TekSMTP

Installation & Configuration Guide
Version 1.5

Document Revision 3.1

https://www.kaplansoft.com/

TekSMTP is built by Yasin KAPLAN

Read "Readme.txt" for last minute changes and updates which can be found under application directory.

Table of Contents

Table of Contents 4
Introduction 5
System Requirements 5
Installation 5
Configuration 5
  Settings / Service Parameters Tab 6
  Settings / Protocols Tab 6
  Settings / Anti-SPAM Tab 7
DKIM 8
Domains / Mailboxes 9
Quarantine 10
Application Log 11
Rules 11
Starting TekSMTP 13
Troubleshooting 14
DNS Service Location Records 14
Index 17

Introduction

TekSMTP is a simple SMTP/POP3 server runs under Windows *(Vista/7/8/10, 2008-2019 Server)*. Major features;

- Simple design and easy to use user interface.
- Simple interface for user definitions.
- Multi domain operation.
- TLS support for both POP3 and SMTP.
- Customizable SMTP ports.
- DMARC *(RFC 7489)* policy checking, DKIM *(RFC 6376)* signing and signature verification, blacklisting, whitelisting, RBL, SPF *(RFC 7208)* support for anti-SPAM.
- Rule engine to process incoming e-mails.
- Performance monitoring through Windows Performance Monitor.
- Can be used as an anti-SPAM gateway.

TekSMTP consists of a GUI *(TekSMTP Manager)* and a service application.

System Requirements

1. A Windows system with at least 4 GB of RAM.
2. Microsoft.NET Framework v4.8 *(Min.)*
3. 4 MB of disk space for installation.
4. Administrative privileges.

Installation

Unzip “TekSMTP.zip” and click “Setup.exe” comes with the distribution. Follow the instructions of setup wizard. Setup will install TekSMTP Manager GUI and TekSMTP Service, add a shortcut for TekSMTP to desktop and the start menu.

Configuration

Run TekSMTP from Start Menu / Program Files / TekSMTP Manager. TekSMTP automatically configures itself at first run. Click the Settings Tab to start configuration. The Settings tab has four sub sections. Enter following information:

Settings / Service Parameters Tab

- **Logging:** Select logging level of TekSMTP. Select “None” if you do not want logging, select “Errors” to log errors and select “Sessions” to log session information and errors. Log files are located under <Application Directory>\Logs directory.
- **Delete log files older than:** TekSMTP deletes old log files older than specified days to save disc space. Set it to 0 to disable this function.
- **Startup Mode:** Set TekSMTP service startup mode, Manual or Automatic. You can also disable service startup.
- **TLS Enabled:** Enable TLS for SMTP / POP3 connections. TekSMTP accepts TLS encrypted SMTP *(TCP port 465)* and POP3 *(TCP port 995)* connections.
- **Server Certificate:** Select a certificate for TLS transport. TekSIP lists valid certificates in Windows Certificate Store / Local Machine. TekSIP will automatically switch the most current certificate after the selected certificate is expired if you create and add a new certificate with the same subject name in Windows Certificate Store / Local Machine / personal folder.
- **Use SQL Server:** Use an MS SQL server database in place of built-in SQLite database. TekSMTP database is created automatically when MS SQL database is selected.

