to transfer the settings from the master template, please enable the Use settings from master template checkbox.

"Advanced View" - Certificate Login



Category Certificate Login at Advanced View

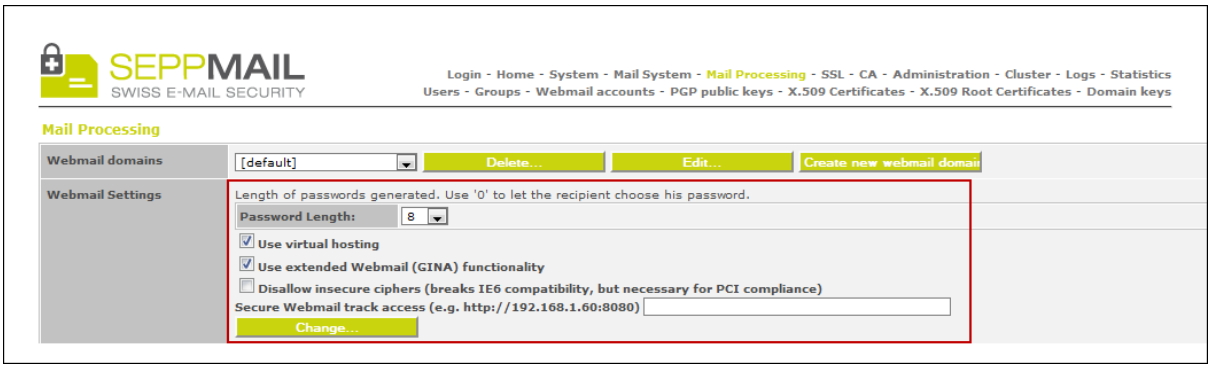
You can use the Certificate Login section to store the root CA certificates (e.g. SuisseID) that can be used in order to identify a webmail user. Each webmail recipient must have installed a certificate within his/her browser that has been issued by one of the root CAs mentioned within the framework of this document.

4.6.4 Managing rules for processing webmails

In order to manage rules for processing webmails, please click the "Mail Processing" menu item within the web administration portal.

You can set the following options within the Webmail Settings category:

- Password length: Length of the generated passwords (0 = passwords are not generated, but selected by the e-mail recipient)
- Use virtual hosting: If you enable this option, an independent URL will be used for each webmail domain. When this option is disabled, the name used by the e-mail system will be displayed as a part of the URL. Example: when the Use virtual hosting option is enabled, https://webmaildomain.ch instead of https://appliancehostname.ch/webmaildomain.ch will be used as webmail URL.
- Use extended Webmail (GINA) funtionality: By activating this option, webmails will be sent by the new GINA webmail interface.
- Disallow insecure ciphers: Ensures that only secure, PCI-compliant SSL encryption is used (Internet Explorer 6 is incompatible with this setting).
- Secure Webmail track access: This function allows for differentiated feedback from EgoSecure Mail Encryption read confirmations. If a webmail containing the request of a read confirmation is sent to several recipients, the sender will be provided with the first read confirmation only. Additionally, the read confirmation e-mail will contain a link that can be used to see the complete overview of the read confirmations. This link will start with the address that is entered in this field. The rear part of the link will be generated dynamically in each case.



Rules for processing webmails

4.6.5 Managing the webmail SMS password transmission

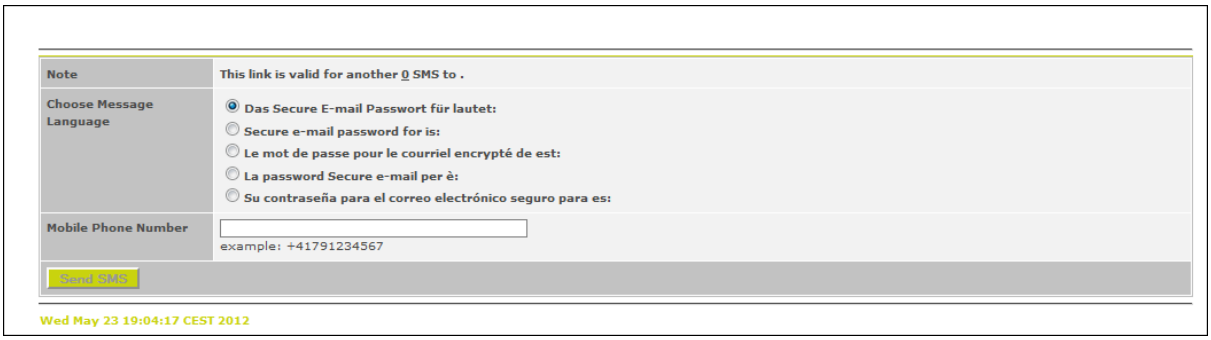
In order to manage rules for processing webmails, please click the “Mail Processing” menu item within the web administration portal.

You can manage the following settings in the Webmail password SMS settings category.

Secure Webmail SMS send access: Address of the application for SMS transmission

- Disable: Disable SMS transmission
- Use cell phone / GSM modem attached to appliance: Use a mobile phone or GSM modem connected to the appliance
- Use Mail to SMS service (configuration below): Use e-mail to SMS service with the following settings
- Use xml service: Use the XML service (for more information contact the technical support)
- Use HTTP GET Service (configuration below): Use the SMS Service over HTTP GET (for more information contact the technical support)

Access to Secure Webmail send password form:
Disabled: The access to the webform for sending an SMS is disabled.
Available via public Webmail GUI: The SMS transmission is done via webbrowser on a specific webform (e.g. https://secmail.customer.ch/pesend.app).
Available via the following URL (e.g. https://192.168.1.60:8443/pwsend.app): The SMS transmission is done via webbrowser on a specific webform.

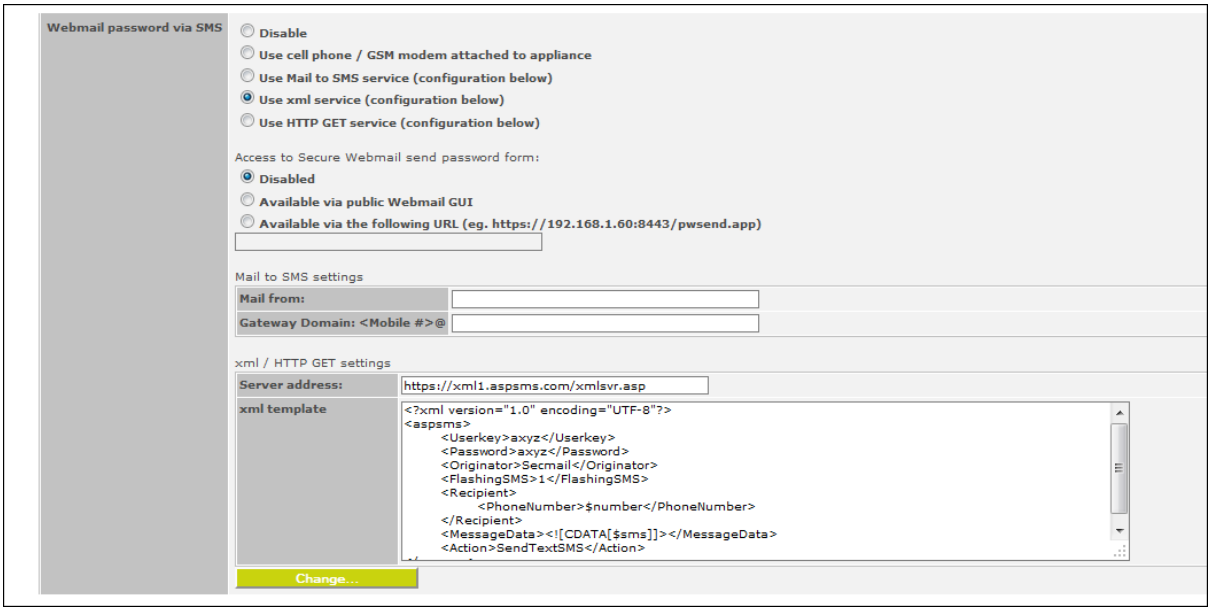


Webmail SMS password transmission

Mail to sms settings:
Mail from: Sender e-mail address for SMS transmission
Gateway Domain <Mobile #>@: Gateway domain for SMS transmission

xml / HTTP GET settings:

Server address: Address of the corresponding XML service
xml template: XML definitions of the corresponding XML service



Managing the webmail SMS password transmission

General infomation for SMS transmission of webmail passwords

If a EgoSecure Mail Encryption is sent to an external recipent, the sender will recieve an e-mail information with a one-time password, which he can provide to the webmail recipent via fax or SMS. This procedure can be simplified by adding the mobile number, that should recieve the one-time password, to the subject of the EgoSecure Mail Encryption. The mobile number will be removed by Mail Encryption before the e-mail is sent through the internet.

You have the following options to provide the one-time password via SMS:

- As part of the e-mail subject

add (mobile: +41123456789) or (sms: +41123456789) to the subject

Example

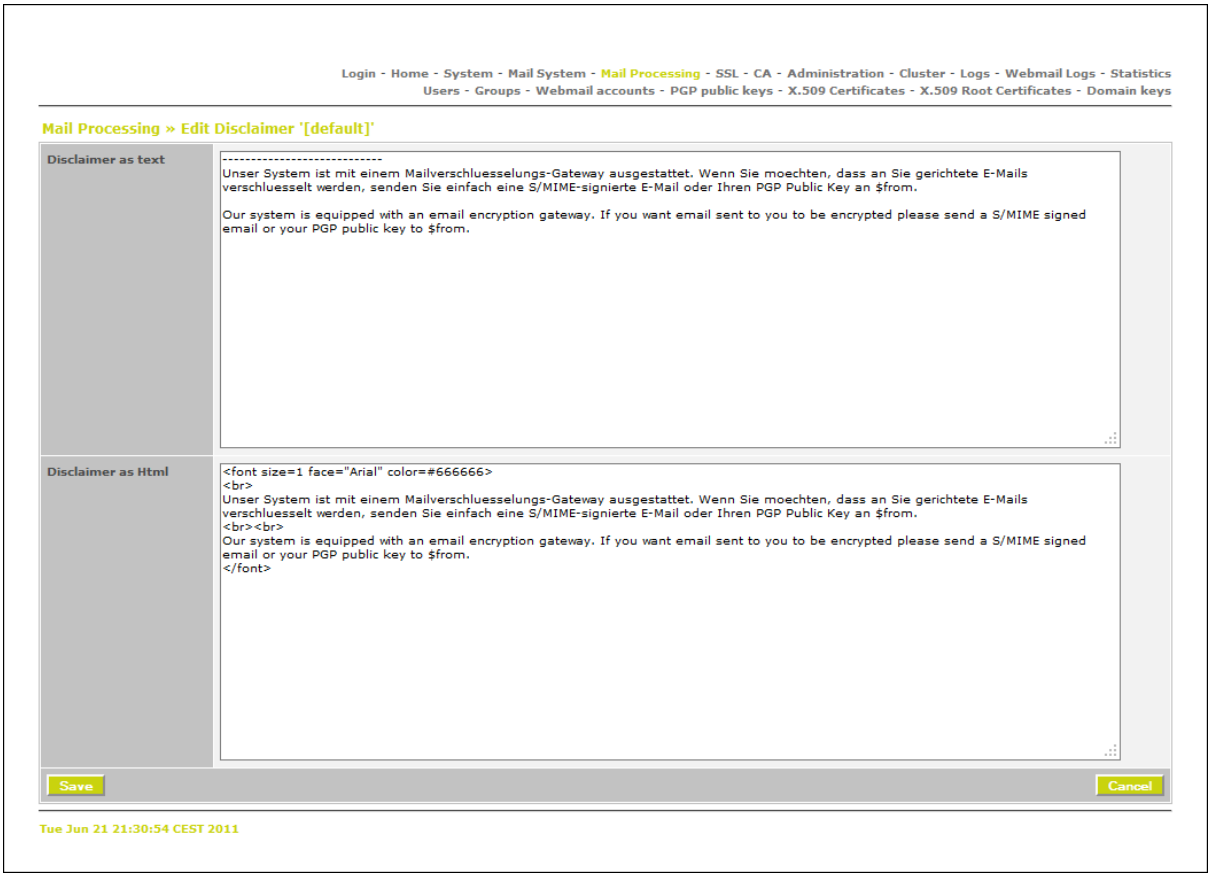
Subject: Secure e-mail encryption without additional effort for the recipent (mobile: +41123456789)
Subject: Secure e-mail encryption without additional effort for the recipent (sms: +41123456789)

- Use a mobile number that has been added before to the webmail user account
- send the one-time password configurationsurface in the menu "WEbmail accounts -> Webmail user account"

4.6.6 Managing disclaimer

In order to manage company disclaimers, you must click the “Mail Processing” menu item in the web administration portal.

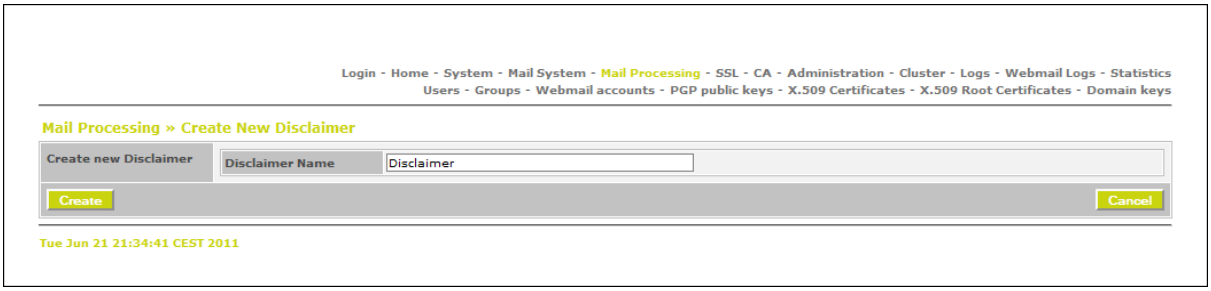
Managing the default disclaimer
The default disclaimer is called [default]. In order to edit the aforementioned, please click the “Edit...” button in the Edit Disclaimer category.



Editing the default disclaimer text

Creating a new disclaimer
If required, you can configure further disclaimers along with the default disclaimer called [default]. A disclaimer is used by a corresponding ruleset instruction in each case.

In order to create a new disclaimer, please click the “Create new disclaimer...” button in the Edit Disclaimer category.



Creating a new disclaimer

Enter a name for the new disclaimer. Afterwards, select your new disclaimer from the drop-down list in the Edit Disclaimer category and click the “Edit...” button. You can now edit the text of the new disclaimer.

Deleting a disclaimer

In order to delete a disclaimer, please select the disclaimer to be deleted in the Edit Disclaimer category and click the “Delete...” button.

4.6.7 Managing e-mail templates

In order to manage e-mail templates, you must click the “Mail Processing” menu item in the web administration portal.

Templates are pre-defined messages that are sent automatically in defined cases.

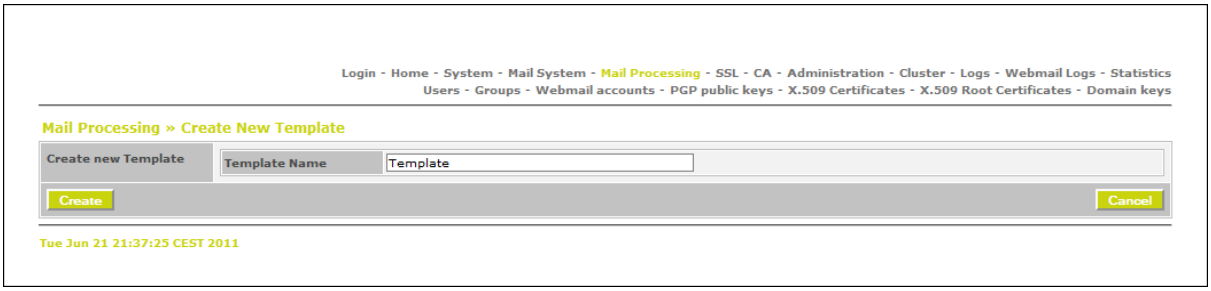
Managing template 'bounce_noenc"
The only template that is available after the Mail Encryption appliance was commissioned is called [bounce_noenc]. This template is used when a sender attempts to send an encrypted e-mail, but if the encryption is not successful.

In order to edit the "bounce_noenc" template, please click the “Edit...” button in the Edit Mail Templates category.

Editing template 'bounce_noenc"

Creating a new template
If required, you can configure further templates. A template is used by a corresponding ruleset instruction in each case.

In order to create a new template, please click the "Create new template..." button in the Edit Mail Templates category.



Creating a new template

Enter a name for the new template. Afterwards, select your new template from the drop-down list in the `Edit Mail Templates` category and click the "`Edit...`" button. You can now edit the text of the new template.

Deleting a template

In order to delete a template, please select the template to be deleted in the `Edit Mail Templates` category and click the "`Delete...`" button.

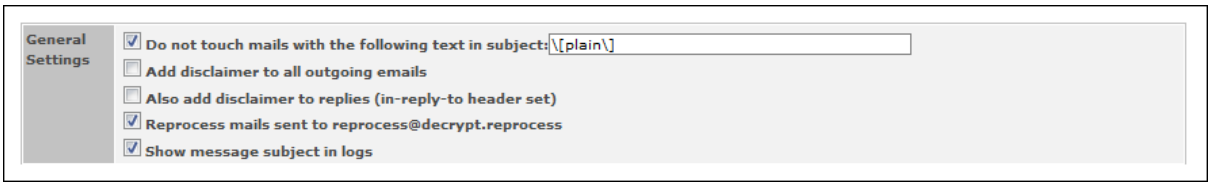
4.6.8 Managing the ruleset

In order to manage the ruleset of the secure e-mail gateway appliance Mail Encryption, please click the "Mail Processing" menu item in the configuration interface.

The ruleset can be found in the Ruleset Generator category and is divided into the following eight sections.

These sections are explained in detail in the following.

General Settings



"General Settings" section of the ruleset

The following settings can be edited in the General Settings section:

- Do not touch mails with the following text in subject: Using this option you can define a term preventing any encryption of e-mails when it is entered into the subject line.
- Add disclaimer to all outgoing mails: Use this setting if you want to attach the default disclaimer to all outgoing e-mail messages.
- Also add disclaimer to replies (in-reply-to header set): Use this setting if you also want to attach the default disclaimer to e-mail messages the internal user has replied to.
- Reprocess mails sent to reprocess@decrypt.reprocess: This setting effects encrypted e-mails that were sent to internal e-mail recipients and could not be decrypted by the Mail Encryption appliance. This may by the case if the appliance does not dispose of the required key material at the time an e-mail is received, for example. Using this option, you allow corresponding users to send e-mails that could not be decrypted to the address reprocess@decrypt.reprocess in order to again resolve the decryption procedure by means of the Mail Encryption appliance.
- Show message subject in logs: Use this setting if the subject line of an e-mail is to be displayed in the log files.

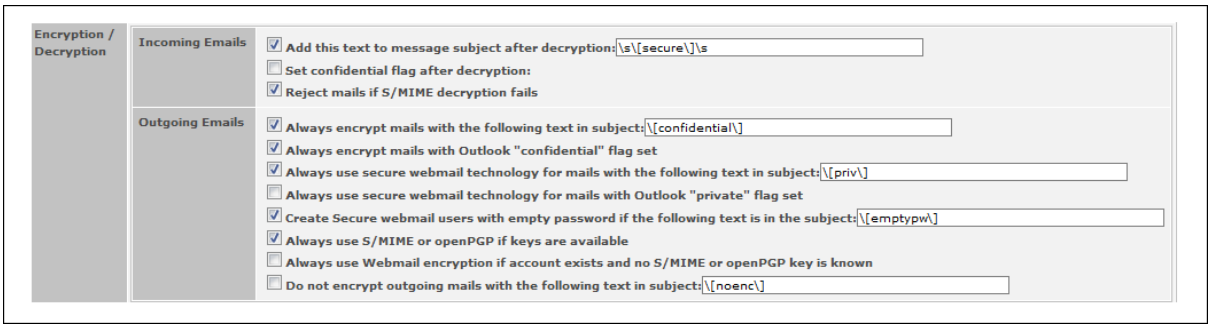
User Creation

"User Creation" section of the ruleset

The following settings can be edited in the User Creation section:

- Manual user creation: Only process outgoing mails from users with an account: Enable this option if you only want to allow the use of the Mail Encryption appliance to those persons already disposing of a user account on the appliance.
- automatically create accounts for new users if user tries to sign / encrypt: This option allows for the automatic creation of new users. If this setting is enabled, internal e-mail senders will be detected automatically as users on the appliance. This is implemented when the internal e-mail sender attempts to sign or encrypt an e-mail.
- automatically create accounts for all users: This option allows for the automatic creation of new users. If this setting is enabled, internal e-mail senders will be detected automatically as users on the appliance.

Encryption / Decryption



Encryption / Decryption" section of the ruleset

The following settings can be edited in the Encryption – Incoming E-mails section:

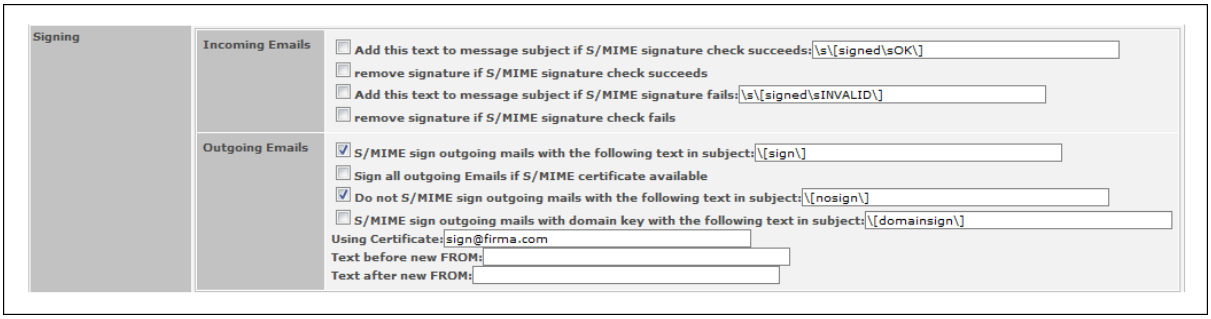
- Add this text to message subject after decryption: You can specify a term here that is to be added to the subject line after the decryption procedure was implemented.
- Set confidential flag after decryption: If an incoming e-mail is decrypted by Mail Encryption, the Outlook option “Confidential” will be enabled automatically for the e-mail forwarded internally.
- Reject mails if S/MIME decryption fails: Enable this option if incoming encrypted e-mails are to be rejected if the decryption procedure is not successful.

The following settings can be edited in the Encryption – Outgoing E-mails section:

- Always encrypt mails with the following text in subject: Using this option you can define a term forcing the encryption of e-mails when it is entered into the subject line.
- Always encrypt mails with Outlook "confidential" flag set: Use this option if e-mails with the option “Confidential” are to be encrypted at all times in Outlook.

- Always use secure webmail technology for mails with the following text in subject: Define a term here that triggers the dispatch of an EgoSecure Mail Encryption (ESWMail)

Signing



"Signing" section of the ruleset

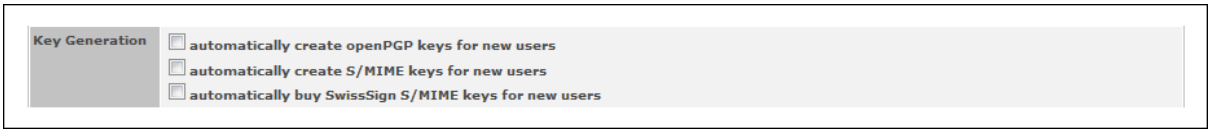
The following settings can be edited in the Signing – Incoming E-mails section:

- Add this text to message subject if S/MIME signature check succeeds: Use this option if you want to attach a text to the subject line for messages signed by means of S/MIME.
- remove signature if S/MIME signature check succeeds:Use this option if you want to remove the S/MIME signature of an e-mail. This is only implemented if the S/MIME signature could be checked successfully by Mail Encryption against a root CA within the proprietary root CA memory. (see menu »X.509 Root Certificates« 189)
- Add this text to message subject if S/MIME signature check FAILS: Use this option in order to add a text to the subject line of e-mails the signature by means of S/MIME has failed for.
- remove signature if S/MIME signature check fails: Use this option if you want to remove the S/MIME signature of an e-mail. This is only implemented if the S/MIME signature could not be checked successfully by Mail Encryption against a root CA within the proprietary root CA memory. (see menu »X.509 Root Certificates« 189)

The following settings can be edited in the Signing – Outgoing E-mails section:

- S/MIME sign outgoing mails with the following text in subject: Enable this option if outgoing e-mails having the defined term in their subject line are to be signed by means of S/MIME.
- Sign all outgoing Emails if S/MIME certificate available: If you use this option, all outgoing e-mails will be signed, provided that the corresponding S/MIME certificates are present.
- Do not S/MIME sign outgoing mails with the following text in subject: This setting causes that outgoing e-mails with the defined term in their subject line will not be signed.
- S/MIME sign outgoing mails with domain key with the following text in subject: You can use this option to sign e-mails with the defined term in their subject line with the domain key of your organisation. Please specify the domain certificate to be used after the text Using Certificate:. Additionally, you can specify which text is to be displayed in front of the domain sender and which text is to be displayed after the aforementioned.

Key Generation

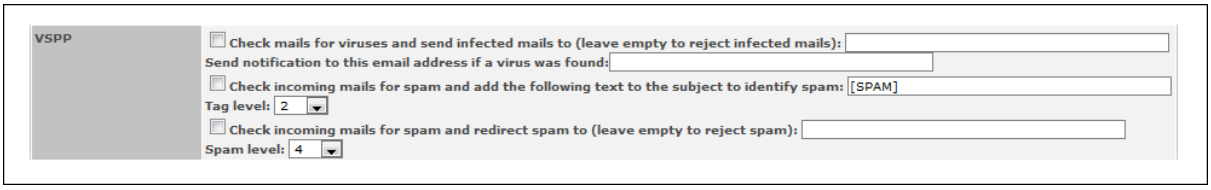


"Key Generation" section of the ruleset

The following settings can be edited in the Key Generation section:

- automatically create OpenPGP keys for new users: This option causes that OpenPGP keys are generated automatically for new users.
- automatically create S/MIME keys for new users: This setting causes that S/MIME certificates are created automatically for new users.
- automatically buy SwissSign S/MIME keys for new users: Use this option if certificates created by SwissSign are to be retrieved automatically for new users.

VSPP



"VSPP" section of the ruleset

The following settings can be edited in the VSPP section:

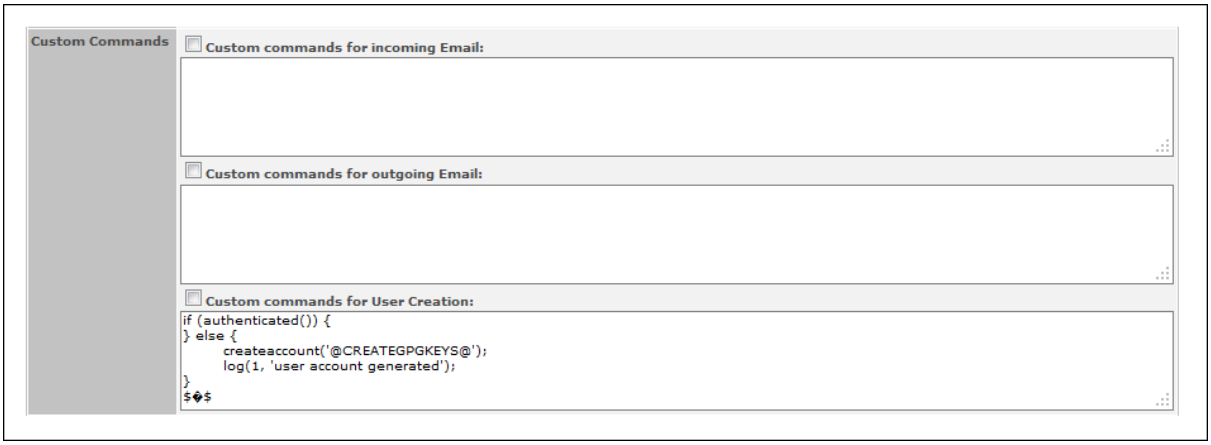
- Check incoming mails for viruses and send infected mails to: You can use this option to check incoming e-mails for viruses and, if viruses are found, to forward these to the defined e-mail address instead of the e-mail recipient. If no e-mail address was defined, the corresponding e-mails will be deleted.
- Check incoming mails for spam and add the following text to the subject to identify spam: If you enable this option, it is checked whether the incoming e-mails are spam e-mails. If this is the case, the defined term will be added to the subject line of the corresponding e-mails.
  Tag level: You can specify the level of spam classification here. The lower this value is set, the more likely it is that e-mails are identified as spam. At the same time, low values will increase the risk that legitimate e-mails will be incorrectly identified as spam e-mails.
- Check incoming mails for spam and redirect spam to: If you are using this setting, detected spam messages will be forwarded to the defined e-mail address instead of the recipient of the e-mail. If no e-mail address was defined, the corresponding e-mails will be deleted.
  Tag level: You can define the threshold value of spam detection here.

Archiving

"Archiving" section of the ruleset

You can use the Archiving section to enter an e-mail address a copy of all e-mails is to be sent to.

Custom Commands



"Custom Commands" section of the ruleset

The following settings can be edited in the Custom Commands section:

- Custom commands for incoming E-mail: Use this section in order to enable rules you defined with regard to incoming messages.
- Custom commands for outgoing E-mail: You can use this section to enable rules you defined with regard to outgoing messages.
- Custom commands for User Creation: Use this section in order to enable rules you defined with regard to the creation of user accounts.

These custom commands will be inserted at the beginning of the corresponding section in each case and, thus, will be processed first.

Advanced Options

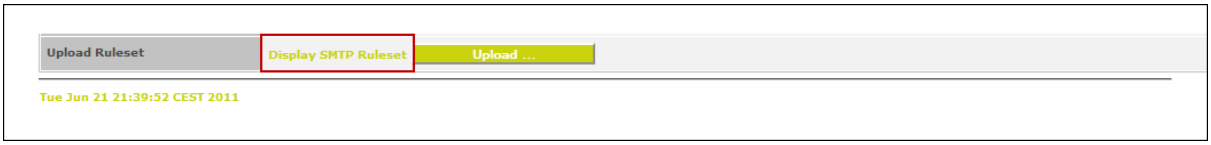
"Advanced Options" section of the ruleset

The following settings can be edited in the Advanced Options section:

- Re-inject mails to sending mailserver (use with care!): You can use this setting to return all e-mails to the server they came from after they are processed (e.g. central e-mail hub).
- Run in queueless mode (use with care!): This setting causes that e-mails to individual recipients are not stored “intermediately” while they are processed. Instead, the incoming connection will be acknowledged only when the outgoing connection has been acknowledged. If, during dispatch to several recipients, the acceptance for some recipients is not acknowledged, these e-mails will be on the appliance for a short period of time until the receiving e-mail servers acknowledge them.

4.6.9 Display the ruleset

In order to display the current ruleset, you must click the “Mail Processing” menu item in the web administration portal. Afterwards, click the link Display SMTP Ruleset in the lowermost Upload Ruleset category.



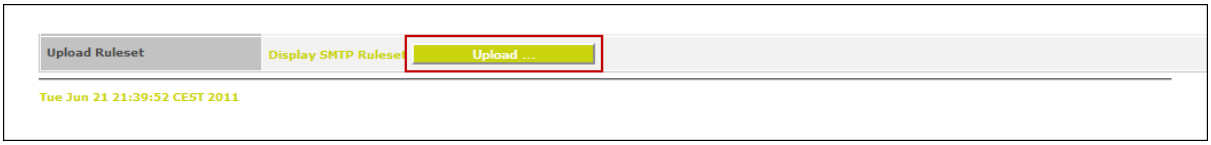
Link for displaying the current ruleset

As a result you will see the current ruleset of your secure e-mail gateway appliance Mail Encryption in text form.

Display of the current ruleset (excerpt)

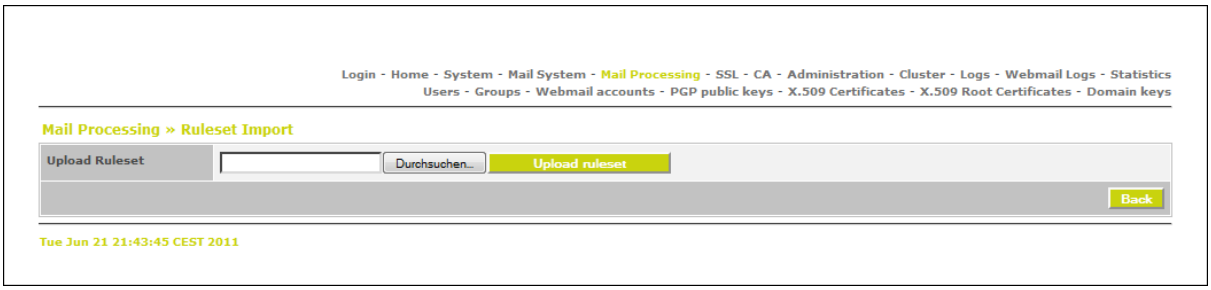
4.6.10 Loading the ruleset

In order to load a previously stored ruleset, you must click the `Mail Processing` menu item in the web administration portal. Afterwards, click the “Upload...” button to load a certain ruleset.



Loading a previously stored ruleset

A dialogue for selecting the ruleset file will be displayed.



Selection of a ruleset file

4.7 Menu item "SSL“

Select the “SSL” menu item in order to manage the SSL device certificate (Secure Sockets Layer) of the Mail Encryption appliance.

The following processes will be described in the following sections:

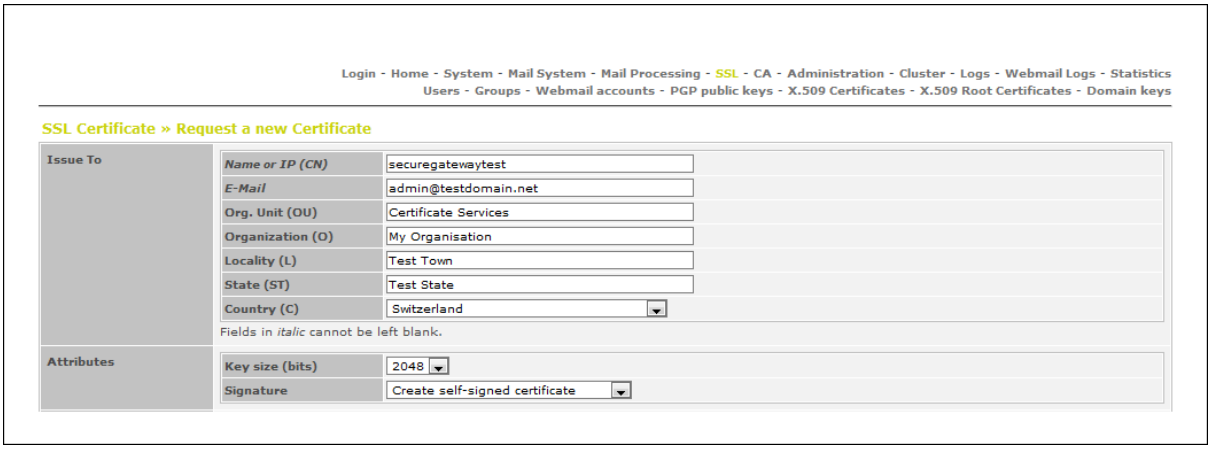
4.7.1 Creating an SSL certificate self-dependently

You do not need any SSL certificate for a test installation. The certificate can be generated and signed automatically on the Mail Encryption appliance. For this, click the “SSL” menu item and then click the “Request a new Certificate...” button.

Please complete the fields shown in the following figure as follows (the fields shown in italics are mandatory fields):

- Name or IP (CN): IP address or host name of the appliance. Must correspond to the name within the URL as the appliance is addressed within the framework of the test scenario (e.g. securegatewaytest, if the URL https://securegatewaytest is used to access the appliance).
- E-Mail: a valid e-mail address within the company that can be used to contact a responsible person
- Org. Unit (OU): the name of the responsible organisational unit (optional)
- Organization (O): the name of the organisation (optional)
- Locality (L): location where the organisation is headquartered (optional)
- State (ST): canton/state where the organisation is headquartered (optional)
- Country (C): country where the organisation is headquartered (optional)
- Key size (bits): key length in bits (1024 or 2048)
- Signature: select “Create self-signed certificate” here in order to create a self-generated and self-signed SSL certificate

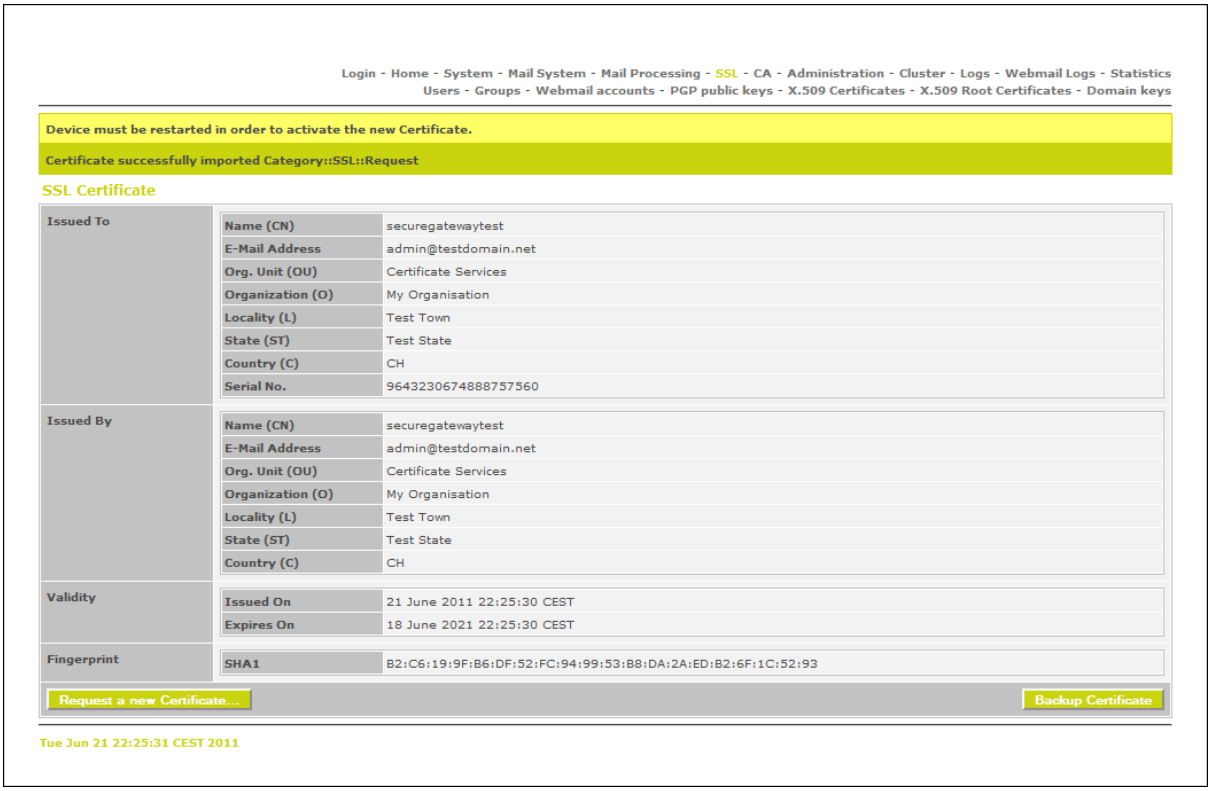
In order to trigger the process of creating an SSL certificate, please click the “Create Request" button.



