TekSIP

Installation & Configuration Guide
Version 4.2

Document Revision 8.7

https://www.kaplansoft.com/

TekSIP is built by Yasin KAPLAN

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

Table of Contents

Introduction

TekSIP is a SIP Registrar and Stateless SIP Proxy for Windows with TCP, TLS and UDP support with WebSocket *(RFC 7118)*. TekSIP can be deployed as a signaling server for WebRTC based SIP phones.

TekSIP complies with RFC 3261, RFC 3263, RFC 3311, RFC 3581 and RFC 3891. It supports NAT traversal and ENUM. You can also log session details into a log file and monitor active registrations and sessions in real-time. TekSIP has a built-in Presence Server *(SIP/SIMPLE based)*.

TekSIP also supports UPnP IGD specification. If it is installed behind an UPnP supported Internet gateway device *(e.g., ADSL router)*, TekSIP automatically detects if it is behind a new NAT gateway and its external IP address. All outgoing requests are manipulated for NAT traversal. You do not need to add manual reverse mappings for SIP or RTP protocols.

TekSIP can optionally act as a B2BUA for incoming 3xx SIP responses. TekSIP supports RADIUS Authentication *(RFC 2865)* and RADIUS Accounting *(RFC 2866)* with the methods described in **draft-sterman-aaa-sip-00.txt** and **draft-schulzrinne-sipping-radius-accounting-00.txt** respectively. TekSIP accepts RADIUS Disconnect request as specified in RFC 5176. TekSIP runs as a Windows service.

You can have multiple SIP accounts *(Destinations)* for number prefix. Please see **"Routing"** section for details. TekSIP can register to upstream SIP servers to receive incoming calls.

TekSIP has a Windows form-based GUI, an HTTP based GUI and JSON based HTTP REST API.

TekSIP can act as an RTP Proxy and record audio streams if the RTP proxy is enabled. Recorded audio streams saved in wave format can be played using TekSIP Manager. TekSIP uses UDP port 6000 and above for RTP traffic. You need to add the necessary mappings to your router if TekSIP is installed behind a NAT gateway that does not support UPnP.

You can also deploy TekSIP as an SBC for Microsoft Teams Direct Routing

TekSIP supports auto provisioning of IP phones based on SUBSCRIBE / NOTIFY PnP mechanism. Please see "Auto Provisioning" section of this manual.

TekSIP can act as SMPP Gateway. Instant messages sent by registered SIP endpoints can be sent as SMS through an SMPP gateway and received SMS' can be routed to registered SIP endpoints as SIP messages.

System Requirements

1. A Windows system with at least 2 GB of RAM.
2. Microsoft.NET Framework 4.8 *(Min.)*
3. 20 MB of disk space for installation.
4. Administrative privileges.

Installation

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

Un-Installation

To uninstall TekSIP, double click TekSIP icon at “Add or Remove Programs” from Control Panel. The following files are kept in TekSIP installation directory after uninstallation.

TekSIP.ini. TekSIP settings file.
TekSIP.gui. TekSIP Manager GUI state file.
Dictionary.db. RADIUS dictionary file.
Quarantine.db. Black listed IP addresses.
IPFilters.db. IP filters database file.
Provisioning.db. Phone provisioning mappings.
Extensions.db. Extensions database file.
Translations.db. Translation rules for SIP headers and payloads.
Routes.db. SIP routes database file.
Registration.key. Commercial license file.
/Logs. Daily rotated log files folder.
/Records. Recorded audio files if recording is enabled.

These files and folders must be removed manually if they are not needed after uninstallation.

Configuration

Run TekSIP Manager from Start Menu / Program Files / TekSIP. TekSIP automatically configures itself at first run. TekSIP selects the first available IPv4 address and makes a reverse lookup of that IPv4 address to obtain the SIP domain information. If TekSIP cannot resolve the selected IP address to an alphanumeric FQDN address, the selected IPv4 address is used as the SIP domain.

TekSIP also checks if it is installed behind an UPnP supported NAT gateway. If so, TekSIP automatically detects the external IP and displays it on the status bar. TekSIP also adds a reverse mapping for incoming UDP connections automatically *(Default UDP port 5060)*.

Settings / Service

Click the Settings Tab to start configuration. The settings tab has four sub sections.