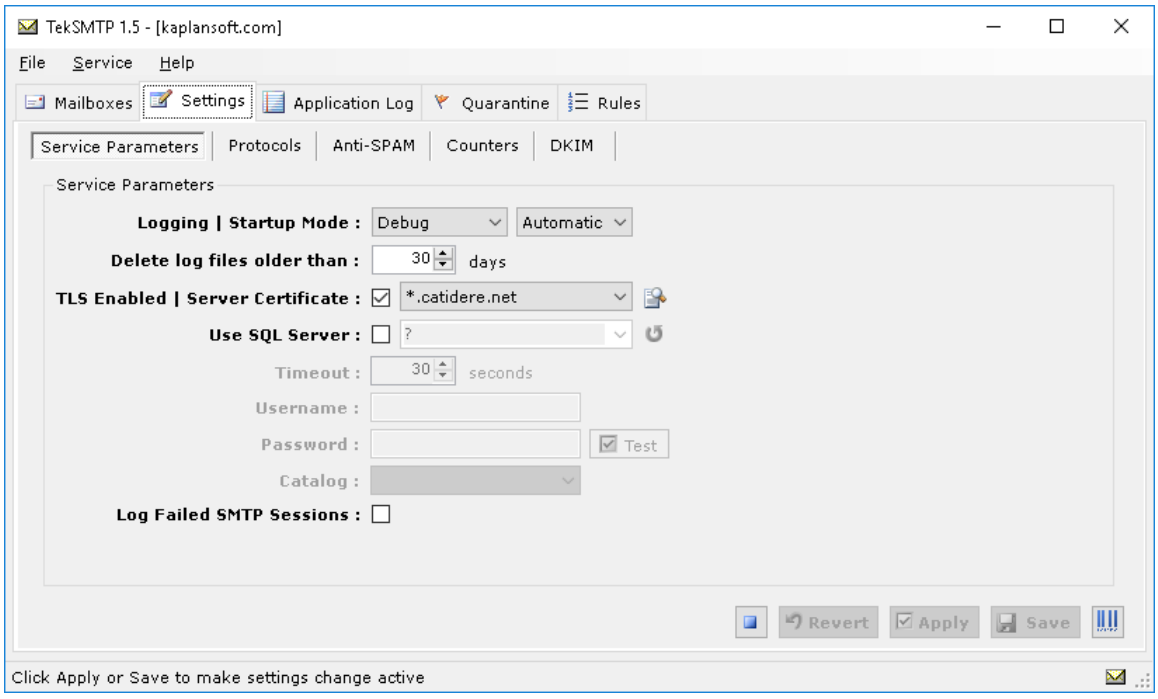

Figure - 1. TekSMTP Settings / Service Parameters tab

Settings / Protocols Tab

You can set SMTP / POP3 listen ports at Protocols tab. You can set multiple ports for SMTP service. You can optionally enable / disable SMTP authentication which is enabled by default. If enabled, TekSMTP monitors failed SMTP/POP3 connection attempts from suspicious endpoints and blacklists them. You can direct all outgoing mail to an SMTP proxy. You can specify an IP address or FQDN for the proxy. You can also specify SMTP port number in <Host name or IP address>:<Port number> format if proxy uses a port number other than 25.

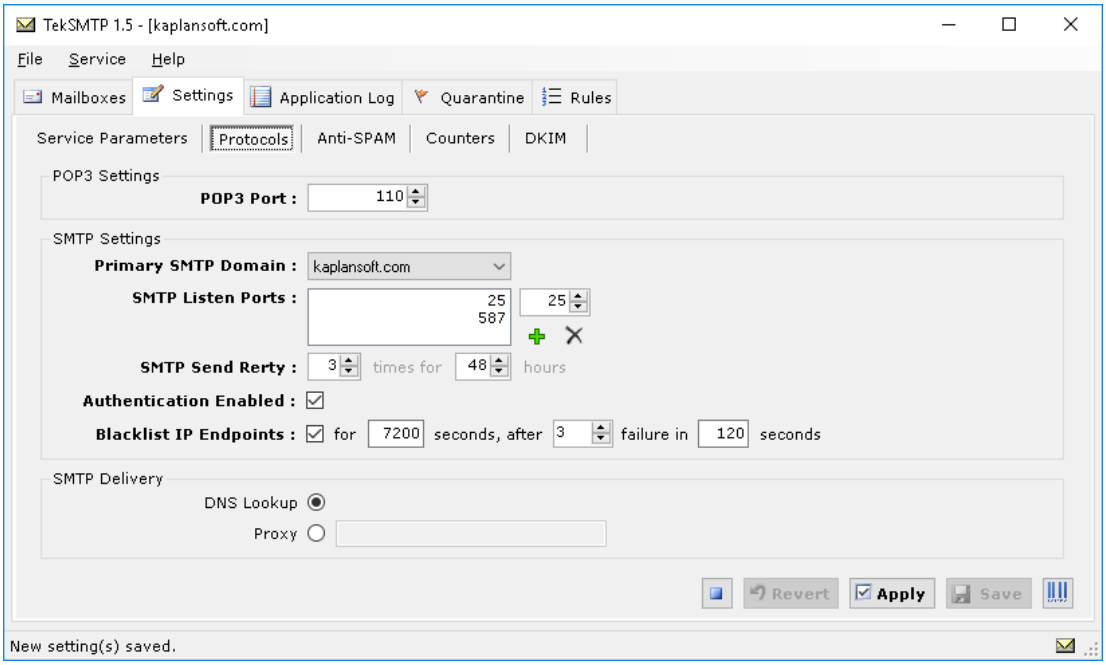

Figure - 2. TekSMTP Settings / Protocols tab

Settings / Anti-SPAM Tab

TekSMTP can query RBL databases to filter SPAM messages. You can specify your own DNS blacklists. Some RBL systems require connecting them directly. You can also check the validity of sender domain.