Requesting respectively creating an SSL certificate

After having entered the information, you will be provided with a confirmation containing the certificate details. Along with the values specified by you, this confirmation contains the following information:

- the serial number of the certificate (serial no.)
- the period of validity (validity)
- the fingerprint (SHA1 fingerprint)



Confirmation of the SSL certificate with details

Please observe that the Mail Encryption appliance must be restarted in order to activate the new SSL certificate. You can trigger the restart procedure by clicking the "Reboot" button in the "Administration" menu item and confirming the security code subsequently displayed.

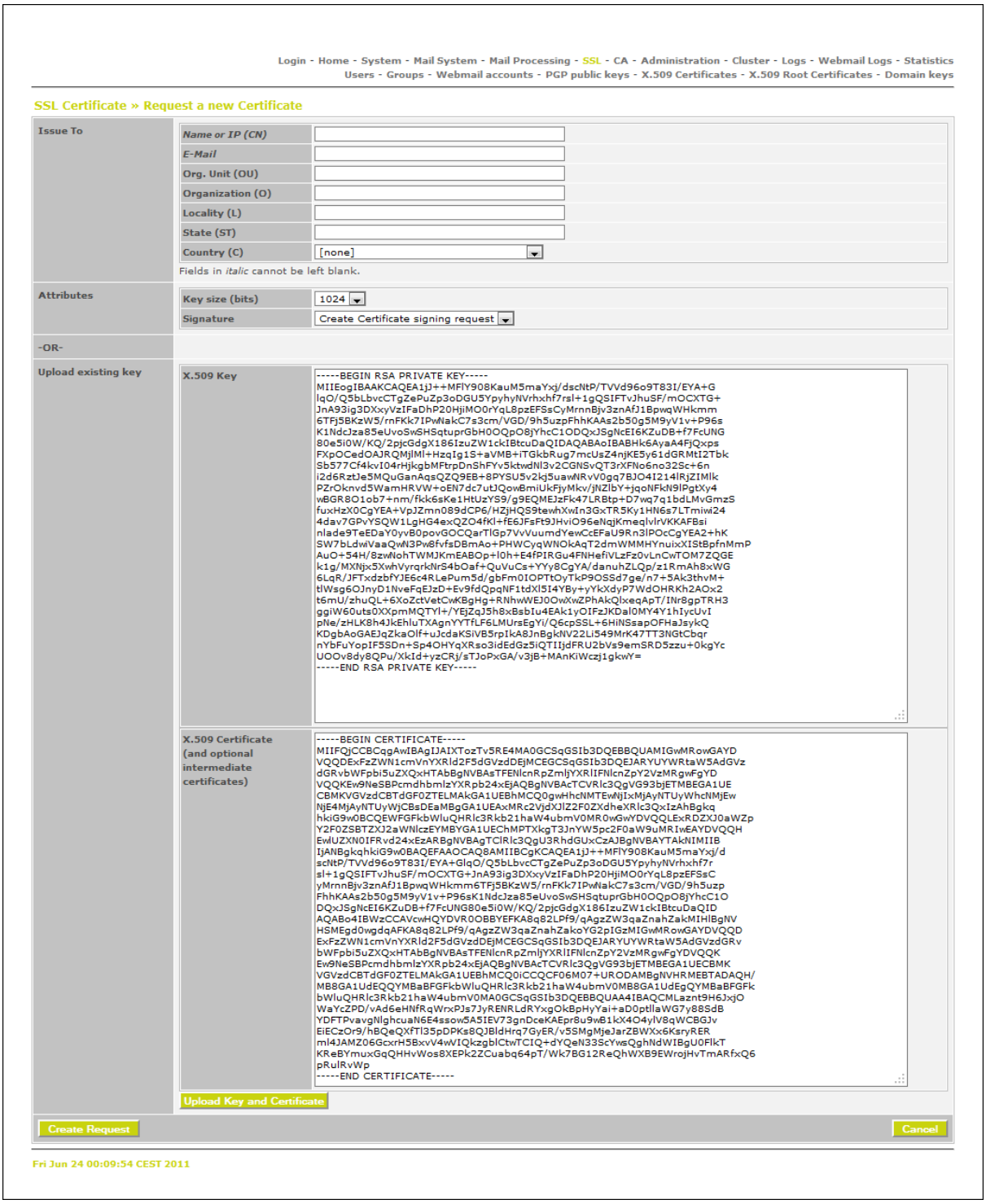
4.7.2 Using an existing SSL certificate

In order to use a proprietary, already existing SSL certificate for your appliance, you must click the "SSL" menu item in the web administration portal. Afterwards, please click the "Request a new Certificate..." button.

Use one of the following fields in the Upload existing key category:

- X.509 Key: Insert your SSL certificate in text form.
- X.509 Certificate (and optional intermediate certificates): Use this field if you want to use a certificate including the certificates of superior certification authorities.

Complete the procedure in both cases by clicking the "Create Request" button.



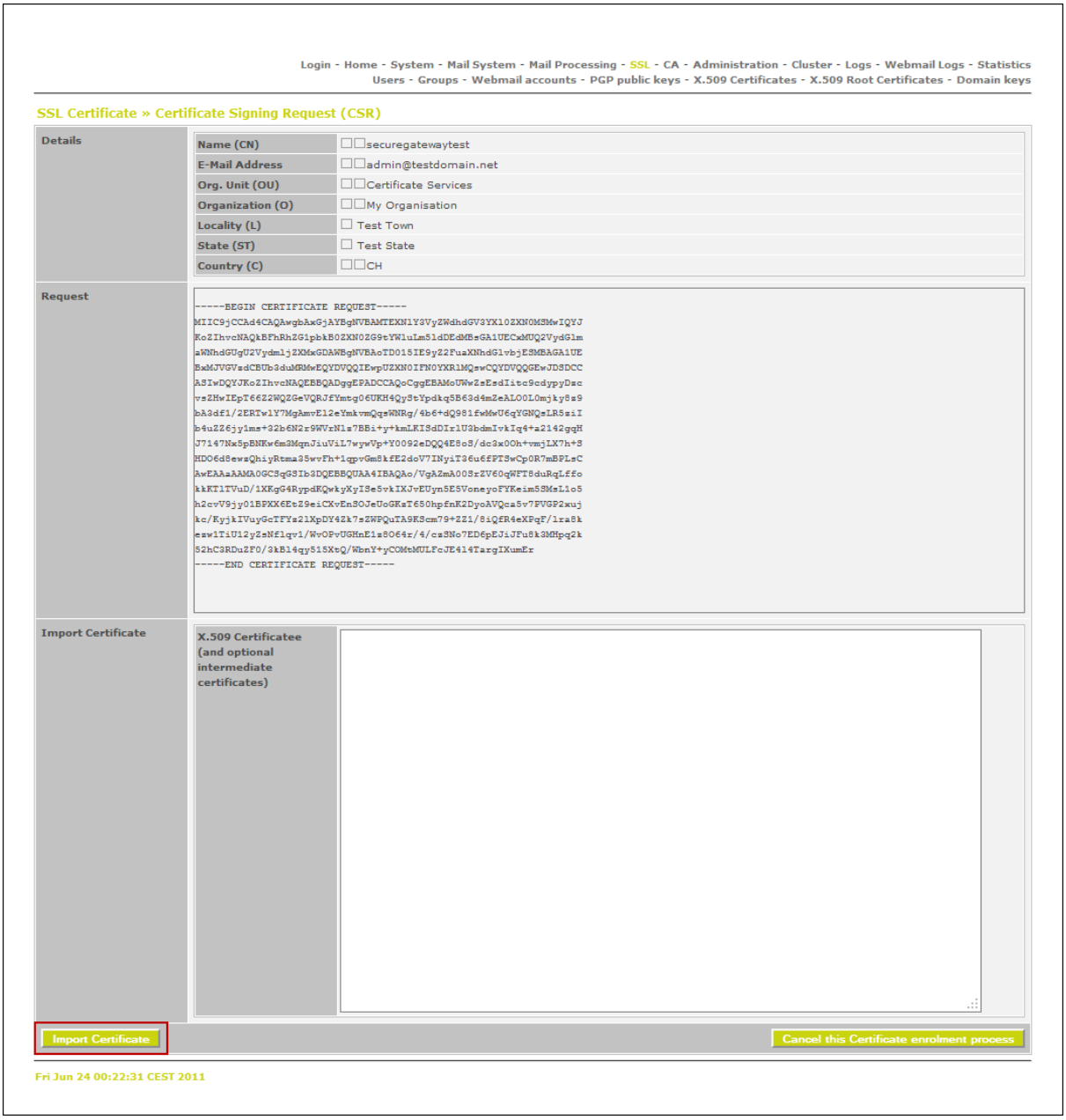
Fields "X.509 Key" and "X.509 Certificate (and optional intermediate certificates)"

4.7.3 Requesting an SSL certificate from a public certification authority

In order to request an SSL certificate for your Mail Encryption appliance from a certification authority, you must click the “SSL” menu item in the web administration portal.

Please proceed as follows:

1. Proceed in analogy to the steps described in the section Creating an SSL certificate self-dependently 104, but select “Create Certificate signing request” instead of “Create self-signed certificate” for the “Signature” option in order to create a certification request.
2. Please click the “Download and Import signed Certificate...” button.
3. Copy the text in the Request category and transfer this text to the certification authority you want to request the SSL certificate from.
4. As soon as you received your SSL certificate from the certification authority, please again click the “Download and Import signed Certificate...” button.
5. Insert the certificate into the Import Certificate category and then click the “Import Certificate” button.

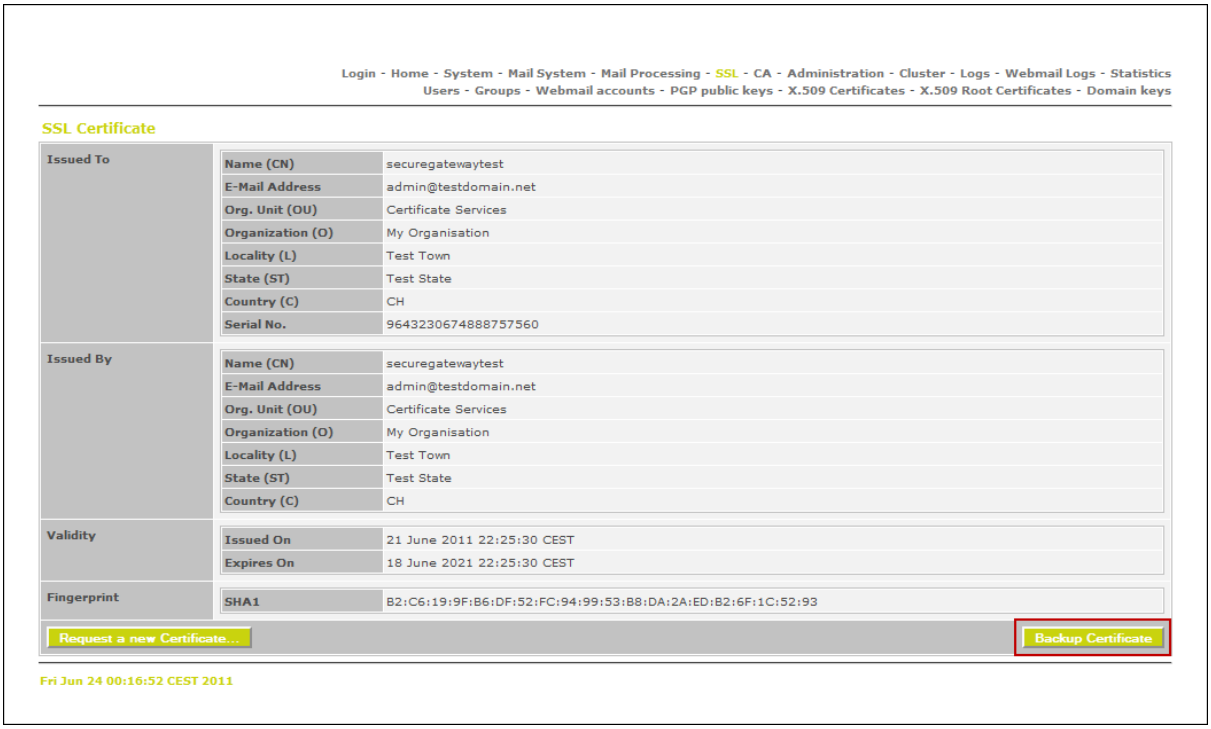


Importing an SSL certificate

4.7.4 Saving an SSL certificate

In order to save an SSL certificate for your Mail Encryption appliance, you must click the “SSL” menu item in the web administration portal.

Save the certificate by clicking the “Backup Certificate” button.



Saving an SSL certificate

4.8 Menu Item "CA"

Select the “CA” menu item to manage the proprietary Certificate Authority (CA) of the Mail Encryption appliance.

The following processes will be described in the following sections:

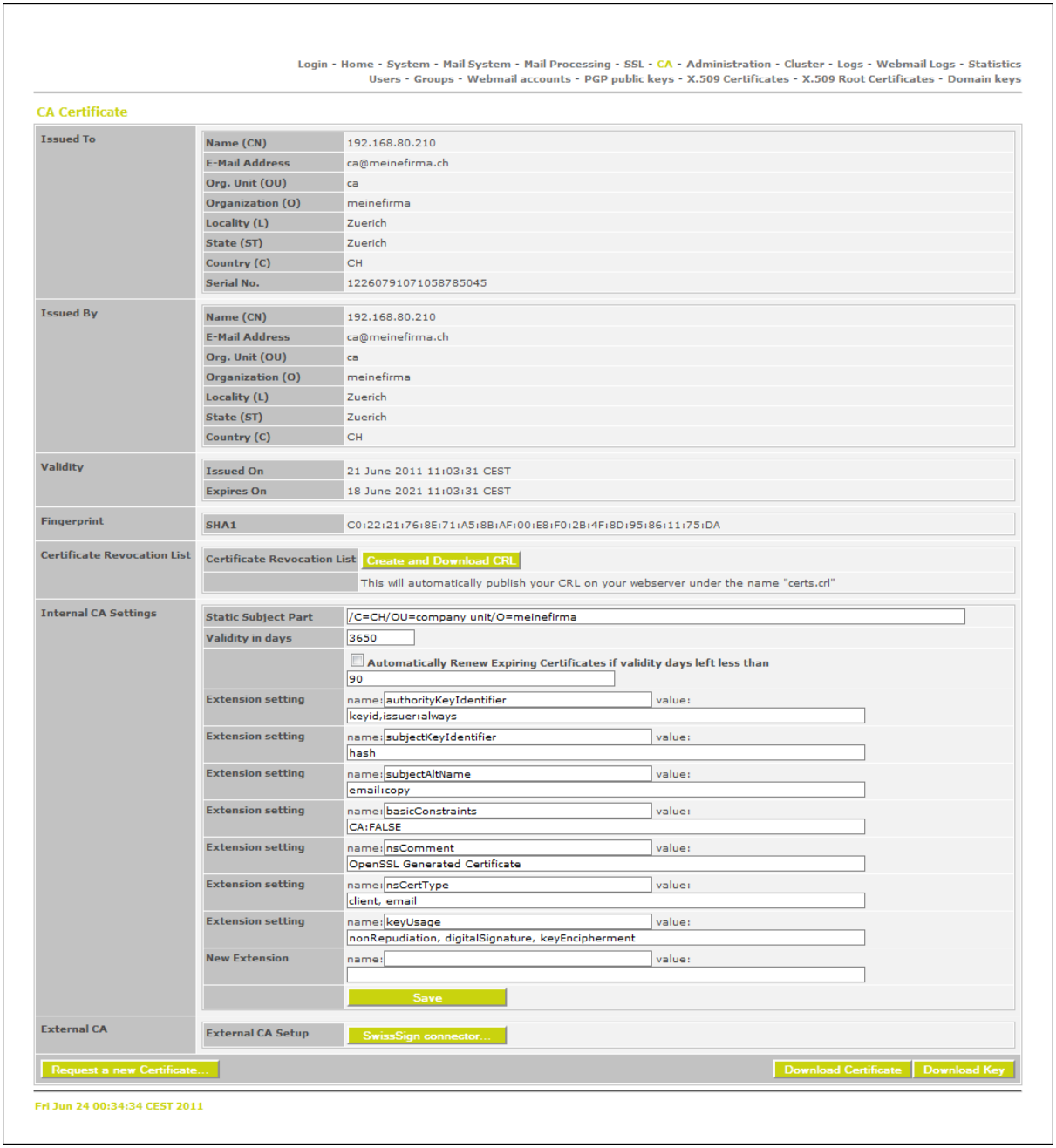
4.8.1 Managing internal CA settings

In order to manage internal CA settings, you must click the “CA” menu item in the web administration portal.

Downloading the Certificate Revocation List (CRL)
Click the “Create and Download CRL” button in order to download and view the CRL.

Adapting internal CA settings
Adapt the settings of the internal CA to the assignments of your organisation as follows:

- Static Subject Part: C=country the organisation is headquartered / OU=name of the responsible organisational unit / O=name of the organisation
- Validity in days: validity of the CA certificate in days
- Extension settings: further parameters (name=name of the parameter, value=corresponding value)



Managing the CA settings

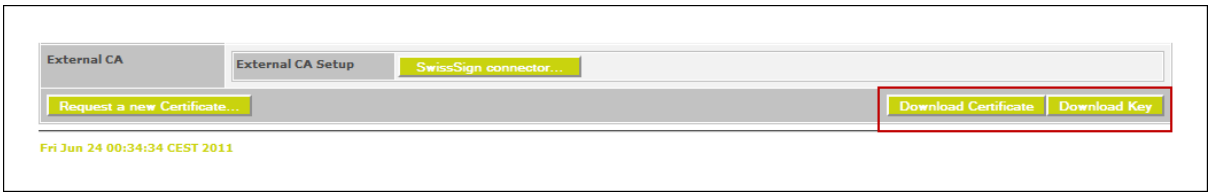
4.8.2 Configuring a CA certificate

In order to configure the certificate of the internal Certificate Authority (CA), you must click the "CA" menu item in the web administration portal.

In order to create a CA certificate, please click the "Request a new Certificate..." button. Regarding the creation of the certificates, please proceed in analogy to the steps in chapter Configuring an SSL certificate 103.

4.8.3 Saving a CA certificate

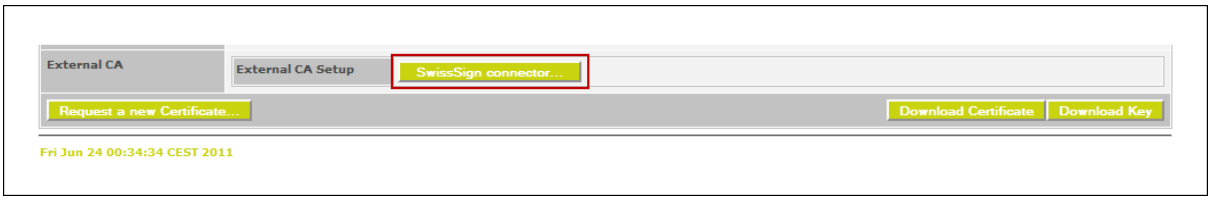
In order to save the certificate of the internal Certificate Authority (CA), you must click the “CA” menu item in the web administration portal.
Please implement the saving procedure by clicking the “Download Certificate” and “Download Key” buttons.



Saving the internal CA certificate

4.8.4 Configuring connection to external CA authority SwissSign

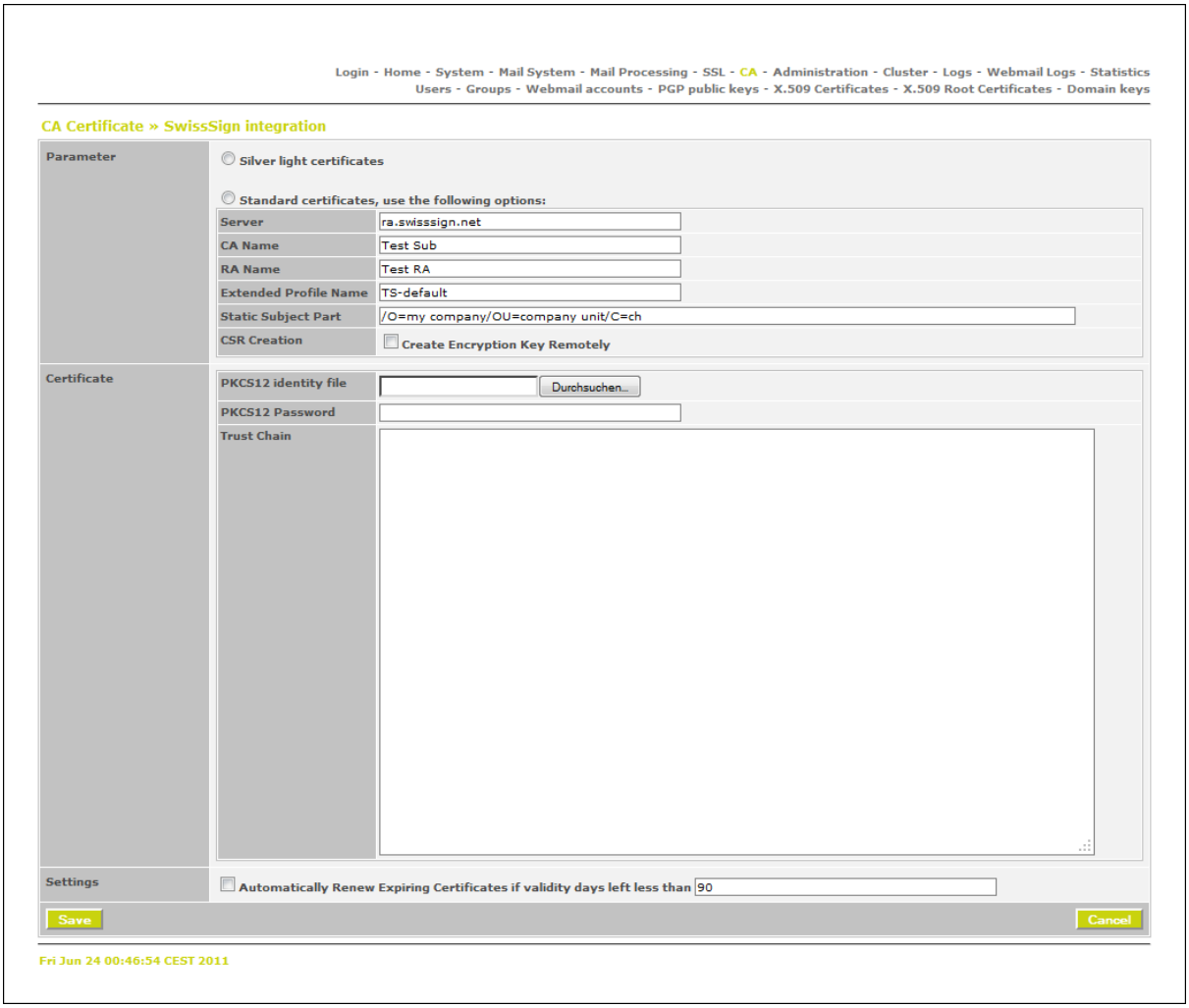
In order to establish the connection to the external CA authority SwissSign please click the “CA” menu item in the web administration portal, followed by the »SwissSign connector...« button. .



Configuring connection to external CA authority SwissSign

You can select between Silver light certificates or Standard certificates. In order to use Silver light certificates, no further information must be provided. For Standard certificates the following values must be entered:

- Server: the SwissSign server for requesting standard certificates
- CA Name: name of your certificate authority (CA)
- RA Name: name of your registration authority (RA)
- Extended Profile Name: extended profile name
- Static Subject Part: O=name of the organisation / OU=name of the responsible organisational unit / C=country the organisation is headquartered
- CSR Creation: option of having the certificate request developed by the external CA authority



Specifications for requesting standard certificates with the certification authority SwissSign

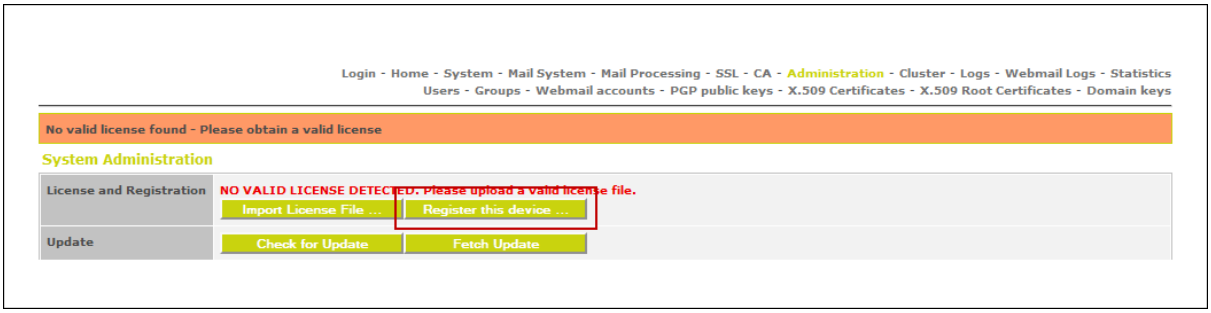
4.9 Menu Item "Administration"

Select the “Administration” menu item in order to manage the administrative assignments of the Mail Encryption appliance.

The following processes will be described in the following sections:

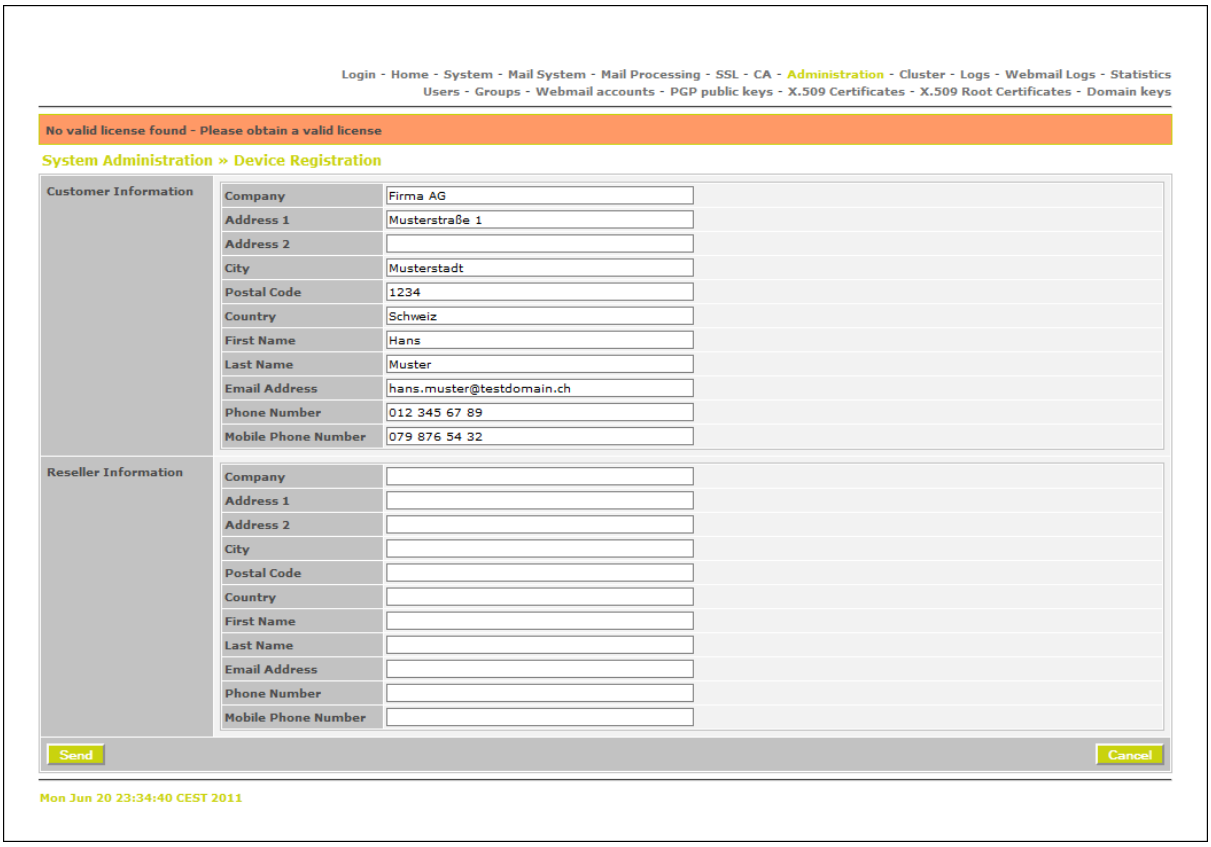
4.9.1 Registering the Mail Encryptionappliance

Register your system so that you are provided with a permanent licence. Please click the "Administration" menu item in the web administration portal. Afterwards, please click the "Register this device" button.



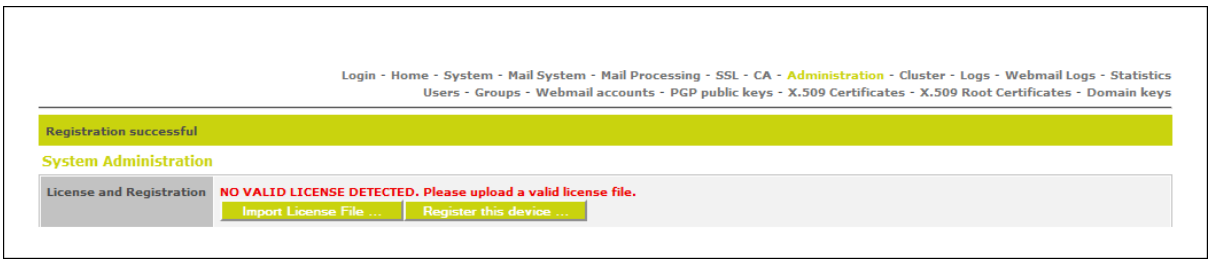
Registering the appliance

After having clicked the "Register this device..." button, a registration window will be displayed. This is shown in the following figure.



Registration window for the collection of your customer information

Please enter your details into the fields of the registration window. Please enter your customer information into the upper half and the details of your reseller into the lower half. Finish your entries by clicking the "Send" button.



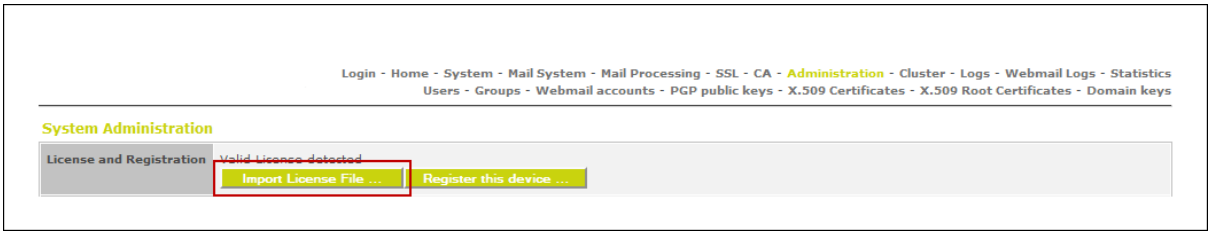
Confirmation upon successful registration

If the message "Registration successful" is displayed, you have completed the registration procedure successfully.

4.9.2 Loading the licence file

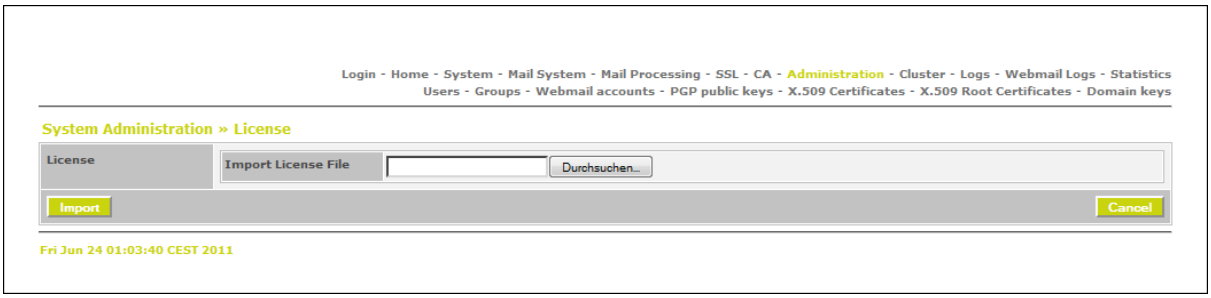
The Mail Encryption appliance will be licensed automatically upon a short period of time when you register the appliance (see chapter Registering the appliance 116).

In order to manually load a licence file, you must click the Administration menu item in the web administration portal. Afterwards, please click the “Import Licence File...” button.



Loading the licence file

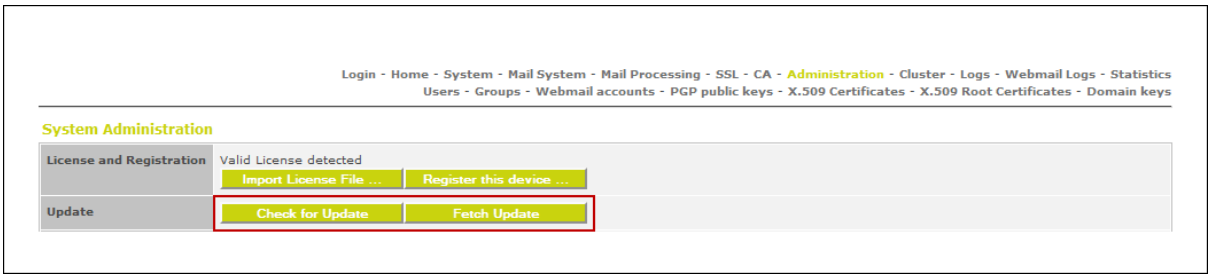
Click the “Browse” button in order to select the licence file you want to load.



Selection of the licence file

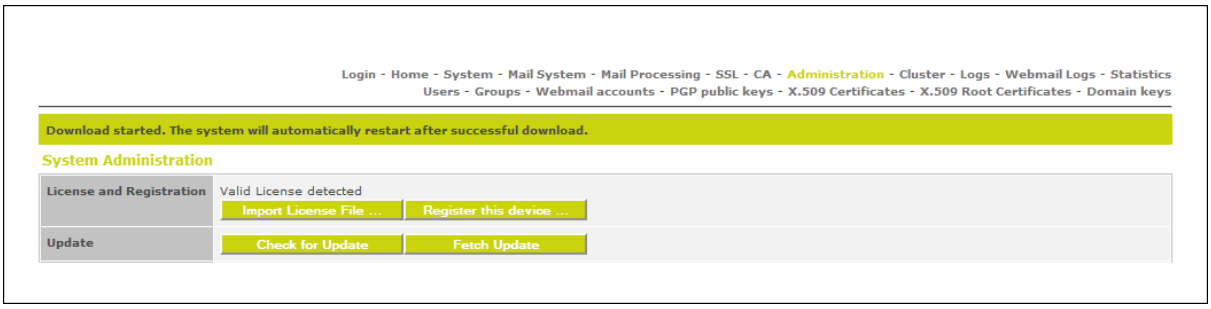
4.9.3 Checking the appliance for available updates

In order to update your Mail Encryption appliance, you must click the Administration menu item and then you must click the "Check for Update" button. If an update is available, please additionally click the "Fetch Update" button. This may be a time-consuming step if the delivered system works with an older firmware and must implement several updates on the basis of the aforementioned.



Buttons to be used to browse for and to install updates

Repeat this step until there are no more updates available. The system will optimise this process so that it is not necessary to make an update for each intermediate version, but only for those involving changes to the data structure.

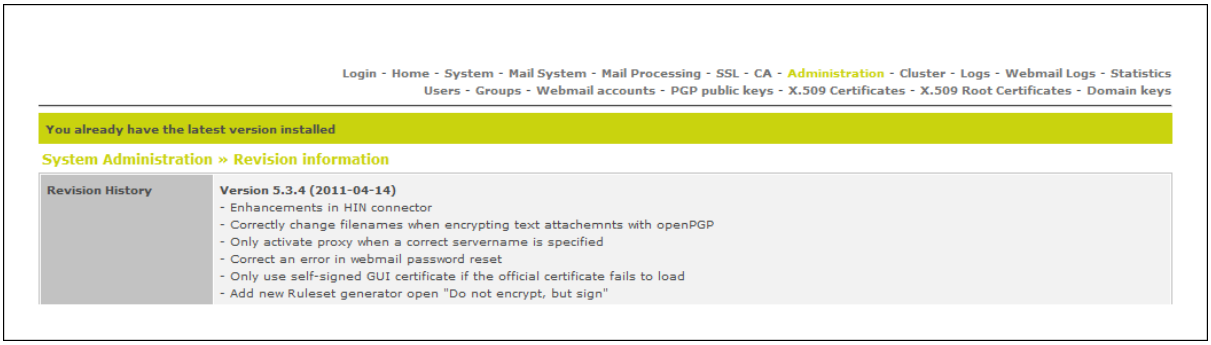


Confirmation that an update is being loaded

It may happen that you are not provided with any feedback over an extended period of time. If this is the case, please update the display by clicking the System Administration link above the buttons. As long as you were not logged off, the update is not finished.

After having been updated, the Mail Encryption appliance must restart and you are required to re-enter your login details. If required, implement this step yourself, if the system does not provide you with any feedback for an extended period of time, i.e. does not display the login mask. You can trigger the restart procedure by clicking the "Reboot" button and confirming the security code displayed afterwards. Upon every restart, please re-check whether further updates are available.

If the message You already have the latest version installed is displayed, your Mail Encryption Appliance is up to date.

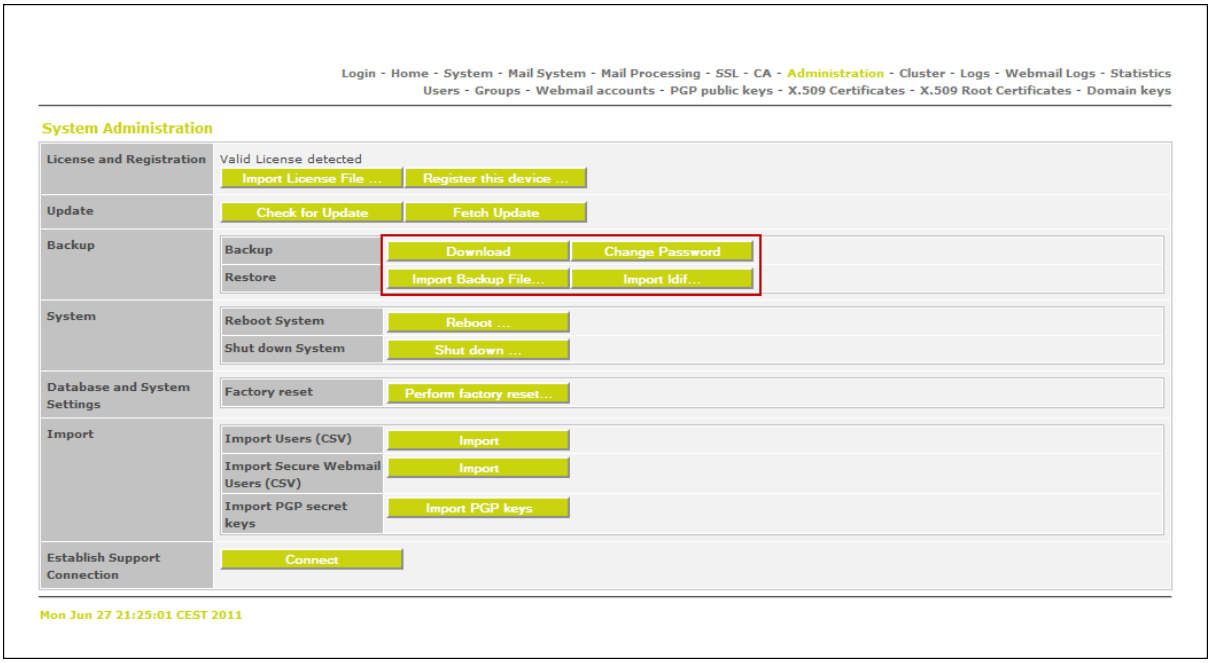


Confirmation that the Mail Encryption appliance is up to date

If further updates are available in the future, this will be displayed automatically upon a restart procedure in each case.

