CIPHERMAIL EMAIL ENCRYPTION

Ciphermail Webmail Messenger Administration Guide

October 27, 2017, Rev: 8630

Contents

1 Introduction

Ciphermail Webmail Messenger is a secure pull delivery webmail add-on to the CipherMail encryption gateway. If the rules of the CipherMail encryption gateway determine that a message must be encrypted, and S/MIME, PGP or PDF cannot be used, the email will be sent to the CipherMail Webmail Messenger box via an S/MIME secured tunnel. The recipient gets a notification that a new message is available. The first time the user receives a message, the user needs to select a secure password. The user can read and reply to the message using any web browser.

Note

This guide provides in-depth information about the webmail appliance. For a quick setup guide of the webmail appliance, see the “webmail quick setup guide”.

The following steps are taken when sending an email to a recipient via Webmail Messenger (see figure 1):

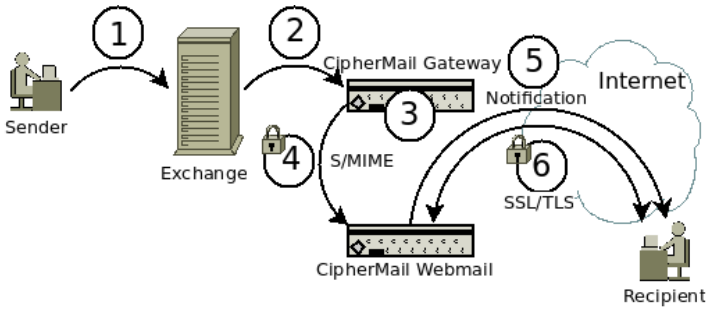

Figure 1: Webmail Messenger mail flow

1. User sends email via Exchange (or some other mail server)
2. Exchange forwards the message to the CipherMail gateway.
3. A rule on the CipherMail gateway flags that the email must be sent to Webmail Messenger.
4. The message gets S/MIME signed with the webmail sender key and encrypted with the webmail recipient certificate and forwarded via email to the webmail appliance. The webmail appliance decrypts the mail, checks the signature and places the email in the mailbox of the recipient(s).
5. A notification message is sent to the recipient that a message is available for pick-up.
6. The user logs-in with a browser via HTTPS and reads the message.

2 Admin login

The administration GUI can be accessed by opening the following URL in a browser:
https://192.168.1.139:8443 (change the IP address to to match the address of the webmail box).

Figure 2: Login dialog

The login page should appear (See figure 2).

Login credentials: Use the following default credentials:

username: admin
password: admin

Note: it can take some time to login after a restart because the web application must be initialized upon first login.

3 Network

Since the CipherMail Webmail Messenger box needs to relay email to external recipients, the DNS servers should be configured. The network settings can be configured from the WEB GUI. The network info page can be opened by clicking Admin → network. The "Network info" page will be opened which provides all the relevant network information like DNS servers, network interfaces etc. (see figure 3).

Note: Since most network settings should be configured from the WEB GUI, the WEB GUI should have a valid IP before the WEB GUI can be accessed. A valid IP address can be setup with the console system application by logging into the console. See the "Virtual Appliance Guide" for more information.

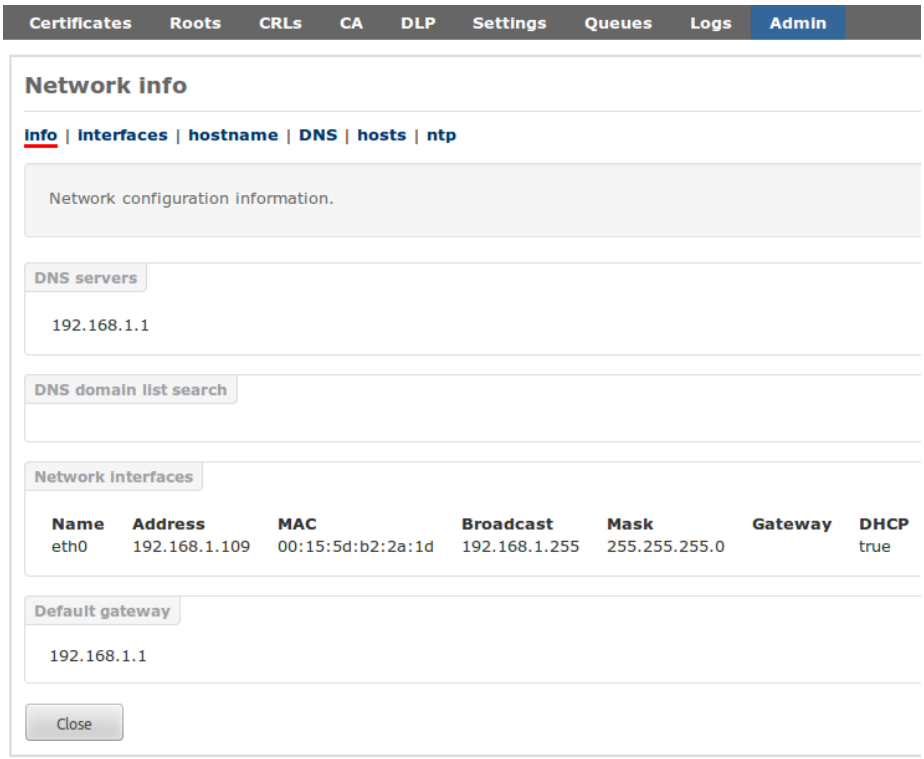

Figure 3: Network info

3.1 Network interfaces

The available network interfaces can be configured by clicking “interfaces”. This opens the interfaces page (see figure 4). A network interface can be configured by clicking the “gear” icon of the interface. The network interface can be configured for a dynamic IP address (DHCP) or for a static IP address (see figure 5

3.2 Hostname

With the hostname page, the hostname of the gateway can set (see figure 6. The hostname is used by many of the networking programs to identify the machine.

Note: It’s advised to use a fully qualified hostname.

3.3 DNS

The gateway requires at least one DNS server. The DNS server can be configured with the DNS page (see figure 7)

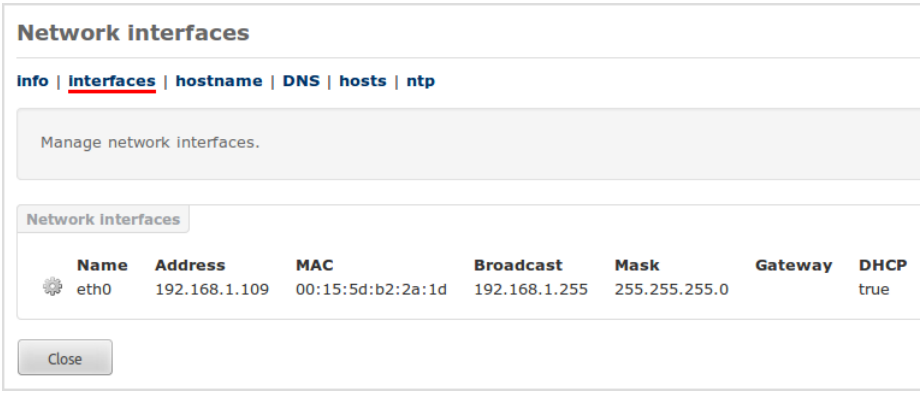

Figure 4: Network interfaces

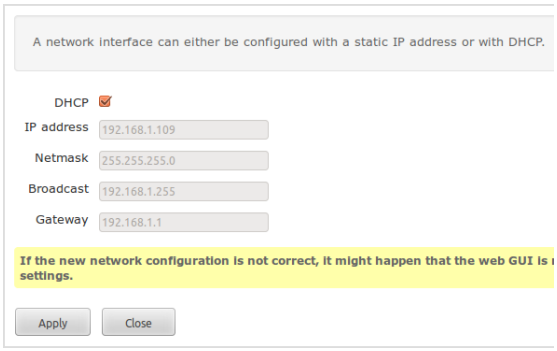

Figure 5: Network interface

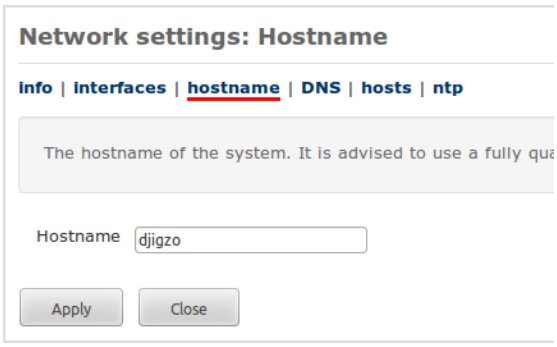

Figure 6: Hostname

3.4 Hosts

The hosts table is a static lookup table for hostnames (see figure 8. In most setups, there is no need to add a static hostname to the hosts table. When the hostname (see hostname setting) is changed, the hosts table is automatically updated.