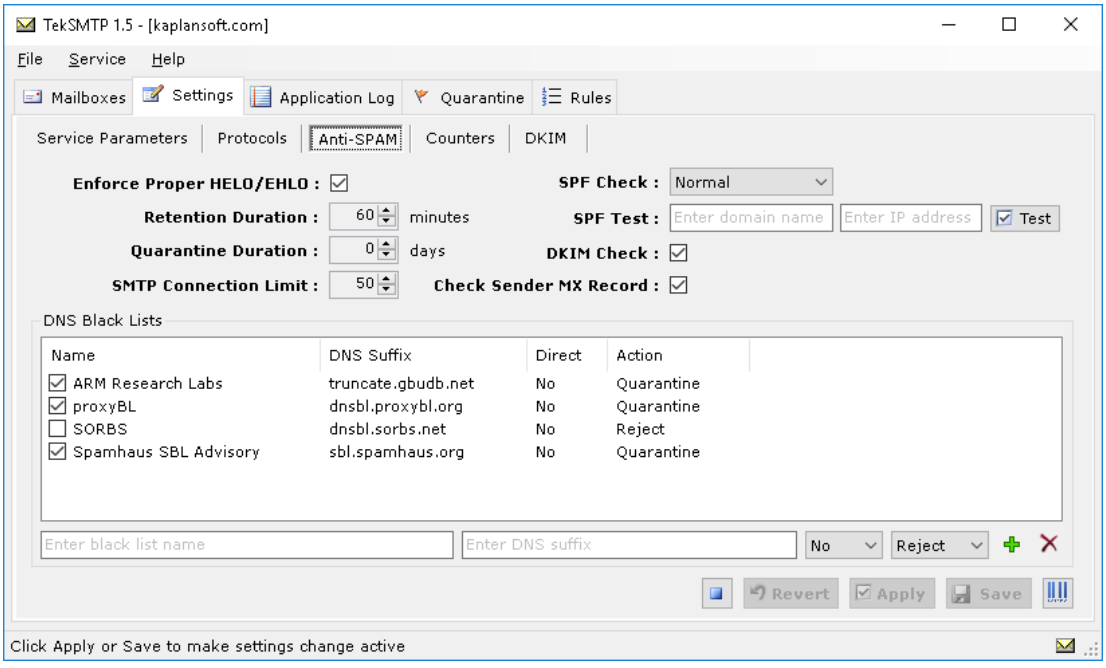

Figure - 3. TekSMTP Settings / Anti-SPAM tab

TekSMTP puts IP address of remote SMTP sender into a blacklist if remote sender IP address is found in one of DNS blacklists. Blacklisted IP addresses are kept in the internal blacklist for a duration specified as **Retention Duration**. Internal blacklisted entries can be browsed at Quarantine tab in real time. You can specify a taken action when a positive match found for a DNSBL entry; reject or quarantine. Quarantined messages can be listed through Quarantine / Message tab.

TekSMTP can check Sender Policy Framework record for incoming senders *(Commercial editions only)*. TekSMTP will reject mails with SPF test result fail if you set Normal mode. TekSMTP will also reject mails with SPF test result softfail if you chose Aggressive mode.

TekSMTP will perform DKIM signature validation for received e-mails when DKIM check is enabled.

TekSIP preforms also DMARC policy check when SPF or DKIM check is enabled.

TekSMTP can check host name in HELO/EHLO command. TekSMTP will reject incoming mail transmission if a proper hostname is not provided. IP addresses, single label alphanumeric host names, improperly formatted FQDNs are rejected when Enforce Proper HELO/EHLO option is set.

You can set a limit for the number of SMTP connections that can be made from a particular SMTP server. TekSMTP will blacklist the server if this threshold is reached.

TekSMTP will automatically delete quarantined mails when the Retention Duration is reached.

DKIM

You can specify domains which outgoing e-mails will have DKIM signatures at DKIM tab. TekSMTP uses certificates located in Windows Certificate Store / Local Machine / Personal folder to sign e-mails. You can copy TXT record contents for a selected domain using by clicking copy button.

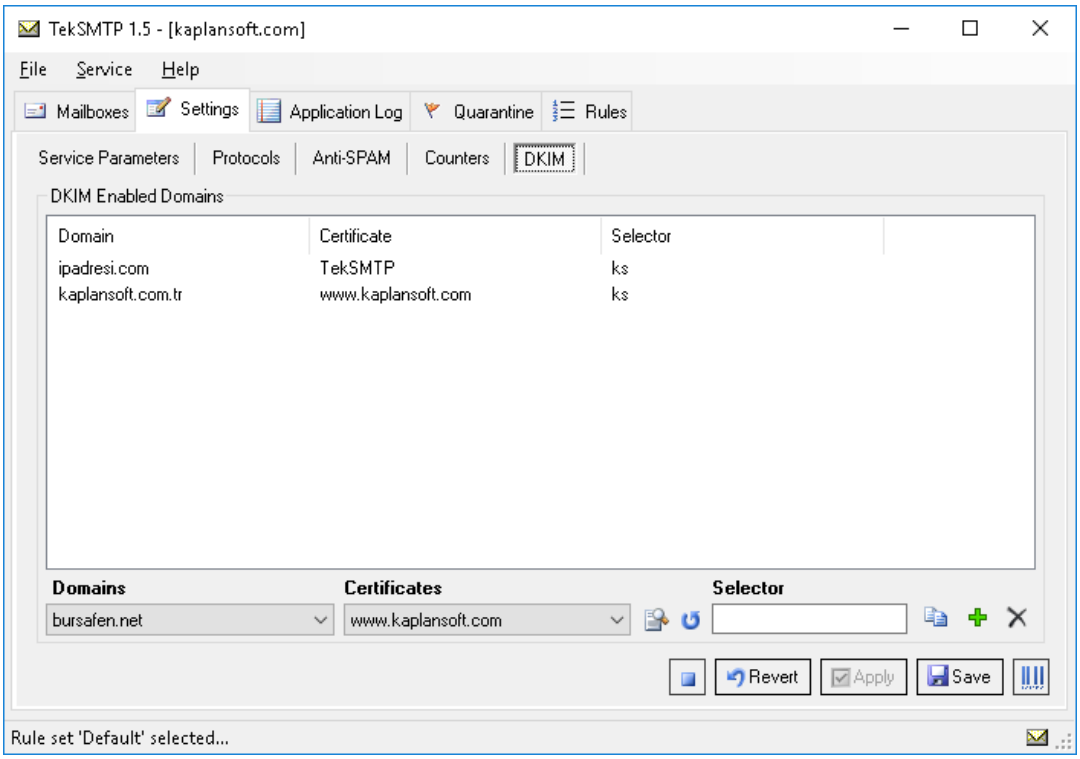

Figure - 4. DKIM Settings

Domains / Mailboxes

You can define e-mail domains and mailboxes in “Mailboxes” tab. TekSMTP allows you to server for multiple DNS domain names. You can create domain name entries by entering domain names into the Domain Name list. Domain parameters;