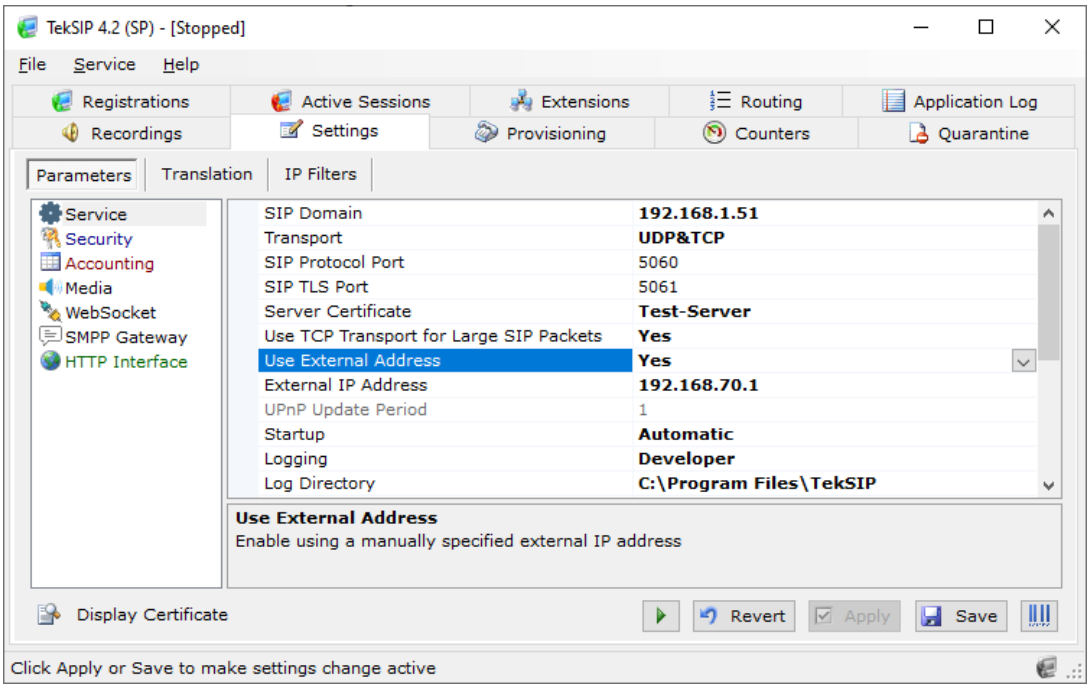


Figure - 1. TekSIP Settings / Parameters

Enter the following information for the Service Parameters:

- **SIP Domain:** Enter the FQDN of your SIP domain. Please make sure that this address is resolvable by your SIP client and has a valid entry *(an A record)* in your DNS server. If you do not have an entry for your SIP domain in DNS, you can simply use the IP address configured for listening to incoming requests.
- **Transport | SIP Protocol Port:** You can define a port number to be listened to *(Default 5060)*. You can select which transport protocol will be used by TekSIP using the **Transport** parameter. TekSIP uses both UDP, TCP and TLS *(TCP port 5061)* transports by default.
- **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 External Address:** If TekSIP is installed behind a NAT gateway which does not support UPnP, you can set external the IP address manually for NAT traversal. If your NAT gateway supports UPnP, set the UPnP Update Period to value greater than "0". You can specify a FQDN *(DynDNS address etc.)* as an external address; TekSIP will query FQDN every minute for possible IP address changes.
- **UPnP Update Period:** You can specify the period for querying the UPnP Internet Access Gateway. Set to "0" to disable UPnP support.
- **Startup:** Set TekSIP service startup mode: Manual or Automatic. You can also disable the service startup.
- **Logging | Log Directory:** Select the logging level of TekSIP. 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 the <Application Directory>\Logs directory by default.

- **Log Rotation:** TekSIP rotates log files daily by default. You can also force TekSIP to rotate log files hourly.
- **Auto Clear:** You can limit the number of days for the log files. Older files will be automatically deleted.
- **Enable Call Pick-Up:** TekSIP provides call pickup option. You can pick up an incoming call to an extension by dialing a user defined pick up prefix and extension number *(Dial *8101 for picking up a call to extension number 101)*. This feature is disabled by default.
- **Save Registrations:** Set this option to keep the endpoint registrations while restarting.
- **ENUM[1] Lookup Enabled:** TekSIP can resolve numbers in incoming SIP requests to an ENUM entry if it exists. If TekSIP cannot find a valid ENUM entry for the dialed number, the SIP request will be forwarded to default route if it's enabled. If a valid ENUM entry is found for the dialed number, it is returned in a 302 response to the originating endpoint by TekSIP. The call is forwarded to the default route if the ENUM lookup fails and the default route is enabled.
- **Enable Presence Server:** TekSIP can act as a presence server for the registered endpoints when the Presence Server is enabled.
- **Process 3xx Responses Locally:** If you wish TekSIP to handle 3xx responses, select this option. When selected, TekSIP processes 3xx responses and resends INVITE to the destination returned in the 3xx response.