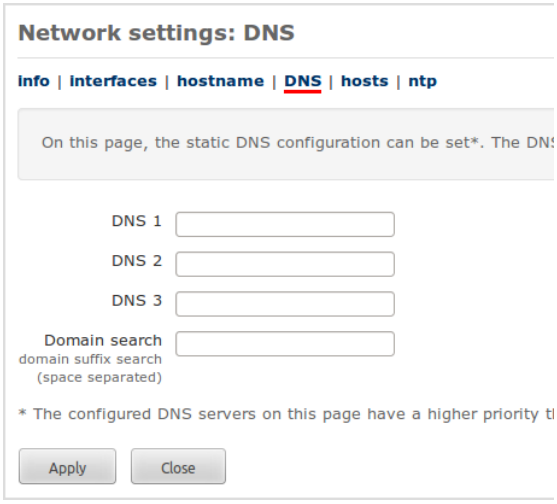

Figure 7: DNS

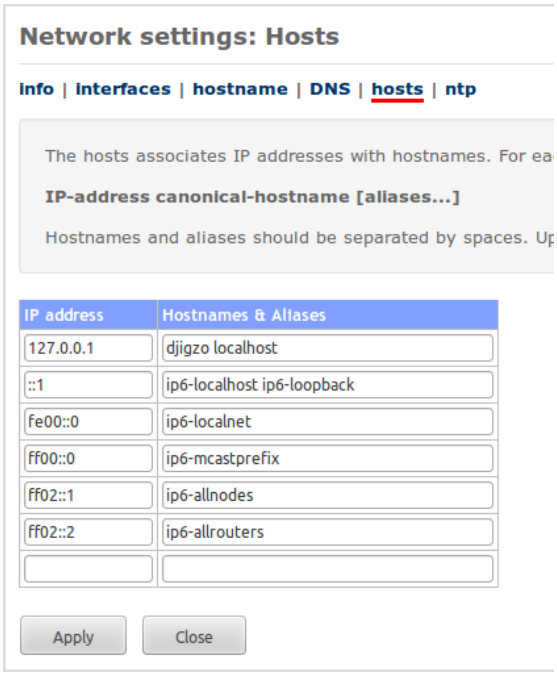

Figure 8: Hosts

3.5 NTP

The gateway uses the Network Time Protocol (NTP) to keep the system clock synchronized with the real time. By default it uses the NTP servers from debian.pool.ntp.org (see figure 9. If you are running your own NTP server, change this to match the IPs or hostnames of the NTP servers.

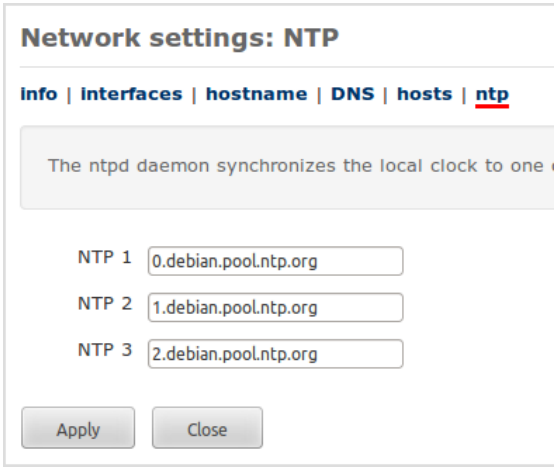

Figure 9: NTP

4 MTA setup

The CipherMail Webmail box uses Postfix as the “Mail Transfer Agent” (MTA). The MTA is responsible for sending and receiving email. Encryption and decryption of email is handled by the “Mail Processing Agent” (MPA). The “MTA config” page can be used to configure most of the relevant Postfix parameters.

The “MTA config” page can be opened from the Admin menu. The “MTA config” page (see figure 10) contains most of the relevant Postfix parameters for a “store and forward” email server. Postfix parameters which cannot be set with the “MTA config” page should be set with the “MTA raw config page” (or alternatively by directly editing the Postfix configuration files). The relevant Postfix settings will be explained in the following section. For a more thorough explanation of all the Postfix settings see the Postfix documentation (http://www.postfix.org/documentation.html).

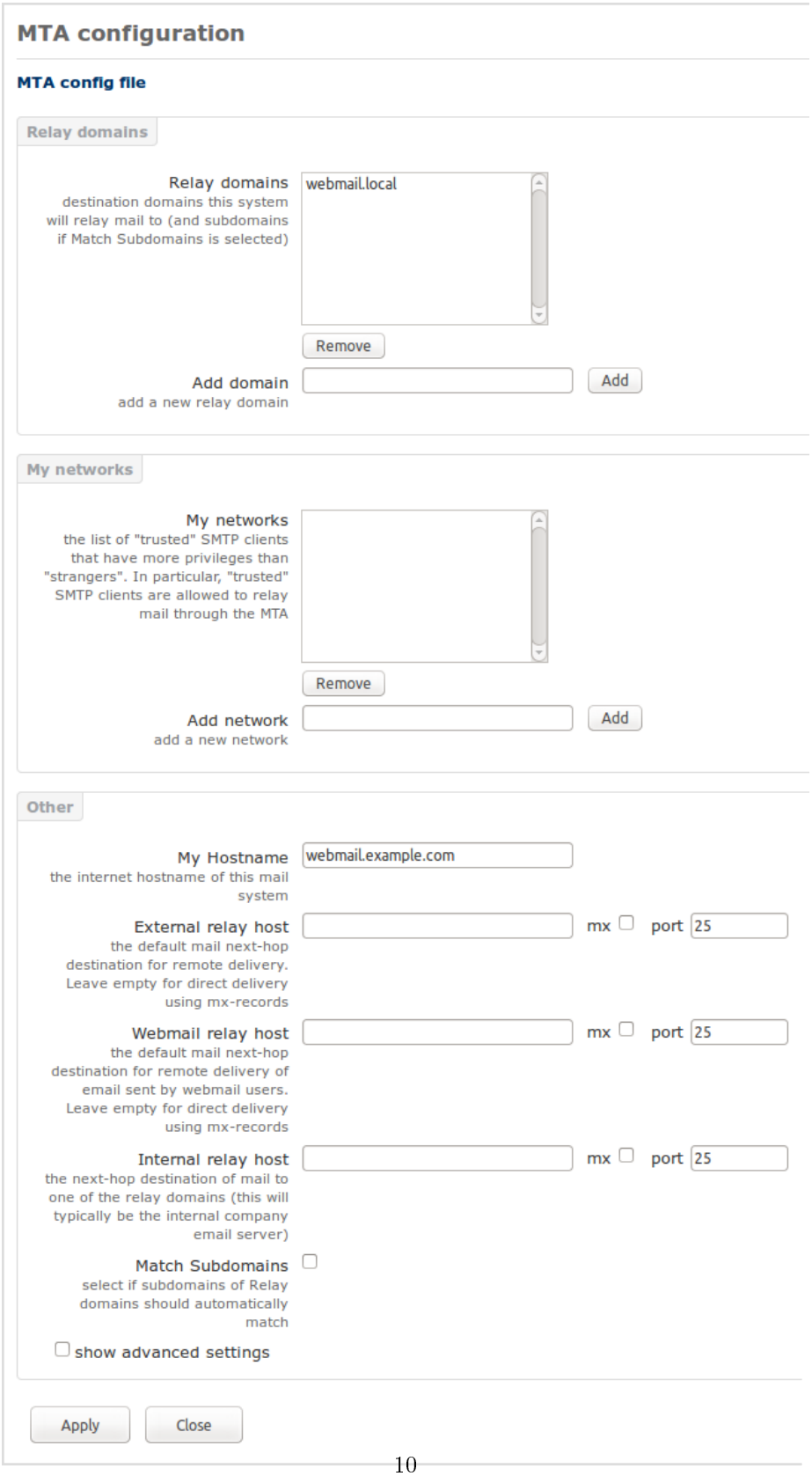

Figure 10: MTA config

4.1 Main settings

Relay domains Relay domains are domains for which the gateway needs to receive email. These are the domains for which the internal users receive email. A “store and forward” server normally has one or more relay domains (unless the CipherMail gateway is only used for sending email).

Note: If “Match Subdomains” is selected (see other settings), subdomains of the relay domains are matched as well. If “Match Subdomains” is not selected, subdomains of the relay domains only match if the subdomains are explicitly added to the relay domains. For most setups, it is advised to explicitly add all the subdomains for which email should be received and leave “Match Subdomains” off.

