Advanced Settings

Advanced Settings section consists of three subsections: **General, Security,** and **DKIM-signature**.

General

- **External SMTP relay.** All outgoing mail will be sent to the specified address. It is used, for example, if mail must pass through the provider's upstream server before being sent to the Internet.
- **Forward all outgoing mail to address.** All outgoing mail will be duplicated to the specified mailbox. It is recommended to turn it on only when absolutely necessary.
- **Forward all incoming mail to address.** All incoming mail will be duplicated to the specified mailbox. It is recommended to turn it on only when absolutely necessary.
- **Maximum box size.** Limit the maximum mailbox size, in megabytes.
- **Maximum letter size.** Limit the maximum size of the message generated by the server, in megabytes.
- **Message storage period in the trash folder.** The number of days during which the mail is stored in the trash before being deleted.

Security

- **SASL support for SMTP client authentication.** Connecting to the mailbox from the Internet and sending an email using the UTM SMTP server will be possible only by logging in with the username and password set for this user account on the server. **Do not enable this parameter if you use UTM as a mail relay.**
- **Secure connection only (TLS) authentication.** Prohibits the unsecured transfer of client credentials during authorization on the SMTP server.
- **Greylisting for incoming mail.** Enables filtering by gray lists (graylisting) for incoming mail. In this case, mail from unknown sender domains may arrive with a slight delay.
- **DNSBL filtering for incoming mail.** Enables DNSBL filtering for incoming mail.
- **Trusted networks.** Authorization on the server to access the mailbox is not required when access attempts come from these networks. IP networks and hosts are specified in CIDR notation or with a network prefix, for example, `10.0.0.5/255.255.255.255` or `192.168.0.0/16`

DKIM-signature

Configured in section **Mail Relay -> Advanced Settings -> DKIM-signature.** Signs correspondence originating from the server with a signature unique to your mail domain so that other mail servers on the Internet can verify that your mail is legitimate and trustworthy.

For the technology to function, you will need to create a TXT record for your domain from the zone holder with a value that our server will generate for your mail domain. TXT records will be generated for the main mail domain configured for SafeUTM and additional mail domains (if specified). The server will also check whether the entry for your zone was specified correctly and whether it resolves to the Internet.

> The volume of a TXT record is quite large and many registrars/zone holders have difficulty providing an interface to clients to specify TXT records longer than 256 characters. They often provide the possibility to specify TXT records up to 256 characters long in accordance with the RFC1035 standard. However, another standard, RFC4408, suggests combining strings in cases where you need to use long TXT records when configuring SPF and DKIM. Use this information in a dialogue with your domain zone holder. As a rule, zone holders find a way to create long TXT records.

> The signature contains a combination of quotation marks (quote-space-quote: " ").
> If your hosting does not accept this recording format, then delete these characters.

Revision #6
Created 27 August 2022 18:56:29 by Val Redman
Updated 13 October 2022 16:02:56 by Val Redman