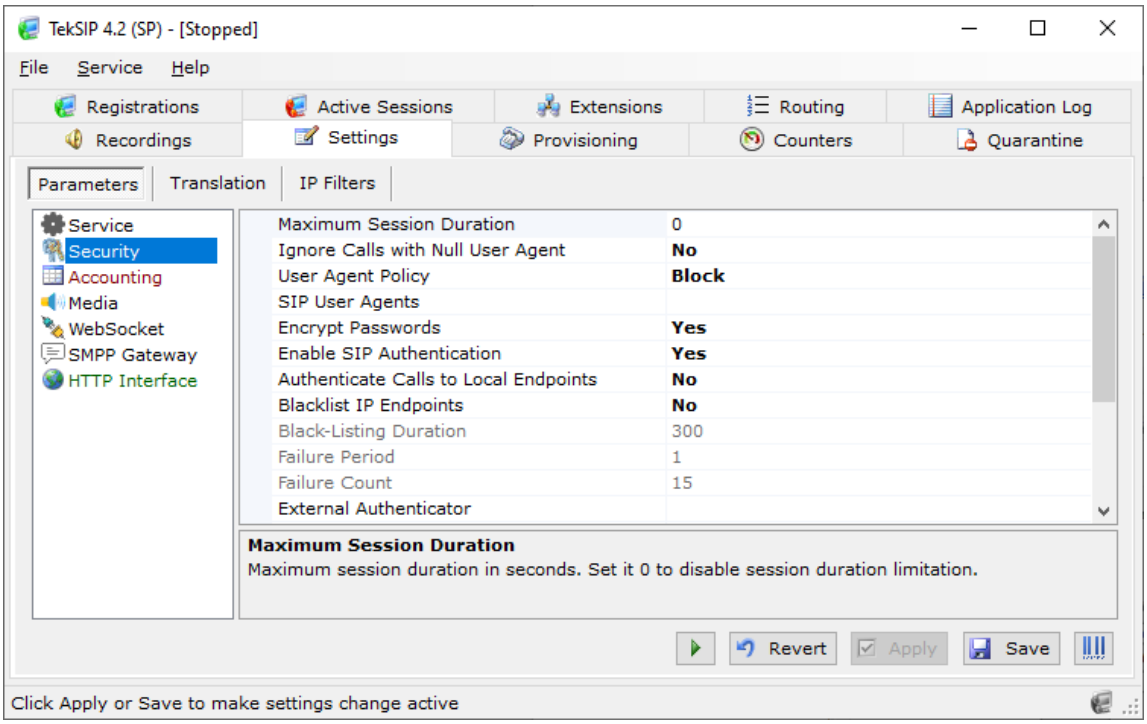


Figure - 2. TekSIP Settings / Security

[1] https://datatracker.ietf.org/doc/html/rfc6116

Settings / Security

Enter following information for Authentication:

- **Maximum Session Duration:** You can limit the maximum session duration for the calls.
- **Maximum Ring Duration:** Maximum ringing duration in seconds for a call attempt. TekSIP will redirect the call to specified alternative endpoint in the extension settings when the maximum ring time expires.
- **Ignore Calls with Null User Agent:** You can force TekSIP to ignore calls without User-Agent header.
- **User Agent Policy: You can also ban or allow specific user agents.**
- **SIP User Agents:** Enter SIP user agent strings concatenated with semicolons. Specified user agents will be allowed if the user agent policy is set to 'Block' otherwise they will be blocked. Multiple user agent identifiers can be concatenated with semicolons ";".
- **Authenticate Calls to Local Endpoints:** You can enable authentication for incoming calls to the registered endpoints by setting this option.
- **Encrypt Passwords:** Set this option to keep the endpoint passwords in encrypted form in TekSIP database files.
- **Enable SIP Authentication:** SIP endpoint authentication is enabled by default. If you do not want to authenticate SIP registration and SIP requests, uncheck this option.
- **Blacklist IP Endpoints:** If selected, TekSIP monitors failed registration and call attempts from suspicious endpoints and blacklists them.
- **External Authenticator:** Enter executable path for an external authenticator application.
- **Enable RADIUS Authentication:** If you prefer to direct authentication requests to a RADIUS Server, check this option. If you do not check this option, TekSIP will use the local endpoint database to authenticate the endpoints.
- **RADIUS Authorization Only:** Disables digest authentication.
- **RADIUS Server Address:** Enter a valid IP address for the RADIUS server.
- **RADIUS Server Port:** Enter the UDP port number of the RADIUS server. The default is UDP port 1813.
- **RADIUS Secret:** Enter the RADIUS secret key for the RADIUS Server.
- **RADIUS Timeout / Retry:** You can set an amount of time which TekSIP waits for a reply for the RADIUS accounting packets from the RADIUS Server. You can also specify how many attempts will be made by TekSIP to deliver RADIUS accounting packets to the RADIUS server.