4.9.4 Saving and restoring the settings of the appliance

In order to save and restore the settings of the Mail Encryption appliance, you must click the **"Administration"** menu item in the configuration interface.



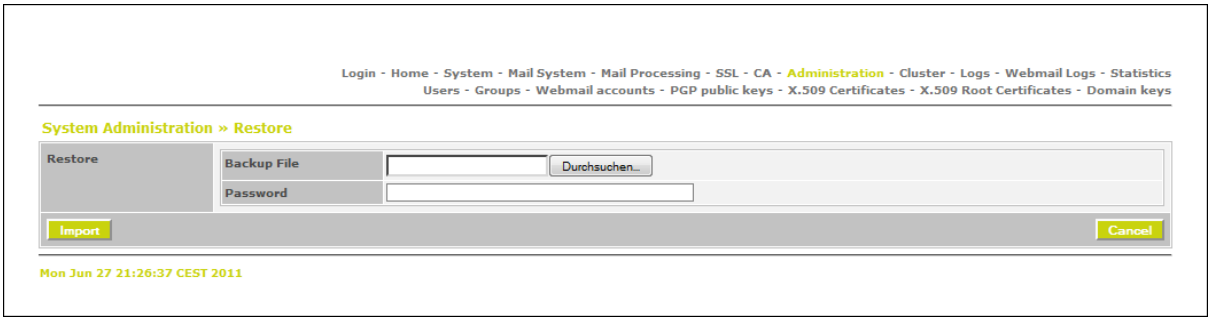
Saving and restoring the settings of the appliance

Saving the settings
In order to secure the current status of your Mail Encryption appliance, you must specify a backup password first. This password will be used when recovering a backup. In order to specify the password, please click the "Change Password" button. In order to implement the process of saving, please click the "Download" button.

Changing the backup password
In order to change the password for future backups, please click the "Change Password" button. Attention! The change will only be applicable to future backups. Backup files from the past are further protected by the corresponding password set in the past.

Restoring the settings
In order to load a backup file and, thus, in order to restore the settings of the appliance, you must click the "Import Backup File..." button.

In order to recover the settings, please select the backup file in the following dialogue and enter the related password.

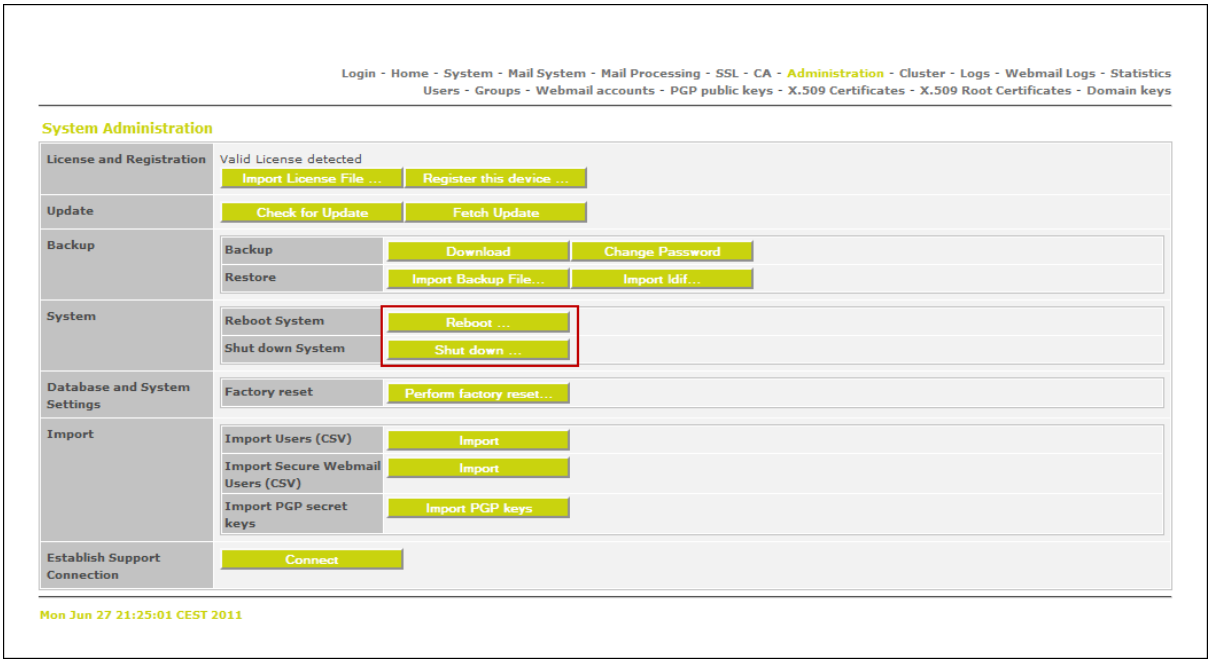


Selection of a backup file and entry of the related password

4.9.5 Restarting or shutting down the appliance

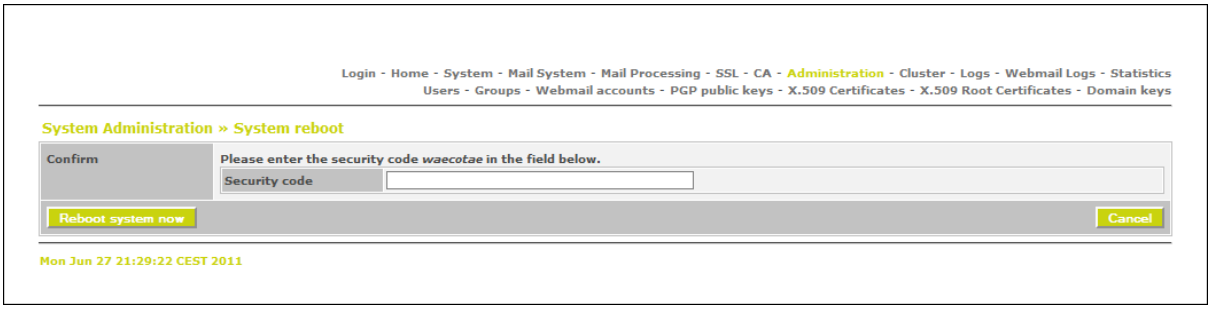
In order to restart or shut down your Mail Encryption appliance, you must click the Administration menu item in the configuration interface.

- Restart: implement a restart by clicking the "Reboot..." button.
- Shut-down: shut down the appliance by clicking the "Shutdown..." button.



Restarting or shutting down the appliance

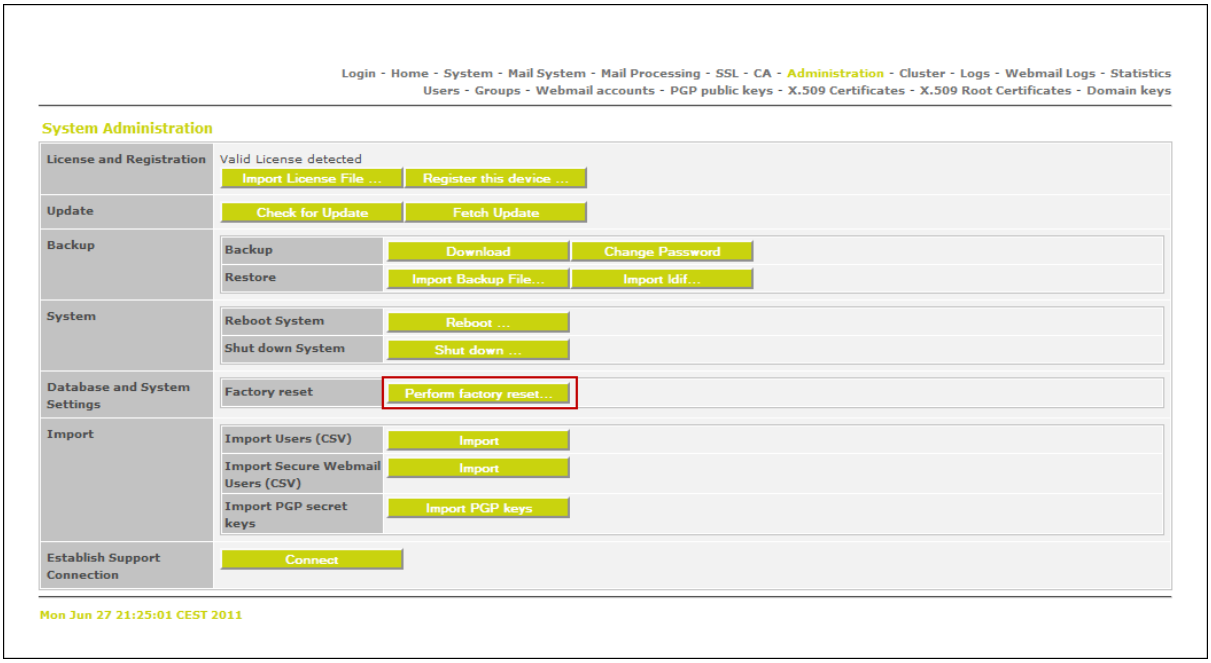
In order to prevent accidental restart or accidental shut-down, these procedures must be confirmed with a security code. The security code is generated and displayed automatically in each case and must be entered by you into the Security code field.



Confirming the restart of the appliance

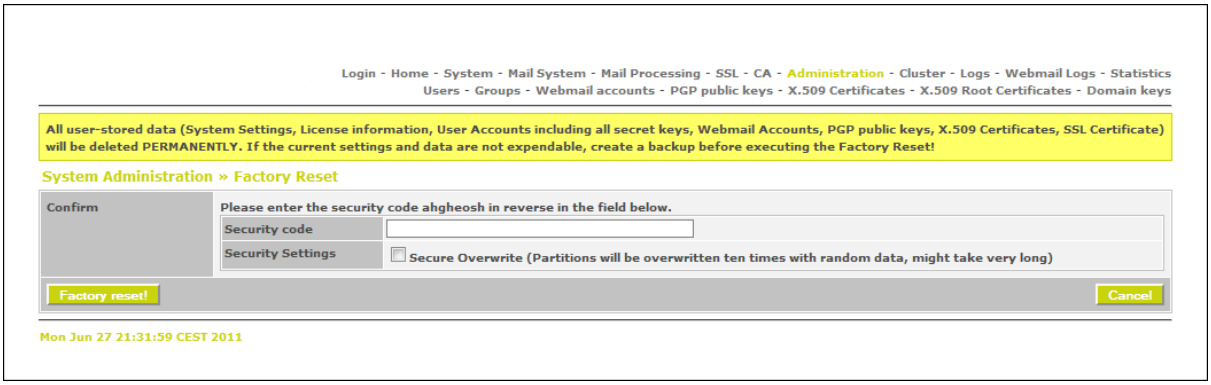
4.9.6 Restoring the factory settings of the appliance

In order to reset your Mail Encryption appliance to its factory settings, you must click the Administration menu item in the configuration interface. Afterwards, please click the “Perform factory reset...” button.



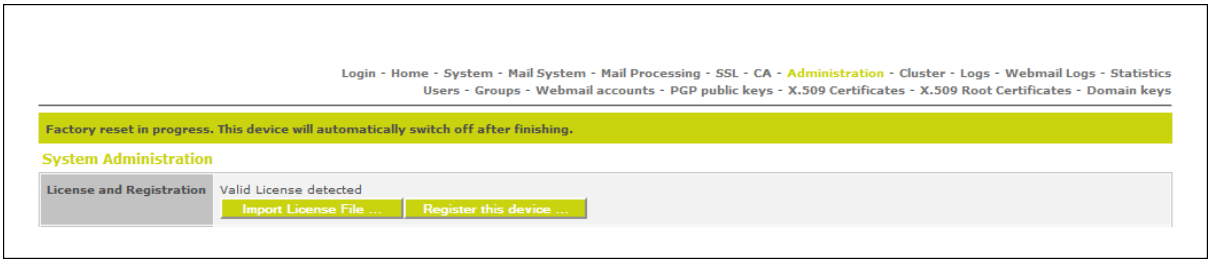
Restoring the factory settings of the appliance

In order to prevent accidental resetting of the appliance, this procedure must be confirmed by means of a security code. The security code is generated and displayed automatically in each case and must be entered in reverse order (from back to front) by you into the Security code field.



Confirmation before the appliance is reset to its factory settings

After having entered the security code correctly and after having clicked the “Perform factory reset...” button, the confirmation message Factory reset in progress. The device will automatically switch off after finishing will be displayed. As soon as the procedure is finished, Mail Encryption will be switched off automatically.



Confirmation after having entered the security code

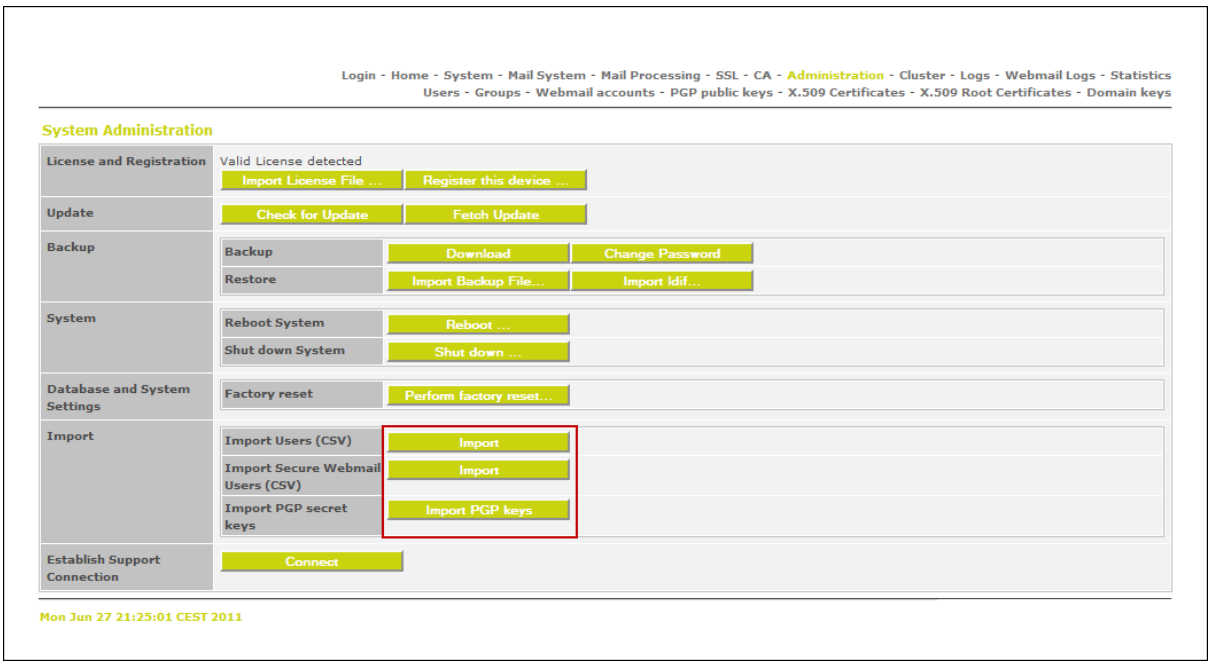
4.9.7 Importing existing users or keys

In order to import existing user accounts or OpenPGP keys, please click the “Administration” menu item in the configuration interface.

You can import user accounts by clicking the “Import” button next to Import Users (CSV). The list containing the user information must be present in CSV (Comma-Separated Values) format and must be characterised by the following syntax: USERID;NAME;E-MAIL;PASSWORD. The PASSWORD field is optional.

In order to import secure webmail accounts, you must click the “Import” button next to Import Secure Webmail Users (CSV). The file containing the information of the webmail accounts must be present in CSV format and must be characterised by the following syntax: E-MAIL;PASSWORD.

You can read-in existing private OpenPGP keys by clicking the “Import PGP keys” button. You can import the private keys as a file or in text form. Additionally, you must enter the pass phrase of the corresponding key.

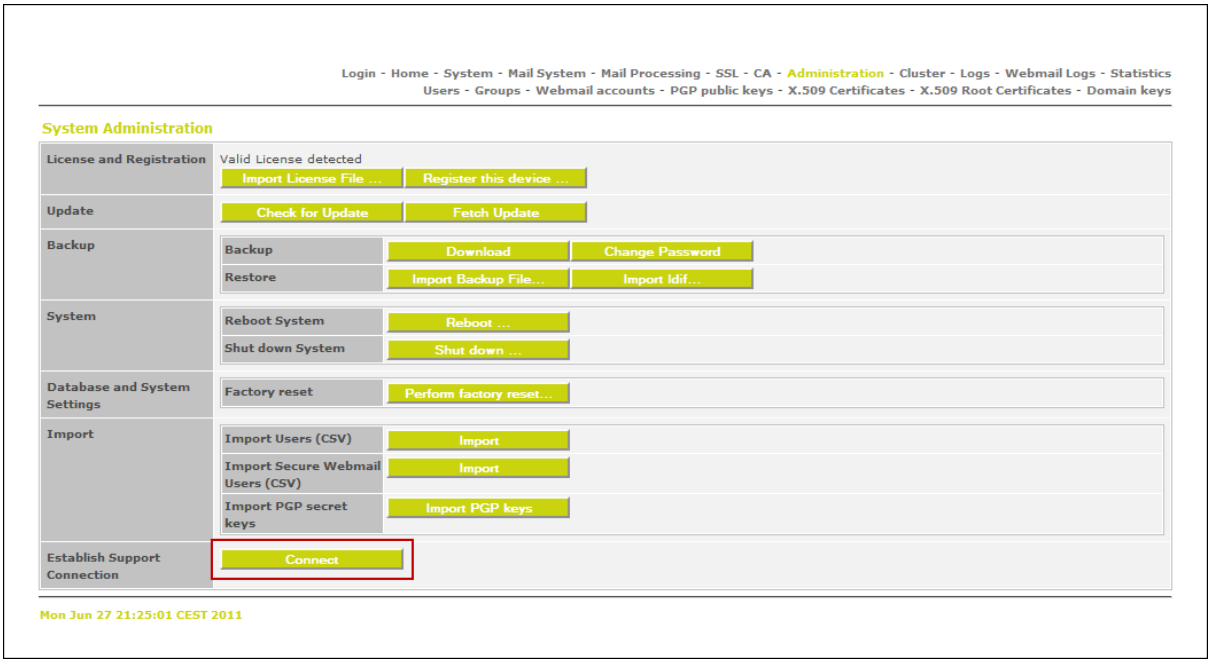


Importing users or PGP keys

4.9.8 Establishing incoming support connection

You can use the "Establish Support Connection" button to establish a connection to the manufacturer. Use this function only if the manufacturer instructs you to do so. In order that the connection can be established, port TCP/22 (SSH) of the Mail Encryption appliance must be opened for the internet on your firewall respectively your router.

In order to establish an incoming support connection, you must click the "Administration" menu item in the configuration interface and afterwards you must click the "Connect" button.



Establishing incoming support connection

4.10 Menu Item "Cluster"

This chapter contains a description of the fundamental mode of operation and the management of the Mail Encryption cluster. You will learn which cluster modes of operation are supported by Mail Encryption and how you can configure them in the configuration the framework of the aforementioned

4.10.1 General

There are different types of cluster operation supported by Mail Encryption.

A cluster is a compound of computers consisting of several networked computer systems. These computer systems networked with each other are separated physically, but must be considered a unit from a logical point of view. This way, it is possible that one cluster can be addressed as a single logical system, while actually consisting of several physical systems.

There are different objectives regarding the utilisation of a cluster that differ depending on the application. There are the following 4 modes of operation for a cluster consisting of several Mail Encryption systems:

1. High-availability cluster for reliability (failover)
2. Load balancing cluster for load balancing
   - Separation of the incoming and outgoing flows of e-mails to one cluster member system in each case
   - Use of an external load balancer for distributing this e-mail to different cluster member systems (depending on the configuration)
   - Load balancing on the basis of the DNS Round Robin procedure (http://de.wikipedia.org/wiki/Lastverteilung_per_DNS)
3. Geo cluster for replicating configuration databases of systems separated in a geographical sense
4. Frontend-backend cluster

The corresponding 4 modes of operation are described in detail in the following sections.

4.10.2 High-availability cluster

The reliability of the Mail Encryption system can be increased by the formation of a cluster.

The Mail Encryption system is characterised by integrated cluster functionality on the basis of the CARP protocol (http://de.wikipedia.org/wiki/Common_Address_Redundancy_Protocol).

In order to create a cluster, at least two Mail Encryption systems are required which monitor each other. If one system fails respectively no longer answers the monitoring requests, the second system will assume this function. When the failed system is available again respectively when it provides responses to monitoring requests, it will re-assume its original assignment.

This function can be mapped with up to 9 Mail Encryption systems, by which means you can achieve a very high level of reliability.

The high-availability cluster can be mapped with Mail Encryption systems on hardware basis and on the basis of the virtualisation with VMware ESX. Mixed operation using systems on hardware basis and virtualised systems is also possible.

How does the high-availability cluster work?

Within the framework of this procedure, a cluster is assigned with one or several virtual IP address(es) with different priorities. Each cluster member system is characterised by its own unambiguous IP address independent of the assigned virtual cluster IP address. This own, unambiguous IP address can be used to explicitly address each cluster member system.

Example:
In the following figure, the virtual cluster IP address of the cluster is 10.10.0.1. Within the framework of our example the cluster member systems have the IP addresses 10.10.0.9 and 10.10.0.10.

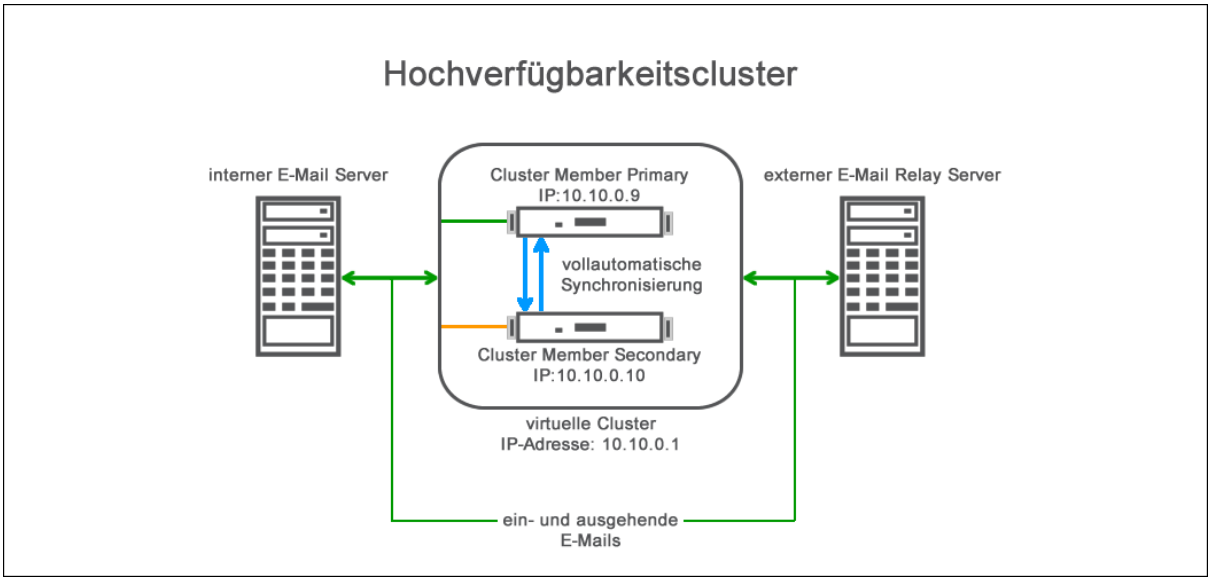


Figure 1 – Schematic representation of a high-availability cluster

The very cluster is addressed by other systems, e.g. an internal e-mail server or an upstream e-mail relay server (gateway), by means of the configured virtual IP address(es). In the example above, this is the IP address 10.10.0.1.

If the very cluster is addressed by means of its cluster IP address, the cluster member system characterised by the highest priority will always respond to the addressed virtual cluster IP address. All other cluster member systems characterised by a lower priority will not respond when the virtual cluster IP address is addressed and a cluster member system with a higher priority is available.

In the event of an error, if a cluster member system characterised by a higher priority that normally responds to the addressed virtual cluster IP address fails, a cluster member system characterised by the next lower priority will automatically assume the virtual cluster IP address, including the function of the failed cluster member system.

The order for the priorities is as follows:

1. Primary
2. Secondary
3. Backup

You can configure the priority of the corresponding cluster member system in the “System” menu.

4.10.3 Load Balancing Cluster

A cluster can additionally be used to increase the e-mail throughput. There are the following options for the aforementioned:

1. Separation of the incoming and outgoing flows of e-mails to one cluster member system in each case 128
2. Use of an external load balancer for distributing these e-mails to different cluster member systems (depending on the configuration) 130
3. Load balancing on the basis of the DNS Round-Robin procedure 131 (http://de.wikipedia.org/wiki/Lastverteilung_per_DNS)

   Application with redundant external and internal MTAs (mail transport agent) 133

The failover behaviour of the cluster is not changed on the basis of these configurations.

Separation of the incoming and outgoing flows of e-mails to one cluster member system in each case.

The separation of the incoming and outgoing data flows of e-mails can be implemented in three ways, as already mentioned above. Figure 1 shows that incoming and outgoing e-mails are sent to a separate virtual IP address in each case by means of a static configuration. There are 2 Mail Encryption systems responding to two virtual IP addresses (alias IP addresses) in each case with a different priority. One system is provided with all incoming e-mails and one system is provided with all outgoing e-mails in each case. On the basis of the creation or two virtual IP addresses, the two Mail Encryption systems can be addressed separately by means of a dedicated virtual IP address.

This is illustrated logically in figure 1. From a physical point of view there are only two Mail Encryption systems.

What happens in detail:

Each Mail Encryption system has its own, completely separate IP address that is used to address this system only, e.g. for the configuration of settings that are not synchronised within the cluster.

These are the IP addresses 10.10.0.9 and 10.10.0.10 in figure 1.

Additionally, there are two virtual IP addresses in order to logically summarise the two Mail Encryption systems to one group in each case. These virtual IP addresses (groups) are represented separated by colours in figure 1.

The virtual IP address 10.10.0.1, represented in green here, is addressed for all outgoing e-mails from the internal e-mail server respectively the outgoing e-mails are sent to this virtual IP address by the internal e-mail server.

The virtual IP address 10.10.0.2, represented in orange here, is addressed for all incoming e-mails from the external e-mail server or an upstream e-mail relay (e.g. firewall) respectively the e-mails are sent to this virtual IP address by the external or upstream systems.

Now, the two physical Mail Encryption systems are summarised logically under one virtual IP address. As a matter of principle, both systems respond when the virtual IP address is addressed. However, this does not always make sense, because we want to use one system for all incoming e-

mails and the other system for all outgoing e-mails. In order to achieve this, the sequence the individual systems are to respond in is specified within the framework of a hierarchy when one of the two virtual IP addresses is addressed.

In figure 1, represented in green, you can see the virtual IP address 10.10.0.1 for all outgoing e-mails. Here, the cluster member system characterised by the IP address 10.10.0.9 is configured as Primary and will always respond as the first system when the virtual IP address 10.10.0.1 is addressed. The cluster member system characterised by the IP address 10.10.0.10 is configured as Secondary and will only respond if the cluster member Primary is not available.

In figure 1, represented in orange, you can see the virtual IP address 10.10.0.2 for all incoming e-mails. Here, the cluster member system characterised by the IP address 10.10.0.10 is configured as Primary (as opposed to the previous representation) and will always respond as the first system when the virtual IP address 10.10.0.2 is addressed. The cluster member system characterised by the IP address 10.10.0.9 is configured as Secondary and will only respond if the cluster member Primary is not available.

Summary:

Each individual Mail Encryption system can be addressed by means of two different virtual IP addresses and will respond with priorities differing in each case, at one point as Primary and at one point as Secondary. This way, continued operation is possible in the event of a failure of one cluster member system. The remaining cluster member system will then assume the work of the no longer available system and will process all incoming and outgoing e-mails.

Regarding the use of EgoSecure Mail Encryption, a virtual cluster IP address 10.10.0.1 can be addressed. Depending on the cluster member priorities, the cluster member system characterised by the IP address 10.10.0.9 will respond in the example in figure 1, because this system is configured with the priority “Primary”. If this system is not available, the cluster member system characterised by the IP address 10.10.0.10 will respond, because it is configured with the priority “Secondary”.

You can configure the virtual IP addresses and assign the priorities in the “System” menu.

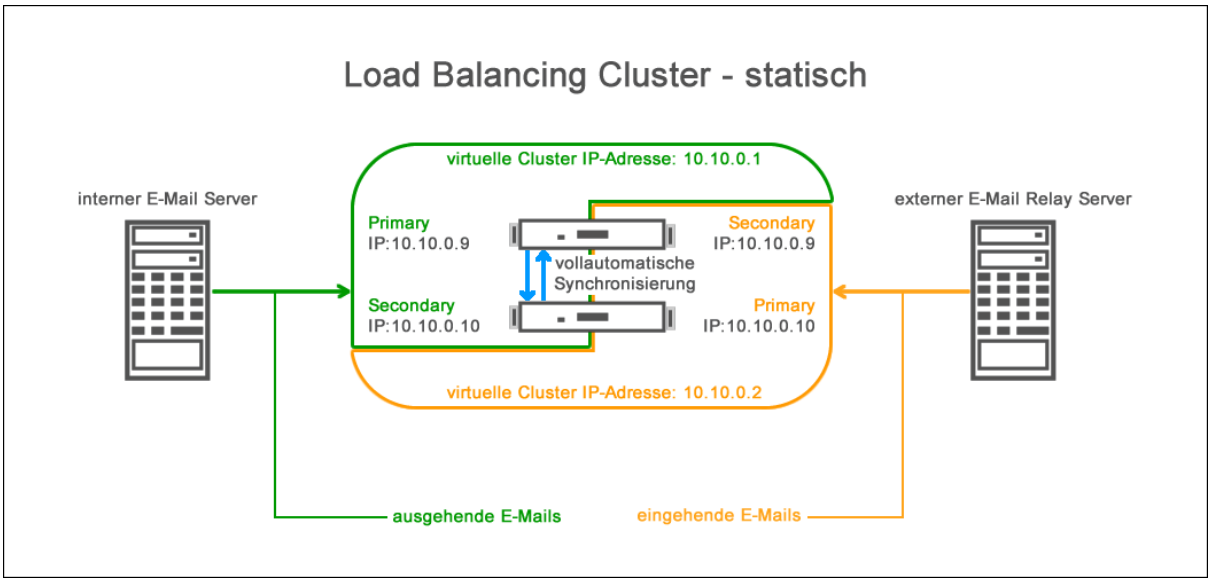


Figure 1 – Schematic representation of the static separation for incoming and outgoing e-mails

Use of an external load balancer for distributing the e-mails to different cluster member systems

In figure 1, incoming and outgoing e-mails are sent to the cluster member system in a dynamic manner by means of an external load balancer. Therefore, each cluster member system receives incoming and outgoing e-mails in equal measure. If a cluster member system is no longer available, the responsibility for detecting the aforementioned and reacting accordingly is incumbent upon the load balancer. Figure 2 shows a logical representation of the scenario.

What happens in detail:

The cluster functionality of Mail Encryption is only used for the synchronisation of the configuration between the cluster member systems in this scenario. The decision which system will respond to incoming and outgoing e-mails will be made by the upstream load balancer. Depending on the configuration and load situation, the load balancer will distribute the e-mails to a cluster member system of its choice. In doing so, the cluster member system is not addressed by means of a virtual IP address, but by means of its own separate IP address.

Each Mail Encryption system has its own, completely separate IP address that is used to address this system only, e.g. for the configuration of settings that are not synchronised within the cluster.

These are the IP addresses 10.10.0.9 and 10.10.0.10 in figure 2.

The essential difference regarding figure 1 is that no virtual IP address is addressed in doing so. In order to distribute outgoing e-mails, the load balancer will distribute these on the internal e-mail server to the cluster member systems characterised by the IP addresses 10.10.0.9 and 10.10.0.10.

Summary:

When using an external load balancer, the Mail Encryption cluster member systems will be addressed directly by the load balancer. If a cluster member system fails, the responsibility for detecting this and for sending the incoming or outgoing e-mails to the remaining system is incumbent upon the load balancer.

Regarding the use of EgoSecure Mail Encryption, a virtual cluster IP address can be addressed further. Depending on the cluster member priorities, the cluster member system characterised by the IP address 10.10.0.9 will respond in the example in figure 2, because this system is configured with the priority „Primary“. If this system is not available, the cluster member system characterised by the IP address 10.10.0.10 will respond, because it is configured with the priority “Secondary”.

You can configure the virtual IP addresses and assign the priorities in the “System” menu.

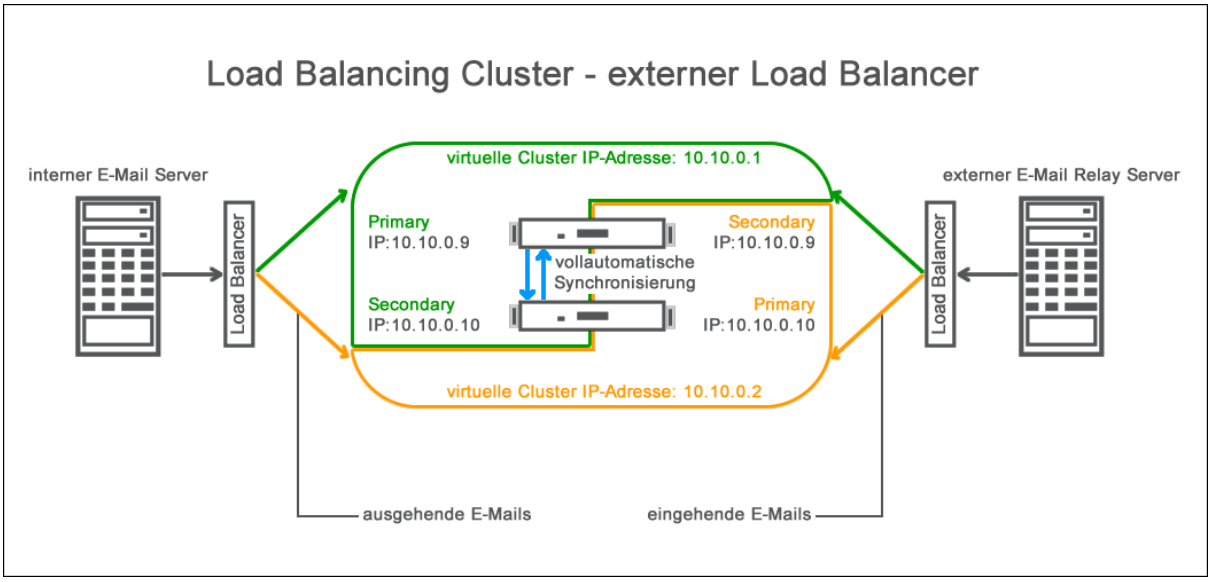


Figure 2 – Schematic representation of the dynamic separation for incoming and outgoing e-mails by means of an external load balancer

Load balancing on the basis of the DNS Round Robin procedure

You will find a detailed description of this function in the following article: http://de.wikipedia.org/wiki/Lastverteilung_per_DNS

Within the configuration of the internal and external e-mail servers, a virtual cluster IP address is no longer specified for e-mail dispatch, but a host name in each case, e.g. “cluster-in.domain.tld” or “cluster-out.domain.tld”, whereby this host name is addressed for incoming and outgoing e-mails. It is possible to specify several IP addresses for each host name within the DNS. This way, simple load balancing can be achieved.

For example, if the internal e-mail server addresses the host name of the Mail Encryption cluster specified for e-mail dispatch within DNS, all IP addresses assigned to this host name will be returned in any case, but this in a different order in each case. The internal server is now able to select one of these IP addresses for sending the e-mail. In the event of an error, the available cluster member system with the next lower priority within the cluster will respond. Figure 3 shows a logical representation of the scenario.

What happens in detail:

Each Mail Encryption system has its own, completely separate IP address that is used to address this system only, e.g. for the configuration of settings that are not synchronised within the cluster.

These are the IP addresses 10.10.0.9 and 10.10.0.10 in figure 3.

Additionally, there are two virtual IP addresses in order to logically summarise the two Mail Encryption systems to one group in each case. These virtual IP addresses (groups) are represented as being separate by colours in figure 3.

The internal and the external e-mail servers address a host name instead of a virtual IP address in

order to send incoming and outgoing e-mails to the Mail Encryption cluster system. If the DNS server receives a request for this host name, the host name will be resolved into all configured IP addresses.

In our case, the resolved IP addresses correspond to the virtual cluster IP addresses, as illustrated by figure 3. The two virtual IP addresses have a different system as cluster member Primary and cluster member Secondary in each case. The aforementioned provides for redundancy in the event of an error, because both cluster member systems monitor each other and are able to assume the assignment of the failed system.

The virtual IP address 10.10.0.1, represented in green here, and the virtual IP address 10.10.0.2, represented in orange here, are assigned to the host name that is listed for sending outgoing e-mails within the internal e-mail server, for example. This host name will be resolved into the following IP addresses.

```
custer-out.domain.tld.   1800  IN  A  10.10.0.1
custer-out.domain.tld.   1800  IN  A  10.10.0.2
```

Within the framework of each resolution of the addressed host name “cluster-out.domain.tld”, the DNS server will return all assigned IP addresses, but in a different order.

```
custer-out.domain.tld.   1800  IN  A  10.10.0.2
custer-out.domain.tld.   1800  IN  A  10.10.0.1
```

The internal e-mail server is now able to select an IP address and to send the outgoing e-mail. As the order of the returned IP addresses will change for each request, the e-mails can be distributed to the cluster member systems available.

Summary:

When sending incoming and outgoing e-mails via the Mail Encryption cluster, a host name will be specified within the corresponding e-mail server instead of a virtual cluster IP address. This host name will then be resolved into the related IP addresses at runtime. This way, the internal and the external e-mail servers can send incoming and outgoing e-mails optionally to one of these resolved IP addresses. As these are virtual cluster IP addresses in each case, the cluster member systems will respond according to their priority, e.g. in the case of an error.

Load balancing can be achieved for incoming and outgoing e-mail data flows on the basis of the DNS Round-Robin function.