Example: if “Match Subdomains” is selected, and example.com is added to the relay domains, then incoming email for the domain subdomain.example.com is accepted as well even if subdomain.example.com is not explicitly added to the relay domains.

My networks Most email senders (users and other internal email servers) are not allowed to send email to domains not specified as a “relay domain”. To allow outgoing email to be sent to external domains, the sender IP address should be “white-listed”. The “My networks” list contains all the networks that are allowed to send email to external domains. The networks must be specified in CIDR notation. **Example**: 192.168.1.1/32, 10.1.2.0/24.

Warning

Only allow IP ranges under your control to relay email to external recipients. If IP ranges not under your control are allowed, the gateway will be an open relay and misused for sending spam.

My Hostname This should be the fully qualified domain name of the email server and is used as the default value for many other configuration parameters. For example “My Hostname” is used as the default domain for email messages sent with a missing domain name and is used for the default SMTP helo/ehlo name (see “SMTP helo name” setting below).

If the gateway directly delivers email to external recipients (i.e., not using an external relay host) it is important that the helo/ehlo name of the gateway is equal to the reverse lookup of the external IP address. If not, outgoing email can be flagged as spam. See Appendix A for more information.

External relay host The external relay host is used when email should be sent to an external domain (i.e., a domain which is not a relay domain). This can be the ISPs email server or some internal email server responsible for sending email to external domains.

If “External relay host” is not specified, email will be delivered using DNS MX-records. “External relay host” can be an IP address or a domain name. If the option “mx” is checked, the MX-records of the “External relay host” will be used instead of the A-record (this setting is only used when the “External relay host” is specified). The “port” setting is the port the “External relay host” server listens on (which in most cases should be the default SMTP port 25).

Internal relay host The internal relay host is used when email should be sent to an internal domain (i.e., sent to a relay domain). Typically this will be the companies internal email server hosting the users email boxes.

If “Internal relay host” is not specified, email will be delivered using DNS MX-records. “Internal relay host” can be an IP address or a domain name. If the option “mx” is checked, the MX-records of the “Internal relay host” will be used instead of the A-record (this setting is only used when the “Internal relay host” is specified). The “port” is the port the “Internal relay host” server listens on (which in most cases should be the default SMTP port 25).

Webmail relay host The webmail relay host is used for email sent by webmail users. Typically this will be set to the same address as the “Internal relay host”.

Match Subdomains If “Match Subdomains” is selected, all subdomains of the “Relay domains” will also be relayed.

4.2 Advanced settings

The advanced settings can be set when the “advanced settings” checkbox is selected (see figure 11).

Before filter message size limit This is the maximum size of a message (in bytes) that the MTA accepts. A message that exceeds the maximum size is rejected by the MTA.

Note: Because of Base64 encoding, binary attachments (for example word documents) will be 4/3 times larger if sent by email. The maximum size limit, limits the total number of bytes including encoding. For example, if the limit is set to 10 MB, the total size of all the attachments cannot exceed 7.5 MB.

After filter message size limit The mail processing agent of the gateway is responsible for encryption and decryption of messages. The size of a message after encryption or decryption (or after signing) can be larger than the size of the message before encryption or decryption. The “after filter message size limit” should therefore be larger than the “before filter message size limit” otherwise the MTA will refuse to send the message after the MPA has handled the message. It is advised that the “after filter message size limit” should be at least 2 times larger than the “before filter message size limit”.

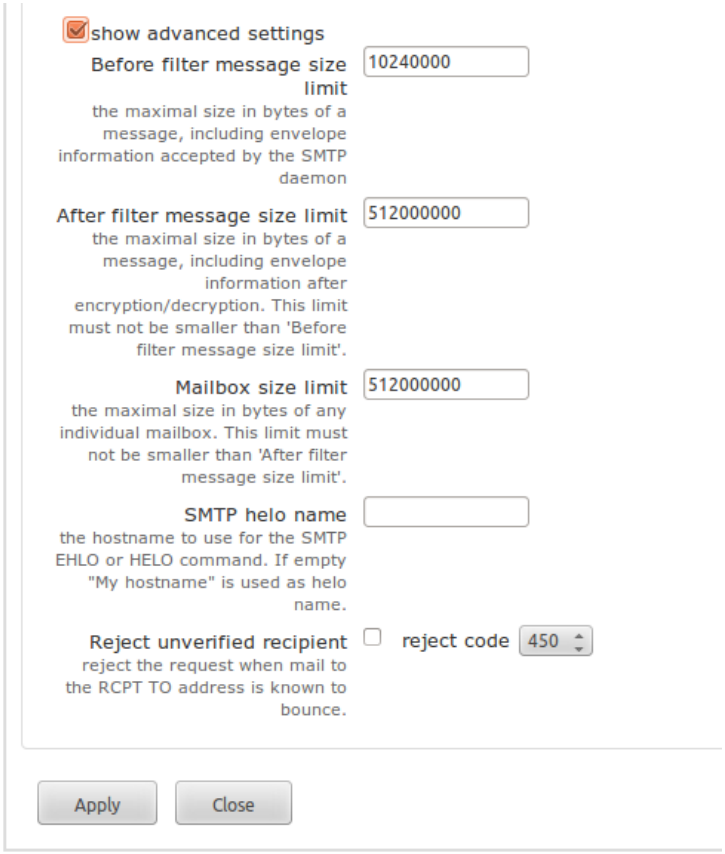

Figure 11: MTA advanced config

Mailbox size limit If mail is locally stored (only when “Local domains” are specified) the “Mailbox size limit” will be the maximum size (in bytes) of an individual mailbox. The “Mailbox size limit” should not be smaller than the “after filter message size limit”. This setting is only required when Postfix receives email for a local domain. By default the gateway does not enable the option to directly specify local domains.

SMTP helo name The “SMTP helo name” is the hostname used for the SMTP “EHLO” or “HELO” command. If “SMTP helo name” is not explicitly specified, “My Hostname” is used as the SMTP helo name.

Note: If the gateway directly delivers email to external recipients (i.e., not using an external relay host) it is important that the helo/ehlo name of the gateway is equal to the reverse lookup of the external IP address. If not, outgoing email can be flagged as spam. See Appendix A for more information.

Reject unverified recipient Normally an email server should know which internal email addresses are valid addresses (i.e., email addresses for which an

inbox exists). When an email server is setup to relay email for certain domains the email server should know which recipients will be accepted by the server it relays to (in other words it should be a smart relay host). If all email is accepted for relay without knowing whether the next email server will accept the email, there is a risk of generating "backscatter" bounces. Backscatter bounces, occur when an intermediate email server accepts a message without checking whether the next email server accepts the message. Because the intermediate email server accepted the message, it has to be bounced back to the original sender when the next server does accept the forwarded email. If the email was a spam message using a forged sender, the sender will be flooded with bounced messages.

There are multiple ways for an email server to known which recipient addresses are acceptable and which are not. One solution is to let the gateway server "learn" which recipient addresses are acceptable by querying the server it relays to. When an email is received for a yet unknown recipient, the server "asks" the server it relays to whether the recipient is a valid recipient or not. The message is only accepted when the next email server reports that the recipient is a valid recipient. The result of this verification process is cached.

The verification procedure is enabled by checking "Reject unverified recipient". The "reject code" is the SMTP result code used when the email is not accepted. This should initially be set to "450" (which tells the connecting SMTP server that the message is not accepted because of a temporary error). It should be changed to "550" (permanent error) when the verification procedure works correctly. See the Postfix documentation for more information on address verification[1].

There are other ways for the email server to know which recipients are valid, for example using LDAP queries or by specifying `relay_recipient_maps`. These other options are however not directly supported by the "MTA config" page and should therefore be configured using the "MTA raw config" page or by directly editing the Postfix configuration files.

Applying changes By clicking the "Apply" button, the changes will be checked and Postfix will be configured with the new settings. Clicking the "Close" button will redirect the browser to the "Admins" page.

5 System status

After login, the system status page will be shown (see figure 12). The system status provides a quick overview of the state of the system. For example it shows the status of several system queues and some historical performance graphs.