TekSIP accepts following attributes in authorization reply from the RADIUS server;

- cisco-h323-credit-amount. Total user credit.
- cisco-h323-credit-time. Maximum allowed call duration in seconds.
- cli *(Encapsulated in cisco-AVPair)*. Caller Id to be replaced with received one.
- route *(Encapsulated in cisco-AVPair)*. Authorized route for the call.

Sample cisco-AVPair usage;

```
cisco-AVPair = cli=02123561212,route=myroute
```

TekSIP will replace the received caller id with 02123561212 while forwarding the call in it will use route entry labeled “myroute”.

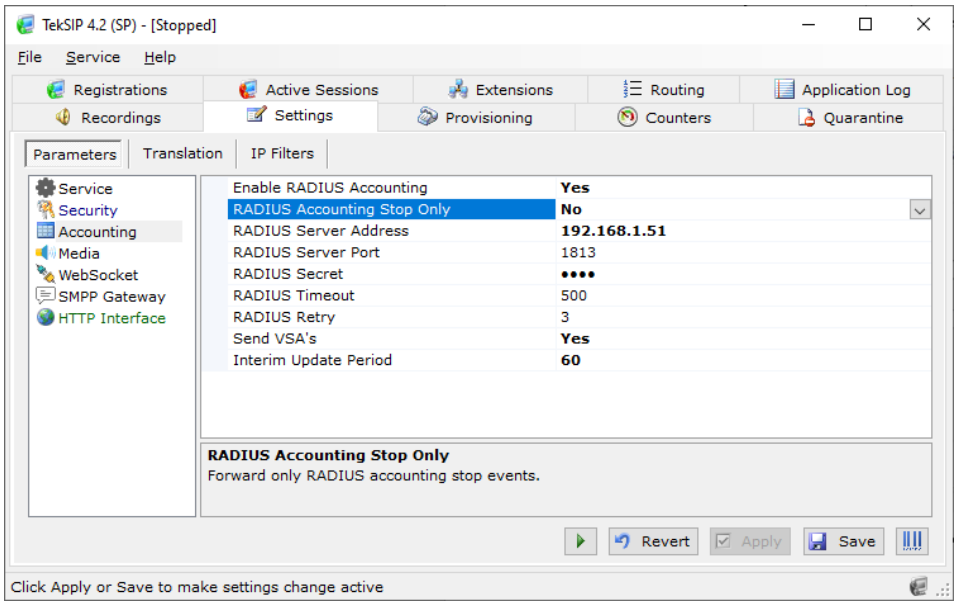


Figure - 3. TekSIP Settings / Accounting

Settings / Accounting

Enter following information for Accounting:

- **Enable RADIUS Accounting:** TekSIP supports RADIUS accounting. RADIUS accounting is disabled by default. Click “Accounting Enabled” to enable RADIUS accounting.
- **RADIUS Accounting Stop Only:** If you prefer to send only RADIUS Accounting stop messages to the RADIUS server, select this option.
- **RADIUS Server Address:** Enter a valid IPv4 address for the RADIUS server.
- **RADIUS Server Port:** Enter the UDP port number of the RADIUS server. The default is UDP port 1813.
- **RADIUS Secret:** Enter the RADIUS secret key for the RADIUS Server.
- **RADIUS Timeout / Retry:** You can set an amount of time which TekSIP waits for a reply for the RADIUS accounting packets from the RADIUS Server. You can also specify how many attempts will be made by TekSIP to deliver RADIUS accounting packets to the RADIUS server.
- **Send VSA’s:** You can optionally send Cisco compatible VSA’s for VoIP to the RADIUS server in RADIUS accounting packets. Supported Cisco *(Vendor Id 9)* VSA’s:
    - cisco-AVPair (1)
    - cisco-h323-conf-id (24)
    - cisco-h323-call-origin (26) [originate]
    - cisco-h323-call-type (27) [VoIP]
    - cisco-h323-disconnect-cause (30)
    - cisco-h323-gw-id (33)

TekSIP transmits following information through cisco-AVPair attribute;

- Destination. Selected destination for the call.
- Proxy. Proxy IP address if calls is received through a SIP proxy.
- Codec. Used codec for the call.
- ARTPrx. Received RTP packet from A leg of the call *(RADIUS Accounting stop only)*
- BRTPrx. Received RTP packet from B leg of the call *(RADIUS Accounting stop only)*

- **Interim Update Period:** Enter the RADIUS interim update sending period in seconds *(SP edition only)*.