- **Enabled.** Enables/disables domain. TekSMTP will reject incoming mails for the domain if it’s disabled.
- **Local.** Set if the domain has local mailboxes.
- **Destination.** Set destination domain/SMTP server to deliver incoming mails if the domain is not local. You can specify multiple targets by concatenating them “;” *(Without quotes)*.
- **Rule Profile.** Select rule set to process incoming mails for the domain.
- **SPAM Threshold.** Enter threshold value to mark incoming mails as SPAM when reached.
- **SPAM Policy.** Select TekSMTP behavior *(None, Quarantine and Reject)* when an incoming mail for the domain is marked as SPAM.

You can create user accounts for a domain name after creating a domain entry. You can configure following parameters for a user mailbox;

- **Password.** Enter a user password for both POP3 and SMPT authentication.
- **Full Name.** You can optionally enter the full name of the user.
- **Description.** You can optionally have a description for the mailbox.
- **Mailbox quota.** Mailbox capacity in bytes.
- **Forward incoming mail to.** Enter an e-mail address to forward incoming e-mails for this mailbox.
- **Keep local copy.** Select “Yes” if you keep a copy of incoming e-mail in the mailbox after forwarding.
- **Enabled.** Set “Disabled” if you block access to the mailbox. Mailbox will not accept incoming e-mail when it is disabled.

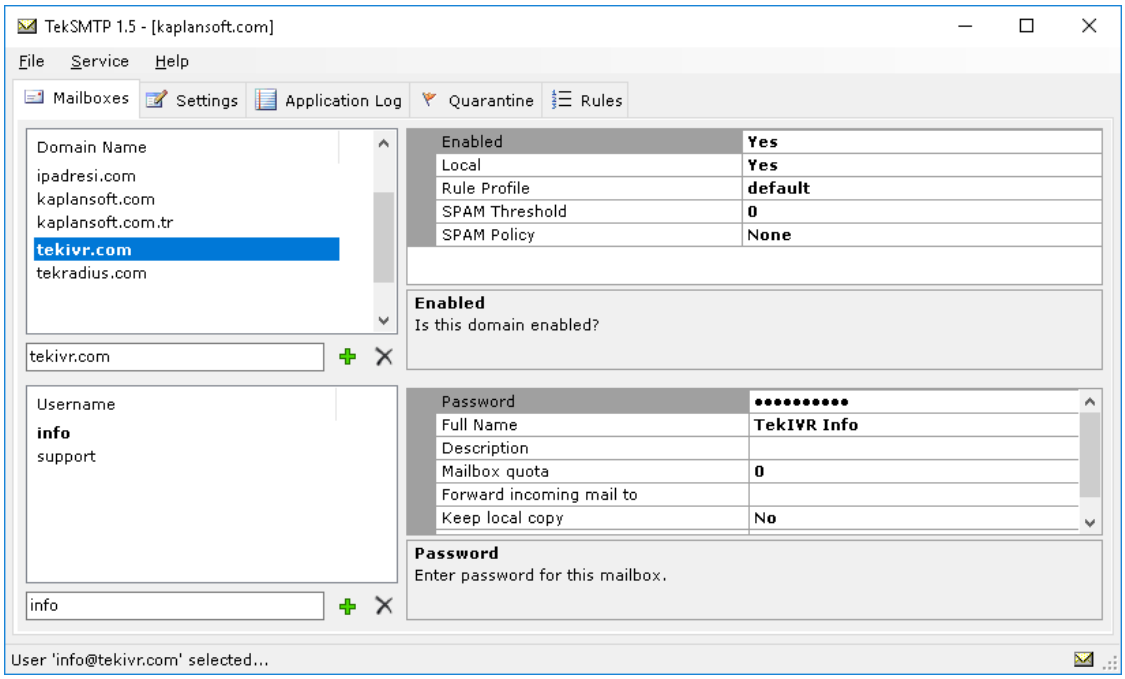

Figure - 5. Mailboxes Tab

User must enter their username in username@domain.name format in POP3/SMTP server settings in their e-mail client software.

Quarantine

You can see quarantined IP address in Quarantine tab. You can delete the quarantined entry by double clicking selected entry. You can drag and drop selected quarantined entries to whitelist or you can add white list entries manually. You can enter a single IP address or an IP subnet in X.X.X.X/Y *(192.168.1.0/24 e.g.)* format.