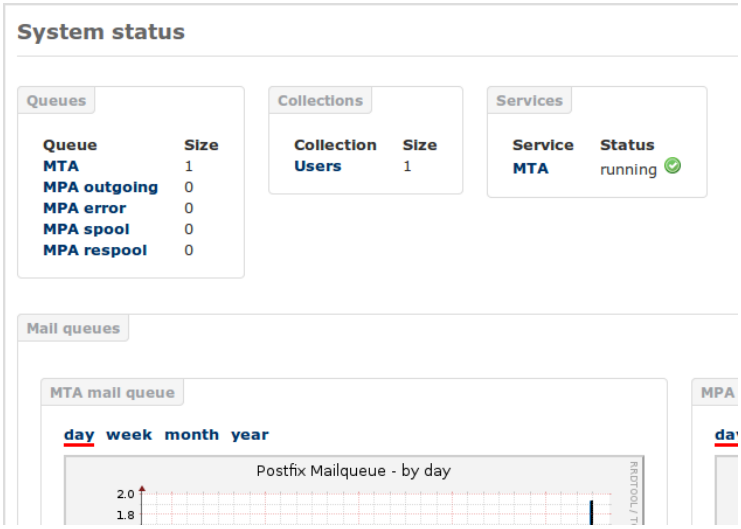

Figure 12: System status

6 Configuration

6.1 Global preferences

The global preferences can be edited by selecting “Settings” from the main menu toolbar. The global preferences page contain a number of required settings (see figure 13).

Min. password strength To make sure that the password of a webmail account is strong enough, some checks on the password strength are activated when a new password is set. The password strength is estimated using the algorithm from “NIST Special Publication 800-63”. A new webmail password is only accepted if the password:

1. is not based on the email address of the account
2. does not contain a QWERTY keyboard sequence of more than 5 characters
3. does not contain more than 5 duplicate characters in a row
4. is of sufficient strength in bits

Relay recipient (required setting) This is the email recipient address to which the tunnelled S/MIME message will be sent from the CipherMail gateway. “Relay recipient” must match the “Webmail recipient” setting on the CipherMail gateway (see figure 13).

[1] See http://www.postfix.org/ADDRESS_VERIFICATION_README.html

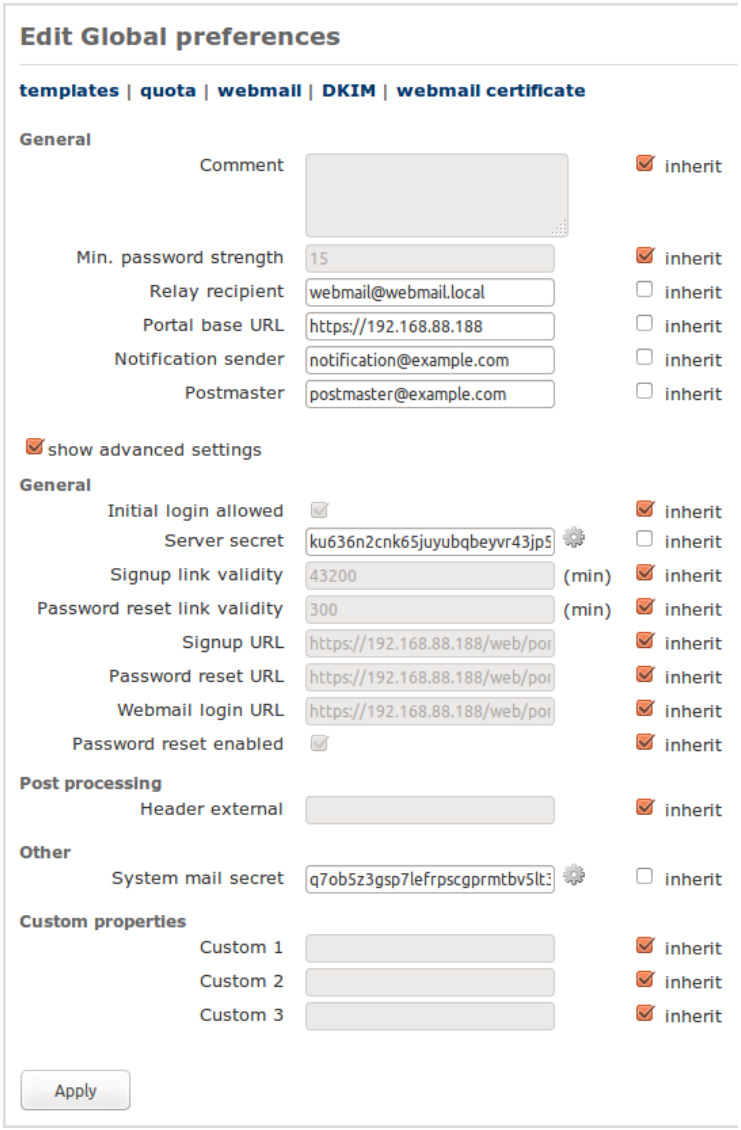

Figure 13: Webmail global settings

Portal base URL (required setting) The base URL for the user sign-up and password reset pages. This should normally be set to the fully qualified domain name (or IP address) of the server. Example: `https://webmail.ciphermail.com`.

Notification sender (required setting) By default, notification messages (sign-up and email notification messages) will use “Notification sender” for the from address of the emails.

Note: The from address handling used for the notification messages can be changed by changing the message templates.

Postmaster (required setting) If there is some error with the S/MIME tunnelled message, for example the message was signed with an untrusted certificate, the email will be forwarded to the "Postmaster".

Initial login allowed By default, a user is allowed to login after signing up. If a two step process is required with final manual approval, "Initial login allowed" can be disabled. When "Initial login allowed" is disabled, an admin should enable the account manually after the user has signed up.

Server secret The server secret is used to protect external resources against tampering (using the HMAC algorithm). For example the sign-up link in the sign-up message is protected to make sure that a recipient cannot change the URL. A global server secret will be automatically generated the first time the server starts. The server secret is a required setting. In most setups there is no need to override the inherited server secret.

System mail secret The "System mail secret" is used together with DIKM to "sign" email generated by the webmail appliance. This allows the gateway to detect that an email was generated by the gateway. If an email was generated by the gateway, and the email is again received by the gateway (for example because of forwarding), the email will be sent as-is and not handled again. This prevents possible mail loops. A system mail secret will be automatically generated the first time the server starts.

Signup link validity The number of minutes a sign-up link is valid.

Password reset link validity The number of minutes a password reset link is valid.

Signup URL The URL for the sign-up page. In most setups this will be automatically set to the correct URL and there is no need to change it.

Password reset URL The URL for the password reset page. In most setups this will be automatically set to the correct URL and there is no need to change it.

Webmail login URL The URL for the Webmail login page. In most setups this will be automatically set to the correct URL and there is no need to change it.

Custom properties The custom properties are only used if custom rules are added to the mail flow (config.xml). This is not used in most setups.

6.2 Quota

The maximum size an individual mailbox may grow is determined by the quota for that user. The user quota can be set on the “User quota” page (see figure 14). The global quota settings page can be opened from the global settings page by clicking the “quota” link. The quota settings page for an individual user can be opened from the preferences page for that user.

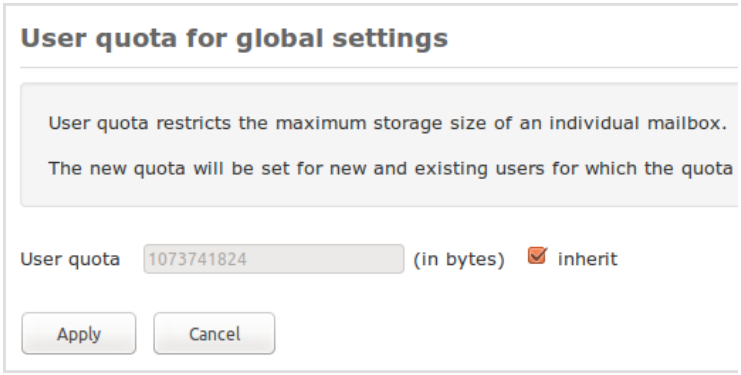

Figure 14: Mailbox quota

6.3 Webmail settings

The “Webmail settings” page contains settings for the webmail client (see figure 15). The webmail settings page can be opened from the global settings page by clicking the “webmail” link. The webmail settings can only be set for the global preferences.

6.3.1 Max attachment size

The “Max attachment size” sets the maximum size of an attachment (in bytes) a user is allowed to add to a message.

6.3.2 Auto cleanup enabled

The webmail appliance can be configured to automatically delete emails older than a configured number of days. This makes managing the gateway easier because it’s less likely to run out of disk space if emails are not kept indefinitely. Removing old email is also advised for security reasons because emails which are deleted cannot be leaked.

To enable auto cleanup, select the checkbox “Auto cleanup enabled”.