Settings / Media

You can re-direct calls to a voice mail server if the user is unavailable to answer *(Busy or off-line)*. Enter the Voice Mail Server information and parameters at the Settings / Services tab:

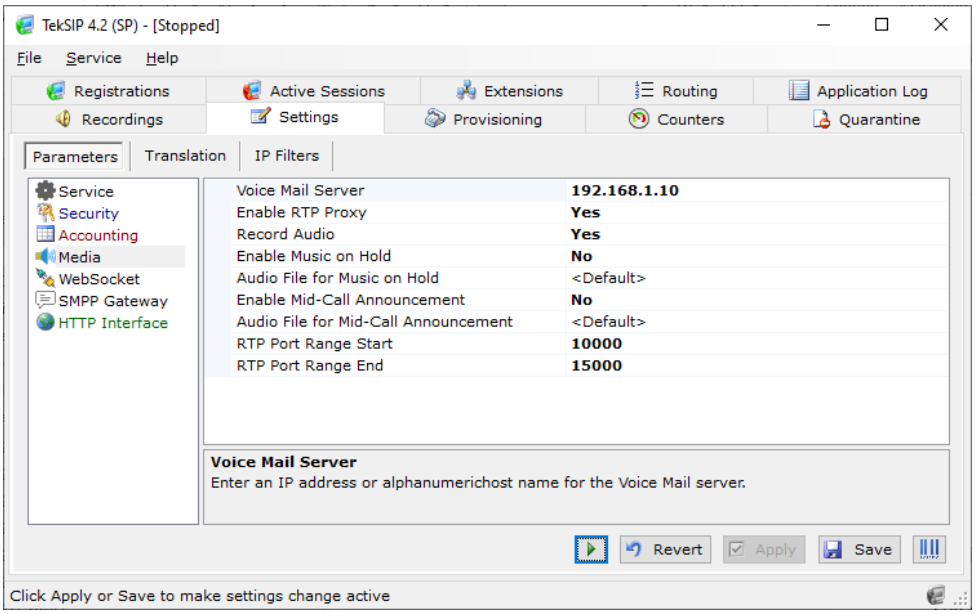


Figure - 4. TekSIP Settings / Media

TekSIP can act as an RTP Proxy and record audio streams if the RTP proxy is enabled. Recorded audio streams are saved in wave format and can be played using TekSIP Manager *(Recordings tab)*. RTP recording can be performed only for G.711 A-law or mu-law calls. If audio recording is enabled, TekSIP will reject calls which do not use G.711 A-law or mu-law codecs.

TekSIP provides Music on Hold feature if RTP proxy enabled. You can choose a valid wave file to be played. TekSIP SP edition allows WebRTC SIP phones to makes calls to and accept calls from legacy SIP systems. TekSIP SP edition provides SRTP <-> RTP interworking with RTP proxy.

You can play out a media file to hold party in call when one participant of a call puts the call on hold. Media file must be a valid wave file.

TekSIP can play a notification message when the authorized time for a call is about to expire. You can specify your own notification audio to be played out 30 seconds before disconnection by enabling Mid-Call Announcement. This can be enabled only if you have enabled RTP Proxy feature.

Settings / WebSocket

TekSIP supports WebSocket Protocol *(RFC 7118)*. Secure WebSocket Protocol is supported only in commercial editions. You can enable WebSocket Protocol support in Settings / Other tab.

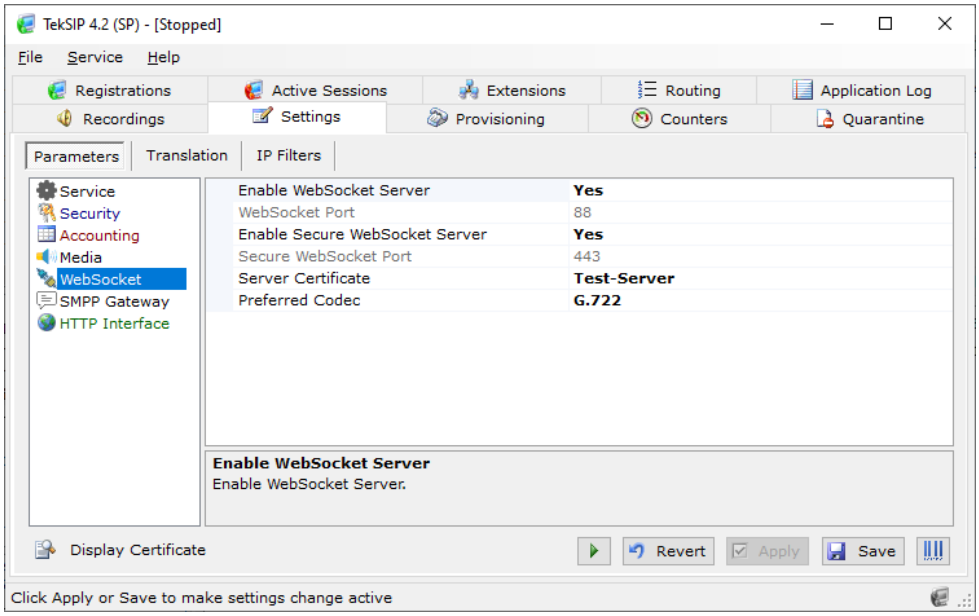


Figure - 5. Settings / WebSocket

Settings / SMPP Gateway

You can enable SMPP gateway by clicking Enable SMPP Gateway option. You can set TCP port for SMPP service and enter remote SMPP server parameters.