Source: Wikipedia, http://de.wikipedia.org/wiki/Lastverteilung_per_DNS (also mentioned in excerpts within the framework of this chapter)

You can configure the virtual IP addresses and assign the priorities in the “System” menu.

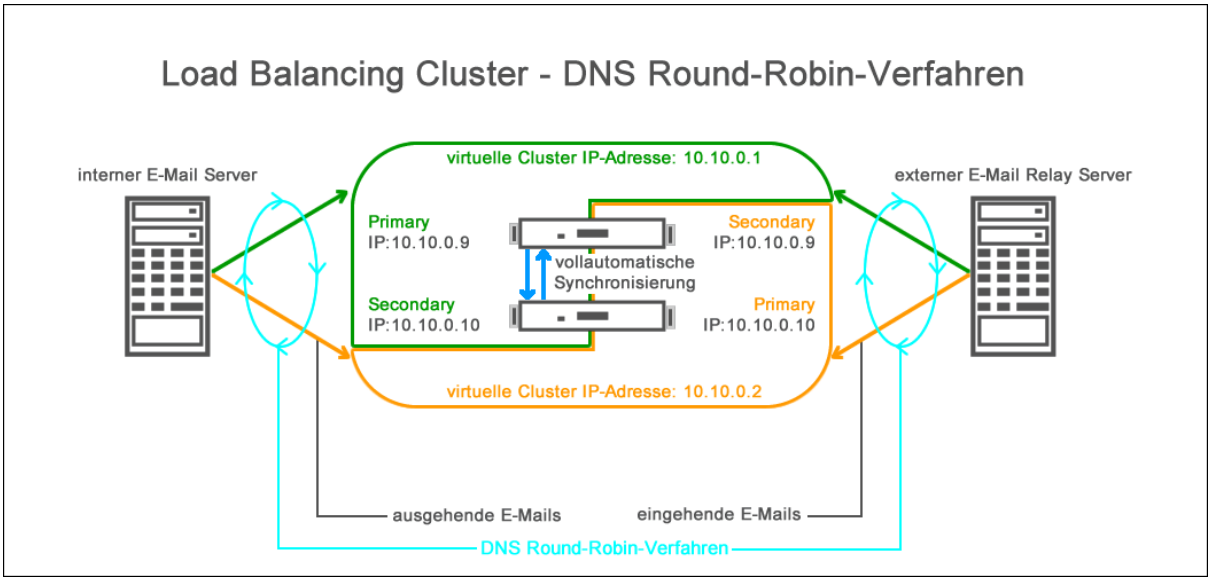


Figure 3 – Schematic representation of load balancing by means of the DNS Round-Robin procedure for incoming and outgoing e-mails

Application with redundant external and internal MTAs (mail transport agent)

You can configure exactly 1 host as external MTA (e-mail relay) within the Mail Encryption configuration. In analogy, exactly 1 internal MTA (e-mail server) can be configured for every internal e-mail domain. The Mail Encryption system is able to support redundant external and internal MTAs by means of the procedure described within the framework of the following sections.

Within the Mail Encryption system, the external respectively internal MTA can be configured in several ways:

- specification of an IP address
- specification of a host name
- specification of a domain an MX Lookup is implemented for

The differentiation between IP address, host name, and domain is implemented by means of square brackets (“[“, “]”): IP addresses and host names must be specified in square brackets; domains an MX Lookup is implemented for must be specified without square brackets.

The Mail Encryption system is able to support redundant external or internal MTAs if one dummy domain that is only available internally is configured for the internal and for the external MTA in each case. 2 MX records with different preferences will be created for each dummy domain within the internal DNS. By default, the Mail Encryption system will forward the e-mails to the host characterised by the lowest preference. In the event of a failure of this host, the e-mails will be forwarded automatically to the host characterised by the higher preference.

You can configure the host names for the redundant internal and external MTAs in the “Mail System” menu.

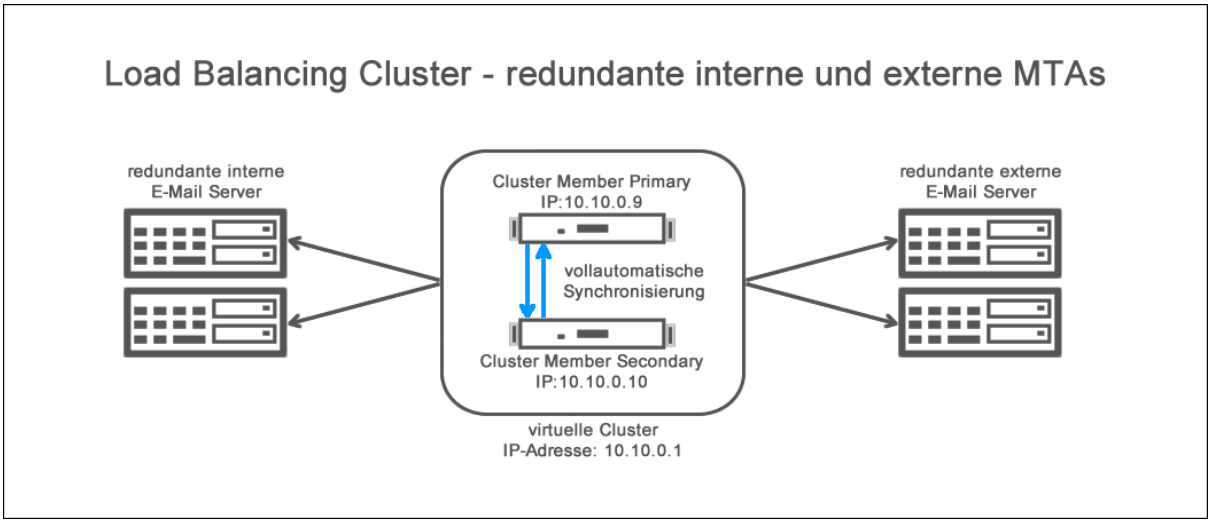


Figure 4 – Schematic representation for the application of redundant internal and external MTAs

4.10.4 Geo Cluster

A geo cluster (also called “multi-site system”) serves to replicate configuration databases between geographically separated Mail Encryption systems at different company locations.

Application example:

A company is operating on a global scale and operates several data centres on different continents on the basis of the aforementioned. The very company locations are all interconnected by means of a VPN and have internet access in each data centre. Within this internal company network there is an e-mail transport system, e.g. on the basis of Microsoft Exchange or Lotus Notes. The e-mails sent to external recipients can be sent to the internet at different internet accesses of the company, depending on the guideline specified internally. (e.g. if an internet access at one location is not working, but the VPN connection between the locations is not affected by the aforementioned and the external dispatch of e-mails is now implemented using the other location).

For this, it is necessary that the required cryptographic e-mail processing is implemented similarly at all internet accesses. All user accounts and their certificates regarding the processes of signing, decrypting, and encrypting must be present and the configuration settings must be identical as well, in order to not to have any deviations regarding e-mail processing.

On the basis of the geo cluster function of the Mail Encryption system, modifications to the configuration can be replicated immediately between all Mail Encryption systems within the geo cluster. This way, consistent configuration of all systems is provided for.

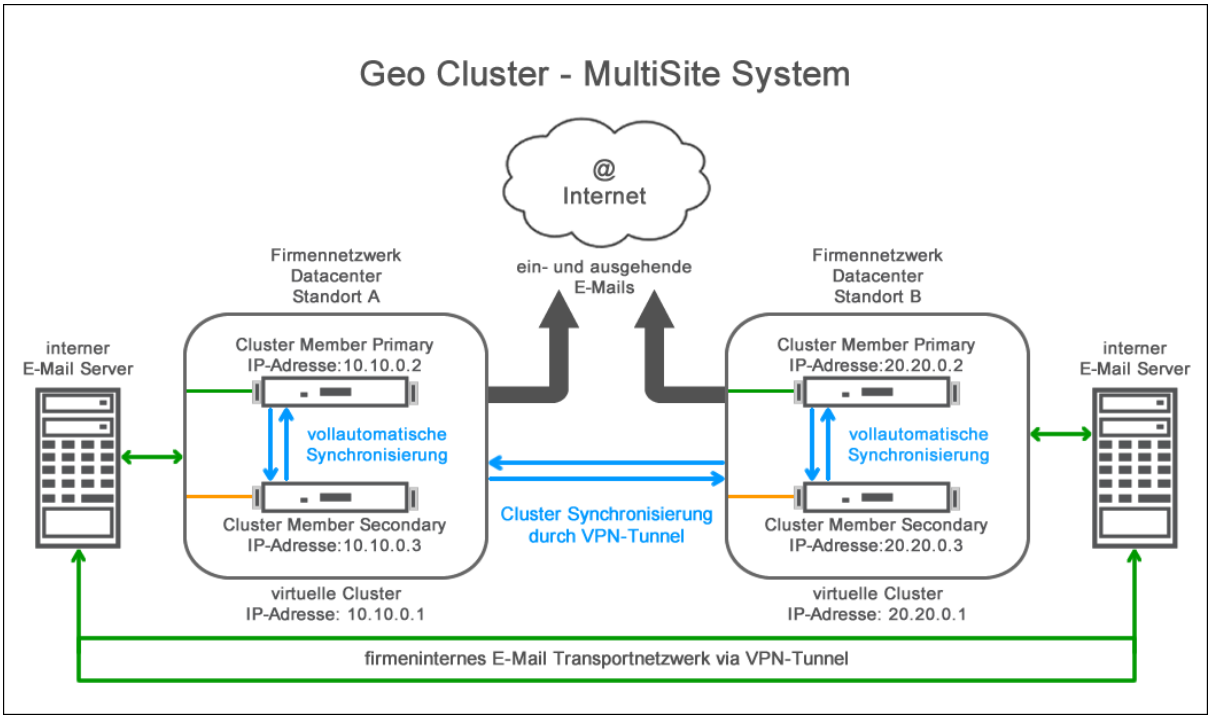


Figure 1 – Schematic representation of a geo cluster structure

4.10.5 Frontend-Backend Cluster

Frontend-Backend cluster, whereby the frontend systems do not dispose of any local configuration database

Operating a Mail Encryption system as frontend server is a very special cluster function. The difference regarding the normal cluster function of the Mail Encryption system is that there is no configuration database on the very frontend server.

The configuration data required at runtime is transferred from the cluster to the frontend server and is only stored temporarily depending on the requirement, e.g. during necessary decryption of an incoming e-mail. After the e-mail has been processed, this configuration data will be deleted immediately.

This function can be used in scenarios where there are corresponding requirements regarding the field of compliance.
.

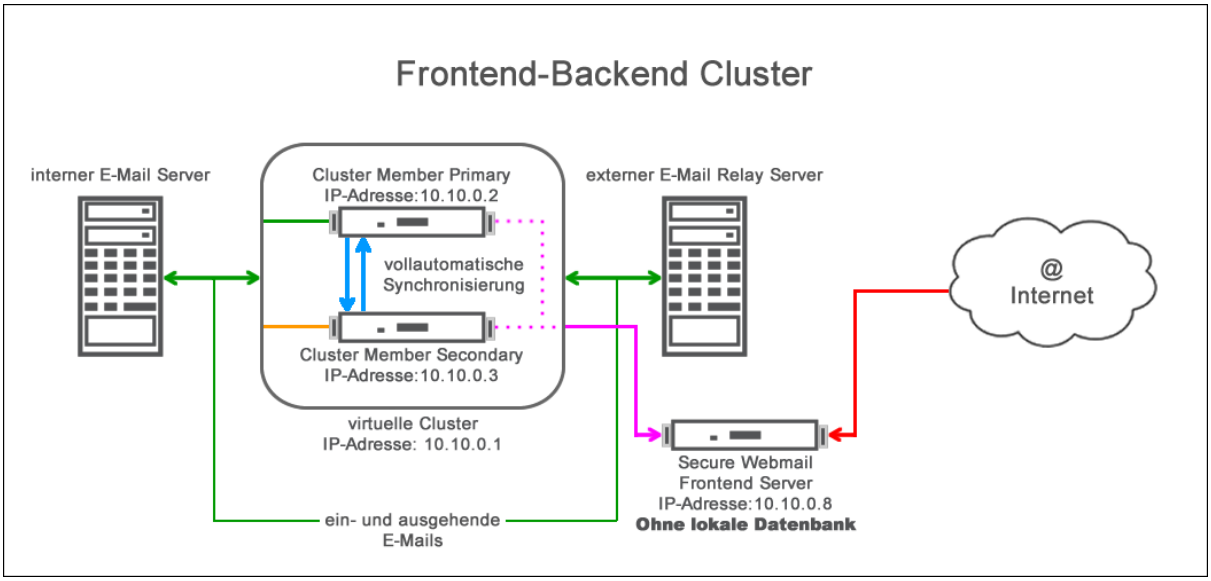


Figure 1 – Schematic representation of a frontend-backend cluster structure

4.10.6 Configuring the cluster configuration

Important note:
Please observe the safety instructions when you are implementing modifications to the parameters of the cluster, removing systems from the cluster, replacing systems in the event of an error, or adding new systems to the cluster.

Non-observance of these safety instructions may render the entire cluster useless.

You can find the safety instructions in chapter Safety instructions 140.

Section	Parameter	Description
Prepare for Cluster	use this key to add a different device to this device/ cluster	Button »Download Cluster Identifier« Select the "Download Cluster Identifier" button in order to download the native RSA PRIVATE KEY and to store the same locally as a file. The downloaded file will be called "clusterid.txt". A cluster identification is required in order to add another Mail Encryption appliance to this device and, thus, to form a cluster.
Add this device to existing cluster WARNING: All data except network configuration of this device will be lost	Cluster Identifier	Import the "Cluster Identifier" file of an existing Mail Encryption cluster system into this input field. The local system will be added to the already existing cluster. Please observe the safety instructions when you are adding a new system to an existing cluster. Please only proceed with the further configuration of the cluster if you have completely understood the principle governing the configuration of a cluster. Non-observance of these safety instructions may render the entire cluster useless. You can find the safety instructions in chapter Safety instructions 140.
	Cluster Member IP	IP of the device you want to connect to. Do NOT use an IP alias address! Please specify the unambiguous IP address of a Mail Encryption system that is already a part of the cluster this system is to be added to. Please do not use a virtual IP address of the cluster! See menu "System > IP-Addresses" in the configuration interface. The cluster systems are interconnected by means of a Secure Shell connection to port TCP/22. Please do not change this port setting.
	IP address of this device	IP address other devices in the cluster can use to connect to this device. Do NOT use an IP alias address! Please specify the unambiguous IP address of the local system here

Section	Parameter	Description
		that is to be added to the existing cluster. See menu “System > IP-Addresses” in the configuration interface. The cluster systems are interconnected by means of a Secure Shell connection to port TCP/22. Please do not change this port setting
	Connect	Button “Start” Select the “Start” button after you have entered all required values for the corresponding parameters in order to start the cluster function on the local system. This system will now become a part of the cluster
Add this device as frontend server (no local database)	Cluster Identifier	Import the “Cluster Identifier” file of an existing Mail Encryption cluster system into this input field. The local system will be added to the already existing cluster as a special frontend server.
	Existing Appliance IP	IP (or virtual IP) of the device (or cluster) you want to connect to. Please specify the unambiguous IP address or the virtual cluster IP address of a Mail Encryption system that is already a part of the cluster this system is to be added to. The cluster systems are interconnected by means of a Secure Shell connection to port TCP/22. Please do not change this port setting.
	Connect	Button “Start” Select the “Start” button after you have entered all required values for the corresponding parameters in order to start the cluster function on the local system. This system will now become a part of the cluster as frontend server.

Reference of the menu parameters in the “Cluster” menu item

4.10.6.1 Overview

This chapter contains a description of the procedures for configuring and operating a Mail Encryption cluster. The Mail Encryption cluster configured within the framework of our configuration example consists of two systems. All required configuration steps will be described in greater detail in the following sections of this chapter.

Configuration steps:

1. Configuration of the first Mail Encryption system completely

2. Configuration of the second Mail Encryption system

3. Regarding the second Mail Encryption system, only the settings in the "System" menu, the registration of the system in the "Administration" menu, and the import of the SSL device certificate in the "SSL" menu are required; all remaining settings, such as the settings in the "Mail Processing" menu and further settings, for example, are transferred automatically when the cluster is configured.

4. A second virtual appliance must be imported in a virtualised environment. The aforementioned must not be a duplicate of the existing first instance.

5. Download of the cluster identification within the first Mail Encryption system.

6. Addition of the second Mail Encryption system to the cluster.

7. Specification and configuration of the virtual IP address(es) of the cluster. Depending on the mode of operation of the cluster, one or two virtual IP addresses are required.
   If the cluster is operated as a pure high-availability cluster (failover cluster) (no separation of the incoming and outgoing e-mail data flow), only one virtual cluster IP address is required.

   If the cluster is additionally configured for load balancing in order to increase the performance, two virtual cluster IP addresses are required.
   The failover behaviour of the cluster will also be maintained for this mode of operation, high-availability cluster with additional load balancing.

4.10.6.2 Security warnings

If you add a new Mail Encryption system to an existing cluster or if you create a cluster for the first time, the entire existing cluster configuration will be replicated to this new cluster member system and it will be synchronised consistently with the cluster afterwards.

All data on this system, except for the settings contained in the menus “System” and “SSL”, as well as the log files and statistics contained in the menus “Logs”, “Webmail Logs”, and “Statistics”, will be lost.

This is important if the system still contains required data, such as S/MIME certificates, PGP keys, secure webmail accounts, etc., for example.

Furthermore, it is important to understand in which order Mail Encryption systems must be added to an existing cluster respectively which system is the source of the replication and which system is the target of the replication. If you confound these systems when creating a new cluster, it may happen that an existing and configured Mail Encryption systems is overwritten with empty data of the newly added system. The aforementioned is even more important regarding an existing cluster that already consists of several cluster member systems. In this case, confusing the source of replication and the target of replication will result in the entire cluster being overwritten with empty data of the new system.

In this case, the entire cluster would be useless. Please remember this in the course of the configuration

4.10.6.3 Configuration of the VMware ESX environment

Regarding the processes of creating and operating a Mail Encryption cluster on the basis of virtual machines in a VMware ESX environment, it is required to configure the safety settings of the vSwitch and the corresponding port groups as follows:

Select “Inventory list-> ESX server -> [Configuration tab] -> Network” within the VMware vSphere client.

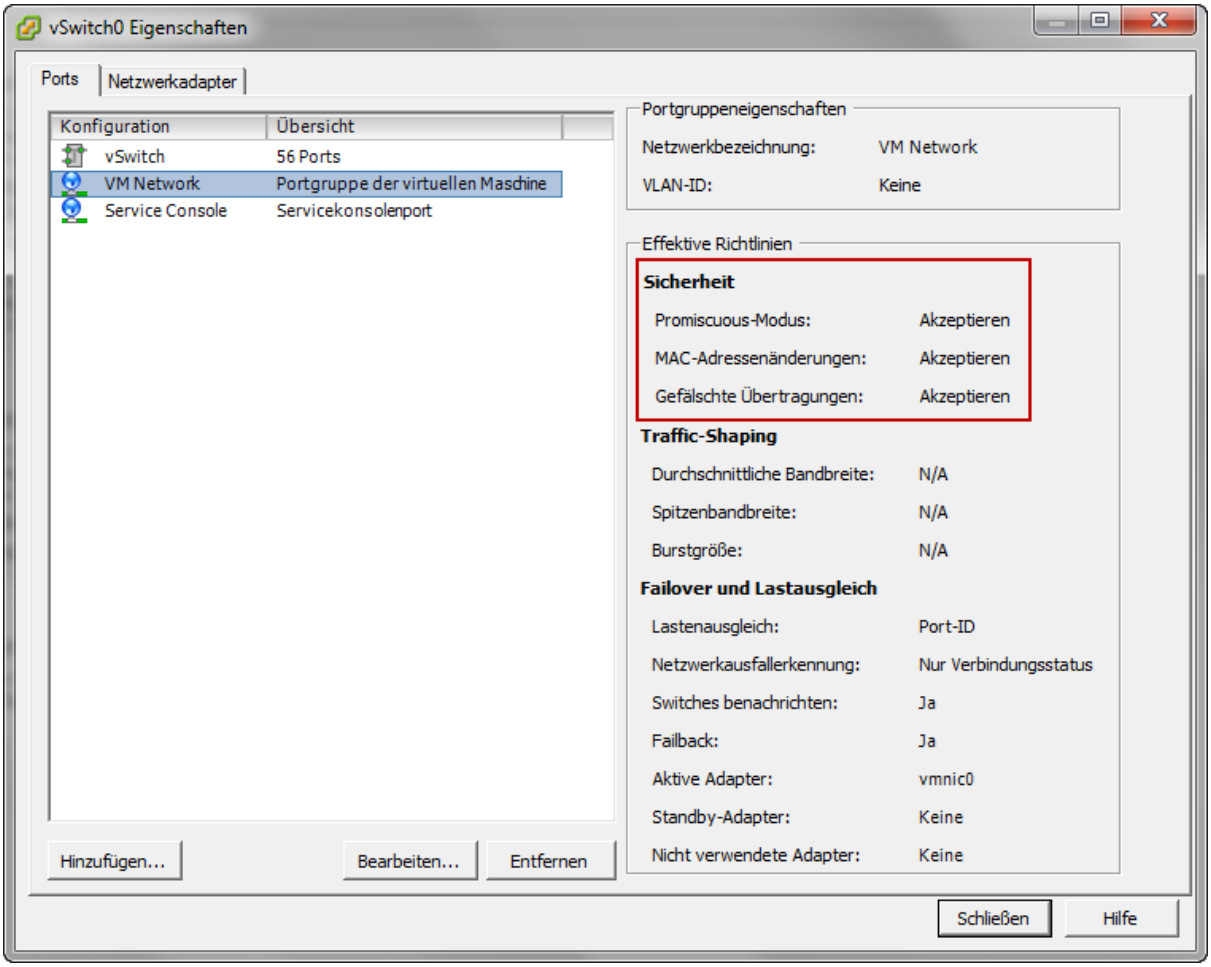


Figure 1 – Safety settings of the port groups within the vSwitch of a VMware ESX system

4.10.6.4 Configuring the basic settings of a Mail Encryption system

In order to configure a Mail Encryption cluster system, you must implement a couple of basic settings on the related system. Any further settings will be replicated automatically to the new cluster member system when a cluster is created or when a new Mail Encryption system is added to an existing cluster. Afterwards, all cluster member systems will synchronise with each other when a modification of the configuration parameters or the transaction data is implemented on a cluster member system. The transaction data contain PGP and S/MIME user certificates/domain certificates, as well as X.509 root certificates.

The basic settings contain the following static, system-specific configuration parameters that are not replicated and synchronised between the cluster member systems:

- all settings in the “System” menu
- the SSL device certificate in the “SSL” menu
- the system licence and the registration data of the system

The log files and statistics within the menus “Logs”, “Webmail Logs”, and “Statistics” are also system-specific and are not replicated. Any other configuration parameters are replicated between the cluster member systems and are synchronised after each modification.

4.10.6.5 Configuring the Mail Encryption cluster systems

The first Mail Encryption system of a cluster must be configured completely. See chapter Commissioning of Mail Encryption 15

The second Mail Encryption system must be configured with the basic settings. This comprises the network configuration and the registration of the system. See chapter EConfiguring the basic settings of a Mail Encryption Systems 142

4.10.6.6 Downloading the cluster identification

A cluster identification is required in order to add a further Mail Encryption system to an existing cluster or to create a cluster with two Mail Encryption systems.

In order to download a cluster identification, please select the “Cluster” menu in the configuration interface. Afterwards, select the “Download Cluster Identifier” button in the “Prepare for Cluster” section. Afterwards, a “Save file” dialogue will be displayed and you can save the cluster identification locally as a file called “clusterid.txt”.

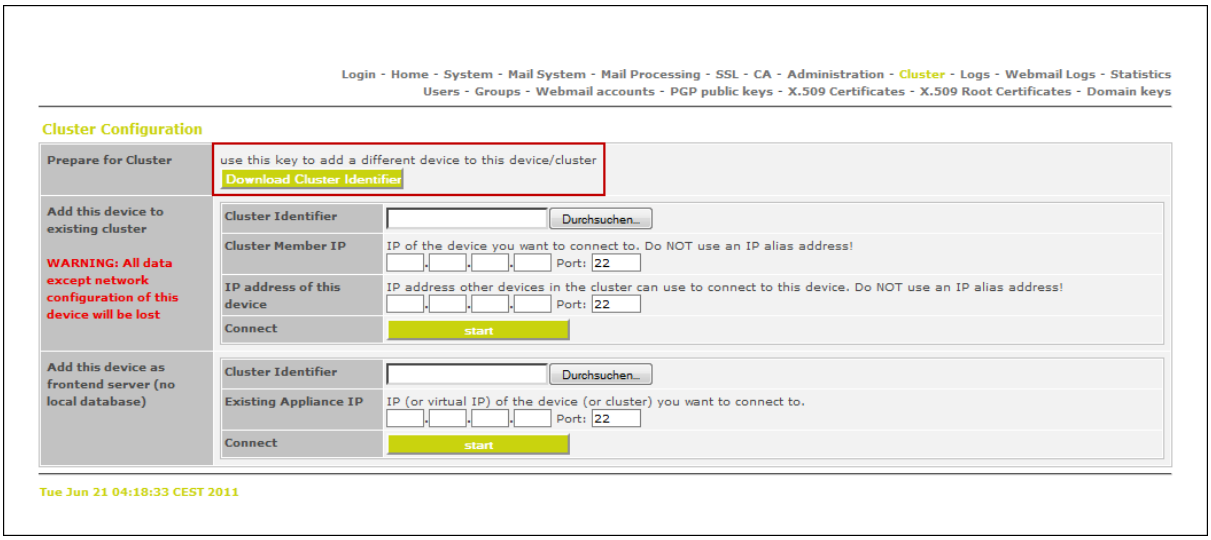


Figure 1 – Downloading the cluster identification

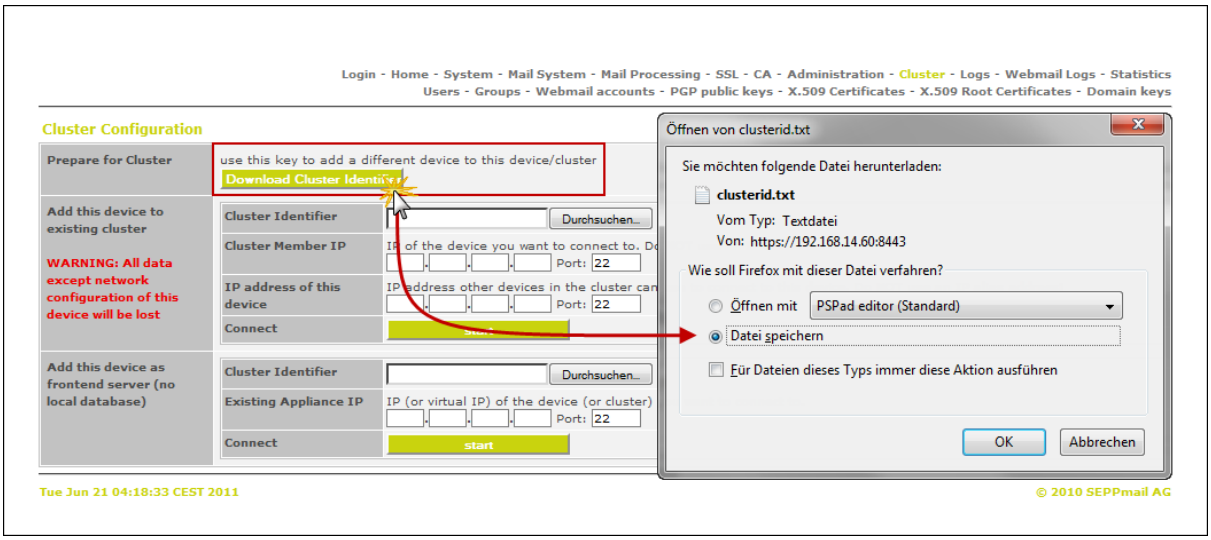


Figure 2 – Downloading and locally saving the cluster identification

4.10.6.7 Configuring the Mail Encryption cluster

At least two systems are required in order to configure a Mail Encryption cluster. As a matter of principle, there is no limitation regarding the number of cluster member systems. You can readily operate 10 systems or more within a cluster. Depending on the specific requirement, this cluster can be configured in a way that all 4 modes of operation are used.

The primary configuration of a Mail Encryption cluster, consisting of at least two systems, is implemented similarly to the process of adding further cluster member systems.

In order to add a EgoSecure Mail Encryption appliance to an existing cluster (or in order to configure a cluster for the first time), please select the "Cluster" menu item in the configuration interface.

For the creation of the cluster the following fields must be completed in the "Add this device to existing cluster" section. For this, please proceed as follows:

1. For the "Cluster Identifier" parameter, please select the file containing the cluster identification that you downloaded.
2. Enter the (physical) IP address of the first Mail Encryption appliance this system is to be added to for the "Cluster Member IP" parameter. If the cluster already contains several appliances, the (physical) address of the cluster member system is sufficient.
3. Enter the proprietary (physical) IP address this appliance is available at for other appliances within the cluster for the Mail Encryption parameter.
4. Please check all values set above. Please exit the procedure by selecting the "Start" button. The cluster will now be created respectively extended by means of replicating the existing cluster configuration to the new cluster member system. All modifications to the configuration within the cluster following after this point in time will immediately be synchronised automatically with the newly added cluster member system.

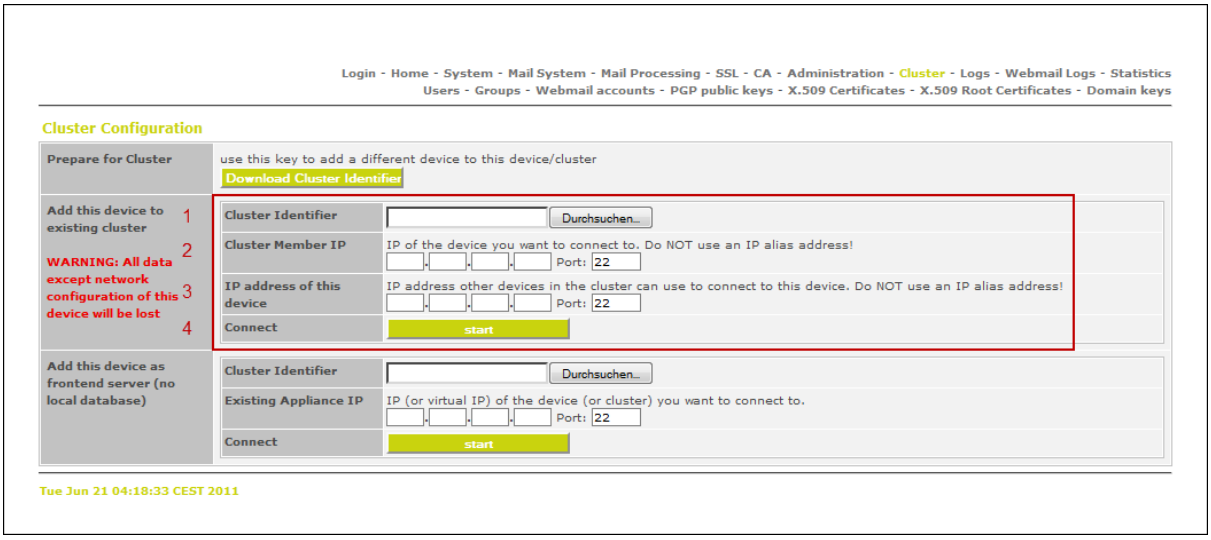


Figure 1 – Adding a Mail Encryption appliance to an existing cluster respectively initial creation of a cluster

After the cluster has been created, the display in the “Cluster” menu will change and the status of the cluster will be displayed now. If you want to remove this system from the cluster, please select the “remove this device from cluster” button in the “remove from cluster” section.

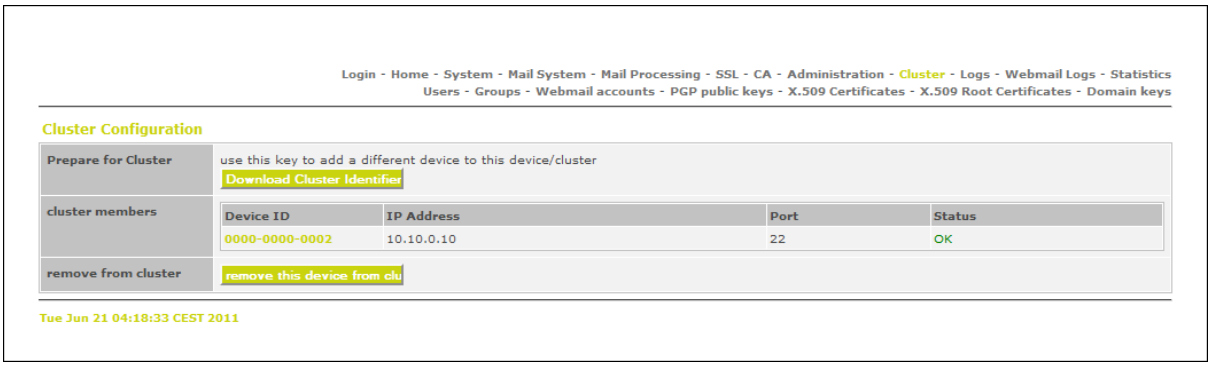


Figure 2 – Cluster status of the 1st cluster member system

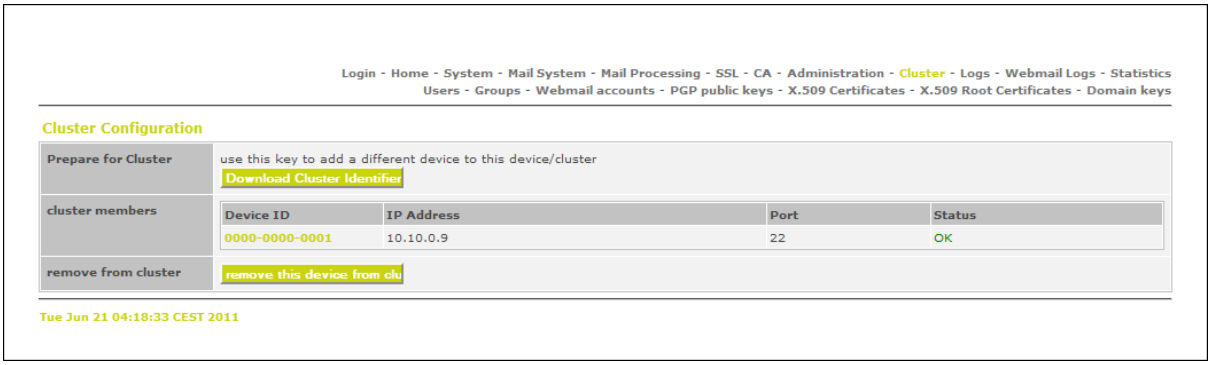


Figure 3 – Cluster status of the 2nd cluster member system

If you add a Mail Encryption system to an existing cluster or if you create a cluster for the first time, the entire existing cluster configuration will be replicated to this new cluster member system and it will be synchronised consistently with the cluster afterwards.

All data on this system, except for the settings contained in the menus “System” and “SSL”, as well as the log files and statistics contained in the menus “Logs”, “Webmail Logs”, and “Statistics”, will be lost.

This is important if the system still contains necessary configuration data, such as S/MIME certificates, PGP keys, secure webmail accounts, etc., for example.

Furthermore, it is important to understand in which order Mail Encryption systems must be added to an existing cluster respectively which system is the source of the replication and which system is the target of the replication. If you confound these systems while creating a new cluster, it may happen, that an existing and configured Mail Encryption system is overwritten with the “empty data” of the newly added system. The aforementioned is even more important regarding an existing cluster if this cluster already consists of several cluster member systems. In this case, confusing the source of replication and the target of replication will result in the

existing cluster being overwritten with “empty data” of the new system.

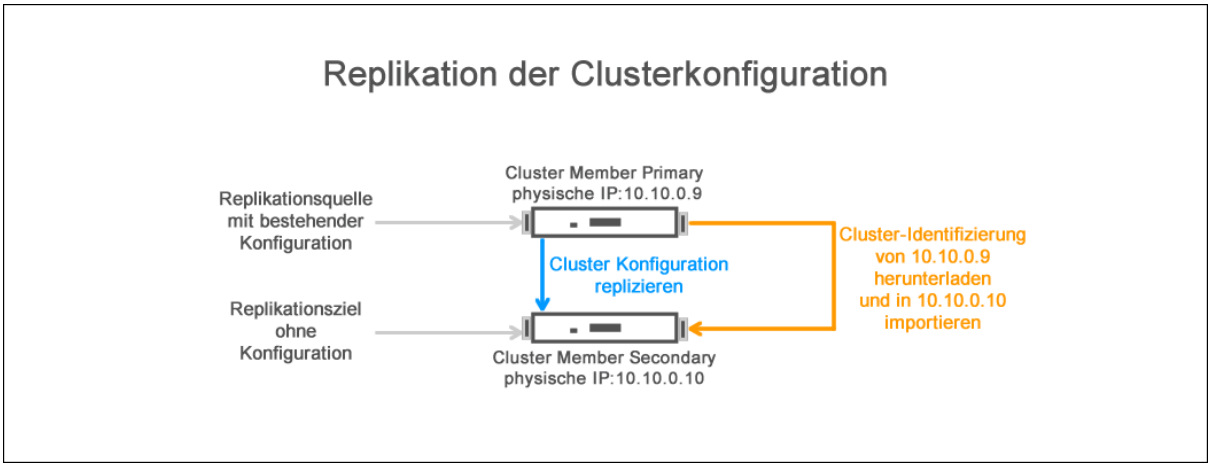


Figure 4 – Schematic representation of the replication of the cluster configuration between two Mail Encryption cluster member systems

Up to this point in time, you configured the primary replication and the then following synchronisation of the configuration data between the cluster member systems. In order to configure a high-availability cluster and load balancing, it is necessary to summarise the individual cluster member systems under one or several virtual cluster IP addresses.

4.10.6.8 Configuring the high-availability cluster

Two different functions are required in order to configure a high-availability cluster.

The "Cluster" menu within the configuration interface must be used to configure and enable the replication and the then following synchronisation of the configuration data of the cluster configuration between the cluster member systems. We already dealt with this item in the previous chapter.

The "System" menu within the configuration interface must be used to configure the monitoring of the cluster member systems amongst each other and the priorities of the individual cluster member systems within the cluster.

The configuration of the virtual cluster IP address(es) is implemented in the "System" menu item (Advanced View) in the "IP ALIAS Addresses" section. This configuration must be implemented in each cluster member system belonging to the cluster.

Regarding the configuration for operation as pure high-availability cluster (failover cluster), the same virtual cluster IP address is configured within the cluster member systems. In this, one system must be configured with the priority "Primary" and one system must be configured with the priority "Backup". See figure 1 and figure 2. We use the IP addresses from the representation in chapter High-availability cluster 126.