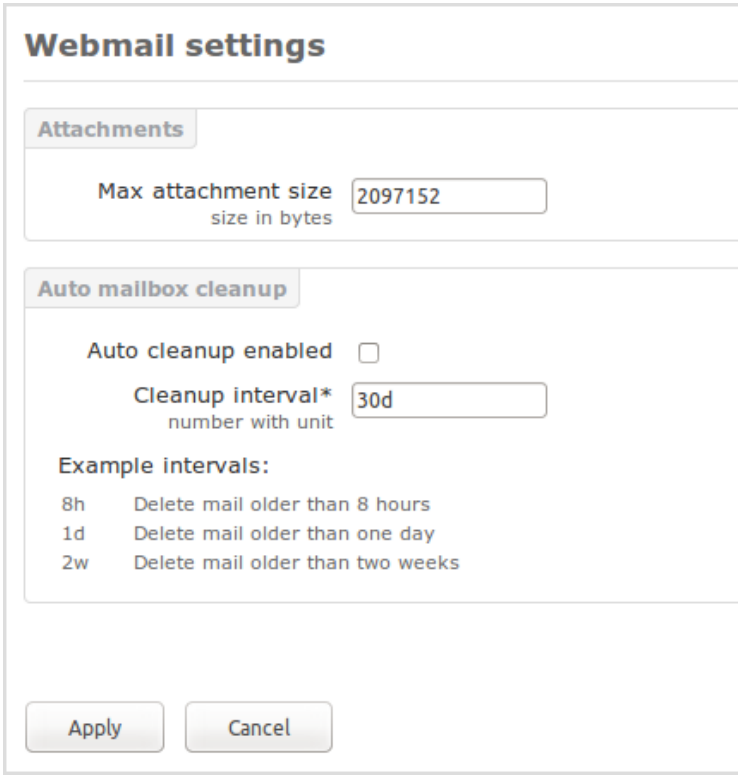

Figure 15: Webmail settings

Note

It's advised to enable "auto cleanup". Auto cleanup makes it less likely that the appliance runs out of space and increases security because sensitive messages are automatically deleted after a defined period.

6.3.3 Cleanup interval

The "Cleanup interval" determines how long email will be kept if "Auto cleanup enabled" is enabled.

Example cleanup intervals:

8h	Delete mail older than 8 hours
1d	Delete mail older than one day
2w	Delete mail older than two weeks

6.4 Webmail certificate

The special message sent from the CipherMail gateway to the webmail appliance (step 4 in figure 1) is signed and encrypted with S/MIME. The webmail appliance therefore requires a certificate with an associated private key.

A webmail tunnel certificate can be created with the “Create webmail relay recipient certificate” page which can be opened by clicking the “webmail certificate” link on the “Edit Global preferences page” (see figure 13). This will open the page on which the certificate and key can be created (see figure 16).

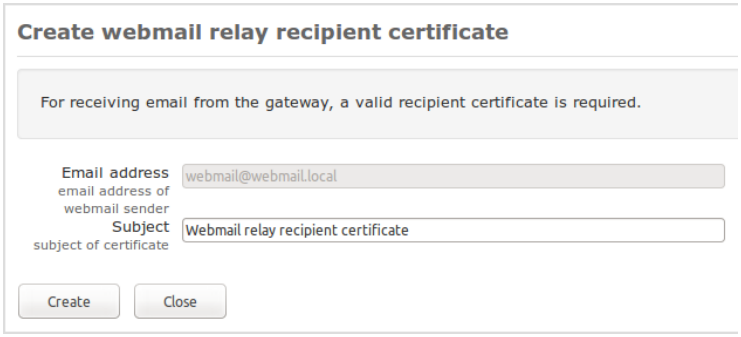

Figure 16: Create tunnel certificate

6.5 S/MIME tunnel

When the CipherMail gateway needs to send a message to the CipherMail Webmail box, the gateway wraps the original message together with some meta information into a new message. The wrapped message will then be S/MIME signed and encrypted and sent to the CipherMail Webmail box (to a special relay email address). The CipherMail Webmail box will decrypt the wrapped message, checks the signature and if the signature is correct, it will deliver the message to the (internal) mailbox of the recipient. The recipient will receive a notification message that a new email is waiting. The first time a message is received (i.e., if there is no internal mailbox yet for the recipient), the user will receive in invitation message with which the recipient can create a password for the mailbox.

The S/MIME tunnel between the CipherMail gateway and the CipherMail Webmail box, requires the following steps:

1. Choose an email address which will be used as the sender address for the email sent from the CipherMail gateway to the CipherMail Webmail box (i.e, the sender of the tunnelled message).
2. On the global Webmail settings of the CipherMail gateway (see figure 17), set “Webmail sender” to the email address selected in the previous step.
3. Choose a recipient email address for the tunnel massage sent from the CipherMail gateway to the CipherMail Webmail box (i.e., the recipient of

the tunnelled message).

4. On the global Webmail settings of the CipherMail gateway, set “Webmail recipient” to the email address selected in the previous step.
5. On the global settings of the CipherMail Webmail box (see figure 13), set “Relay recipient” to the email address from step 3.
6. On the global settings of the CipherMail Webmail box, set “Notification sender”.
7. On the global settings of the CipherMail Webmail box, set “Postmaster”.
8. On the global settings of the CipherMail Webmail box, set “Portal Base URL” to the full URL of the Webmail box.
9. Generate or import a signing certificate (with private key) on the CipherMail gateway (set the email address of the certificate to the email address from step 1).
10. Import the public certificate from the previous step into the CipherMail Webmail box (Admin → PKI → Certificates) and make sure the certificate is trusted (either because it is issued by a trusted root or by white-listing the certificate).
11. Generate or import an encryption certificate (with private key) on the CipherMail Webmail box.
12. Import the public certificate from the previous step into the CipherMail gateway and make sure the certificate is trusted (either because it is issued by a trusted root or by white-listing the certificate).

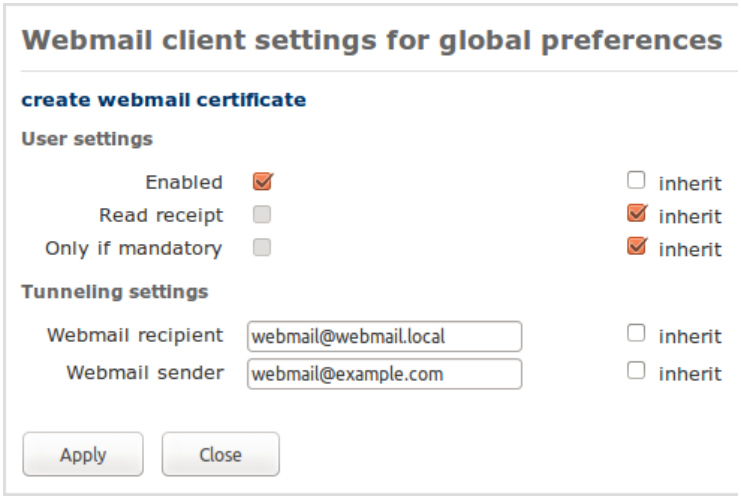

Figure 17: CipherMail gateway webmail global settings

7 Users

For every user a webmail account will be automatically created by the system. When a new webmail account is created for a user, a local webmail box is created and a user objects is added to the user store. The user settings can be viewed and edited by clicking the user on the Users page. The user settings page shows information about the mailbox of the user (see figure 18).