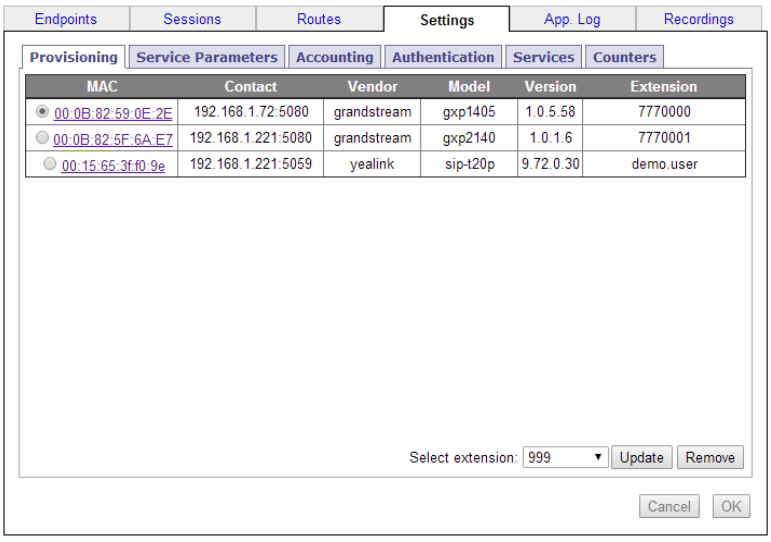


Figure - 6. HTTP Interface

Settings / HTTP Interface

You can enable the built-in web server for remote management. You can set the HTTP port and interface password. The built-in web server is disabled by default.

You can undo all settings changes by clicking the [Revert] button. If you click the [Apply] button, the setting changes will be applied and TekSIP will be re-started. If you click the [Save] button, the settings will be saved to TekSIP.ini. You can start and stop TekSIP at any time by clicking the service control button which is located to the left of the [Revert] button.

Settings / Translation

Some SIP phones, IP PBX systems and gateways may have interoperability problems due to SDP structure. TekSIP can manipulate the SDP portion and headers of SIP messages.

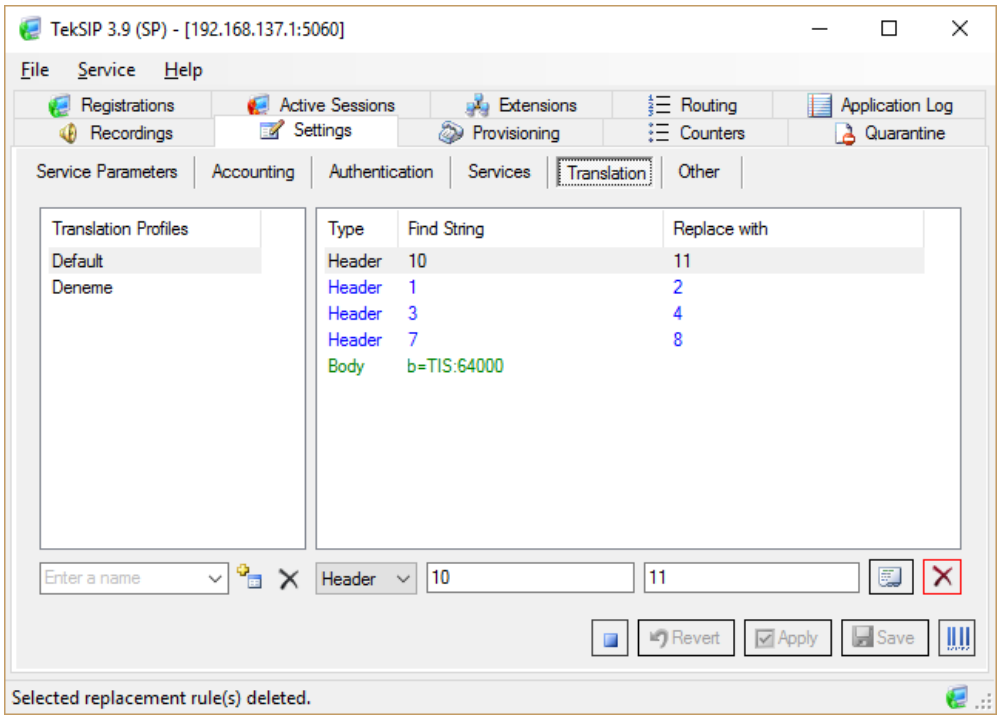


Figure - 7. Translation tab

You can create translation profiles to be applied to route profiles. The default translation profile is applied to the calls between registered endpoints. Translation rule order can be changed by dragging and dropping rule items. Upper rules are processed first. You can combine translations rules for SIP headers and body in the same translation profile. Translation profiles can be used only in SP edition of TekSIP.