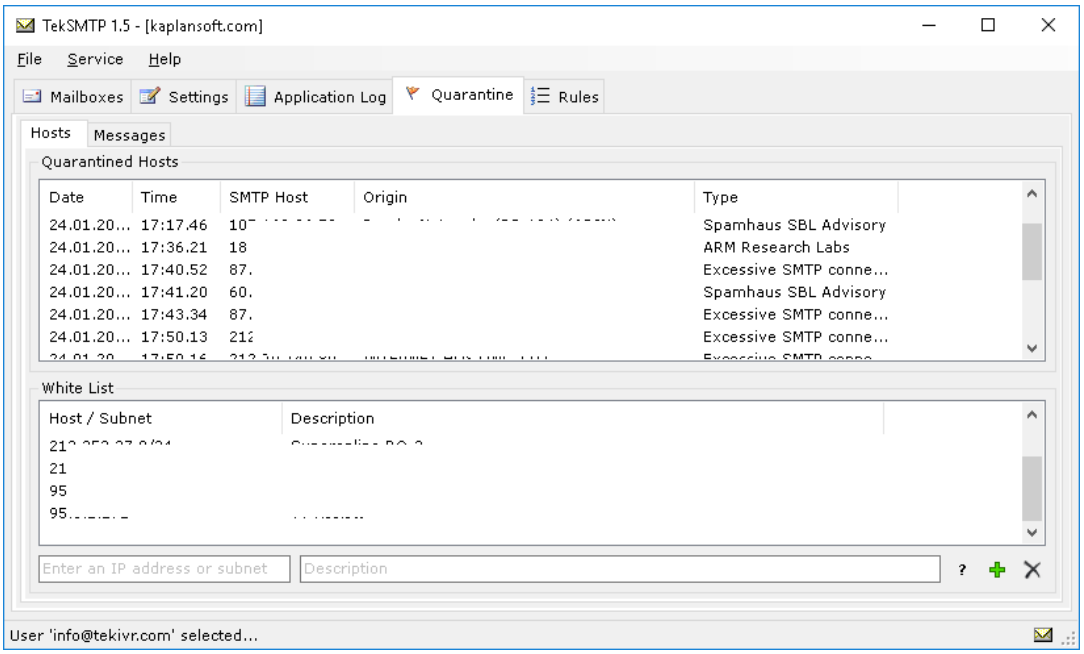

Figure - 6. Quarantine / Host Tab

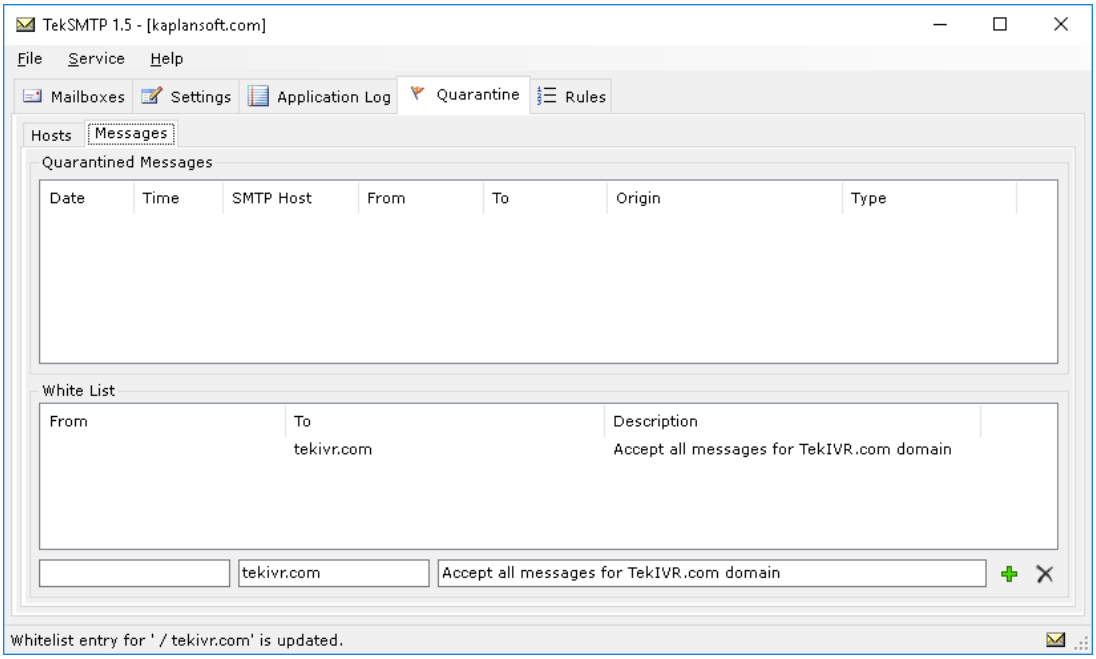

Figure - 7. Quarantine / Messages Tab

Application Log

You can monitor system events in Application Log tab. You can manually refresh log entries and clear log entries. Click Enable Auto Refresh option to refresh log list every second.