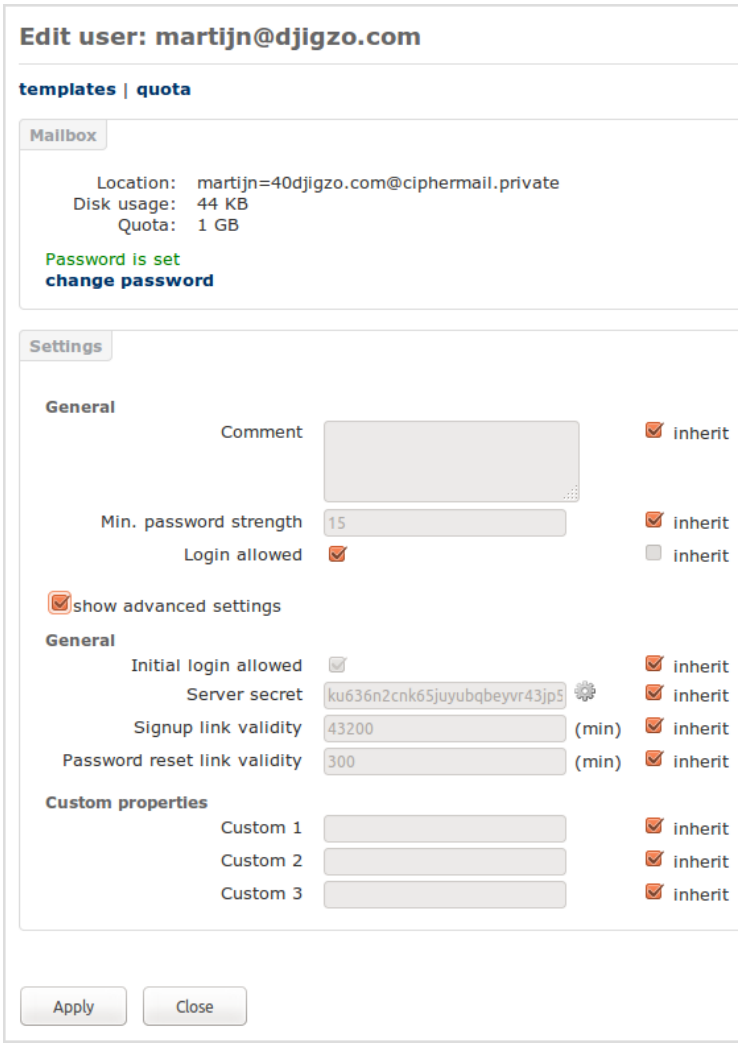

Figure 18: Webmail user preferences

Mailbox If a user has a mailbox, the name if the mailbox will be shown [2]. If the user has signed-up and a password was set, "Password is set" will be shown. If "Password is not set" is shown, but the user has a mailbox, it means that a sign-up message was sent to the user but the user did not yet set a password.

[2] The mail will be stored on the filesystem in a directory similar to the name of the mailbox

Settings All other user settings are similar to the global settings. By default these settings will be inherited from the domain or global settings.

7.1 Removing users

User can be removed by selecting the users and then click “delete selected”. Alternatively the user can be directly deleted by clicking the red “cross” in from of the email address of the user. After a user has been deleted and a new message is sent to the user, the user receives a new sign-up email with which the account can be recreated.

Note

Deleting the user does not result in the removal of the users mailbox. After the re-sign up, the user again has access to old emails. To completely delete all email for a user, remove the complete mailbox.

7.2 Mailboxes

The user mailboxes can be managed on the “Mailboxes” (see figure 19) which can be opened by clicking the “mailboxes” link on the “Users” page. The mailboxes pages provides details about the available mailboxes like size of the mailbox.

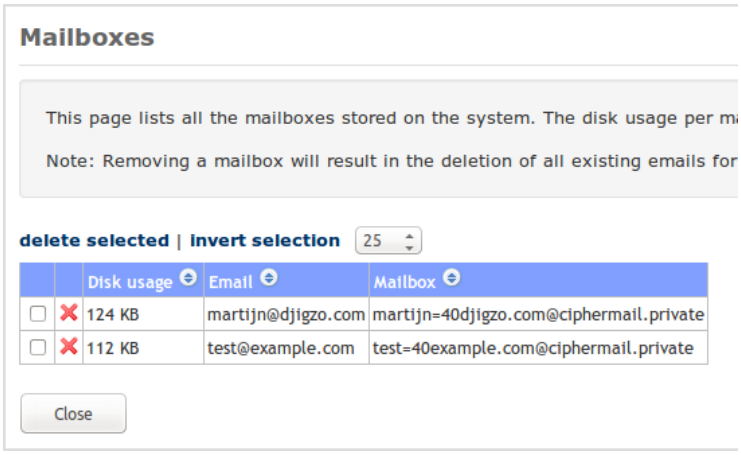

Figure 19: Mailboxes

8 Backup and restore

8.1 System backup

The backup manager can be used to backup and restore all the relevant system settings (including the certificates, keys and MTA settings). A backup can

be created and downloaded to the administrators computer or a backup can be stored on a remote SAMBA share (see figure 20). A backup can be automatically initiated at set intervals and stored (encrypted or non encrypted) on a remote SAMBA share. A backup can be password encrypted. If no password is specified the backup will not be encrypted.

Warning: restoring a backup will overwrite all local settings and cannot be undone. The system will be restarted after the restore.

Note

The backup procedure does not backup the user email.

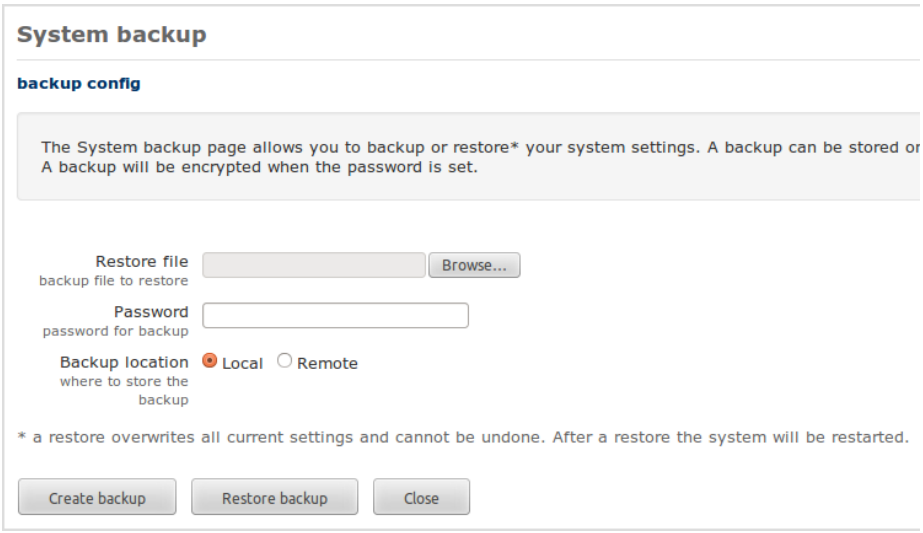

Figure 20: System Backup

8.2 Backup configuration

The backup configuration page is used to configure the remote SAMBA share and configure the automatic backup (see figure 21).

8.2.1 SMB share settings

The SMB share settings specify which remote SAMBA share should be used for remote backups (automatic backups can only be stored on a remote share). The remote share can be any server that supports the SMB protocol (for example Microsoft Windows Network or SAMBA). “Test connection” can be used to test whether the specified share can be accessed with the provided settings and credentials.