You can use \t macro for tab character, \r for the carriage return and \n for line feed in “Replace with” string. TekSIP accepts “Find String” in regular expression format.

TekSIP allows you to alter codec id for a specified codec. This just changes codec id, transcoding is not preformed.

Settings / IP Filters

You can specify IP filter rules for incoming SIP and SMPP traffic. Rules can be specified for source IP address or subnet. Rules are processed up to down in order. Use a.b.c.d/e syntax for IP subnets where e is subnet bits 0-24. TekSIP will allow all incoming traffic if there is not any IP rule entry specified.

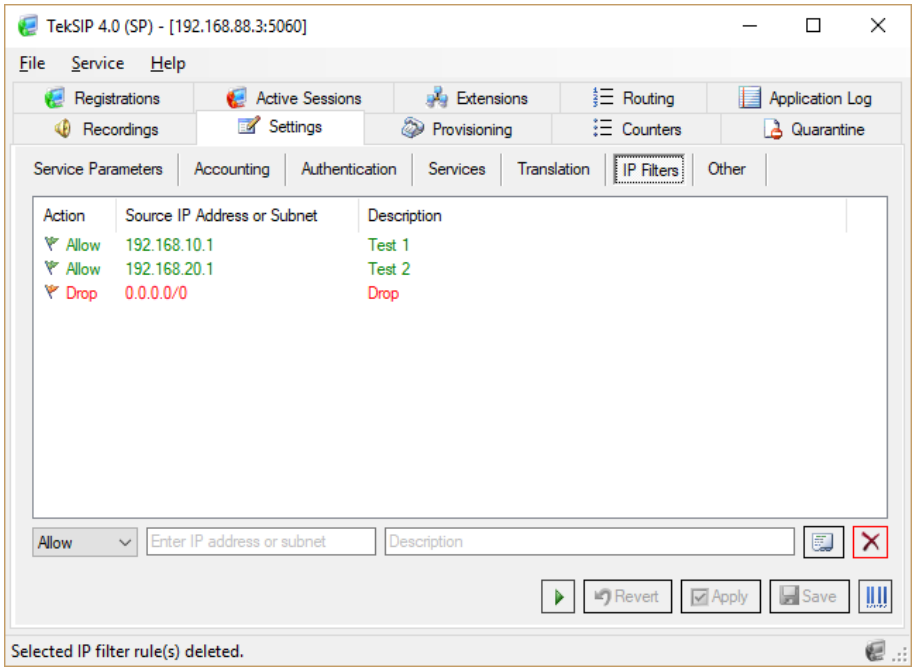


Figure - 8. IP Filters tab

You can specify three types of action for each IP filter rule entry; Allow, Bypass, Trust and Drop. Bypass action *(Trust action when RADIUS authentication is enabled)* instructs TekSIP to allow and bypass authentication for SIP requests originated from the matched IP address or subnet. SIP requests match for an Allow rule still to need to be authenticated if authentication is enabled.

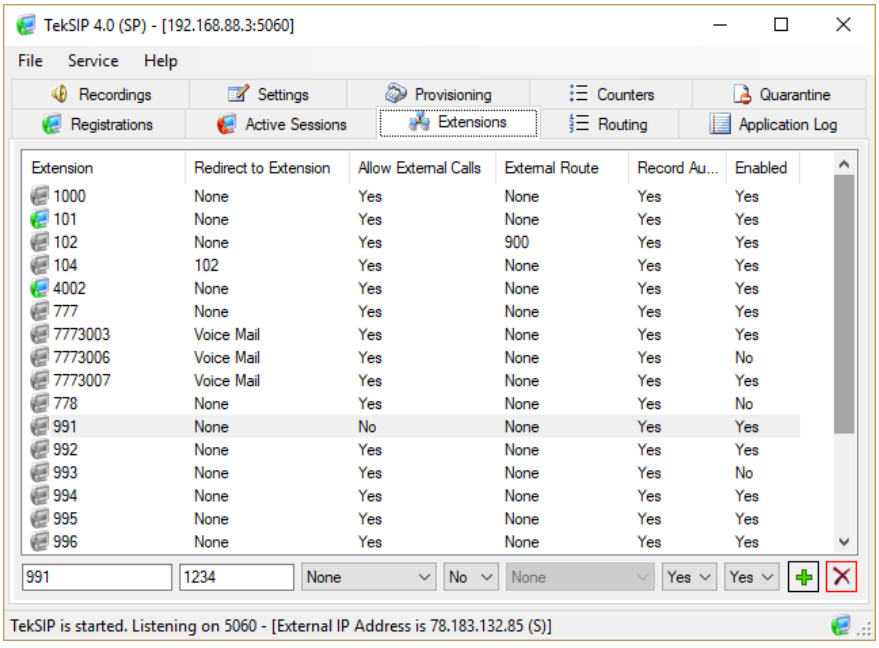


Figure - 9. Extensions Tab

Extensions

You can define the SIP endpoints using the "Extensions" tab. Enter a SIP username in the bottom leftmost textbox, enter the password to the textbox at the right of the username entry.