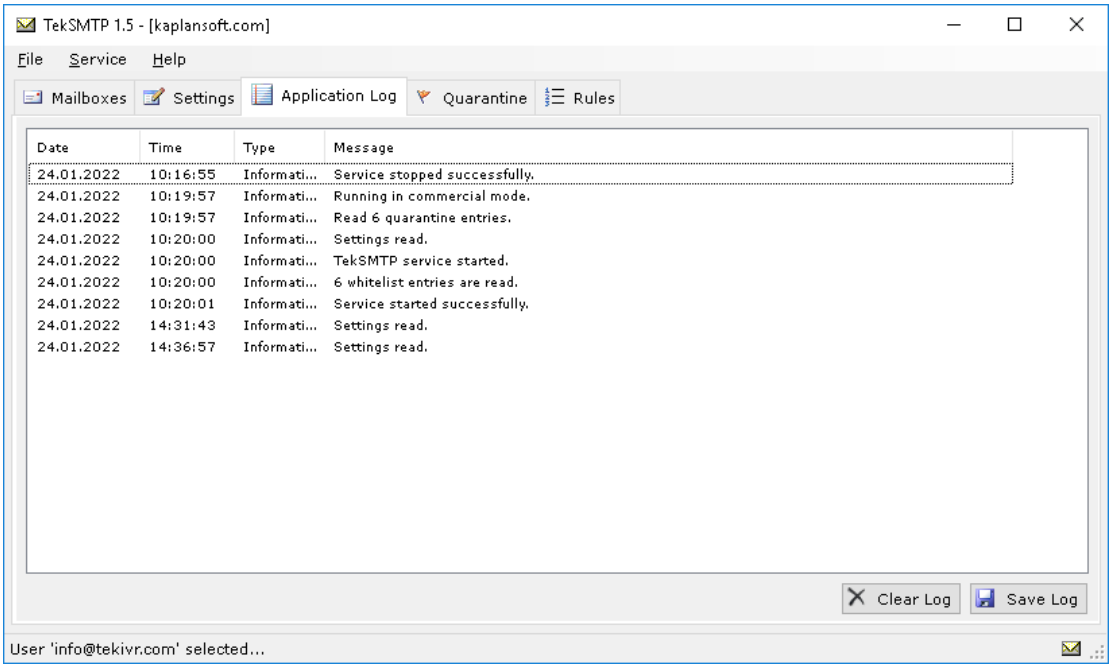

Figure - 8. Application Log Tab

Rules

You can process incoming e-mails by using a rule set. Each rule set has its own rules processed by order as specified in Rules tab.

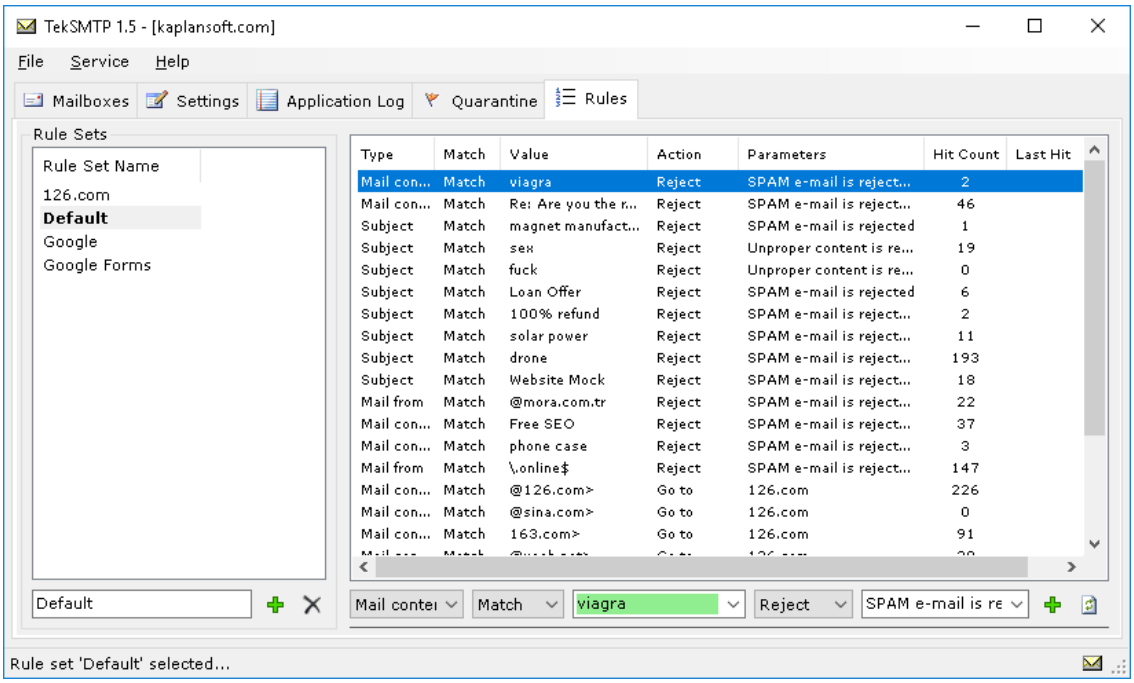

Figure - 9. Rules Tab

You can use following match types for rules;

- **Host IP address.** Send IP address *(IPv4 only)*.
- **HELO/EHLO FQDN.** FQDN received in HELO / EHLO request.
- **Mail from.** Sender e-mail address *(Received in SMTP negotiation)*.
- **Mail to.** Recipient e-mail address *(Received in SMTP negotiation)*.
- **Content.** E-mail content including headers.
- **Date.** Date of e-mail received.
- **Time.** Time of day of e-mail received.
- **Subject.** Subject of the received e-mail.
- **Size.** Size of the content part of the received e-mail.
- **Absent Header.** Check if specified header does not exist.
- **Attachment.** Check if an attachment with specified extension exists.

