Advanced Settings

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.

Setting up Domain at Registrar/Zone Holder

To create a mail server, you will need a domain name. You can register it with your Internet service provider or directly with the registrar.

After you register a domain name, you will need to make changes to the zone description on the DNS server (at the domain zone holder, which is often the registrar).

1. Create an A-type resource record with a name for the mail server in your domain, pointing to the external IP address of SafeUTM. **Make sure that a public address accessible from the Internet is assigned on the UTM external interface.**
2. Add an MX-type resource record pointing to the A record that was created in the previous step. An MX-type record points to a network node that processes mail messages for the domain. It should refer to the domain name of the mail server, not the IP address.

We also recommend

3. Adding a reverse PTR-type resource record. This entry must be registered in the reverse zone file. These changes must be made on your Internet provider's side. Contact them with a request to register a reverse resource record for your IP address, which should refer to your MX-type record.
4. Configuring an SPF record for your mail server.
5. After configuring the mail server, also configure the DKIM signature of mail messages. To do this, go to **Mail Relay -> Advanced Settings -> DKIM-signature** and activate the item **Sign outgoing mail with DKIM**.

Also, create a TXT record for your domain from the zone holder with the name from the *Record Name* line and with the content that was generated by SafeUTM in **Record Value.**

Let's look at the set of necessary records using the example of a fictional domain example.net:

- A-record of the type: `mail. example. net.  IN A 23. 45. 67. 89`, where 23.45.67.89 is the external IP address of SafeUTM.
- MX-record of the type: `example. net.  MX 10 mx. example. net`
- Contact your hosting to register a PTR record for the desired IP address of the type: `89. 67. 45. 23. in- addr. arpa IN PTR mail. example. net`
- SPF-record that announces to other mail servers on the Internet that sending emails from your domain is allowed only from the mail server host specified in the MX-record: `example. net.  IN TXT "v=spf1 a mx -all"`

SPF syntax:
"v=spf1" — SPF version, required parameter, always spf1, no other versions work.
"+" — accept emails (by default).
"-" — reject.
"~" — "soft" rejection (the email will be accepted, but will be marked as spam).
"?" — neutral attitude.
“MX" — includes all server addresses specified in MX records of the domain.

When using a mail server on UTM as a mail relay, resource records will look the same, since on the Internet your LAN mail server will be represented by an SMTP relay on UTM.