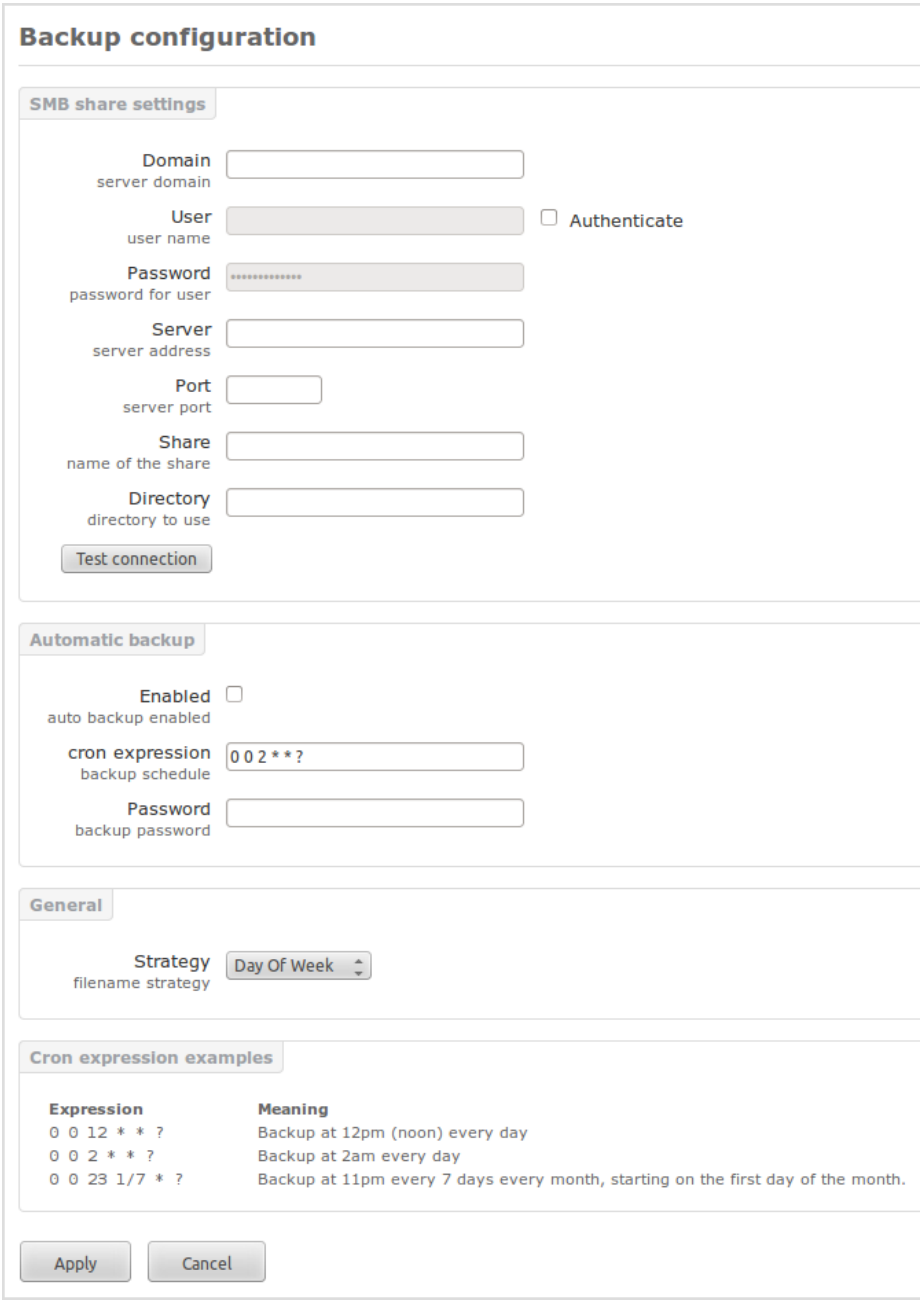

Figure 21: Backup configuration

8.2.2 Automatic backup

Enabled Remote backups can be automatically initiated at set intervals. To enable automatic backups the “enabled” checkbox should be checked.

Cron expression The cron expression[3] determines at which intervals a backup will be started. The default cron expression **0 0 2 * * ?** automatically starts a backup every night at 2 o'clock (see Appendix B for more cron expression examples).

Password The password with which the backup will be encrypted.

8.2.3 Other

Strategy The filename of the backup is determined by the "strategy". Choose between "day of week", "day of month", "day of year" and "timestamp". "Day of week" uses the day of the week as a filename postfix (1-7). "Day of month" uses the day number as a filename postfix (1-31). "Day of year" uses the day (1-365) as a filename postfix. "Timestamp" uses a filename based on the number of milliseconds since January 1, 1970 UTC.

9 Log export

With the log export, all system log files can be exported to a remote SAMBA share or downloaded to the local computer (see figure 22).

Figure 22: Log export

Password If a password is set, the exported logs will be PGP password encrypted.

Last modified If set, only log files which were modified within the last number of minutes will be exported. If not set, all logs files will be exported.

[3]For more info on the cron trigger format see http://www.quartz-scheduler.org/docs/tutorials/crontrigger.html

Export location The logs can be exported to the local computer (i.e., downloaded with the browser) or to a remote SAMBA share.

9.1 Log export config

The log export configuration page is used to configure the remote SAMBA share and configure automatic log export (see figure 23).

9.1.1 SMB share settings

The SMB share settings specify which remote SAMBA share should be used for remote log export (automatic log exports can only be stored on a remote share). The remote share can be any server that supports the SMB protocol (for example Microsoft Windows Network or SAMBA). “Test connection” can be used to test whether the specified share can be accessed with the provided settings and credentials.

9.1.2 Automatic log export

Enabled Remote exports can be automatically initiated at set intervals. To enable automatic exports the “enabled” checkbox should be checked.

Cron expression The cron expression[4] determines at which intervals a log export will be started. The default cron expression **0 0 3 * * ?** automatically starts an export every night at 3 o’clock (see Appendix B for more cron expression examples).

Password The password with which the exported logs will be encrypted.

9.1.3 Other

Strategy The filename of the export is determined by the “strategy”. Choose between “day of week”, “day of month”, “day of year” and “timestamp”. “Day of week” uses the day of the week as a filename postfix (1-7). “Day of month” uses the day number as a filename postfix (1-31). “Day of year” uses the day (1-365) as a filename postfix. “Timestamp” uses a filename based on the number of milliseconds since January 1, 1970 UTC.

10 System runtime control

The “System runtime control” page can be used to manage the runtime of the gateway (rebooting, and start/stopping the MTA etc. see figure 24). The “System runtime control” page can be opened by clicking Admin → system.

[4] For more info on the cron trigger format see http://www.quartz-scheduler.org/docs/tutorials/crontrigger.html