You need to specify match time for the rule. It can be either “Match” or “No Match”.

TekSMTP expects parameters in regular expression format so take care of regular expression special characters to be escaped. TekSMTP Manager GUI gives a hint by changing background color of parameter entry. Green background means correct entry. Here are actions can be performed if rule satisfies specified condition;

- **Pass.** TekSMTP accepts the e-mail and process no preceding rule.
- **Reject.** TekSMTP rejects the e-mail and process no preceding rule.
- **Forward.** TekSMTP accepts and forwards to the e-mail address or SMTP host specified in action parameter and process no preceding rule.
- **Copy.** TekSMTP accepts and forwards a copy of the e-mail to specified in action parameter and process no preceding rule.
- **Run.** TekSMTP executes specified application in action parameter and returned DOS error level code is evaluated. Here is a list of action performed based on returned DOS error level code;

    1. Pass
    2. Reject
    3. Forward
    4. Copy
    5. Run
    6. Go to
    7. Quarantine
    8. Increase SPAM score

    Parameters for Forward, Copy, Run and Go to actions can be returned as console output of your application. TekSMTP will read the output of your application and process as action parameter. You can also add flowing built-in variables as parameter to executable;

`%ipaddr%`	Send IP address *(IPv4 only)*.
`%helohost%`	FQDN received in HELO / EHLO request.
`%content%`	Temporary file created for received e-mail. This variable return filename with full path.
`%mailfrom%`	Sender e-mail address *(Received in SMTP negotiation)*.
`%mailto%`	Recipient e-mail address *(Received in SMTP negotiation)*.

- **Go to.** TekSMTP executes specified rule set in action parameter. You cannot point to a rule to itself. TekSMTP will break the execution of rule if the traversed rules contain the selected rule.
- **Quarantine.** Quarantine incoming mail.
- **SPAM Score.** Increase SPAM score for the incoming mail by adding amount specified in action value.

The freeware edition allows one rule set and a maximum of 5 rules. You must have a “Default” rule set. TekSMTP will start processing rules in Default rule set first.

You can move or copy selected rules to other rule sets. Right click on selected rule entries and use functions in opened context menu.

Rule processing will be terminated if a matched rule with Reject or Quarantine is reached or cumulative SPAM score is equals or greater than domain’s SPAM threshold.

Starting TekSMTP

Click “Service” menu and select “Start Service” to run TekSMTP after making necessary configuration and saving configuration. If service starts successfully you will see “TekSMTP is started” message at bottom left message section of TekSMTP Manager. Optionally you can start/stop TekSMTP using the button on Settings tab. When you make any change(s) in configuration, TekSMTP must be restarted.

If TekSMTP cannot start, please examine Application Log tab as well as TekSMTP log file under <Application Directory>\Logs if you were enabled logging in Settings tab.

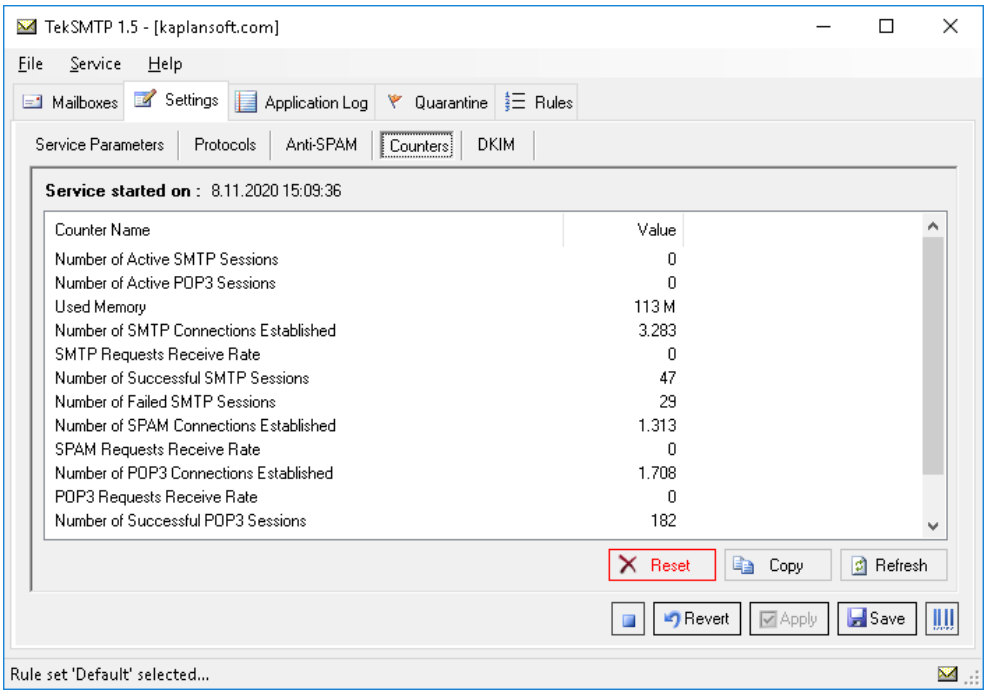

Figure - 10. TekSMTP Windows Performance Counters

Troubleshooting

TekSMTP provides many messages when problems occur. You can see error messages on TekSMTP Status bar or in the log file of TekSMTP service. You can enable logging in Settings Tab. There are three levels of logging; None, Errors, Sessions. If you select Errors, TekSMTP logs just error messages. If you select Sessions both Session and Error messages will be logged. You must save or apply settings changes if you change logging level setting. Log files are located under <Application Directory>\Logs directory.