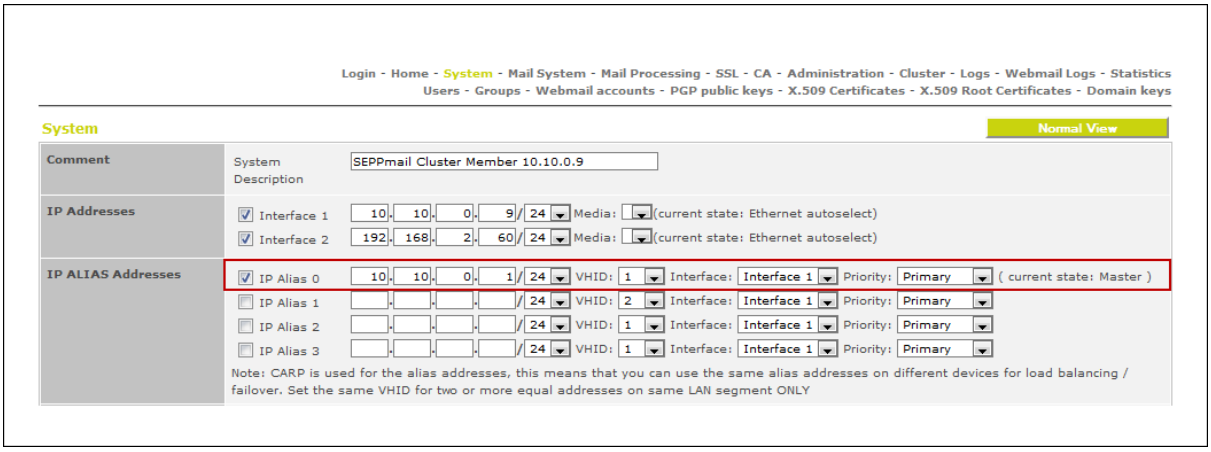


Figure 1 – High-availability cluster – virtual cluster IP address of the 1st Mail Encryption cluster member system

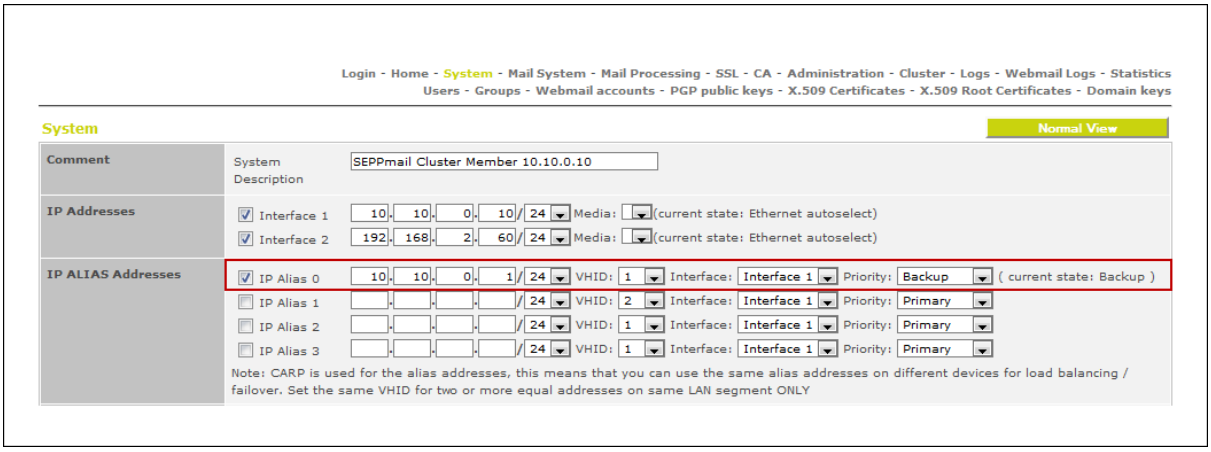


Figure 2 – High-availability cluster – virtual cluster IP address of the 2nd Mail Encryption cluster member system

The two cluster member systems are now summarised under a virtual cluster IP address. When this cluster IP address is addressed, the system having the priority "Primary" will respond. If this system is not available, the system characterised by the priority "Backup" will respond. The status will be switched automatically when the primary system is not available. The system having the status "Backup" will be automatically returned to its initial status as soon as the primary system is available again. In this case it is ensured that incoming and outgoing e-mails can be processed further and that there is no failure regarding the e-mail data flow in the event of an error.

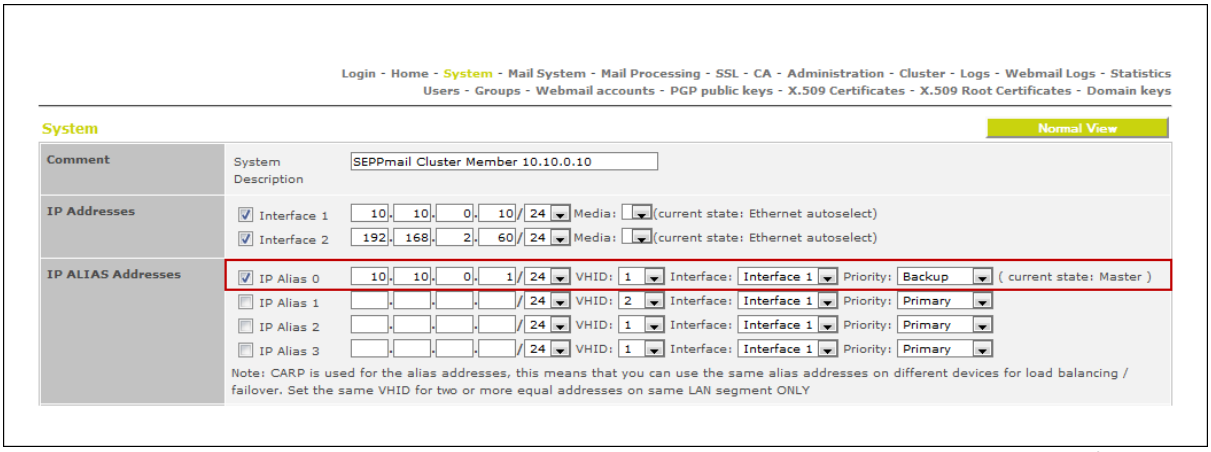


Figure 3 – High-availability cluster – automatic status switch-over of the secondary system (the primary cluster member system is not available)

This way, the cluster configuration is complete. The following must be observed when using a cluster:

- When routing e-mails to the Mail Encryption cluster the virtual cluster IP address should be addressed at all times.
- Within the internal e-mail server and the external MTA, all IP addresses of the cluster must be authorised to deliver e-mails, i.e. all physical and virtual IP addresses of the Mail Encryption cluster (e-mail relay settings of the corresponding components).
- Within the firewall, all IP addresses of the cluster must be authorised to establish an SSH connection (port TCP/22) with the update server within the Mail Encryption computer centre, i.e. all physical and virtual IP addresses of the Mail Encryption cluster.
- Within a cluster the configurations of the two Mail Encryption systems will be synchronised automatically (except for the settings in the "System" menu).

4.10.6.9 Configuring the load balancing cluster

The additional configuration of a load balancing cluster requires an already functionally configured high-availability cluster. A load balancing cluster distributes the data flow for incoming and outgoing e-mails to a cluster member system in each case and allows for an ideal utilisation of the existing system resources.

Each group of cluster member systems is equipped with a virtual IP address, in addition to the individual physical IP addresses of the individual systems. Depending on the assigned priority, the systems will respond when the virtual cluster IP address is addressed. If two or more cluster member systems are characterised by the same priority within the cluster, the systems will respond in the order they were started.

This documentation shows a cluster consisting of two Mail Encryption systems. You can also configure a cluster consisting of three or more systems. In this case, each virtual cluster IP address must be created as additional IP alias address.

Regarding the configuration for operation as high-availability cluster (failover cluster) with a separation of the incoming and outgoing e-mail data flows (load balancing cluster), at least two virtual cluster IP addresses will be configured within the cluster member systems.

One virtual cluster IP address for the incoming e-mail data flow (IP Alias 0) and a second virtual cluster IP address (IP Alias 1) for the outgoing e-mail data flow. This way, in the event of a failure of one cluster member system it is ensured that the second system is able to assume the function of the failed system. In this, one cluster member system must be configured with the priority “Primary” and one cluster member system must be configured with the priority “Backup”. The priorities must be assigned in an opposing manner for each virtual IP address.

Now, two (or even more if 3 systems are used, for example) IP alias addresses are assigned as virtual cluster IP addresses to each cluster member system in each case. Depending on the configured priority, the individual cluster member systems will respond to one virtual cluster IP address in each case. If a system fails, the remaining system can always work as a backup system.

Additionally, an unambiguous “Virtual Host ID” must be assigned to each virtual cluster IP address, because we have bound more than one alias IP address per cluster member system (the “VHID” must be identical for the corresponding virtual cluster IP address on each system).

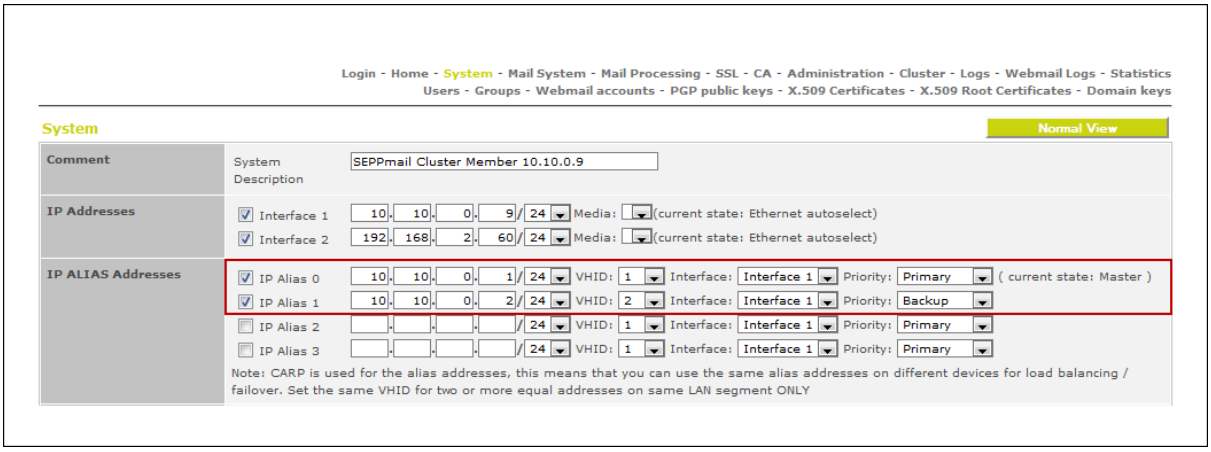


Figure 5 – High-availability cluster with additional load balancing – two virtual cluster IP addresses of the 1st Mail Encryption cluster member system

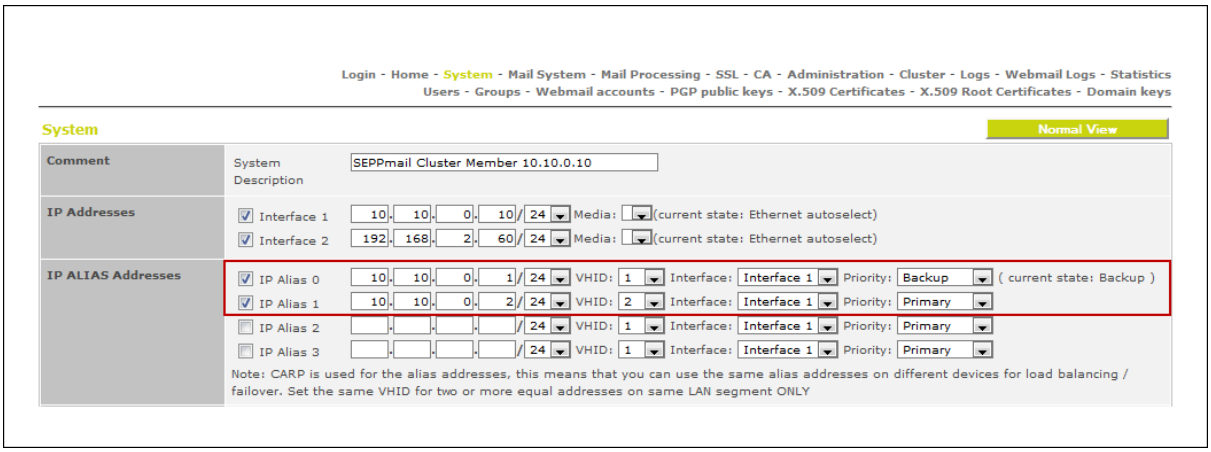


Figure 6 – High-availability cluster with additional load balancing – two virtual cluster IP addresses of the 2nd Mail Encryption cluster member system

This way, the cluster configuration is complete. The following must be observed when using a cluster:

- When routing e-mails to the Mail Encryption cluster the virtual cluster IP address should be addressed at all times.
- Within the internal e-mail server and the external MTA, all IP addresses of the cluster must be authorised to deliver e-mails, i.e. all physical and virtual IP addresses of the Mail Encryption cluster (e-mail relay settings of the corresponding components).
- Within the firewall, all IP addresses of the cluster must be authorised to establish an SSH connection (port TCP/22) with the update server within the Mail Encryption computer centre, i.e. all physical and virtual IP addresses of the Mail Encryption cluster.
- Within a cluster the configurations of the two Mail Encryption systems will be synchronised automatically (except for the settings in the “System” menu).

4.10.6.10 Geo Cluster einrichten

Local Mail Encryption clusters located at several different geographic locations of a company can use a geo cluster to synchronise their configuration data automatically.

We will base the application of a geo cluster on the following scenario.

Along with the company headquarters, a company may have further geographically separated locations and the company can be connected via VPN between these locations. The internal communication within the company is mapped by means of a company-wide groupware system.

For example, each geographic location is equipped with its own internet access for receiving and sending e-mails locally. Each location operates its own groupware servers that are interconnected. The intra-company e-mail communication is mapped by means of this proprietary e-mail transport network.

Each geographic location can send and receive its e-mails by means of its own internet access.

Dynamic e-mail routing allows for sending and receiving e-mails basically at all locations by means of the intra-company e-mail transport network. This requires a separate Mail Encryption cluster for e-mail signature and e-mail decryption and encryption at each location in each case.

The Mail Encryption clusters configured locally at each location are configured as high-availability clusters in each case. Therefore, each cluster at the different locations would be a self-dependent, but locally limited system in which the cluster member systems monitor each other and synchronise their configuration with each other.

In order to additionally configure the global synchronisation of the individual cluster systems between the geographically separated locations, we can configure a geo cluster, also known as “multi-site system”. A geo cluster synchronises the configurations between the individual local cluster systems of the geographically separated locations for a global Mail Encryption cluster system. Such a system is called a geo cluster. It connects all local cluster systems of the geographically separated locations to one company-wide geo cluster.

Within this geo cluster, all modifications to the configuration that are implemented with regard to one Mail Encryption cluster member system will be synchronised immediately to all cluster member systems at all locations automatically. This way, it is ensured that the required data is available at each point in time, such as new user accounts, including user certificates or secure webmail accounts, on all cluster member systems. A manual configuration of each individual system respectively a manual synchronisation of the configuration between the cluster member systems is no longer required and reduces the administrative effort required for configuration purposes.

How can I configure a geo cluster?

When a geo cluster is configured, a cluster member system at location B will be added to a cluster member system at location A. These cluster member systems are not connected by means of a virtual cluster IP address, as is the high-availability and load balancing cluster. There will only be a synchronisation of the configuration data.

For this, please proceed in accordance with the description in chapters Downloading the cluster identification 142 and Configuring a Mail Encryption cluster 144

4.10.6.11 Configuring the frontend-backend cluster

If, due to reasons of safety, you wish to operate a newly added Mail Encryption system without local database (e.g. user certificates, domain certificates, etc.), you can alternatively add the new system as frontend server. In this, the actual configuration and user data are stored to the remaining Mail Encryption systems operating as backend server appliances. For this, select the “Cluster” menu item in the configuration interface.

In order to add the new Mail Encryption system as frontend server to an existing cluster, all fields in the “Add this device as frontend server (no local database)” section must be completed. For this, please proceed as follows:

1. For the “Cluster Identifier” parameter, please select the file containing the cluster identification that you downloaded. See chapter Downloading the cluster identification 142.
2. Enter the physical IP address of the cluster member system respectively the alias IP address of the existing cluster you want to establish a connection to for parameter “Existing Appliance IP”.
3. Please check all values set above. Please exit the procedure by selecting the “Start” button.

No adaptation is required for the backend servers.

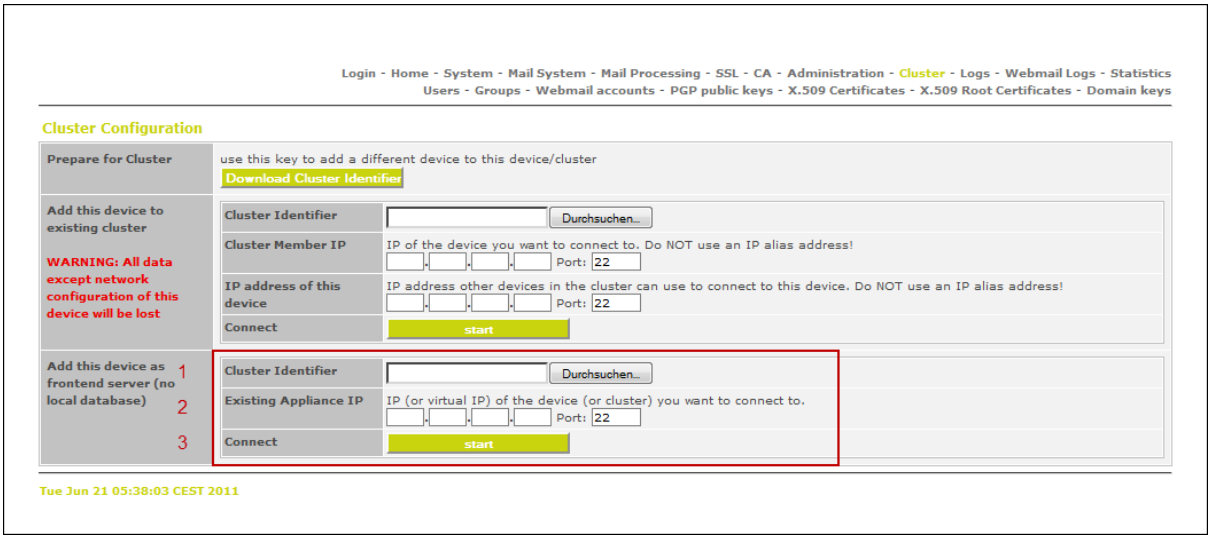


Figure 1 – Adding a Mail Encryption appliance as frontend server to an existing cluster member system respectively to the cluster

4.11 Menu Item "Logs"

Select the “Logs” menu item in order to manage the e-mail log files and to display the log information of the most recent 500 e-mail transactions. The most recent e-mail transactions are listed in the “Mail Log (last 500)” section.

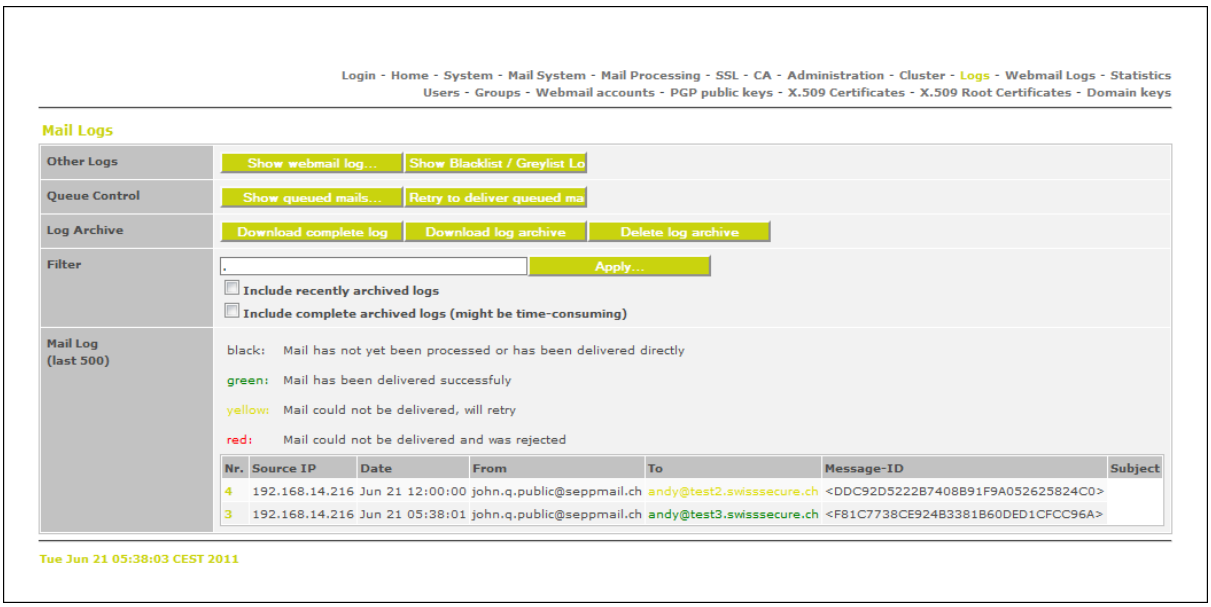


Figure 1 – “Logs” menu

Section – Parameter – Description5

Section: Other Logs

Button “Show webmail log...”
Button “Show Blacklist / Greylist Log...”

Section: Queue Control

See chapter Display e-mails in the queue 155

Button “Show queued mails...” – Select the “Show queued mails...” button in order to display the e-mails that are currently located in the queue.

Button “Retry to deliver queued mails...” – Select the “Retry to deliver queued mails...” button in order to trigger the delivery of e-mails that are in the queue.

Section: Log Archive

Button “Download complete log” – Select the “Download complete log” button in order to view the entire e-mail log file. The current e-mail log file contains the current and the archived log information.

Button "Download log archive" – Select the "Download log archive" button in order to view all archived log information.

Button "Delete log archive" – Select the "Delete log archive" button in order to delete the log archive.

Section: Filter

You can use this input field to enter the values the log files are to be browsed for. As a result you will receive an overview containing the log information corresponding to the specified filter values.

Additionally, please select the "Include recently archived logs" option, because recently archived log information will also be integrated into the search this way.

In order to apply the filter to all archived log files, please select the "Include complete archived logs (might be time-consuming)" option. Depending on the size of the archived log files, it may take some time until the result can be displayed.

Section: Mail log (last 500)

You can use this section to view the log file entries of the most recent 500 e-mail transactions. This is the quickest and most common way of viewing log information.

Colour code for the current processing status of an e-mail:

black: The e-mail was not processed yet or was delivered directly.
green: The e-mail was delivered successfully.
yellow: The e-mail could not be delivered successfully; this procedure will be repeated in intervals
red: The e-mail could not be delivered and was rejected.

You can view the processing status of an e-mail in the "To" column (recipient e-mail address). The recipient e-mail address is displayed in accordance with the colour codes mentioned above. This way, you can identify deviations regarding the processing of incoming and outgoing e-mails in a quick manner.

The most recent e-mail transactions are displayed with the following details:

No.	A serial enumeration of the e-mail messages. The value of this column is highlighted in colours and also serves as a link to the detailed view of the log information. Select this link and you can view the entire log information for this e-mail.
Source IP	IP address of the sender. The IP address describes the e-mail server that sent the e-mail directly to Mail Encryption. (This does not mean the corresponding workstation computer.)
Date	The date the e-mail was sent.
From	E-mail address of the sender
To	E-mail address of the recipient

Message-ID	Unambiguous identification of the e-mail
Subject	Subject line of the corresponding e-mail

Reference of the menu parameters in the “Logs” menu item

4.11.1 Display e-mails in the queue

E-mails currently queued will be displayed with the following details:

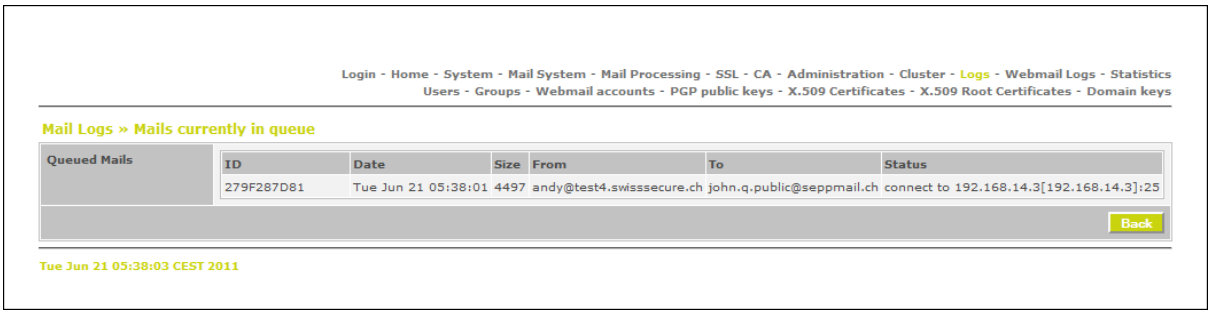


Figure 1 – Displaying e-mails that are located in the queue

Section – Parameter – Description

Section: Queued Mails

ID

Unambiguous identification of the corresponding message

Date

The date the corresponding e-mail was sent

Size

Size of the e-mail

From

E-mail address of the sender

To

E-mail address of the sender

Status

The current status of e-mail dispatch

Reference of the parameters in the “Mail Logs > Mails currently in queue” menu item

4.12 Menu Item "Webmail Logs"

Dieses Kapitel beschreibt die Verwaltung der EgoSecure Mail Encryption Logdateien. Um die letzten 500 EgoSecure Mail Encryption Bewegungen anzuzeigen, wählen Sie in der Konfigurationsoberfläche den Menu Item »Webmail Logs«.

Die letzten EgoSecure Mail Encryption Bewegungen sind in der Sektion »Webmail Log (last 500)« aufgelistet.

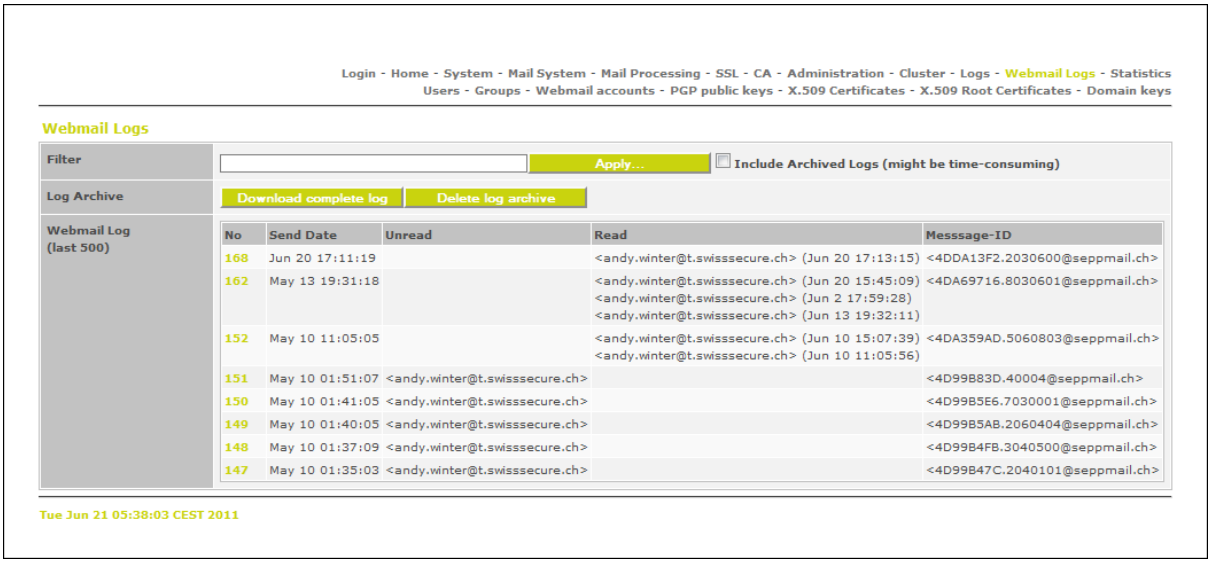


Abbildung 1 - Menü »Webmail Logs«

Section – Parameter – Description

Section: Filter

You can use this input field to enter the values the log files are to be browsed for. As a result you will receive an overview containing the log information corresponding to the specified filter values. Additionally, please select the "Include Archived Logs (might be time-consuming)" option, because already archived log files can also be browsed for the filter values this way. Depending on the size of the archived log files, it may take some time until the result can be displayed.

Section: Log Archive

Button "Download complete log" – Select the "Download complete log" button in order to view the entire EgoSecure Mail Encryption log file.

Button "Delete log archive" – Select the "Delete log archive" button in order to delete the historic log files from the system completely.

Section: Webmail log (last 500)

You can use this section to view the log file entries of the most recent 500 EgoSecure Mail Encryption

transactions.

The most recent EgoSecure Mail Encryption transactions are displayed with the following details:

No	A serial enumeration of the EgoSecure Mail Encryption messages. The value of this column is highlighted in colours and also serves as a link to the detailed view of the log information. Select this link and you can view the entire log information for this EgoSecure Mail Encryption.
Send Date	The date the EgoSecure Mail Encryption was sent.
Unread	E-mail address of the recipient of the EgoSecure Mail Encryption, if he/she has not read the message yet. If the EgoSecure Mail Encryption was sent to several recipients, only the e-mail addresses of the recipients who have not read this message yet will be displayed in this column.
Read	E-mail address of the recipient of the EgoSecure Mail Encryption, if he/she has already read the message. If the EgoSecure Mail Encryption was sent to several recipients, only the e-mail addresses of the recipients who have already read this message will be displayed in this column.
Message-ID	An unambiguous identification of the corresponding EgoSecure Mail Encryption message.

Reference of the menu parameters in the “Webmail Logs” menu item

4.13 Menu Item "Statistics"

Please select the “Statistics” menu item in order to display a statistical analysis of the Mail Encryption system data.

The overview will display the statistics for throughput, technology, anti-spam, processor, and memory statistics. These statistics will be displayed for the time intervals Today, Last Week, Last Month, Last Year, and the last 3 years.

Figure 1 contains an example for a corresponding statistics.

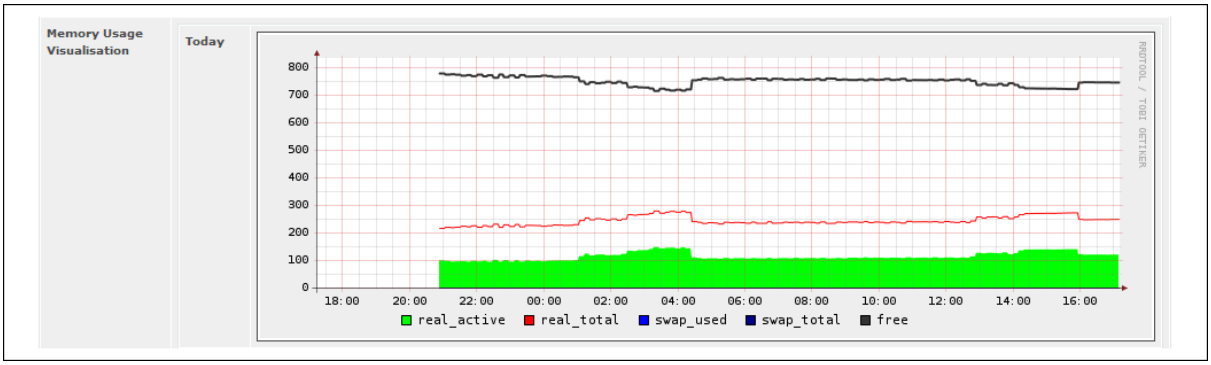


Figure 1 – Statistics regarding the utilisation of the internal memory

Section – Parameter – Description

Section: Throughput Visualisation

You will see the number of sent and received messages and the number of implemented encryption and decryption procedures. Additionally, the number of messages processed on average and the value regarding the maximum number of processed messages per minute in the corresponding period of interest will be displayed

Today	Throughput statistics for the following time interval: today
Last Week	Throughput statistics for the following time interval: last week
Last Month	Throughput statistics for the following time interval: last month
Last Year	Throughput statistics for the following time interval: last year
Last 3 Years	Throughput statistics for the following time interval: last 3 years

Section: Technology Visualisation

You will see the number of processed e-mails separated in accordance with the types secure webmail, S/MIME, OpenPGP, and domain encryption. Additionally, the number of messages processed on average and the value regarding the maximum number of processed messages per minute in the corresponding period of interest will be displayed.

Today	Technology statistics for the following time interval: today
Last Week	Technology statistics for the following time interval: last week
Last Month	Technology statistics for the following time interval: last month
Last Year	Technology statistics for the following time interval: last year
Last 3 Years	Technology statistics for the following time interval: last 3 years

Section: Spam Visualisation

You will see the number of received messages, the number of spam identifications, and the number of e-mails that were treated on the basis of blacklisting or greylisting. Additionally, the number of spam messages processed on average and the value regarding the maximum number of processed spam messages per minute in the corresponding period of interest will be displayed.

Today	Spam statistics for the following time interval: today
Last Week	Spam statistics for the following time interval: last week
Last Month	Spam statistics for the following time interval: last month
Last Year	Spam statistics for the following time interval: last year
Last 3 Years	Spam statistics for the following time interval: last 3 years

Section: CPU Usage Visualisation

You will see the processor utilisation separated in accordance with system processing, processing in user mode (execution of applications), and processes that were controlled by the nice utility with regard to the process priority.

Today	Statistics on the processor utilisation for the following time interval: today
Last Week	Statistics on the processor utilisation for the following time interval: last week
Last Month	Statistics on the processor utilisation for the following time interval: last month
Last Year	Statistics on the processor utilisation for the following time interval: last year
Last 3 Years	Statistics on the processor utilisation for the following time interval: last 3 years

Section: Memory Usage Visualisation

You will see the active and the total utilisation of the internal memory, memory removals, as well as free capacities of the internal memory.

Today	Internal memory statistics for the following time interval: today
Last Week	Internal memory statistics for the following time interval:last week
Last Month	Internal memory statistics for the following time interval: last month
Last Year	Internal memory statistics for the following time interval: last year

Last 3 Years	Internal memory statistics for the following time interval: last 3 years

Reference of the menu parameters in the “Statistics” menu item

4.14 Menu Item "Users"

Select the “Users” menu item in order to manage the internal users of the Mail Encryption appliance.

The following processes will be described in the following sections:

4.14.1 Overview Menu Item "Users"

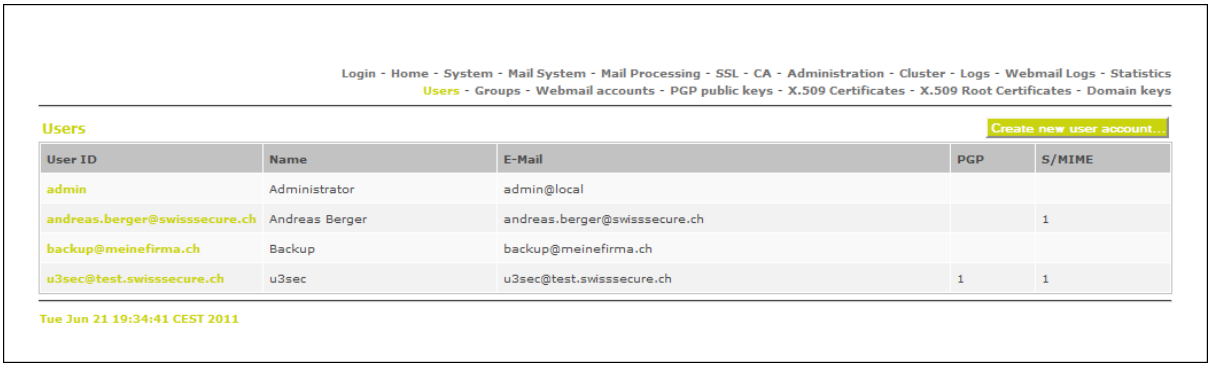


Figure 1 – "Users" menu

Section – Description

User ID

Name of the user account for logging in to the Mail Encryption configuration interface.

Name

Actual user name, e.g. Robert Lander

E-Mail

E-mail address of the user

PGP

Number of the PGP user keys installed in the user account

S/MIME

Number of the S/MIME user certificates installed in the user account

Reference of the menu parameters in the "Users" menu item

4.14.2 Creating internal users

In order to create a new internal user, please select the "Users" menu item in the configuration interface. In order to create an internal user, please select the "Create new user account..." button.

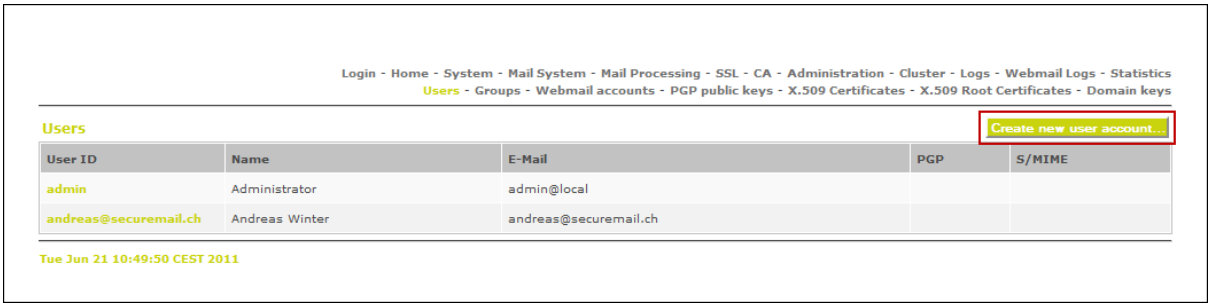


Figure 1 – Creating an internal user

Please complete the following fields in order to create the user:

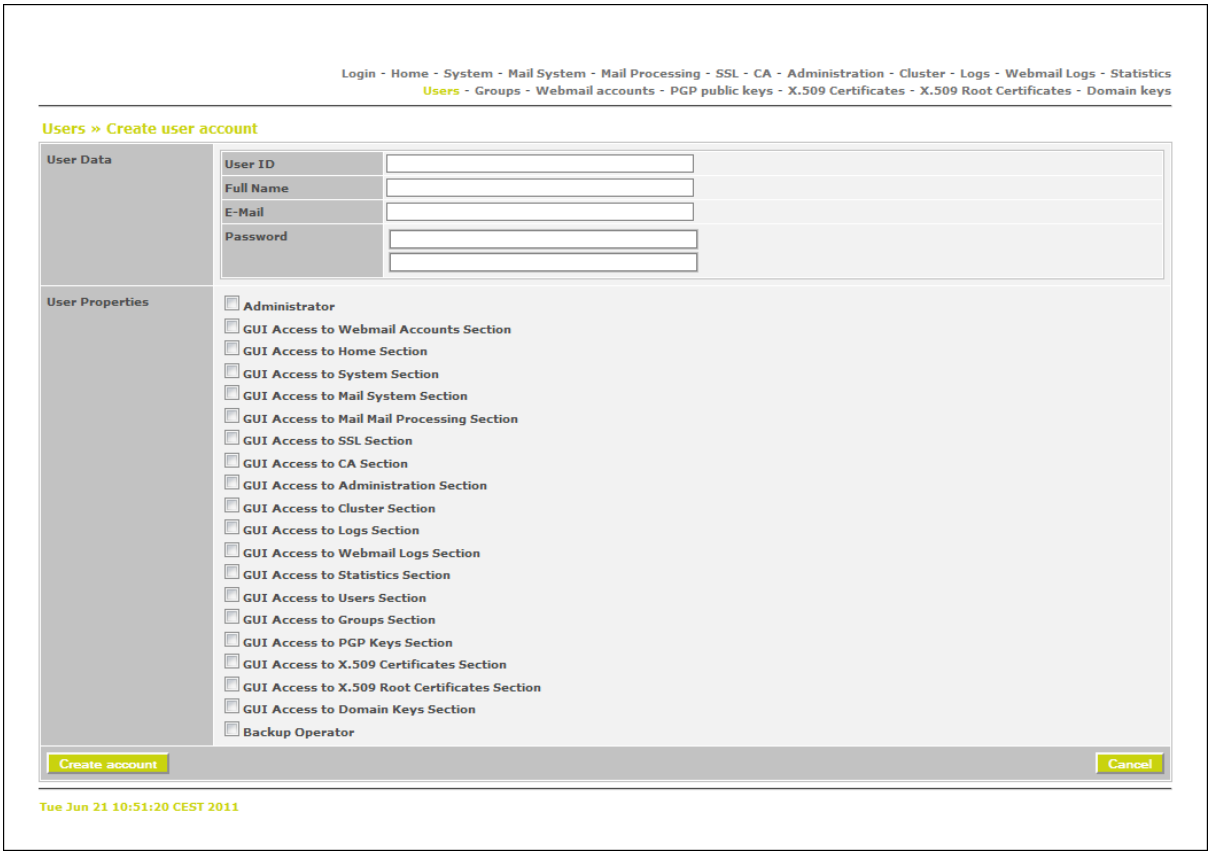


Figure 2 – Creating an internal user

Section – Parameter – Description

Section: User Data

User ID

ID of the user

Full Name

Full name of the user

Note:
It is absolutely required to enter the full name of the user, because this value is required for the creation of user certificates.