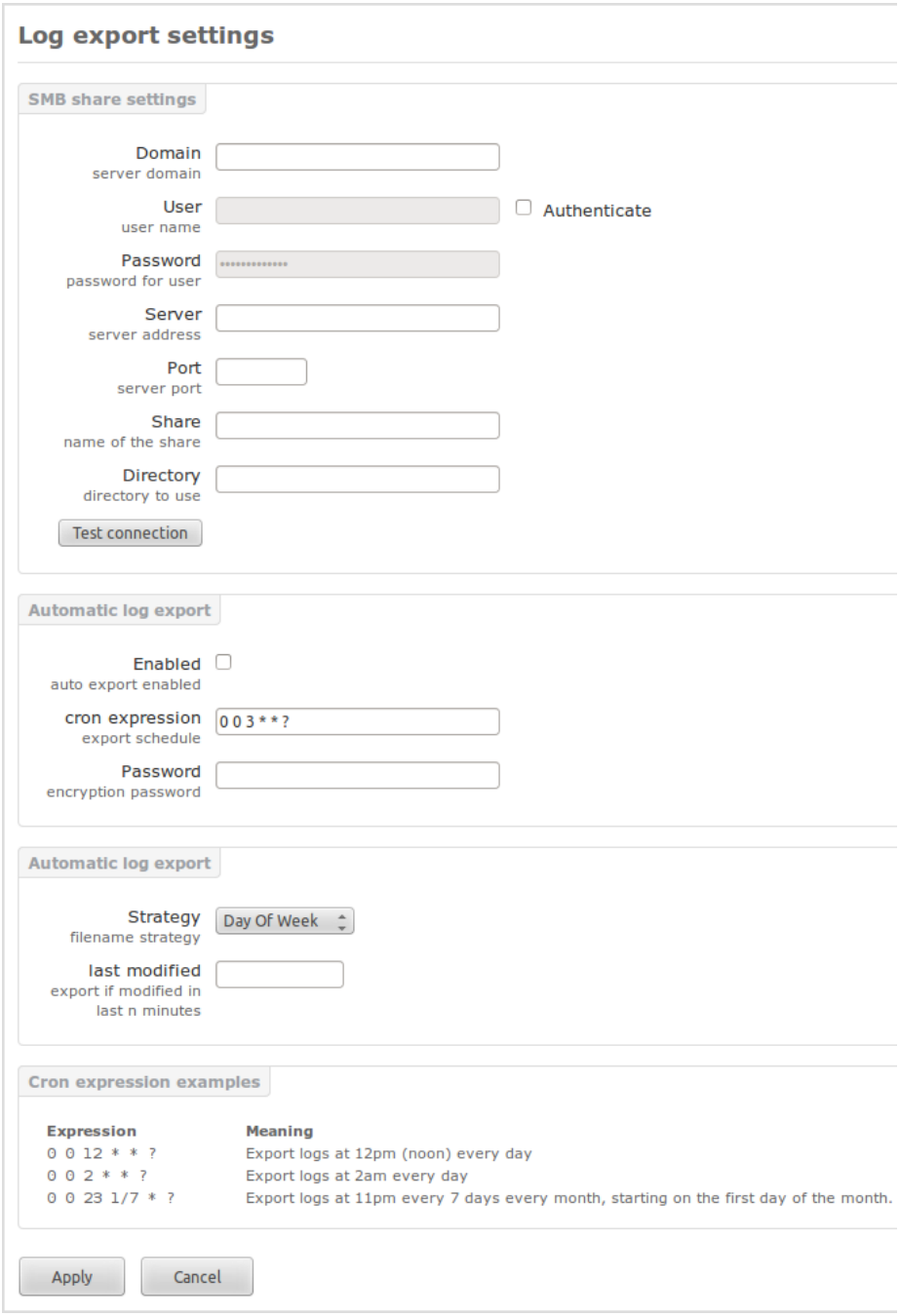

Figure 23: Log export settings

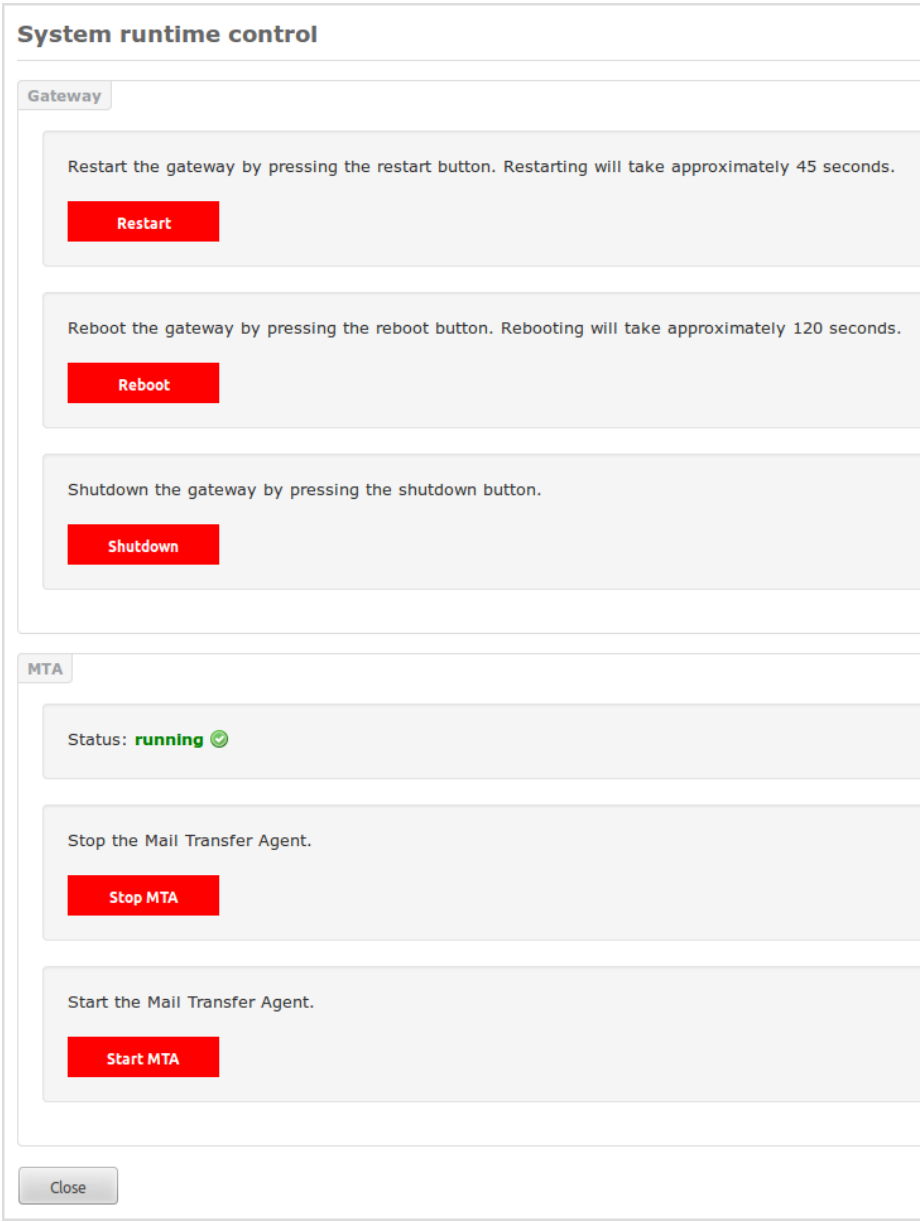

Figure 24: System runtime control

11 Compose test email

The “Compose test email” page can be used to create a test email to test the gateway settings (see figure 25). The “Compose test email” page can be opened by clicking Admin → other → send email.

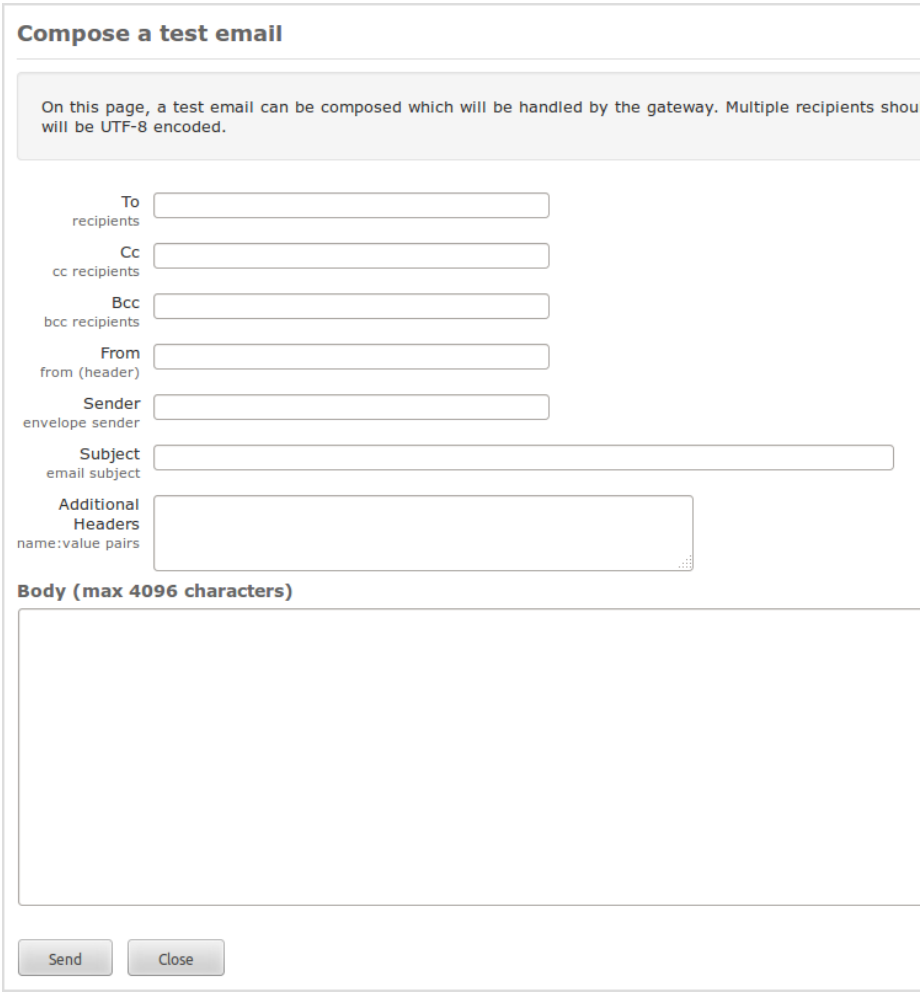

Figure 25: Compose test email

A SMTP HELO/EHLO name

The SMTP helo/ehlo name is the hostname the SMTP server sends with the SMTP EHLO or HELO command (CipherMail Webmail uses the HELO or EHLO command when sending email to another email server). Some email servers check whether the helo/ehlo name is equal to the reverse IP lookup (with a reverse IP lookup the name is retrieved that belongs to the IP address) and if the names do not match they will flag the email as spam.

If email is directly sent to external recipients (i.e., outgoing email is not relayed through an external relay host) the gateway should be setup with the correct helo/ehlo. The SMTP helo name should be equal to the reverse lookup of the external IP address.

If the external IP address is not known and the gateway uses the same IP address as the web browser, the external IP address and hostname (reverse

IP) can be retrieved using on-line services like http://www.whatismyipaddress.com. The IP address shown is the external IP address. The shown hostname (the reverse IP lookup) should be used for the SMTP helo name. If the hostname of the gateway is set to the external hostname, the SMTP helo name can be left empty because the SMTP helo name will then be equal to the gateway hostname.

Checking the HELO/EHLO name whether the HELO/EHLO name is correctly setup can be checked using the helo check services from http://cbl.abuseat.org/helocheck.html by sending an email to "helocheck@cbl.abuseat.org". The email will be immediately bounced. The bounce message contains the HELO name used by the gateway.

```
<helocheck@cbl.abuseat.org>: host mail-in.cbl.abuseat.org said:
    550 HELO for IP 82.94.189.170 was "secure.djigzo.com"
    (in reply to RCPT TO command)
```

Where 82.94.189.170 is the external IP address of the gateway (IP address will be different for every server) and "secure.djigzo.com" was the HELO name used by the gateway.

B Cron Expressions

The following cron examples are taken from http://www.quartz-scheduler.org/docs/tutorials/crontrigger.html.

Expression	Meaning
0 0 12 * * ?	Fire at 12pm (noon) every day
0 15 10 ? * *	Fire at 10:15am every day
0 10,44 14 ? 3 WED	Fire at 2:10pm and at 2:44pm every Wednesday in March.
0 15 10 15 * ?	Fire at 10:15am on the 15th day of every month
0 15 10 L * ?	Fire at 10:15am on the last day of every month

For more cron examples see the “Quartz Scheduler” website.