TekSMTP also utilizes Windows Performance Monitor providing numerous counters;

- Used Memory
- Number of Active SMTP Sessions
- Number of Active POP3 Sessions
- Number of SMTP Connections Established
- SMTP Requests Receive Rate
- Number of Successful SMTP Sessions
- Number of Failed SMTP Sessions
- Number of POP3 Connections Established
- POP3 Requests Receive Rate
- Number of Successful POP3 Sessions
- Number of Failed POP3 Sessions
- Number of SPAM Connections Established
- SPAM Requests Receive Rate
- Number of rejected mails by policy

You can add and monitor them using Windows Performance Monitor *(Perfmon.exe)*. You can also monitor these counters through TekSMTP Manager interface *(Settings / Counters)*.

DNS Service Location Records[1]

SRV records *(Known as Service Location Records)* are used by clients to automatically configure the host and port for messaging services when an account is created. These records are created within the advertised DNS zone for a domain.

Microsoft clients typically use an autodiscovery service to detect mail client settings, many clients including iOS/OSX and mobile clients use DNS to locate a user's messaging service settings.

The following table lists typical SRV records that should be created for a domain to improve the experience when user's create e-mail accounts:

_pop3	POP3 Mail Access Support
_pop3s	POP3 Mail Access Support over SSL
_submission	SMTP Client Mail Transfer Support
_autodiscover	The server and port responsible for providing autodiscovery for mail services

These DNS records typically appear within a domains DNS Zone as `[SRV]._tcp.teksmtp.com`.

[1] RFC-6186: https://tools.ietf.org/html/rfc6186

The process for configuring these records depends on which vendor is providing DNS for the domain. It can only be done by a person who has administrative access to the DNS service responsible for the domain. As an example, to create a DNS SRV record for SMTP using Microsoft's DNS, you should do the following:

- On the DNS server, click Start, click Control Panel, click Administrative Tools, and then click DNS.

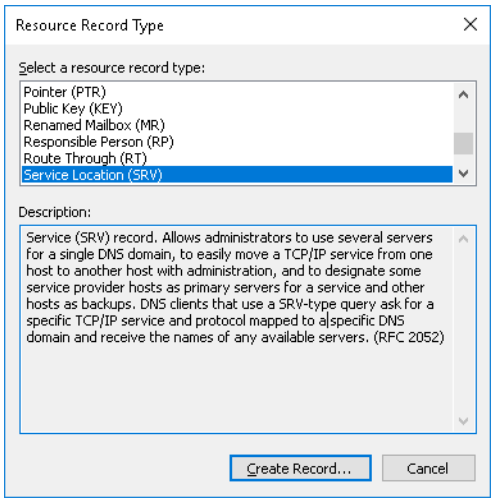

Figure - 11. Select Resource Record Type

- In the console tree for your domain, expand Forward Lookup Zones, and then right-click the domain in which you wish to create an SRV record.
- Click Other New Records.
- In Select a resource record type, click Service Location (SRV), and then click Create Record.
- Click Service, and then type _submission, click Protocol, and then type _tcp. and click Port number, and then type 587.

Figure - 12. New Resource Record Entry for SMTP

- Click Host offering this service, and then type the FQDN of the host providing IMAP connectivity. eg: mail.teksmtp.com

- Click OK and then click Done.

TekSMTP can respond to autodiscovery requests from e-mail clients. Outlook and Thunderbird requests are supported. There must not be a web server running on TCP port 443 on the same server with TekSMTP for this feature and you must enable TLS transport in Settings / Service parameters. You need to have an RSV record as `_autodiscover._tcp.teksmtp.com` for teksmtp.com domain as an example;

Figure - 13. New Resource Record Entry for autodiscovery

Host name and certificate subject name must be matched, or certificate must be a wildcard certificate *(*.teksmtp.com e.g.)*.

Index

Application Log, 10, 11, 13
Attachment, 12
autodiscovery, 14, 16
certificate, 6, 16
DKIM, 4, 5, 8
DMARC, 5, 8
EHLO, 8, 12
HELO, 8, 12
Mailbox, 9
POP3, 5, 6, 14
Quarantine, 4, 8, 9, 10, 12, 13
quota, 9
RBL, 5, 7
Retention Duration, 8
RFC 7208, 5
RSV record, 16
Rule engine, 5
Sender Policy Framework, 8
SMTP, 5, 6, 14
SPAM, 4, 5, 7, 9, 12, 13, 14
SPF, 5, 8
TLS, 5, 6