E-Mail

E-mail address of the user

Password

Password (please enter the password twice)

Note:
A password for the user is only required if the user will receive administrative rights regarding the configuration interface. The authorisation regarding the access to certain menu items can be defined by selecting the groups..

Section: User Properties

Groups the user is to be added to.

Reference of the menu parameters in the “Users > Create new user” menu item

4.14.3 Managing internal users

In order to manage internal users, please select the “Users” menu item in the configuration interface.

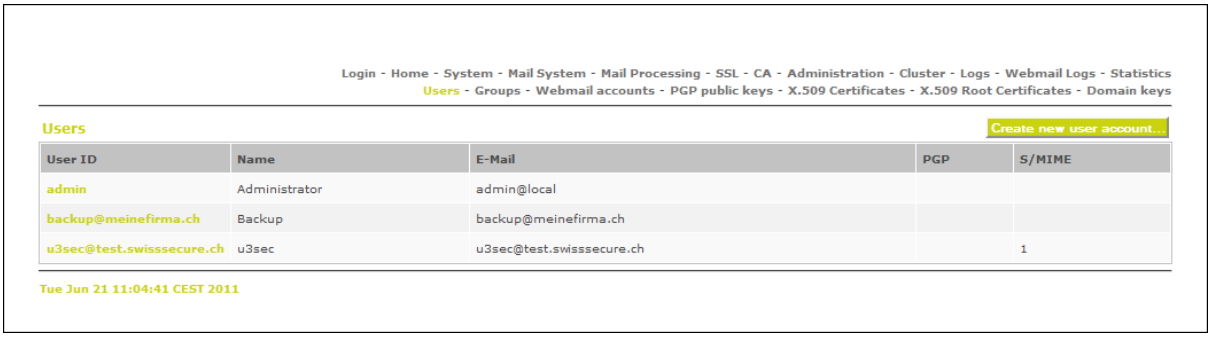


Figure 1 – Managing internal users

In order to edit the details of a user, please click the User ID of the corresponding user. You can implement the following settings then:

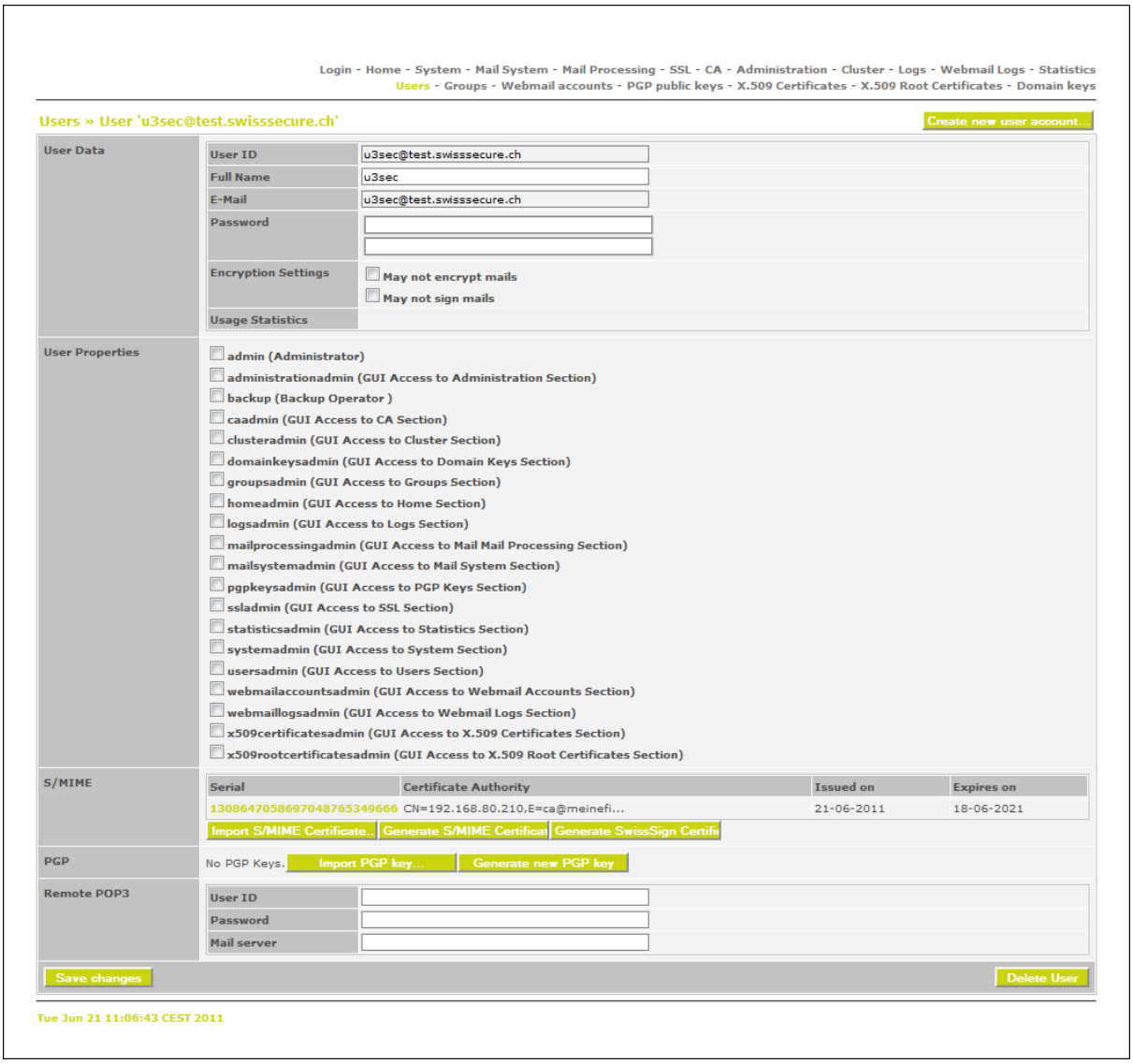


Figure 2 – Editing user details

Section – Parameter – Description

Section: User Data

User ID

ID of the user

Full Name

Full name of the user

Note:
It is absolutely required to enter the full name of the user, because this value is required for the creation of user certificates.

E-Mail

E-mail address of the user

Password

Password (please enter the password twice)

Note:
A password for the user is only required if the user will receive administrative rights regarding the configuration interface. The authorisation regarding the access to certain menu items can be defined by selecting the groups

Encryption Settings

May not encrypt mails	prohibit e-mail encryption
May not sign mails	prohibit e-mail signature

Prohibiting e-mail encryption and/or e-mail signature:
In order to prevent that a user is enabled to encrypt and/or sign e-mails, please enable the checkbox May not encrypt mails respectively May not sign mails. A user both of the checkboxes are enabled for does not occupy any user licence on the Mail Encryption appliance.

Note:
You can use this option to disable the account of an employee leaving the company regarding the outgoing e-mail encryption and e-mail signature, for example. Incoming encrypted e-mails for this employee can then be further decrypted and forwarded to the internal e-mail server in clear text.

If you deleted the user account, it would not be possible to decrypt any incoming encrypted e-mails for this user. The user certificate of an employee who left the company can exist further and can be used further for encryption purposes with the external communication partner.

Usage Statistics

Different statistical data regarding the usage of the functions of the Mail Encryption appliance by the corresponding user will be displayed here.

Section: User Properties

Groups the user is to be added to.

Section: S/MIME

Serial

Serial number of the certificate

Certificate Authority

Subject of the CA that has issued this certificate

Issued on

Date the certificate was issued

Expires on

Date of expiration of the key

Buttons

Import OpenPGP certificate – Select the “Import PGP key...” button in order to import an existing OpenPGP certificate..

Generate OpenPGP certificate – Select the “Generate new PGP key” button in order to create a new OpenPGP certificate for the user by the Mail Encryption appliance self-dependently.

.

Section: PGP

Key ID

Identification of the key

User ID

ID of the user

Issued on

Date the key was issued

Expires on

Date of expiration of the key

Buttons

Import OpenPGP certificate – Select the “Import PGP key...” button in order to import an existing OpenPGP certificate.
Generate OpenPGP certificate – Select the “Generate new PGP key” button in order to create a new OpenPGP certificate for the user by the Mail Encryption appliance self-dependently.

Section: Remote POP3

Enter the POP3 authentication details of the user in order to retrieve e-mails of the user from a POP3 server at regular intervals.

ID

User name

Password

Password

Mail server

IP address or host name of the POP3 e-mail server the e-mails are to be fetched from

Reference of the menu parameters in the “Users > Detailed view of the user” menu item

4.15 Menu Item "Groups"

Select the “Groups” menu item in order to manage the group structure of the Mail Encryption appliance.

The following processes will be described in the following sections:

4.15.1 Overview Menu Item "Groups"

If you want to provide further users with administrative rights regarding the configuration interface in addition to the “admin” user, you can make a user a member of different groups. The group structure corresponds to the individual menu items.

The aforementioned does not include the “backup (Backup Operator)” group. This group does not serve for assigning authorisations regarding menu items of the configuration interface. Using the “Groups” menu item you will be provided with an overview over all users assigned to the corresponding groups.

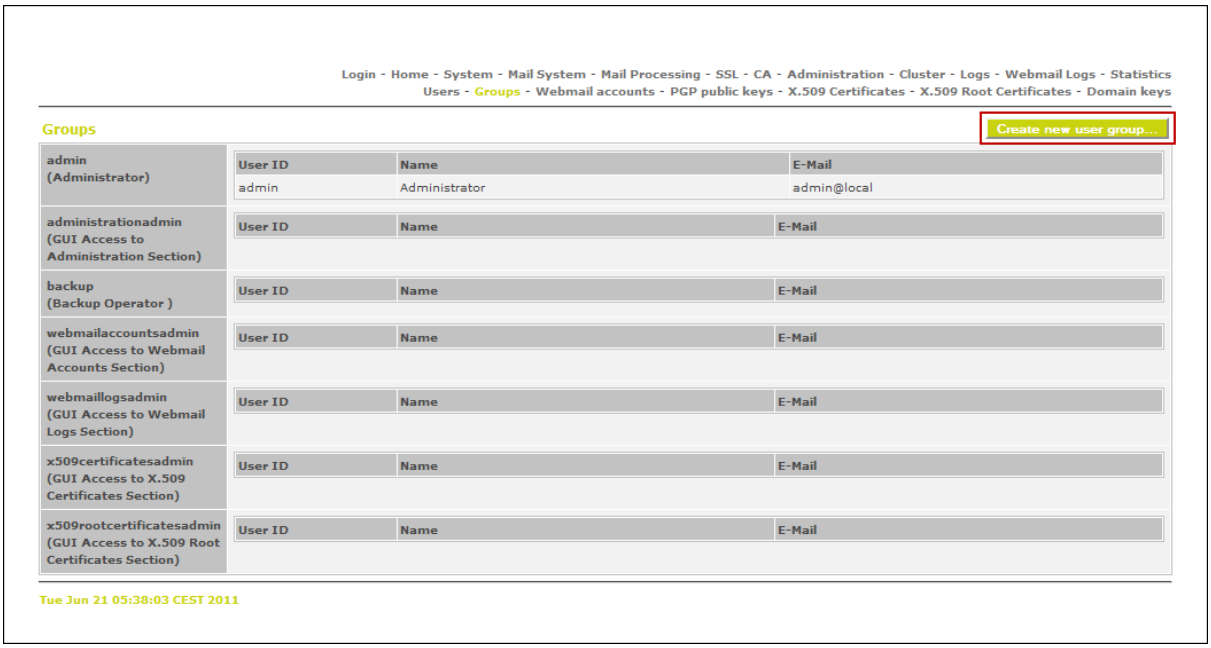


Figure 1 – “Groups” menu (selection)

Group	Description
	Select the “Create new user group...” button in order to create a new user group. See chapter Creating groups 172. Groups that were created once cannot be subsequently deleted.
admin (Administrator)	All members of this group are on the same level as the default user “admin” and have unlimited administrative access to the configuration interface, including all authorisations. In order to make a user equivalent to the default user “admin” in terms of safety, you must add this user to the “admin (Administrator)” group.
administrationadmin (GUI Access to Administration Section)	All members of this group will be provided with access to the “Administration” menu in the configuration interface.
backup (Backup Operator)	This group is assigned a special importance. It differs from the system groups regarding access to the configuration interface by the fact that no access to the configuration interface is implemented. All

Group	Description
	members of this group will receive the system backup of the corresponding system once a day via e-mail. The system backup is created daily at 12 pm and is sent to all members of this group via e-mail.
caadmin (GUI Access to CA Section)	All members of this group will be provided with access to the “CA” menu in the configuration interface.
clusteradmin (GUI Access to Cluster Section)	All members of this group will be provided with access to the “Cluster” menu in the configuration interface..
domainkeysadmin (GUI Access to Domain Keys Section)	All members of this group will be provided with access to the “Domain keys” menu in the configuration interface.
groupsadmin (GUI Access to Groups Section)	All members of this group will be provided with access to the “Groups” menu in the configuration interface..
homeadmin (GUI Access to Home Section)	All members of this group will be provided with access to the “Home” menu in the configuration interface.
logsadmin (GUI Access to Logs Section)	All members of this group will be provided with access to the “Logs” menu in the configuration interface.
mailprocessingadmin (GUI Access to Mail Mail Processing Section)	All members of this group will be provided with access to the “Mail Processing” menu in the configuration interface.
mailsystemadmin (GUI Access to Mail System Section)	All members of this group will be provided with access to the “Mail System” menu in the configuration interface.
pgpkeysadmin (GUI Access to PGP Keys Section)	All members of this group will be provided with access to the “PGP public keys” menu in the configuration interface.
ssladmin (GUI Access to SSL Section)	All members of this group will be provided with access to the “SSL” menu in the configuration interface.
statisticsadmin (GUI Access to Statistics Section)	All members of this group will be provided with access to the “Statistics” menu in the configuration interface. .
systemadmin (GUI Access to System Section)	All members of this group will be provided with access to the “System” menu in the configuration interface..

Group	Description
usersadmin (GUI Access to Users Section)	All members of this group will be provided with access to the “Users” menu in the configuration interface.
webmailaccountsadmin (GUI Access to Webmail Accounts Section)	All members of this group will be provided with access to the “Webmail accounts” menu in the configuration interface..
webmaillogsadmin (GUI Access to Webmail Logs Section)	All members of this group will be provided with access to the “Webmail logs” menu in the configuration interface.
x509certificatesadmin (GUI Access to X.509 Certificates Section)	All members of this group will be provided with access to the “X.509 Certificates” menu in the configuration interface.
x509rootcertificatesadmin (GUI Access to X.509 Root Certificates Section)	All members of this group will be provided with access to the “X.509 Root Certificates” menu in the configuration interface..

Reference of the menu parameters in the “Groups” menu item

4.15.2 Creating groups

In order to create a new group, please select the “Groups” menu item in the configuration interface and then select the “Create new user group...” button. Enter the name of the new group, including a short description, and select the “Create” button afterwards in order to save the creation of the new group.

Note:

Deleting a group created once is not possible subsequently. .

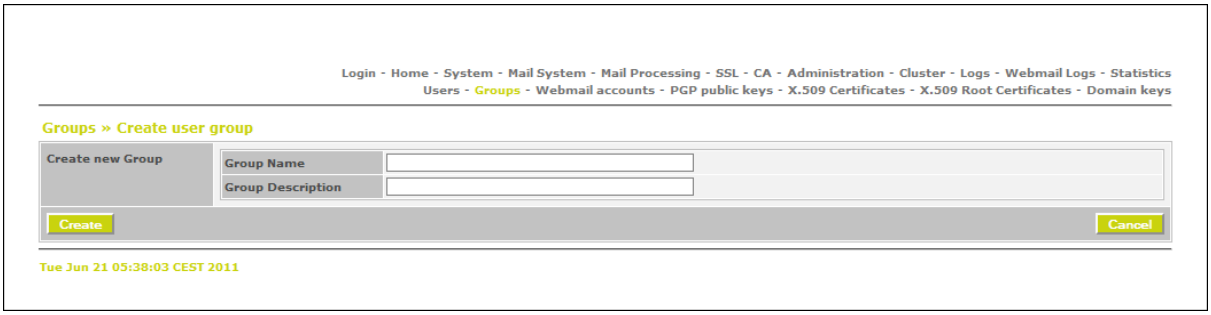


Figure 1 – Creation of a new group

Section – Parameter – Description

Section: Create new Group

Group Name

Name of the new group

Group Description

Short description of the new group

Reference of the menu parameters in the “Groups > Create user group” menu item

4.15.3 Managing groups

Depending on their role, users can be assigned to one or several groups. In order to manage internal groups, please select the “Groups” menu item in the configuration interface.

All members of the “backup (Backup Operator)” group will receive the system backup of the corresponding system once a day via e-mail. The system backup is created daily at 12 pm and is sent to all members of this group via e-mail. (See chapter Creating a backup user) 38.

The further pre-defined groups enable their members to manage the Mail Encryptionappliance. For example, the members of the “webmailaccountsadmin” are allowed to access the “Webmail accounts” menu item in the Mail Encryption configuration interface.

There is a corresponding group for every menu item in the configuration interface, mentioned with “GUI Access to...” in each case. This way, different administration assignments can be transferred to several persons.

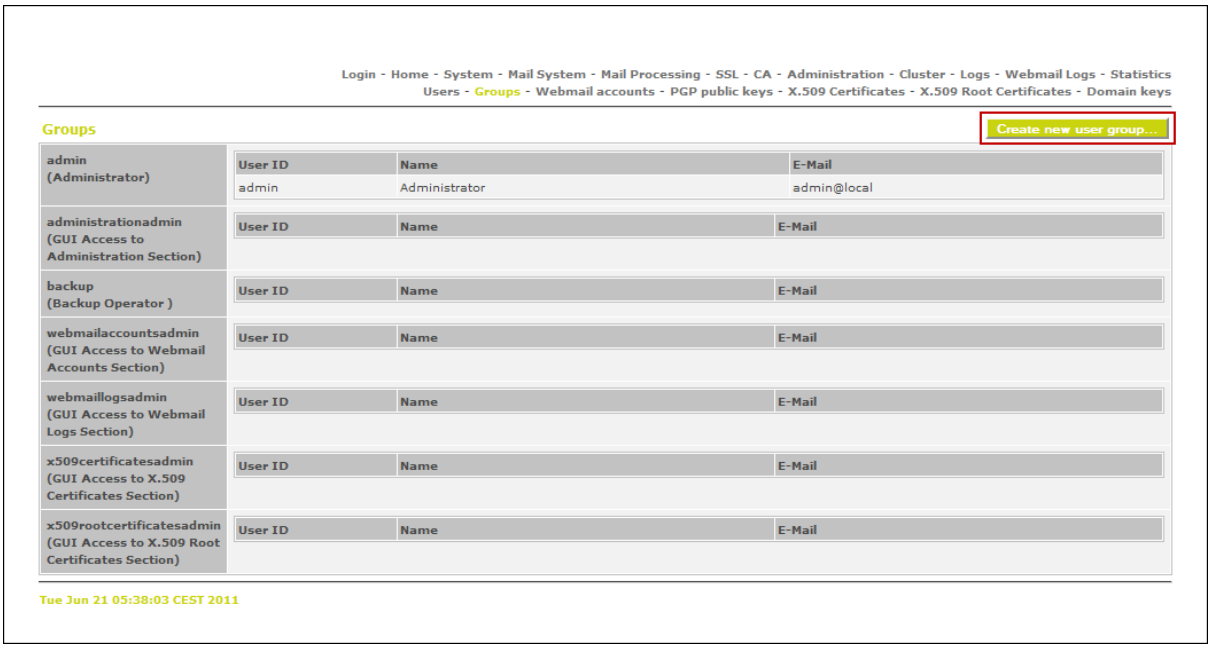


Figure 1 – “Groups” menu Managing groups (selection)

4.16 Menu Item "Webmail accounts"

Select the “Webmail accounts” menu item to manage the webmail accounts of the Mail Encryption appliance created automatically.

The following processes will be described in the following sections:

4.16.1 Overview Menu Item "Webmail accounts"

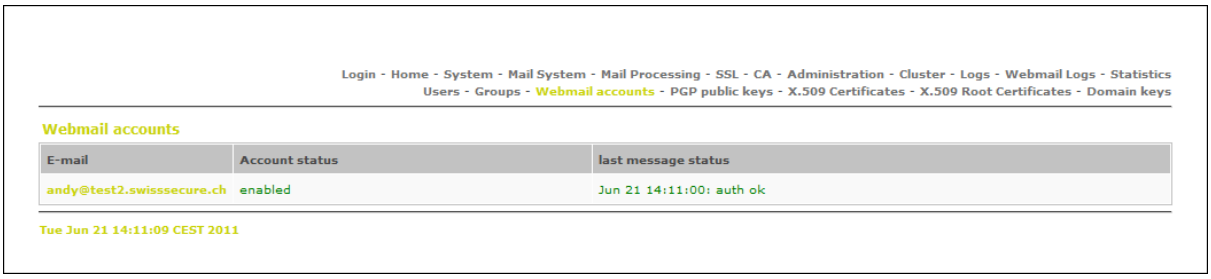


Figure 1 – “Webmail accounts” menu item

Section – Description

E-mail

E-mail address of the EgoSecure Mail Encryption recipient

Account status

Administrative status of the EgoSecure Mail Encryption user account of the recipient. The “Account status” can display the following values:

locked	The EgoSecure Mail Encryption account of the recipient is blocked.
enabled	The EgoSecure Mail Encryption account of the recipient is active.

last message status

The status of the last user interaction of the recipient is displayed in this column. The “last message status” can display the following values:

<Statusmeldung>	If a status message is displayed in red, the last user interaction, e.g. the user login to the EgoSecure Mail Encryption account, was not implemented successfully	
	Examples:	
	May 2 18:00:00: auth failure, pwdCount 4	The user password of the recipient was entered incorrectly for 4 times.
	May 2 18:00:00: auth failure, disable account	The user account of the recipient was disabled after the user password was entered incorrectly 4 times..
<Statusmeldung>	If the status message is displayed in green, the last user interaction, e.g. reading an EgoSecure Mail Encryption, was implemented successfully	
	Examples:	
	May 2 18:00:00: success. message-ID: <4DA69716.8030601@freidenker.ag>	An EgoSecure Mail Encryption was decrypted and displayed successfully by the recipient..
	May 2 18:00:00: auth ok	The recipient managed to successfully log into his/her EgoSecure Mail Encryption user account.

Reference of the menu parameters in the “Webmail accounts” menu item

4.16.2 Disabling webmail accounts

In order to disable webmail accounts, please click the Webmail accounts menu item in the web administration portal and then click the e-mail address of the corresponding webmail user. In order to disable the selected webmail account, please click the locked option.

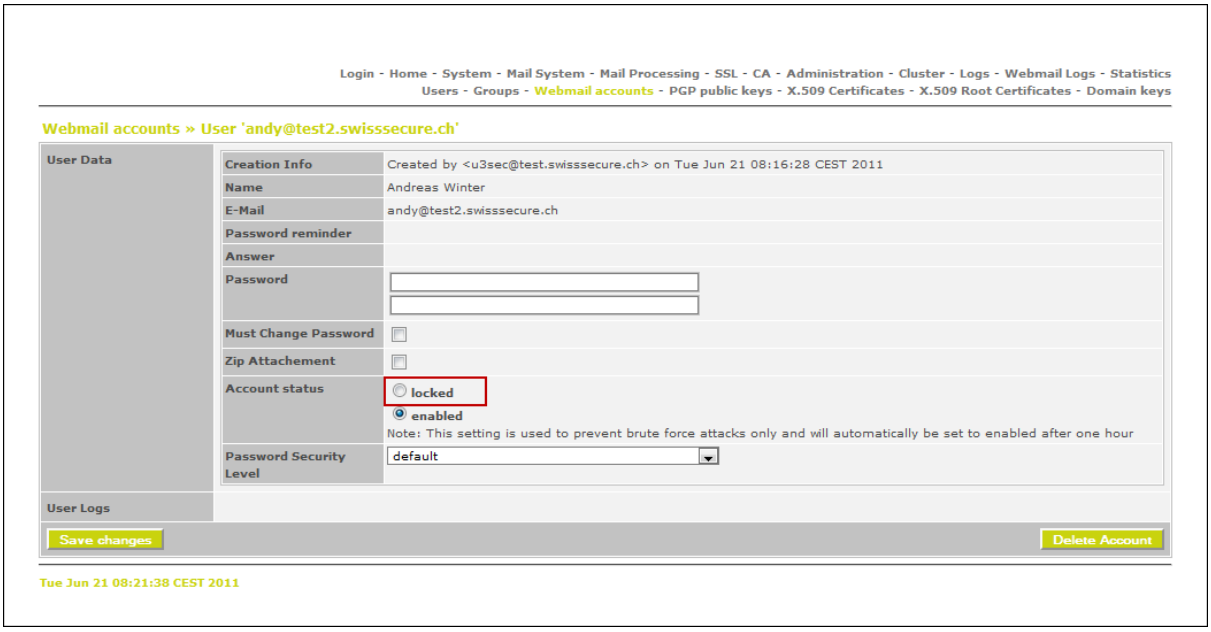


Figure 1 – Disabling a webmail account

4.16.3 Deleting webmail accounts

In order to delete webmail accounts, please click the Webmail accounts menu item in the web administration portal and then click the e-mail address of the corresponding webmail user. In order to delete the selected webmail account, please click the "Delete Account" button.

Important note:

When creating a new webmail account an unambiguous pair of keys, consisting of a private and a public key, is created in order to decrypt and encrypt the EgoSecure Mail Encryption.
All EgoSecure Mail Encryption for this recipient will be encrypted by means of the public key belonging to this webmail account and can be decrypted and read by means of the related public key.

If a webmail account is deleted, the unambiguous pair of keys in this webmail account will also be deleted. This does not mean that the recipient can no longer decrypt and read all EgoSecure Mail Encryption received up to this point in time.

If a new webmail account is created for a previously deleted recipient, a new unambiguous pair of keys will be generated. The recipient can only decrypt and read EgoSecure Mail Encryption that were encrypted with the new key. All EgoSecure Mail Encryption received at a point in time before the new webmail account was created can no longer be decrypted and read. The aforementioned holds true regardless of the fact whether a newly created webmail account has the same name as a webmail account deleted beforehand.

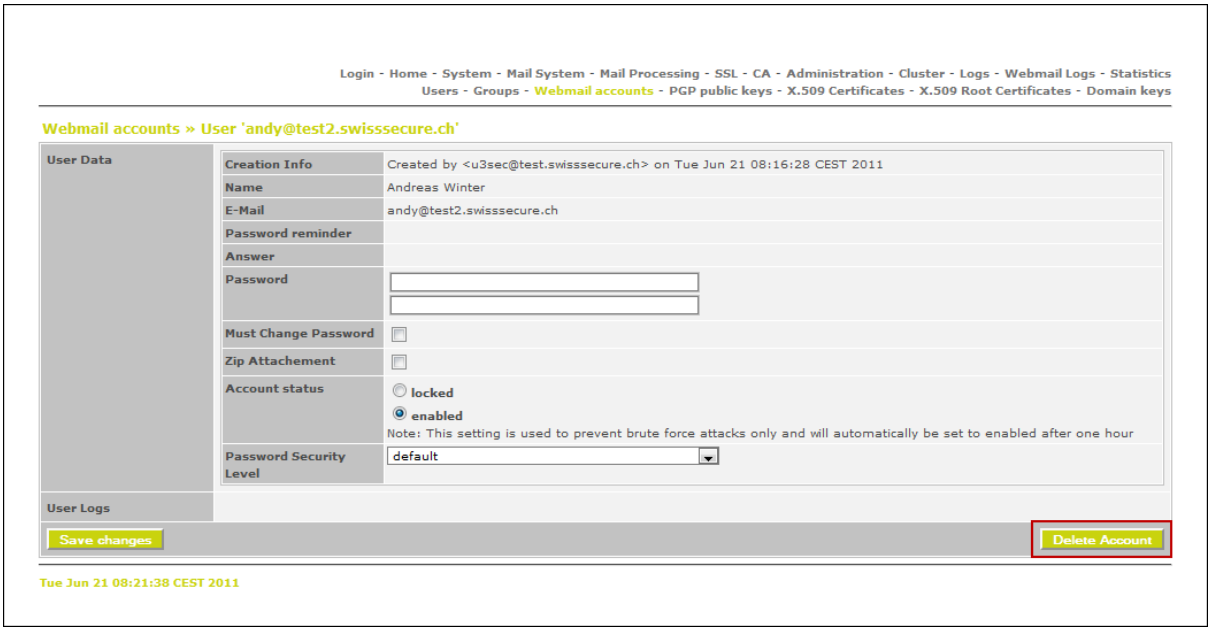


Figure 1 – Deleting a webmail account

4.16.4 Managing webmail accounts

In order to manage webmail accounts, please click the Webmail accounts menu item in the web administration portal and then click the e-mail address of the webmail account you wish to manage.

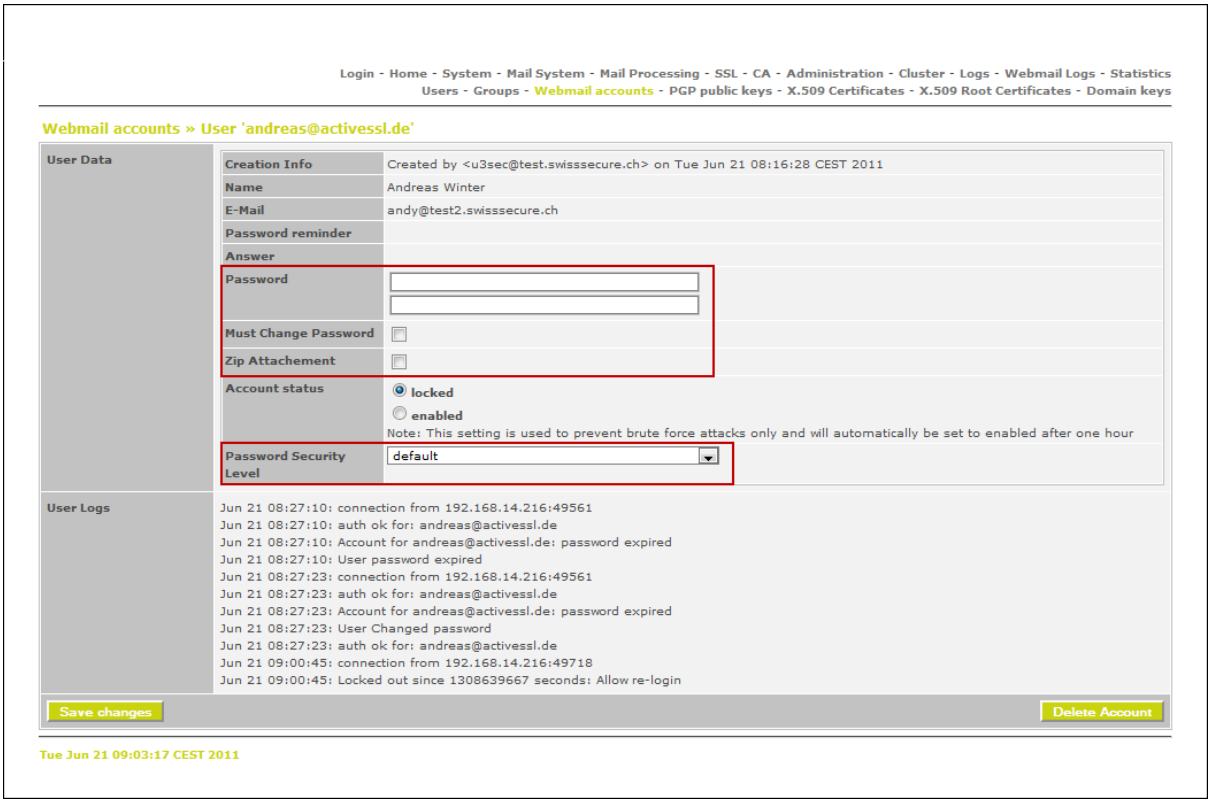


Figure 1 – Managing a webmail account

Section – Parameter – Description

Section: User Data

Creation Info

E-mail address of the sender and time stamp for the creation of the webmail account

Name

Name of the webmail recipient. This information can be managed self-dependently by the webmail recipient within the framework of his/her webmail account.

E-Mail

e-mail address of the recipient

Password reminder

Reminder question for the password of the recipient respectively question and answer for the purposes of identifying the recipient.

Answer

Answer to the reminder question for the identification of the recipient.

Password*

Setting a new password – Enter the new password twice.

Must Change Password*

If you set this option, the webmail recipient must change his/her password within the framework of the next login.

Zip Attachment*

Use this setting if you want that webmail attachments are made available as ZIP files. This option is required for recipients using Outlook Web Access (OWA), because webmails in HTML format cannot be decrypted by means of OWA. In order to use this setting for individual webmails only, the term [owa] can be used in the subject line. If an EgoSecure Mail Encryption in HTML format should arrive with an OWA recipient, the Mail Encryption appliance will detect this. Afterwards, the sender will be requested to send the e-mail again. Simultaneously, the “ZIP Attachment” option will be set within the webmail account of the recipient. Regarding all newly sent EgoSecure Mail Encryption, the webmail attachments will be sent as ZIP file and can be retrieved by means of Outlook Web Access.

Account Status*

locked	Webmail account is disabled temporarily
enabled	Webmail account is activated

This option is used in order to avoid Brute Force** attacks. The webmail account will be disabled automatically after the password has been entered incorrectly 4 times. The webmail account will be blocked for a period of one hour. Afterwards, you may try to log in once again

Password Security Level*

If a webmail user forgets his/her password, he/she can click the link called “Forgot password” when retrieving an EgoSecure Mail Encryption. If the Reset by E-mail option is selected, the recipient will be provided automatically with a new password via e-mail. If you select Reset by hotline, the responsible webmail administrator will be provided with a corresponding e-mail notification (this corresponds to default setting [default]).

Sektion - User Logs

A history of the user interactions can be seen in this area.

Reference of the menu parameters in the “Webmail accounts > Properties of the webmail account” menu item

* These settings can be edited within the webmail account using the configuration interface.
** A Brute Force attack is a term for trying all possible (or at least a large number) password combinations.

4.17 Menu Item "PGP public keys"

Select the “PGP public keys” menu item in order to manage the OpenPGP user keys of the communication partners on the Mail Encryption appliance.

The following processes will be described in the following sections:

4.17.1 Overview Menu Item "PGP public keys"

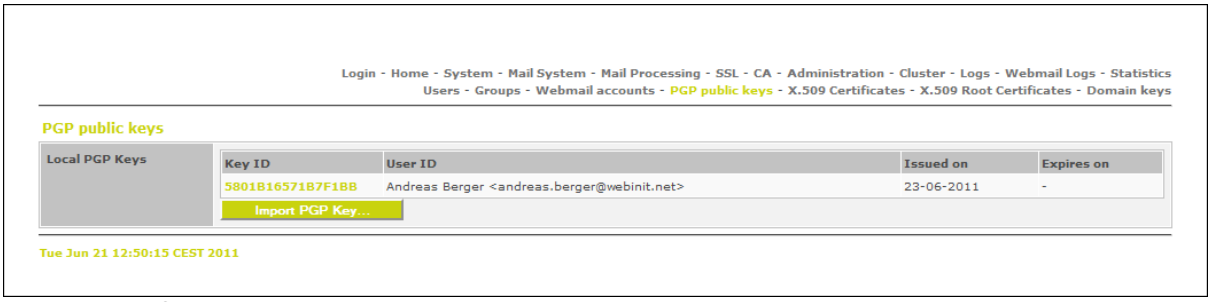


Figure 1 – "PGP public keys" menu item

Section – Parameter – Description

Section: Local PGP keys

Key ID

Key ID

User ID

ID of the user (e-mail address)

Issued on

Date the key was issued

Expires on

Date of expiration of the key

Reference of the menu parameters in the "PGP public keys" menu item

4.17.2 Importing OpenPGP keys

In order to import OpenPGP keys, please select the "PGP public keys" menu item in the configuration interface and then select the "Import PGP Key..." button.

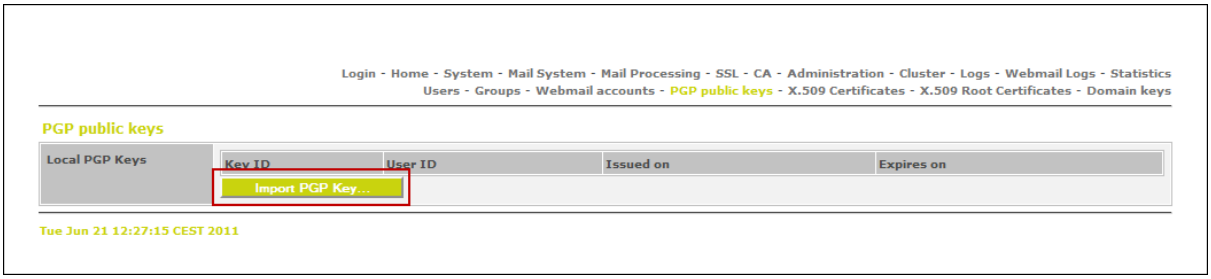


Figure 1 – Button for importing a PGP key

When importing an OpenPGP key, you can select the corresponding file or insert the key in text form.

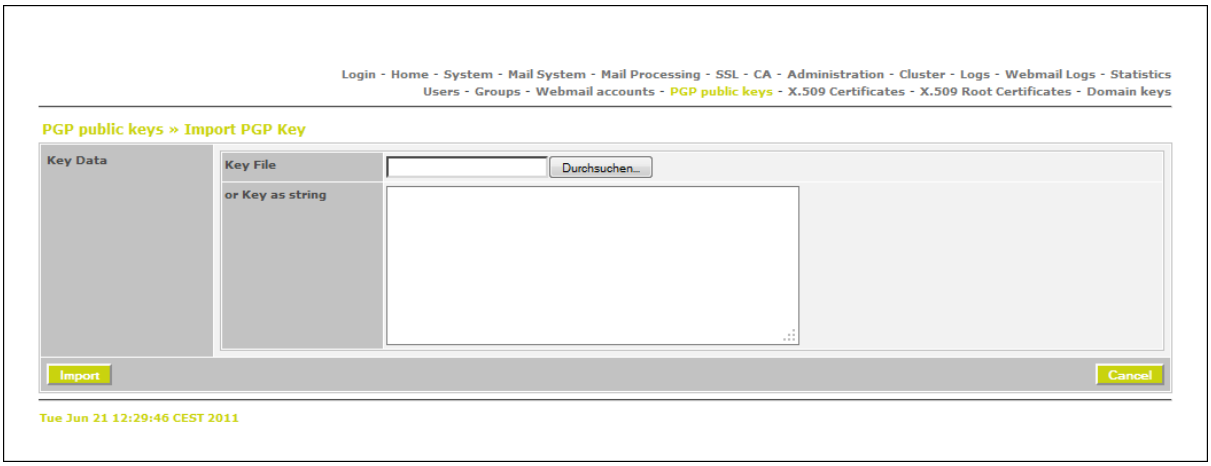


Figure – Selection of the PGP key to be imported

4.17.3 Downloading or deleting OpenPGP keys

In order to download or delete OpenPGP keys, please select the "PGP public keys" menu item in the configuration interface.

In order to download a public OpenPGP key from the Mail Encryption appliance to your PC or to delete a public OpenPGP key, please click the Key ID of the key.

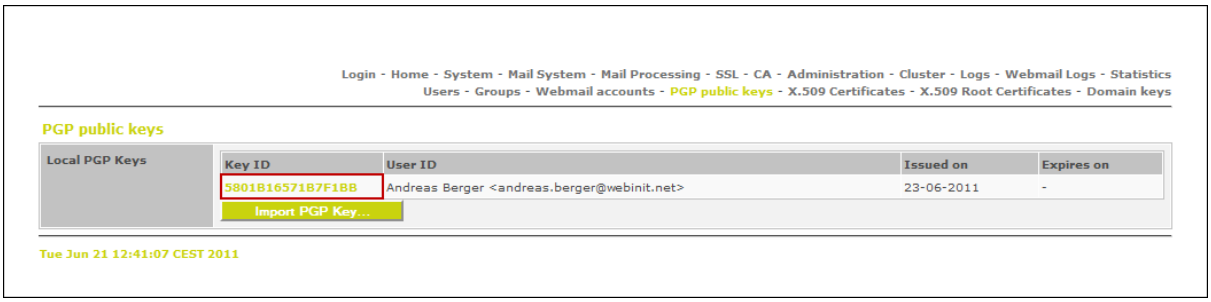


Figure 1 – Overview of the imported PGP user keys

In order to download an OpenPGP key, please select the "Download public key" button. However, if you wish to delete the OpenPGP key, please select the "Delete Key" button.

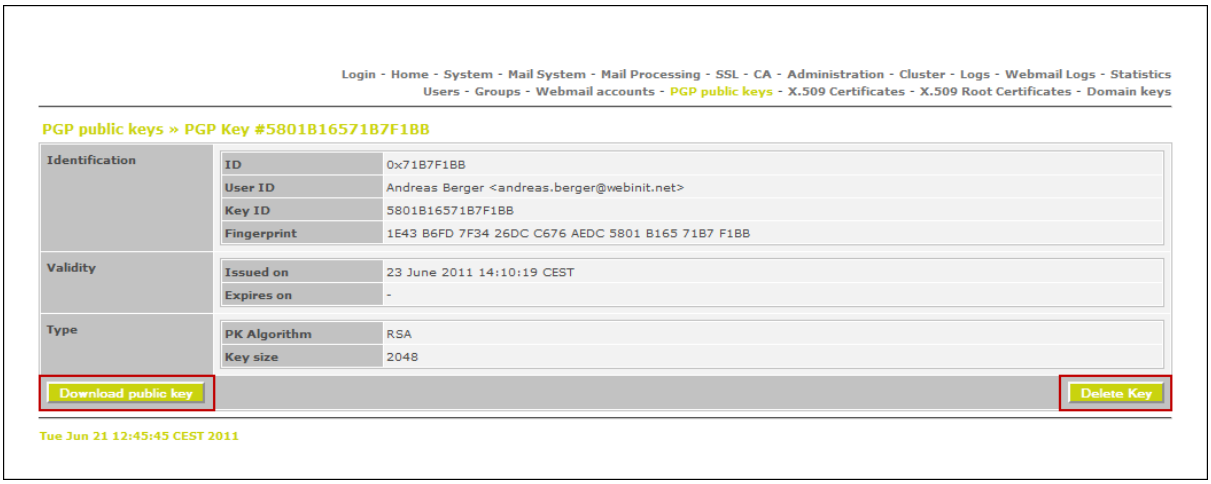


Figure 2 – Buttons for downloading or deleting an OpenPGP key

4.18 Menu Item "X.509 Certificates"

Select the “X.509 Certificates” menu item in order to manage the S/MIME user certificates of the communication partners on the Mail Encryption appliance.

The following processes will be described in the following sections:

4.18.1 Overview Menu Item "X.509 Certificates"

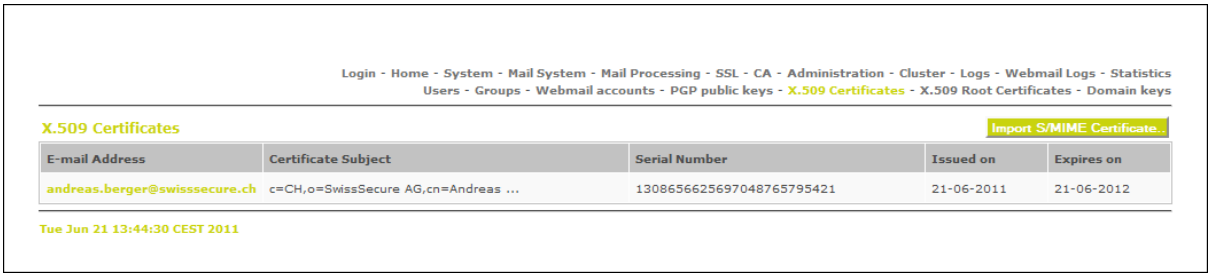


Figure 1 – “X.509 Certificates” menu item

Parameter – Description

E-mail Address

E-Mail Address

Certificate Subject

ID of the user (e-mail address)

Serial Number

Serial number

Issued on

Date the certificate was issued

Expires on

Date of expiration of the certificate

Reference of the menu parameters in the “X.509 Certificates” menu item

4.18.2 Importing the S/MIME user certificate

In order to import S/MIME user certificates manually, please select the “X.509 Certificates” menu item in the configuration interface and then select the “Import S/MIME Certificate...” button.

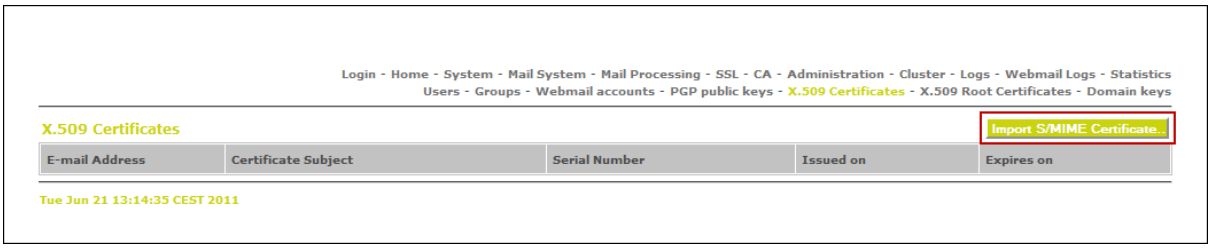


Figure 1 – Button for importing an S/MIME user certificate

Select the corresponding file in order to import an S/MIME user certificate.

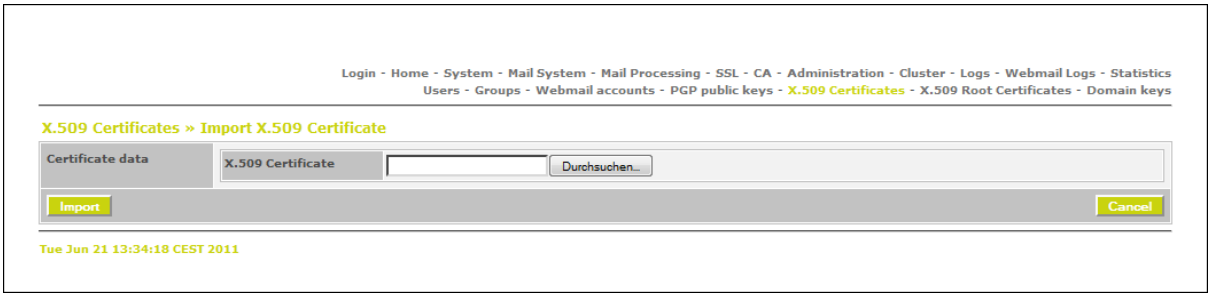


Figure 2 – Selection of the S/MIME user certificate to be imported

4.18.3 Downloading or deleting the S/MIME user certificate

In order to download or delete S/MIME user certificates, please select the "X.509 Certificates" menu item in the configuration interface.

In order to download an S/MIME user certificate from the Mail Encryption appliance to your PC, please click the E-mail address of the certificate.

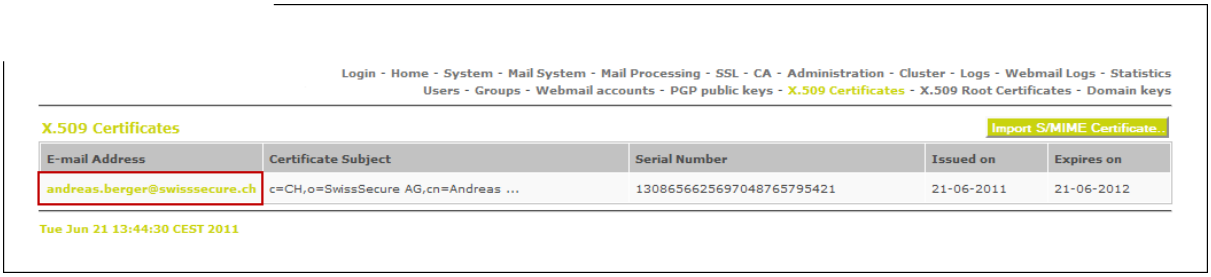


Figure 1 – Overview of the imported S/MIME user certificates

In order to download the S/MIME user certificate, please select the "Download Certificate" button. However, if you wish to delete the S/MIME user certificate, please select the "Delete Certificate" button

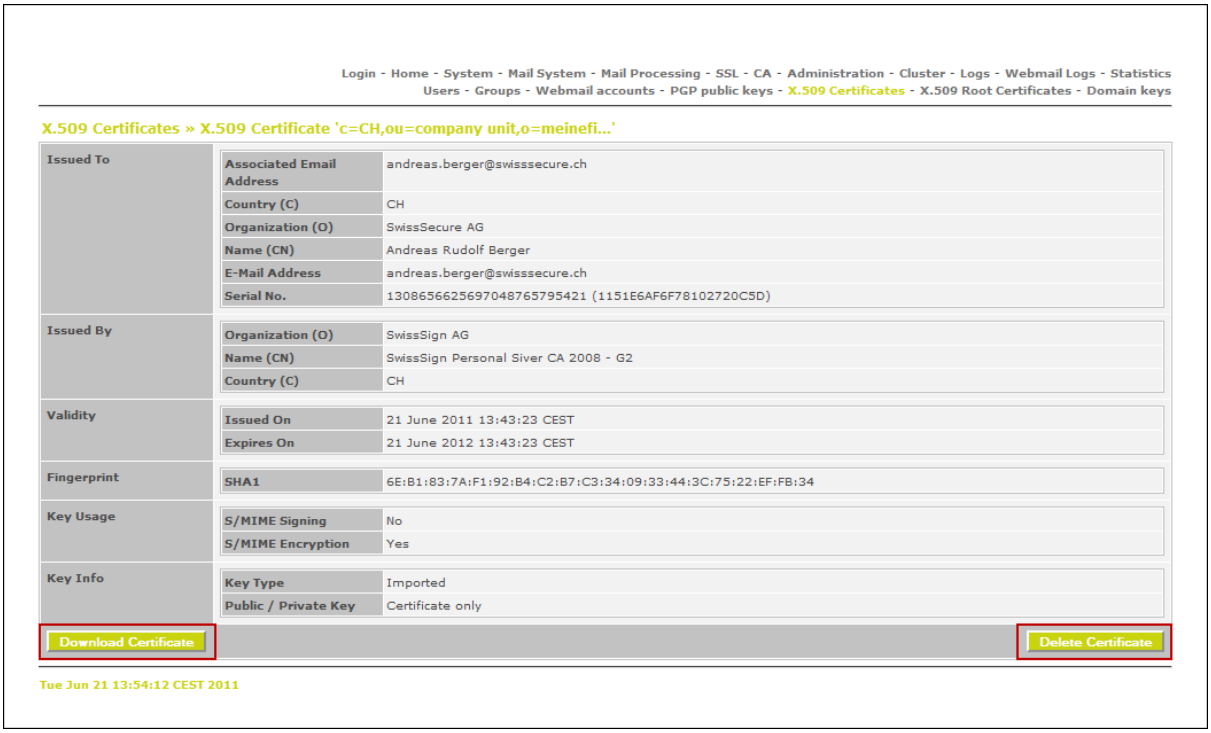


Figure 2 – Buttons for downloading or deleting an S/MIME user certificate

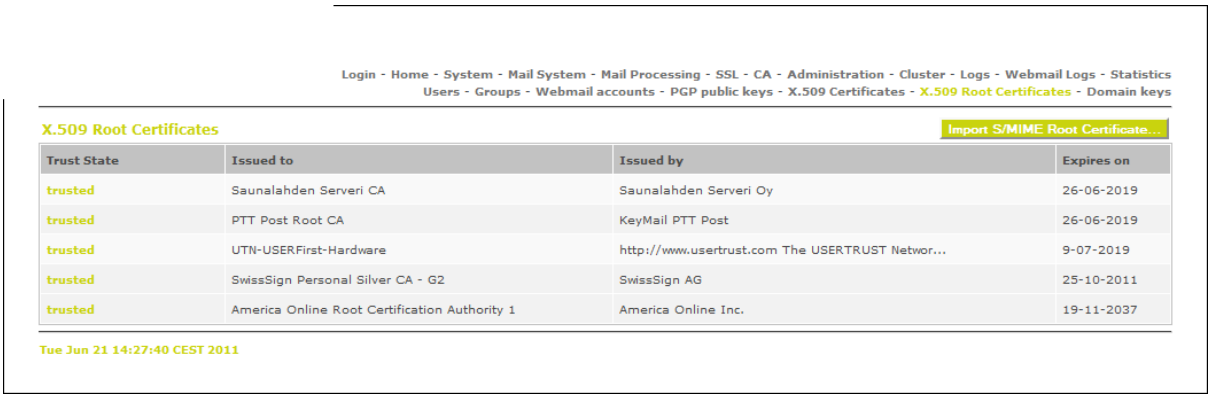
4.19 Menu Item "X.509 Root Certificates"

Select the “X.509 Root Certificates” menu item in order to manage the X.509 root CA certificates of the trustworthy certification authorities on the Mail Encryption appliance.

The following processes will be described in the following sections:

4.19.1 Overview Menu Item "X.509 Root Certificates"

Already at the time of delivery, the Mail Encryption contains a comprehensive list detailing the X.509 root certificates. This list comprises the most common public certification authorities. However, in productive operation it may be required to extend this list with proprietary X.509 root certificates of communication partners or to delete already imported X.509 root certificates.



Trust State	Issued to	Issued by	Expires on
trusted	Saunalahden Serveri CA	Saunalahden Serveri Oy	26-06-2019
trusted	PTT Post Root CA	KeyMail PTT Post	26-06-2019
trusted	UTN-USERFirst-Hardware	http://www.usertrust.com The USERTRUST Networ...	9-07-2019
trusted	SwissSign Personal Silver CA - G2	SwissSign AG	25-10-2011
trusted	America Online Root Certification Authority 1	America Online Inc.	19-11-2037

Figure 1 – List containing the X.509 root certificates on the Mail Encryption appliance (excerpt)

Parameter – Description

Trust State

Trust status of the certificate. The following values are possible:

? (undefined)	The trust status “?” (undefined) is assigned to all X.509 root certificates automatically “harvested” by Mail Encryption from incoming S/MIME-signed e-mails and automatically imported by Mail Encryption into the certificate memory. As these X.509 root certificates are not known at this point, it is required that the use of the aforementioned is authorised by an administrator. Note: All newly imported X.509 root certificates having the status “?” (undefined) will be mentioned within the framework of the daily status report that is sent to all users of the “ststisticsadmin” group at midnight via e-mail.
trusted	The trust status “trusted” is assigned to all X.509 root certificates that are used for the purposes of productive certificate examination of all incoming signed e-mails.
untrusted	The trust status “untrusted” is assigned to all X.509 root certificates that are not used for the purposes of productive certificate examination of all incoming signed e-mails..

Note:
The identifiers of the “Trust State” column are shown highlighted in colours and serve as a link to the display of detailed information of the corresponding certificate. If you want to display detailed information regarding the corresponding certificate in this menu item, please use the mouse pointer to select the identifier of the “Trust State” of the corresponding certificate.

Issued to – “Issued for”

Regarding X.509 root certificates, this value mostly describes the operator (company) of the root CA respectively describes the specific use of an intermediate certificate.

Issued by – “Issued by”

Regarding X.509 root certificates, this value mostly describes the company respectively the operator of the root CA that issued this certificate.

Expires on – Period of validity – “Expires on”

The date of expiration of the corresponding certificate defines the end of the use of the corresponding certificate. After the date of expiration has been reached respectively exceeded, this certificate is no longer used for certificate examination and e-mail signature purposes. Import a new X.509 root certificate of this CA if these are to be used further.

Reference of the menu parameters in the “X.509 Root Certificates” menu item

4.19.2 Importing X.509 Root certificates

In order to import X.509 root certificates, please select the “X.509 Root Certificates” menu item in the configuration interface and then select the “Import S/MIME Root Certificate” button.

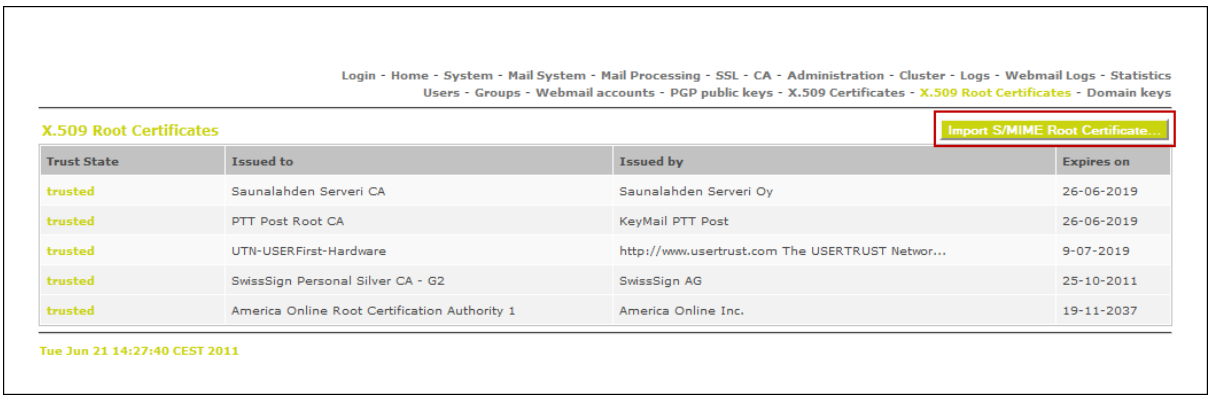


Figure 1 – List containing the X.509 root certificates on the Mail Encryption appliance (excerpt)

Select the corresponding file in order to import an X.509 root certificate.

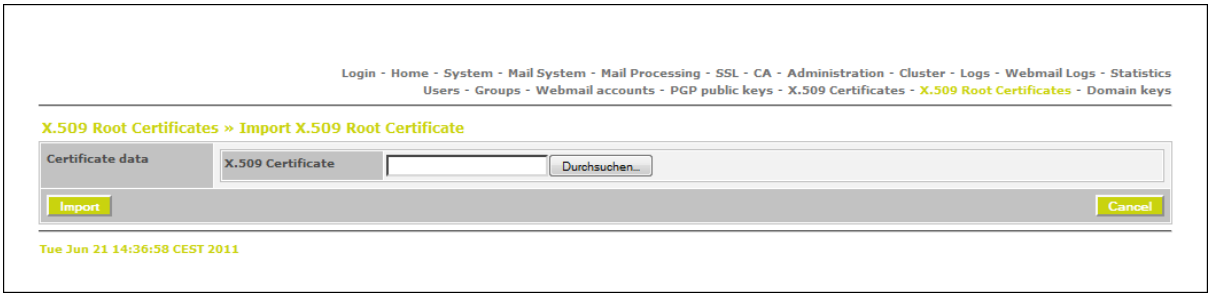


Figure 2 – Selection of the X.509 root certificate to be imported

4.19.3 Downloading or deleting X.509 root certificates

In order to download or delete X.509 root certificates, please select the “X.509 Root Certificates” menu item in the configuration interface.

In the list containing the X.509 root certificates (first column) select the link of the certificate you want to edit.

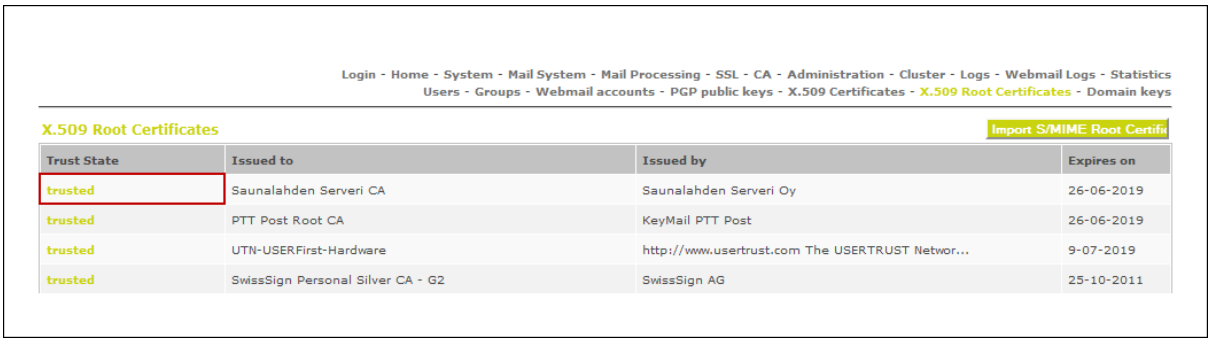


Figure 1 – List containing the X.509 root certificates on the Mail Encryptionappliance (excerpt)

In order to download an X.509 root certificate from theMail Encryption appliance to your PC, please select the “Download Certificate” button. However, if you wish to delete the X.509 root certificate, please select the “Delete Certificate” button.

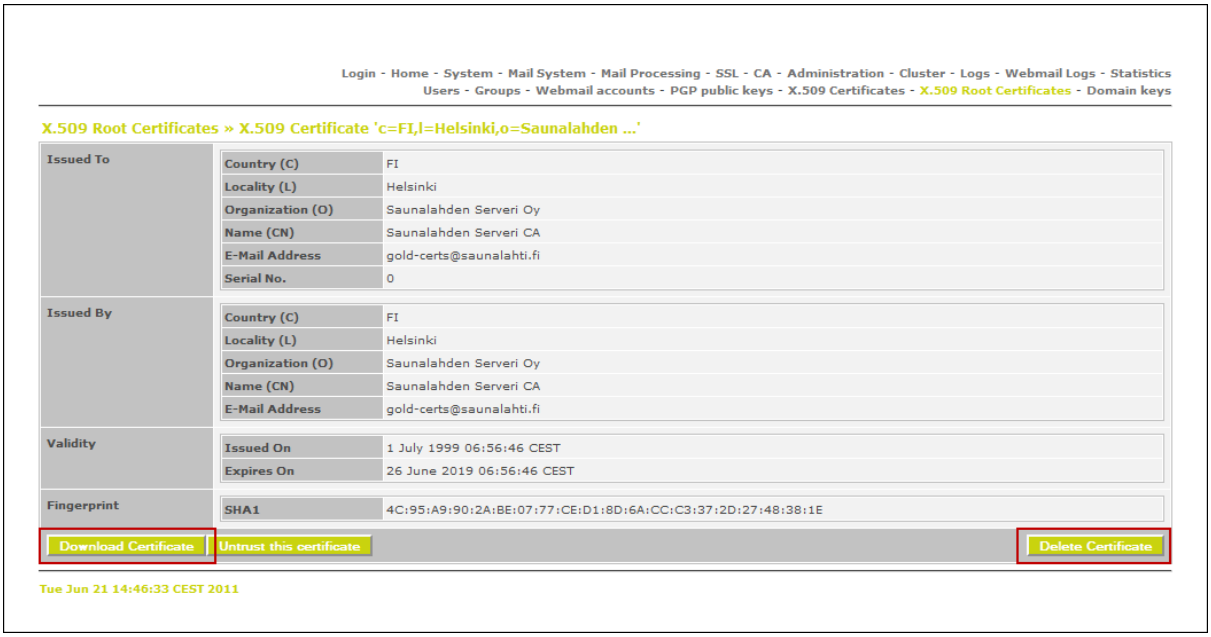


Figure 2 – Buttons for downloading or deleting an X.509 root certificate

4.19.4 Trust X.509-Root-Certificates

In order to trust X.509 root certificates, please select the “X.509 Root Certificates” menu item in the configuration interface. Afterwards, click the “UNTRUSTED” link in the Trust State column regarding an X.509 root certificate you do not trust. The following figure shows an example for the aforementioned.

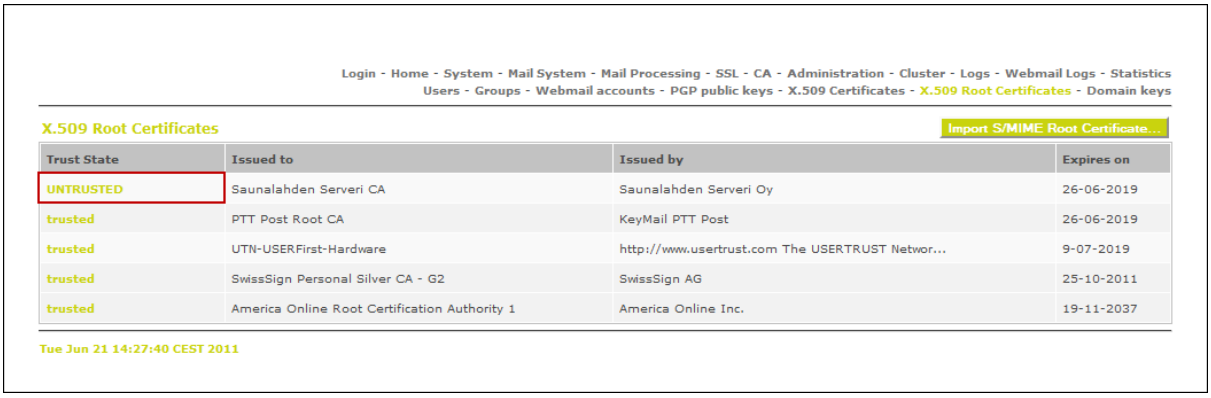


Figure 1 - Trust status “UNTRUSTED” of an X.509 root certificate

You can trust the X.509 root certificate by clicking the “Trust this certificate” button in the following step.

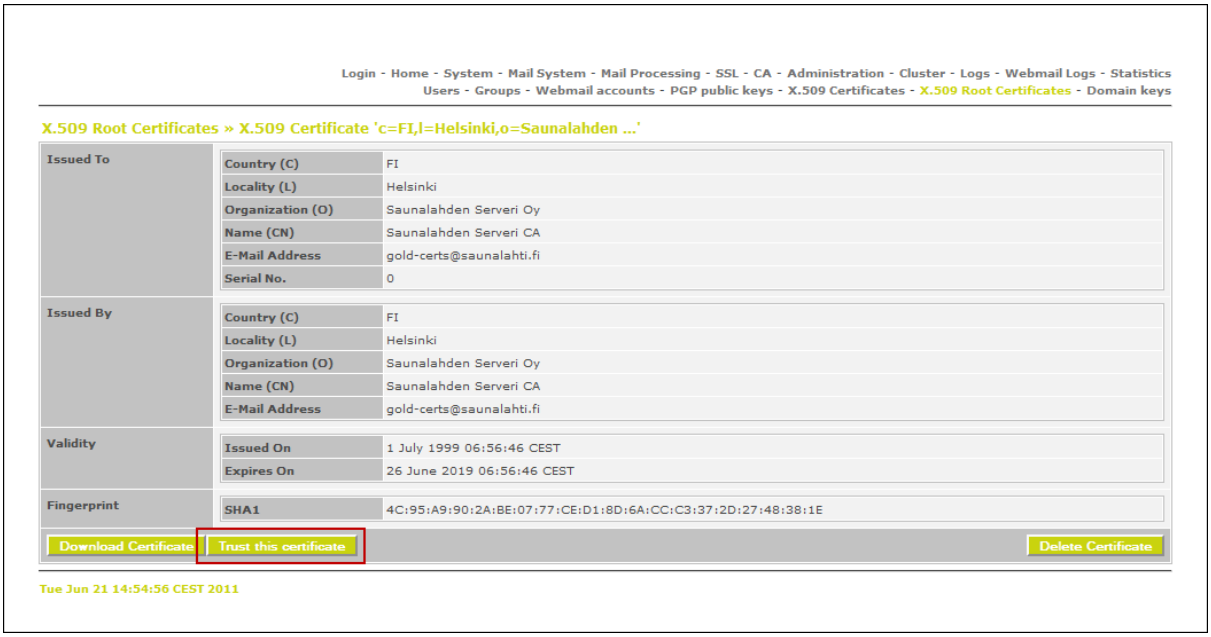


Figure 2 – Button “Trust this certificate”

After having trusted the X.509 root certificate, you will receive the confirmation message Trust status changed and the certificate will be characterised by the new status trusted.

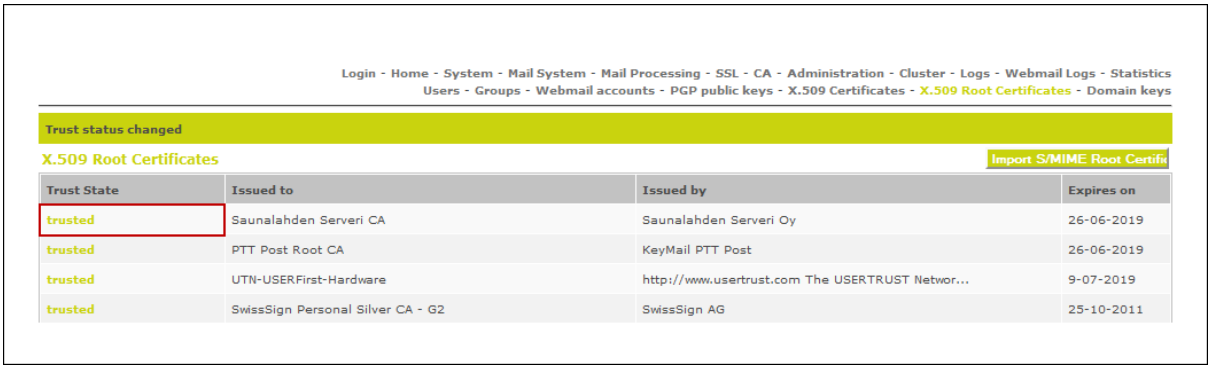


Figure 3 – List of the X.509 root certificates with the status “trusted”

4.19.5 Importing X.509 Root certificates automatically

The process of manually importing X.509 root certificates is described in chapter Importing X.509 root certificates 190 Additionally, Mail Encryption offers the option of importing still unknown X.509 root certificates from incoming S/MIME-signed e-mails automatically. This function is also called “Certificate harvesting”.

These automatically imported X.509 root certificates are always given the status (trust state) “undefined”. This status is displayed by means of a “?” question mark in the configuration interface. The administrator is informed on newly imported X.509 root certificates within the framework of the daily system report.

The administrator must change the trust status manually in the configuration interface. Before changing the trust status, please check the new X.509 root certificate for authenticity.

In order to trust a new X.509 root certificate imported automatically, please select the “X.509 Root Certificates” menu item in the configuration interface. Afterwards, click the “?” link in the Trust State column regarding an X.509 root certificate you do not trust. The following figure shows an example for the aforementioned.

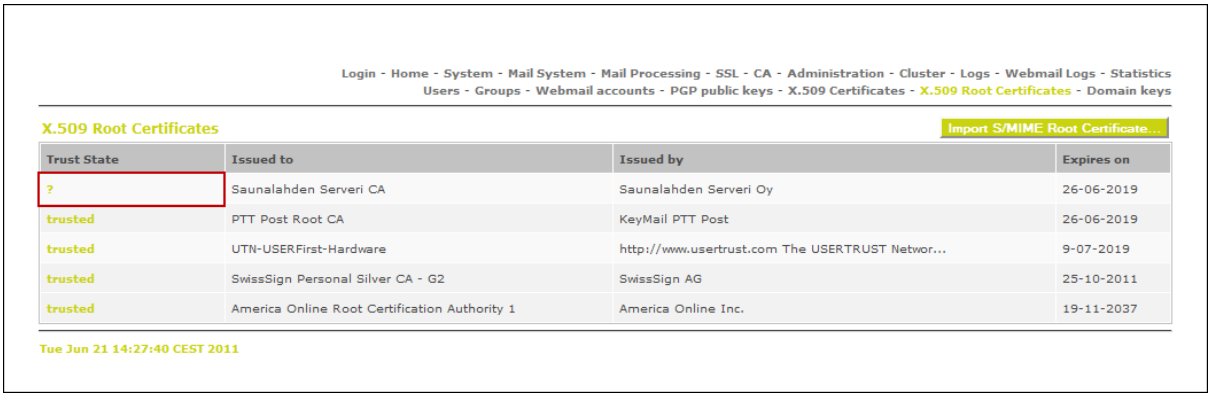


Figure 1 - Trust status “?” of an automatically imported X.509 root certificate

In order to change the trust status, please proceed as described in chapter “Trusting X.509 root certificates” 192

4.20 Menu Item "Domain keys"

Select the “Domain keys” menu item in order to manage the OpenPGP and S/MIME domain keys of the communication partners on the Mail Encryption appliance.

The following processes will be described in the following sections:

4.20.1 Overview Menu Item "Domain keys"

The Mail Encryption appliance offers the option of automatically importing S/MIME domain certificates of other Mail Encryption systems. These S/MIME public domain keys are imported by means of a central update service provided by EgoSecure GmbH.

Depending on the setting, an S/MIME domain certificate will be created automatically when configuring an e-mail domain using the Mail Encryption configuration interface. The public part of this certificate (public key) is forwarded automatically to a central update service of EgoSecure GmbH and forwarded automatically to all Mail Encryption systems installed all over the world upon manual examination.

You can use the “Domain keys” menu item to see the manually installed OpenPGP and S/MIME domain keys and you can also use it to browse for the automatically imported S/MIME domain keys.

If you do not want the S/MIME domain keys to be updated automatically, please disable the “Auto-Update SMIME Domain Certificates” option.

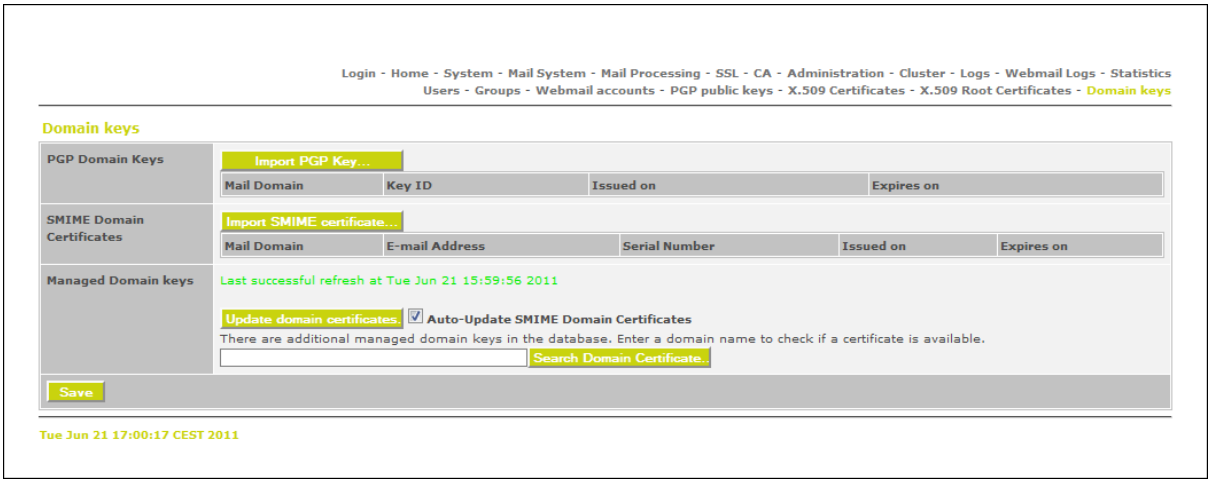


Figure 1 – List of the manually and automatically imported domain keys on the Mail Encryption appliance.

4.20.2 OpenPGP Domain keys importieren

In order to import OpenPGP domain keys, please select the “Domain keys” menu item in the configuration interface and then select the “Import PGP Key…” button.

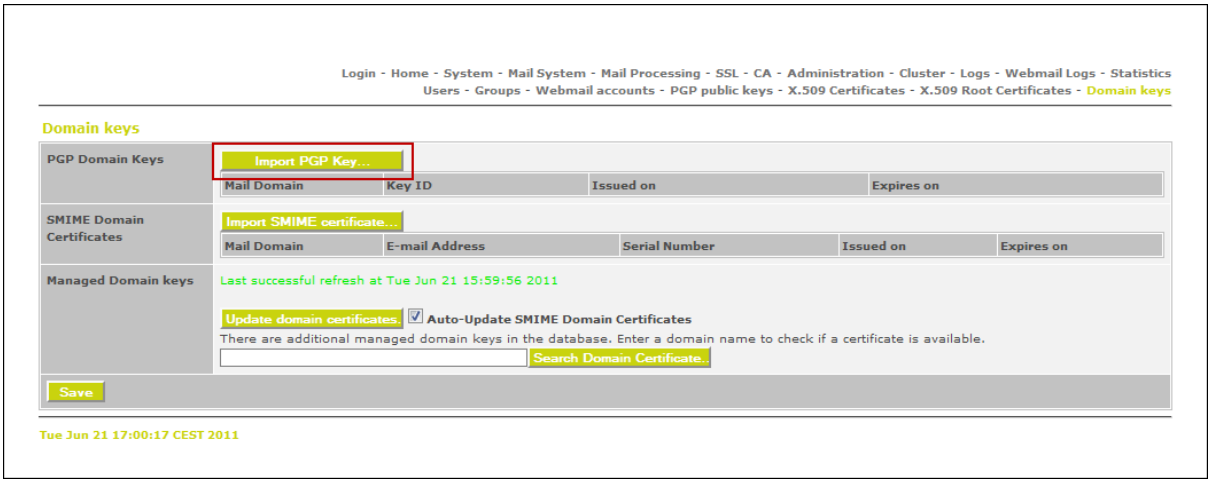


Figure 1 – Button for importing an OpenPGP domain key

Enter the related e-mail domain name in the “Domain name” field. Afterwards, you can select the corresponding file or insert the key in text form.

Figure 2 – Selection of the OpenPGP domain key to be imported

4.20.3 OpenPGP Domain keys herunterladen oder löschen

In order to download or delete OpenPGP domain keys, please select the “Domain keys” menu item in the configuration interface.

In order to download an OpenPGP domain key from the Mail Encryption appliance to your PC, please click the name of the displayed E-mail Domain of the corresponding keys and then click the

“Download public key” button. However, if you wish to delete an OpenPGP domain key, please select the “Delete Key” button.

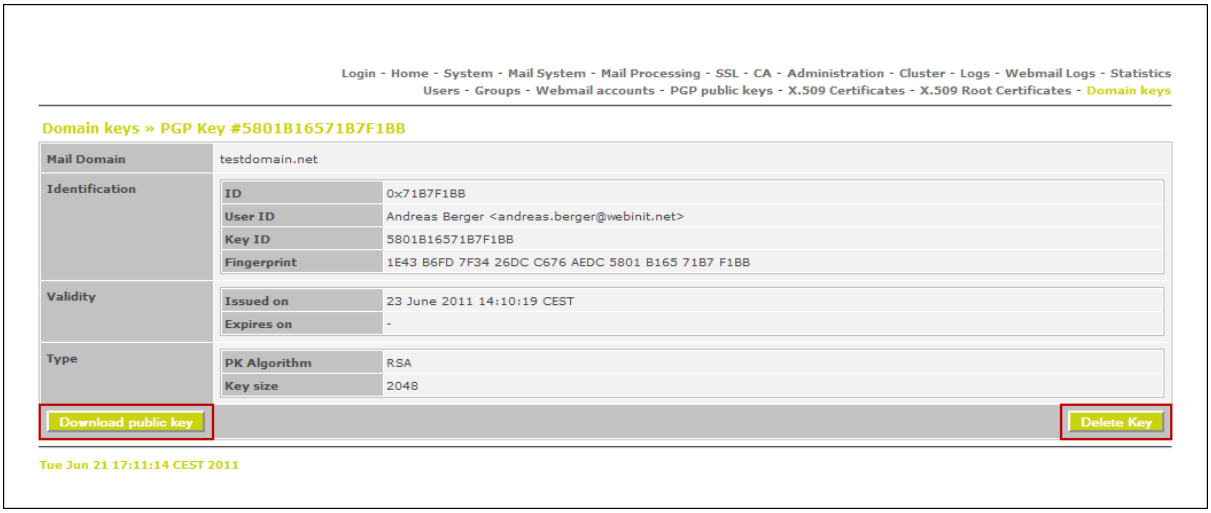


Figure 1 – Buttons for downloading or deleting an OpenPGP domain key

4.20.4 S/MIME Domain keys importieren

In order to import S/MIME domain keys, please select the “Domain keys” menu item in the configuration interface and then select the “Import S/MIME certificate...” button.

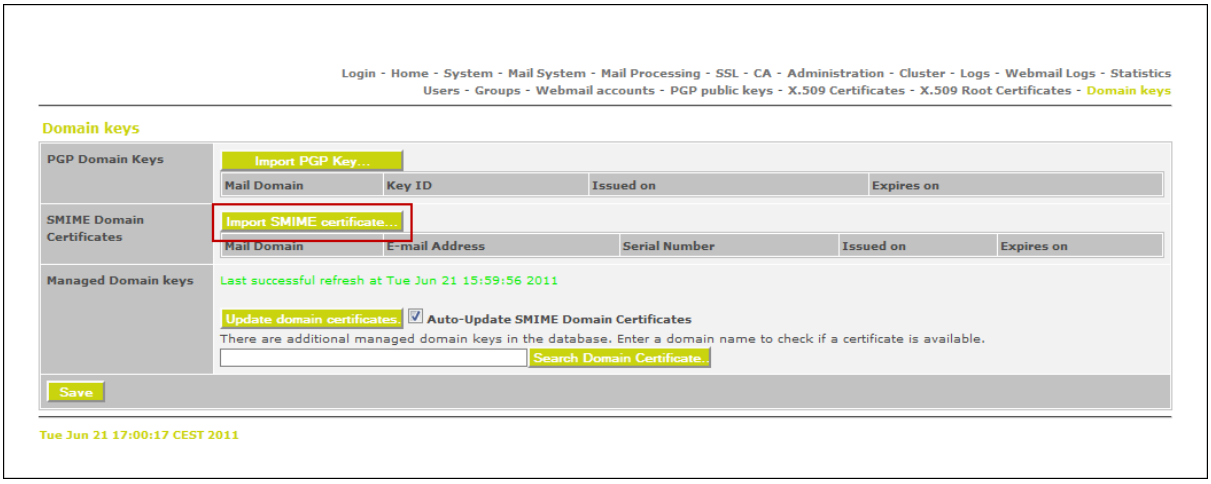


Figure 1 – Button for importing an S/MIME domain key

Enter the related e-mail domain name in the “Domain name” field and select the corresponding file in order to import an S/MIME domain key.

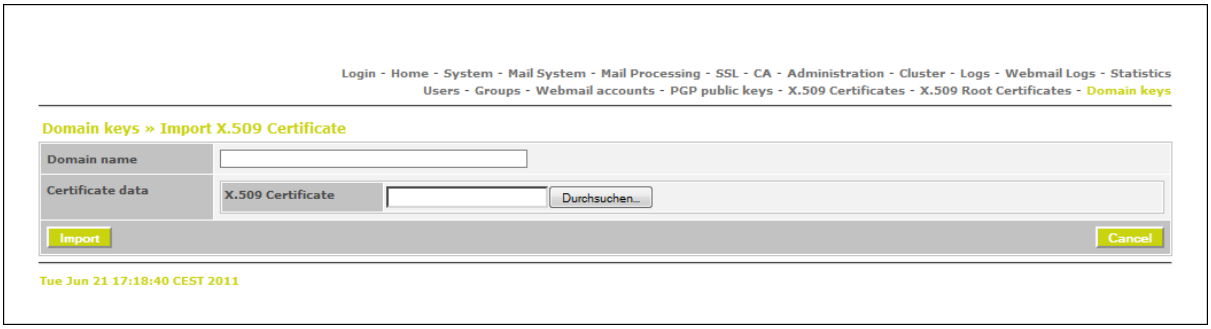


Figure 2 – Selection of the S/MIME domain key to be imported

4.20.5 S/MIME Domain keys herunterladen oder löschen

In order to download or delete S/MIME domain keys, please select the "Domain keys" menu item in the configuration interface.

In order to download an S/MIME domain key from the Mail Encryption appliance to your PC, please click the name of the displayed Mail Domain of the corresponding key and then click the "Download Certificate" button. However, if you wish to delete an S/MIME domain key, please select the "Delete Certificate" button.

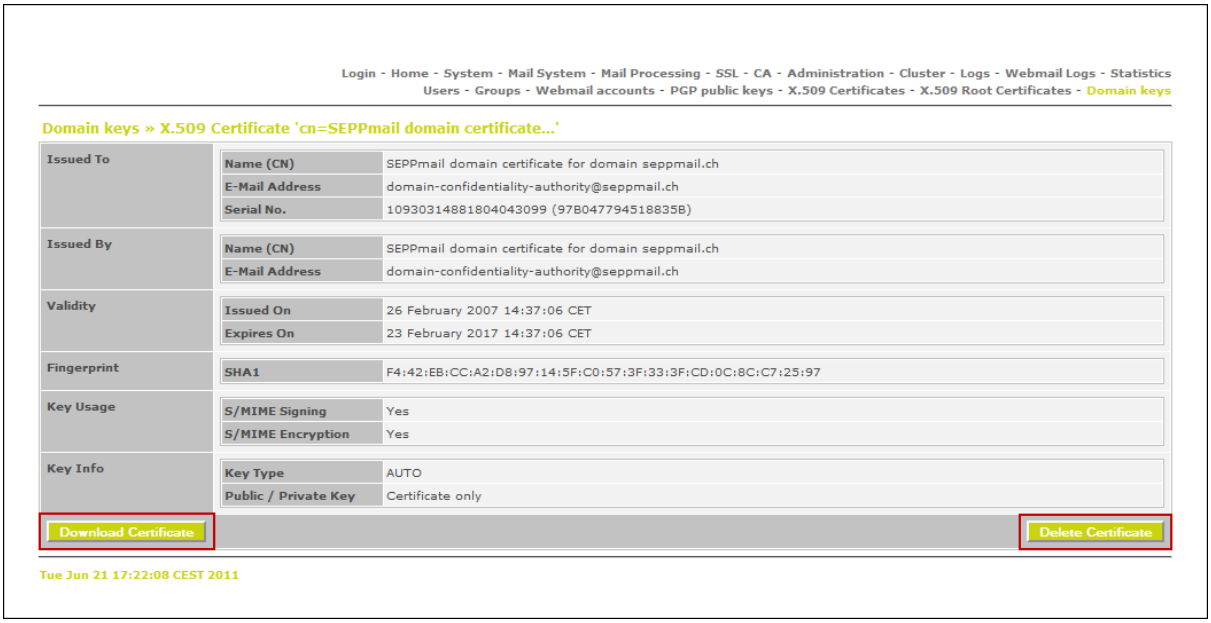


Figure 1 – Buttons for downloading or deleting an S/MIME domain key

4.20.6 Domain keys verwalten

In order to manage domain keys, please select the "Domain keys" menu item in the configuration interface.

Select the "fetch domain certificates..." button in order to compare domain keys of other Mail

Encryption appliances to your own Mail Encryption appliance. This comparison is implemented automatically at periodic intervals if the Auto-Update SMIME Domain Certificates checkbox is enabled.

If you want the check whether a certain domain key is present and if you want to view the details of this domain key, please enter the corresponding domain name and click the "Search Domain Certificate..." button.

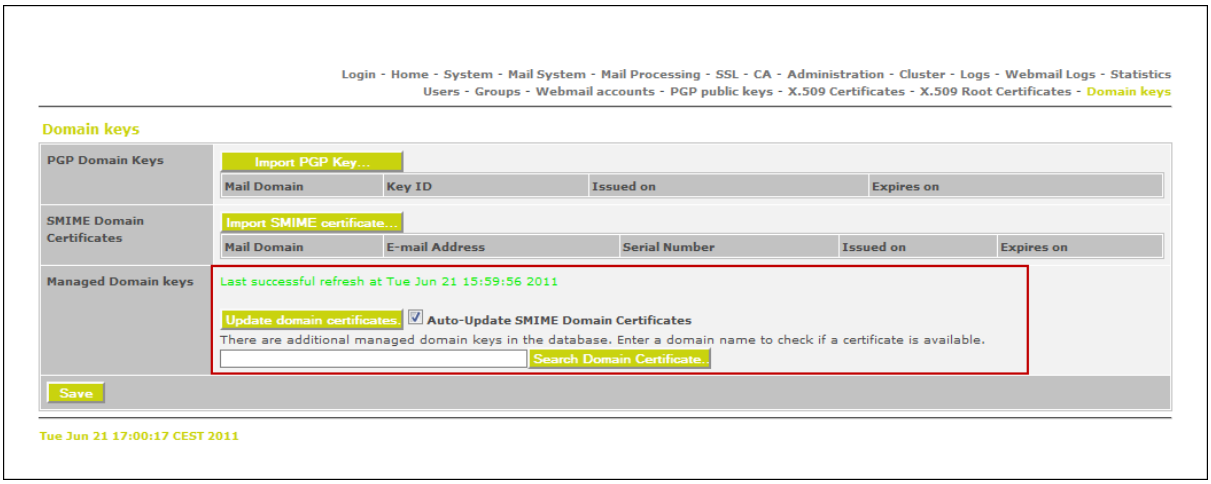


Figure 1 – Managing domain keys

5 Reference of the ruleset commands

5.1 if/else comands

The `if/else` commands serve for sequence control, depending on the conditions. They are an essential part of the ruleset. If a condition is complied with, a corresponding action is or several actions are triggered. Using the `if` command you can define which prerequisite must be complied with for an action to be executed. Using the `else` command you can initiate an alternative action in case the condition required by the `if` command is not complied with.

The command is designed as follows:

```
if ( condition ) {
   command block  1;
}
```

or

```
if ( condition ) {
   command block 1;
} else {
   command block  2;
}
```

On the basis of the return value of the `Condition` this command determines the further sequence within the rule programme. The condition consists of an individual command that is characterised by at least one return value. `Command block 1` will only be executed if the return value is positive. Otherwise, `Command block 2` will be executed exclusively, if applicable; `if/else` commands can be nested.

`Note`: Results of functions that can be analysed by means of `add_report`, etc. do not lose their range of applicability when leaving a command block.

Example: If the e-mail is signed, the signature will be checked for validity. Afterwards, a report on the validity of the signature will be attached to the e-mail. The command is as follows:

```
if ( smime_signed () ) {
   validate_smime_sig ();
}
add_report ("signaturinfo", "auto");
```

5.2 General commands

5.2.1 attach

The attach command can be used to attach a file to the e-mail as attachment. The command is designed as follows:

```
attach ("File name", "Content-ID", "Content-Type")
```

This command attaches a file to the e-mail. The `File name` must contain the absolute path to the file. If the file is not existent, an empty attachment will be generated. Both the `Content-Type` and the `Content-ID` of the attachment can be selected freely.

The return value will always be positive.

5.2.2 authenticated

The `authenticated` command can be used to check the identification status of the sender. The command is designed as follows:

```
authenticated ([“header“])
```

This command checks whether the sender has identified and authenticated.

The return value will be positive if the sender has authenticated himself/herself successfully; otherwise, the value will be negative.

If “header” is specified as value, the user will be authenticated again. For this, the address in the "FROM” field of the header is used.

Note: “Authenticated” either means that the user authenticated himself/herself via SMTP or that the e-mail comes from an e-mail server that is entered under “Relaying”.

5.2.3 compare

The compare command can be used to compare header fields. The command is designed as follows:

```
compare ("Header-Feld", "Operator", "Value")
```

With the help of the `Operator` this command compares the contents of the `Header field` with the `Value`.

- `equal` compares for identity..
- `match` checks for the relevance of a regular expression.
- `substitute` is identical to match, but removes the applicable part from the header field.

The return value will be positive, if there is at least one incident; otherwise, the value will be negative.

Note: Coded fields are decoded before the comparison. The special characters tabulator, carriage return, line feed, and end of page are removed before an `equal` comparison.

5.2.4 compareattr

The `compareattr` command can be used to check attributes / system variables. The command is designed as follows:

```
compareattr ("Attribut", "Operator", "Value")
```

With the help of the `Operator` this command compares the contents of the `Header field` with the Value.

- `equal` compares for identity.
- `match` checks for the relevance of a regular expression

The return value will be positive, if there is at least one incident; otherwise, the value will be negative.

`Attribute` can address the variable "connect_from" or variables written with "ldap_read" or "setuserattr".

Example:

```
if (compareattr('connect_from','equal','172.16.161.1')) {
   log(1,'Message comes from 172.16.161.1'); }
else {
   log(1,'Message does NOT come from 172.16.161.1');
}
```

5.2.5 disclaimer

The disclaimer command can be used to attach text to an e-mail. The command is designed as follows:

```
disclaimer (["Template"] [,"Position"])
```

This command will attach a text from a `Template` to an e-mail. The `Position` is either `top or bottom`. The default setting is bottom.

If an empty string of characters is specified as template, it is tried to select the proper disclaimer on the basis of the settings in “Managed Domains”.

The return value will always be positive.

5.2.6 incoming

The incoming command can be used to define the delivery destination. The command is designed as follows:

```
incoming ()
```

The command checks whether an e-mail is delivered locally. If not all recipients of the e-mail are exclusively local or exclusively not local, two groups will be created.

The return value for the group of local recipients will be positive. It will be negative for the group of non-local recipients.

5.2.7 log

The `log` command can be used to record a message in the Syslog. The command is designed as follows:

```
log ("Stufe", "Eintrag")
```

This command sends an Entry to the system logger. An identification (message ID) is attached to the entry in brackets. Due to reasons of traceability, the same identification will be entered in the header of the e-mail at `X-SEPP-Logtrace`. Level can assume a value between 0 and 7 and defines the relevance of the entry.

The meaning of the levels is specified as follows:

n	Meaning	n	Meaning
0	Debug	4	Error
1	Info	5	Critical
2	Notice	6	Alert
3	Warning	7	Emerg

Meaning of the log levels

The return value will always be positive.

Example: The string of characters “Hello World” is to be recorded in the Syslog with the priority “info”. The command is as follows:

```
log ("1", "Hello World");
```

The header of the e-mail:

```
Date: Fri, 27 Jun 2002 11:40:00 +0200
From: sender@mydomain.ch
To: recipient@mydomain.ch
Subject: Some Topic
Content-Type: text/plain;
Message-Id: <E0D4DE42-DCB5-11D7>
```

Record within the log:

```
Jun 27 11:40:04 test gateway: <E0D4DE42-DCB5-11D7> Hello World
```

5.2.8 notify

The notify command can be used to send notifications regarding the e-mail. The command is designed as follows:

```
notify ("Empfängeradresse", "Vorlage" [,"Header als Anlage"],'From: "System Ad
```

This command generates an e-mail and sends it to the `Recipient address`. Along with the e-mail address, the `Recipient address` may also be `sender` for senders or `admin` for the administrator. The appearance of the e-mail is defined with the `Template`. The header of the original e-mail is attached to the e-mail as an attachment if `Header as attachment` is characterised by the Boolean value true. Instead of true it is also possible to use yes or 1. The third parameter allows for inserting proprietary headers additionally. Several headers can be separated by means of a “;”.

Example:

```
notify ('sender','bounce_noenc','From: "System Admin" <admin@securemail.com>;X
```

The return value will always be positive.

5.2.9 replace_rcpt

The replace_rcpt command can be used to change recipients of an e-mail. The command is designed as follows:

```
replace_rcpt ([OLDRECIPIENT],NEWRECIPIENT)
```

Several recipients can be separated by means of semi-colons “;”.

If `OLDRECIPIENT` is specified, only this recipient will be adapted. In this case, the command will be as follows, for example:

```
replace_rcpt ('\@mydomain\.com','\@mydomain\.ch')
```

This would change all recipient addresses from mydomain.com to mydomain.ch.

5.2.10 rmatch

The match command can be used to check whether a regular expression is applicable to all users. The command is designed as follows:

```
rmatch (REGEXP)
```

5.2.11 rmatchsplit

The `matchsplit` command can be used to divide an e-mail according to users in accordance with a regular expression. The command is designed as follows:

```
rmatchsplit (REGEXP)
```

The e-mail will be divided into several groups.

5.2.12 rmheader

The rmheader command can be used to delete a header line within the e-mail. The command is designed as follows:

```
rmheader (HEADER)
```

Note: If there are several headers with the name HEADER, all of them will be deleted.

The return value will always be positive.

5.2.13 setheader

The setheader command can be used to change or add a header line within the e-mail. The command is designed as follows:

```
setheader (HEADER, TEXT)
```

Note: If there are several headers with the name HEADER, the first header will be adapted in each case.

The return value will always be positive.

5.2.14 tag_subject

The tag_subject command can be used to adapt the subject of an e-mail. The command is designed as follows:

```
tag_subject (TEXT)
```

A TEXT will be attached to the subject of the e-mail.

The return value will always be positive.

5.2.15 comparebody

The comparebody command can be used to compare header fields with each other.

```
comparebody ("Wert")
```

This command browses the text of the e-mail for the value “Value”.

“Value” is in the regular expression format.

Example:

```
    if (comparebody('(\d{1,3}\.){3}\d{1,3}')) {
```

```
        log(1, 'Mail contains an IP address');
    } else {
        log(1, 'Mail does not contain an IP address');
    }
```

5.3 Commands for user management

5.3.1 createaccount

The createaccount command can be used to create a new user. The command is designed as follows:

```
createaccount ([KEYS],[USERID],[NAME])
```

Note:
- Variables that were set by ldap_read can be used for `USERID` and `NAME`.
- Special characters in `USERID` and `NAME` will be replaced automatically.

The following system attributes are available:

KEYS	Bit 0: generate OpenPGP key Bit 1: generate S/MIME key Bit 2: SwissSign Key generieren
USERID	User ID of the user
NAME	Name of the user

System attributes of the “createaccount” command

5.3.2 member_of

The `member_of` command can be used to check whether a sender is assigned to a certain group. The command is designed as follows:

```
member_of(group1 [,group2 [,group3]])
```

The return value will be positive if the sender is a member of all specified groups.

5.3.3 setuserattr

The setuserattr command can be used to store additional information for the current user. The command is designed as follows:

```
setuserattr (ATTR, VALUE)
```

An additional variable will be set for the current user. The user must be authenticated.

Note:
- Variables that were set by ldap_read can be used for `VALUE`.
- All attributes of InetOrgPerson can be used.
- The attributes can be displayed in the GUI.

The following system attributes are available:

accountOptions	Bit 0: user must not encrypt Bit 2: user must not sign
Sn	Name of the user
userPassword	Password of the user for GUI access
Uid	User ID

System attributes of the “setuserattr” command

5.4 Commands for certificate management

5.4.1 attachpgpkey

The attachpgpkey command can be used to attach an OpenPGP certificate of the sender to the e-mail. The command is designed as follows:

```
attachpgpkey ()
```

This command will attach the OpenPGP certificate (the public key) of the sender to the e-mail.

The return value will always be positive.

5.4.2 has_smime_key

The has_smime_key command can be used to check whether the user disposes of a valid private S/MIME key. The command is designed as follows:

```
has_smime_key ()
```

Note:
- The return value will also be negative if the user disposes of expired keys only.
- The return value will also be negative if the user is set to “may not encrypt”.

5.4.3 smime_create_key

The smime_create_key command can be used to create an S/MIME key for a user. The command is designed as follows:

```
smime_create_key ([SUBJECT])
```

Optionally, the `SUBJECT` for the key can be specified.

5.4.4 swisssign_create_key

The swisssign_create_key command can be used to create an S/MIME key of the certification authority SwissSign for a user. The command is designed as follows:

```
swisssign_create_key ()
```

5.4.5 smime_revoke_keys

The smime_revoke_keys command revokes all S/MIME certificates of a user that have not expired yet.

```
smime_revoke_keys ()
```

The return value will be positive if all certificates could be revoked respectively have expired.

The return value will be negative if at least one certificate could not be revoked, e.g. because it is an imported certificate.

5.5 Commands for handling messages

5.5.1 archive

The `archive` command can be used to re-process an e-mail. The command is designed as follows:

```
archive (MAIL)
```

An additional recipient is added to the e-mail.

5.5.2 bounce

The bounce command can be used to refuse to process the e-mail. The command is designed as follows:

```
bounce ("Template","Header als Anlage")
```

This comment will create a “bounce” e-mail and will delete the original e-mail. The appearance of the report is defined with the `Template`. The sender of this e-mail is the admin. The header of the original e-mail is attached to the e-mail as an attachment if `Header as attachment` is characterised by the Boolean value true. Instead of true it is also possible to use yes or 1.

The command does not have any return value.

Note:
- All following commands will be ignored.
- This command cannot be the condition of an if/else command (see chapter if/else commands 200).

Example: The delivery of the e-mail is to be prevented and the sender is to be provided with an e-mail. The contents of the e-mail are defined in the bounce template. The header of the e-mail that was not delivered is to the attached to the e-mail as an attachment. The command is as follows:

```
bounce ("bounce", "yes");
```

5.5.3 deliver

The `deliver` command can be used to deliver an e-mail. The command is designed as follows

```
deliver (Mailserver[:Port]|“loop“|“queueless“|“”);
```

This command will deliver the e-mail to the specified e-mail server / port. If no argument is specified, the e-mail will be transferred to the local mail transport agent (MTA).

Spezielle Argumente:
- `“loop“`: The e-mail will be returned to the e-mail server it was accepted by.
- `“queueless“`: This setting causes that e-mails to individual recipients are not stored “intermediately” while they are processed. Instead, the incoming connection will be acknowledged only when the outgoing connection has been acknowledged. If, during dispatch to several recipients, the acceptance for some recipients is not acknowledged, these e-mails will be on the appliance for a short period of time until the receiving e-mail servers acknowledge them

Notes:
- All following commands will be ignored.
- This command cannot be the condition of an if/else command (see chapter if/else Anweisungen 200).

5.5.4 drop

The drop command can be used to reject an e-mail. The command is designed as follows:

```
drop ([CODE],[ERROR])
```

This command will delete the e-mail. The command does not have any return value.

Using CODE and ERROR, alternative return values can also be set.

Example: The e-mail is to be rejected with the temporary error "420 system temporarily unavailable“. The command is as follows:

```
drop ("420", "system temporarily unavailable ");
```

Notes:
- Neither a bounce e-mail to the sender nor a notification to the recipient will be generated.
- All following commands will be ignored.
- This command cannot be the condition of an if/else command (see chapter if/else commands 200).

5.5.5 reprocess

The reprocess command can be used to re-process an e-mail. The command is designed as follows:

```
reprocess ()
```

All e-mails attached to this e-mail will be re-processed and returned to the sender. This makes sense if there still are encrypted e-mails in the mailbox of a user.

The command does not have any return value.

Note:
- The original message ID will be removed from the newly decrypted e-mails.
- No bounce e-mail to the sender will be generated.
- All following commands will be ignored.
- This command cannot be the condition of an if/else command (see chapter if/else commands 200).

5.6 Commands for decryption and encryption

5.6.1 decrypt_pgp

The `decrypt_pgp` command can be used to decrypted PGP-encrypted and signed e-mails. The command is designed as follows:

```
decrypt_pgp ()
```

This command tries to decrypt all PGP-encrypted and signed texts and attachments of the e-mail and to check the signatures of the aforementioned.

The return value will be positive if at least one text or one attachment was decrypted or the signature of the aforementioned was validated successfully. Otherwise, the return value will be negative.

5.6.2 decrypt_smime

The `decrypt_smime` command can be used to decrypt S/MIME-encoded messages. The command is designed as follows

```
decrypt_smime ()
```

This command attempts to decrypt an S/MIME-encrypted e-mail.

The return value will be positive if the e-mail was decrypted; otherwise, the value will be negative.

5.6.3 delete_smime_sig

The `delete_smime_sig` command can be used to delete an S/MIME signature. The command is designed as follows:

```
delete_smime_sig ()
```

This command will delete a signature from the signed e-mail.

The return value will be positive if the e-mail was signed in accordance with the S/MIME procedure. Otherwise, the return value will be negative.

`Note`: The validity of the signature is not checked at all.

5.6.4 encrypt_pgp

The `encrypt_pgp` command can be used to encrypt and sign e-mails by means of PGP. The command is designed as follows:

```
encrypt_pgp ( "Signatur" [,"Address"])
```

This command encrypts all texts and attachments of the e-mail. The e-mails will be signed additionally if the `Signature` is characterised by the Boolean value true. Instead of true it is also

possible to use yes or 1. If the `Address` is specified, only the certificate of this recipient address will be used in order to encrypt all e-mails for all recipients. If certificates are not available for all recipients, two groups will be formed.

Regarding the group of recipients that could be encrypted, the return value will be positive.
Regarding the group of recipients that could not be encrypted, the return value will be negative.

5.6.5 encrypt_webmail()

The `encrypt_webmail()` command can be used to encrypt e-mails by means of the EgoSecure Mail Encryption (ESWMail) procedure. The command is designed as follows:

```
encrypt_webmail([TEMPLATE])
```

This commend will encrypt the webmail for the recipient address. The encrypted message can be processed further in the rule engine afterwards (recommendation: send directly with delivery()). The recipient address will be taken from the currently processed message.

If `TEMPLATE` is specified, a special template will be used for the webmail. If this is not the case, the template will be selected on the basis of the sender address.

5.6.6 encrypt_smime

The `encrypt_smime` command can be used to encrypt e-mails by means of S/MIME. The command is designed as follows:

```
encrypt_smime ()
```

This command will encrypt the e-mail in accordance with the S/MIME standard. If certificates are not available for all recipients, two groups will be formed.

Regarding the group of recipients that could be encrypted, the return value will be positive.
Regarding the group of recipients that could not be encrypted, the return value will be negative.

5.6.7 pgp_keys_avail

The `pgp_keys_avail` command can be used to check the availability of PGP certificates. The command is designed as follows:

```
pgp_keys_avail ("Application")
```

This command checks whether PGP certificates are available for all recipients. If the `Application` of the command is `strict`, the return value will only be positive, if certificates are available for all recipients. If the application is `auto`, the command will divide the recipients in two groups and will provide each group with the corresponding return value.

5.6.8 webmail_keys_avail

The `webmail_keys_avail` command can be used to check whether webmail accounts are available. The command is designed as follows:

```
webmail_keys_avail( "Appliction" )
```

This command checks whether a webmail account is available for all recipients of the e-mail. If the `Application` of the command is `strict`, the return value will only be positive if certificates are available for all recipients. If the application is `auto`, the command will divide the recipients in two groups and will provide each group with the corresponding return value.

5.6.9 webmail_keys_gen

The `webmail_keys_gen` command can be used to create webmail accounts. The command is designed as follows:

```
webmail_keys_gen(["Recipient address"])
```

This command will generate a webmail account and will send the password to the sender of the e-mail or to the `Recipient address`, if this address is specified.

5.6.10 sign_smime

The `sign_smime` command can be used to provide an e-mail with the S/MIME signature of the sender. The command is designed as follows:

```
sign_smime ()
```

The return value will be positive if the e-mail was signed successfully; otherwise, the value will be negative.

5.6.11 smime_encrypted

The `smime_encrypted` command can be used to check an e-mail for S/MIME encryption. The command is designed as follows:

```
smime_encrypted ()
```

This command checks whether the present e-mail was encrypted by means of the S/MIME procedure.

The return value will be positive if the e-mail is encrypted; otherwise, the value will be negative.

5.6.12 smime_keys_avail

The `smime_keys_avail` command can be used to check the availability of S/MIME certificates. The command is designed as follows:

```
smime_keys_avail ("Application")
```

This command checks whether S/MIME certificates are available for the recipients of the e-mail. If the `Application` of the command is `strict`, the return value will only be positive if certificates are available for all recipients. If the application is `auto`, the command will divide the recipients in two groups and will provide each group with the corresponding return value.

5.6.13 smime_signed

The smime_signed command can be used to check an e-mail for S/MIME signature. The command is designed as follows:

```
smime_signed ()
```

This command checks whether the present e-mail was signed by means of the S/MIME procedure.

The return value will be positive if the e-mail is signed; otherwise, the value will be negative.

5.6.14 validate_smime_sig

The validate_smime_sig command can be used to check an S/MIME signature for validity. The command is designed as follows:

```
validate_smime_sig ("Zertifikat speichern")
```

This command checks the validity of the e-mail signed by means of the S/MIME procedure.

The return value will be positive if all of the following items are applicable:
- The e-mail was signed in accordance with the S/MIME procedure.
- The e-mail is complete and has not been subject to changes.
- The e-mail was signed with a certificate that was issued by a certificate authority (CA) that is classified as trustworthy.
- The certificate used to attach the signature is neither listed within the framework of a “Revocation list” known to the appliance, nor is the date of expiration of the certificate exceeded.

If one of the items mentioned above is not applicable, the return value will be negative.

5.7 Commands for LDAP (access to external sources)

5.7.1 ldap_compare

The ldap_compare command can be used to compare a value stored within an LDAP register. The command is designed as follows:

```
ldap_compare(URI;USER;PASSWORD;BASEDN;FILTER,ATTR,VALUE);
```

This command will establish a connection to an LDAP server and will check the value of the attribute. The return value will be positive if value exists within the attribute; otherwise, the value will be negative.

Explanation of the parameters:

URI	The IP address or the name of the LDAP server. It is also possible to enter two values separated by a comma. In this case, the second server will be used automatically if the first server is not available..
USER	The user to be used for the purposes of access
PASSWORD	The password of the user.
BASEDN	The base DN (distinguished name) for the query.
FILTER	The filter for the query.
ATTR	The attribute that is to be queried.
VALUE	The value that is to exist within the attribute.

Parameters of the ldap_compare command

Example: It is to be checked whether the current user is a member of the group “Mygroup”. The command is as follows:

```
ldap_compare('192.168.10.10;CN=Peter Mueller,OU=SBSUsers,
OU=Users,OU=MyBusiness,DC=Firma,DC=local;mypassword;OU=SBSUsers,
OU=Users,OU=MyBusiness,DC=Firma,DC=local;
(mail=$sender)','memberOF',Meinegruppe');
```

Note:
- If the specified attribute or the entry browsed for does not exist, the return value will be negative.
- If several entries are found, only the first one will be analysed.
- If several attributes are present, all attributes will be analysed (multi-value).
- If none of the specified LDAP servers is available, the e-mail will be rejected with a temporary error.

5.7.2 ldap_read

The ldap_read command can be used to read a value stored within an LDAP register. The command is designed as follows:

```
ldap_read(URI;USER;PASSWORD;BASEDN;FILTER,ATTR,VAR);
```

This command will establish a connection to an LDAP server and will store the value of the queried attribute in the variable VAR. The return value will be positive if a value can be assigned to the variable

VAR; otherwise, the value will be negative.

Explanation of the parameters:

URI	The IP address or the name of the LDAP server. It is also possible to enter two values separated by a comma. In this case, the second server will be used automatically if the first server is not available..
USER	The user to be used for the purposes of access.
PASSWORD	The password of the user.
BASEDN	The base DN (distinguished name) for the query.
FILTER	The filter for the query
ATTR	The attribute that is to be queried.
VAR	The value that is to exist within the attribute.

Parameters of the ldap_read command

Example: The value of the attribute "name" is to be read from an LDAP register. The aforementioned is to be stored in the variable “name”.

```
ldap_read('192.168.10.10;CN=Peter Mueller,OU=SBSUsers,OU=Users,
OU=MyBusiness,DC=Firma,DC=local;mypassword;OU=SBSUsers,OU=Users,
OU=MyBusiness,DC=Firma,DC=local;
(mail=$sender)','name','name'););
```

Note:
- If the specified attribute or the entry browsed for does not exist, an empty value will be assigned to the variable.
- If several entries (objects) are found, only the first one will be analysed.
- If several attributes are present, all attributes will be read out and assigned to the variable (multi-value attribute) separated by means of semi-colons “;”.
- If none of the specified LDAP servers is available, the e-mail will be rejected with a temporary error.

5.8 Commands for content management

5.8.1 iscalendar

The `iscalendar` command can be used to check an e-mail in accordance with the mime type "text/calendar". The command is designed as follows:

```
iscalendar ()
```

Checks whether the e-mail has the mime type “text/calendar”. If this is the case, the return value will be positive. This command can be used to prevent invitations from being signed. Microsoft Outlook is not able to deal with signed calendar entries.

5.8.2 isspam

The `isspam` command can be used to implement a spam check. The command is designed as follows:

```
isspam (MARKLEVEL,TAG,REJECTLEVEL)
```

5.8.3 partoftype

The `partoftype` command can be used to check the type of the e-mail attachments. The command is designed as follows:

```
partoftype ("Typ", "Action", "Check Archives")
```

This command checks whether the attachments of the e-mail are of a certain `Type`. The `Action` defines what will happen with the attachments the examination of which has resulted in a positive result.
The following operations are available for `Action:`

- `info` makes the result available for the following commands.
- `delete` additionally removes the corresponding attachment from the e-mail.

Contents of file archives will be browsed if `Check archive contents` is characterised by the Boolean value true. Instead of true it is also possible to use yes or 1.

The return value will always be positive if at least one finding of the examination of the attachments of the e-mail is positive. Otherwise, the value will be negative.

You can find further information on the argument `Type` in chapter List of file types 220.

5.8.4 vscan

The `vscan` command can be used to check e-mail attachments for viruses. The command is designed as follows:

```
vscan ("Action", "Check archive contents")
```

This command will check all attachments of the e-mail for known viruses. The `Action` defines what will happen with the attachments the examination of which has resulted in a positive result. The following operations are available for `Action`:

- `info` makes the result available for the following commands..

- `clean` additionally disinfects the affected attachment.
- `delete` removes the corresponding attachment from the e-mail

Contents of file archives will be browsed if `Check archive contents` is characterised by the Boolean value true. Instead of true it is also possible to use yes or 1.

The return value will always be positive if at least one finding of the examination of the attachments of the e-mail is positive. Otherwise, the value will be negative.

5.9 File types

5.9.1 List of File Types

The following file types are differentiated:

ID	Description
BMP	PC Bitmap
BZIP	BZIP Compressed
CAB	Microsoft CAB file
COM	MSDOS Computable
EMF	Enhanced Windows Metafile
EXE	MSDOS Executable
FAX	G3 Fax
GIF	GIF Image
GZIP	GZIP Compressed
ICO	Windows Icon
ISO9660	ISO 9660 CD-ROM
JPEG	JPEG Image
JPG2000	JPEG 2000 Image
LHA	LHa 2.x? Archive
LHARC	LHarc 1.x Archive
LWF	LuraWave Image
MPEG.L3	MPEG Layer 3
MPEG.SYS	MPEG System Stream
MPEG.VID	MPEG Video
MS.ASF	Microsoft ASF
MS.OFF	MS Office document
MS.XLS	MS Excel 5.0 Worksheet
NIFF	NIFF Image
PBMPLUS	PBMPLUS Bitmap
PCX	Z-Soft Image
PDF	PDF Document
PNG	PNG Image
RAR	RAR Archive
RIFF.ANI	MS RIFF Animated Cursor
RIFF.AVI	MS RIFF Audio Video Interleave
RIFF.DIB	MS RIFF DIB Bitmap
RIFF.MID	MS RIFF MIDI File
RIFF.MMF	MS RIFF Multimedia Movie
RIFF.WAV	MS RIFF Wave Audio
RTF	Rich Text Format
TAR	TAR Archive

ID	Description
TARGA	TARGA Bitmap
TIFF	TIFF Image
ZIP	PKZIP Archive
ZOO	Zoo Archive

List of the file types

5.9.2 File Type Groups

The following groups of file types are differentiated:

ID	Description	File types comprised
ARCHIVES	Archive files	ZIP ZIP.SFX RAR LHARC LHA SQUISH UC2 ZOO TAR CAB BZIP GZIP
EXE	Executable files	EXE.PE EXE COM
FS	File systems	ISO9660 HISIERRA
IMAGES	Images	JPEG BMP TIFF PNG GIF TARGA PBMPLUS NIFF FAX PCX LWF ICO JPG2000 EMF
MEDIA	Multimedia	RIFF.WAV RIFF.AVI RIFF.ANI RIFF.MID RIFF.MMF RIFF.DIB RIFF RIFX MPEG.VID MPEG.SYS MPEG.L3 MS.ASF
OFFICE	Office documents	RTF PDF MS.OFF MS.XLS

Groups of file types