If you wish TekSIP to route incoming requests destined to this extension to another extension when it's unavailable *(Off-line, busy, timeout…)*, select the endpoint to be used as an alternative extension, select voice mail or leave as "None". You can set the voice mail information at the settings / services tab. Click the "Add/Update" button to add a new entry. If a valid entry is found with the same SIP username, that entry will be replaced or updated with the new entry. Click the [Edit] button to edit an existing entry or double click on the entry.

Click the [Remove] button to remove a SIP extension. All SIP extension data is stored in TekSIP.mdb which is located under the application directory. TekSIP clears expired registrations automatically. You can monitor extension status through the Extension tab. You can restrict extension to access external destination defined in Routing tab by settings **Allow External Calls** option. You can specify a default external route for the extension if you allow external calls. If you would like to use all available external routes leave default value "None" for the external route parameter.

You can also instruct TekSIP not to record audio conversations for an extension by setting **Record Audio** option if audio recording is enabled in global settings.

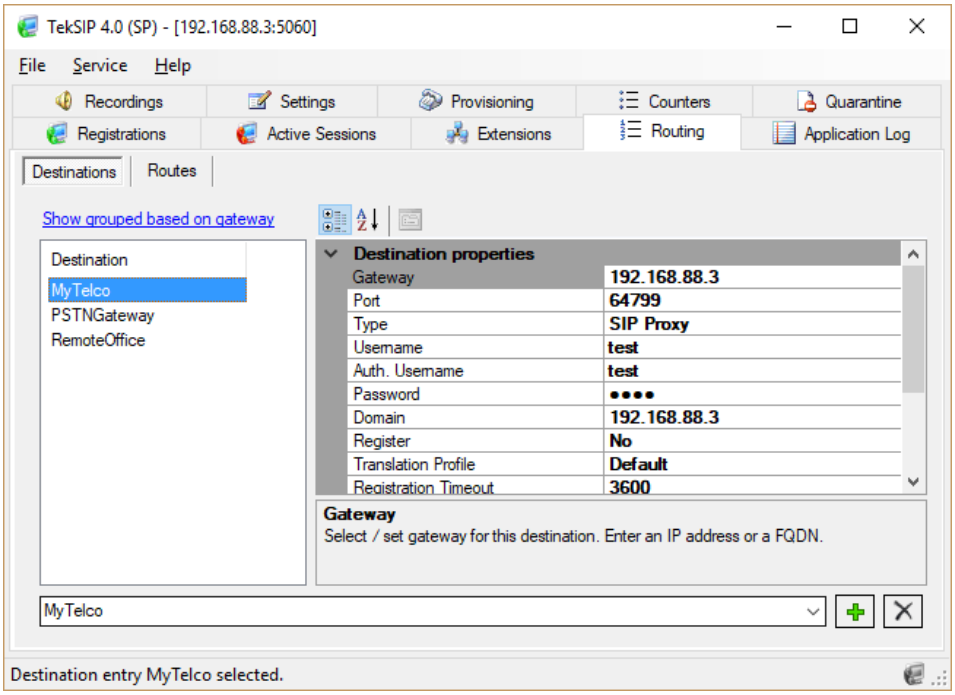


Figure - 10. Routing / Destinations Tab

Routing

You can define static routes to SIP endpoints through the "Routing" tab. You need to create destination profiles first. Enter a name to bottom leftmost textbox and click + to add a destination profile. Enter SIP destination parameters. Enter FQDN or IP address of the destination *(Gateway)*, the SIP port *(Default 5060)* used by the SIP Endpoint and the Endpoint type *(Default SIP UA)*.

TekSIP will forward incoming SIP request to a route like it is being originated from a SIP User Agent if you set route type to SIP UA. There will be only one via header for TekSIP IP address in outgoing SIP request. TekSIP will route calls to a registered endpoint if you set Type as Extension *(SP edition only).*

You can also have a default route entry as shown in the figure below. TekSIP chooses the longest match prefix route. You can change the order of route entries by dragging. If any match cannot be found, the default route is chosen if it exists. ENUM lookup has precedence over static routes. If ENUM lookup fails, TekSIP consults the static routing table. If the next hop configured for a phone prefix requires authentication, you can specify a username and password for the routing entry. If authentication is not required, you can leave the username and password fields blank.

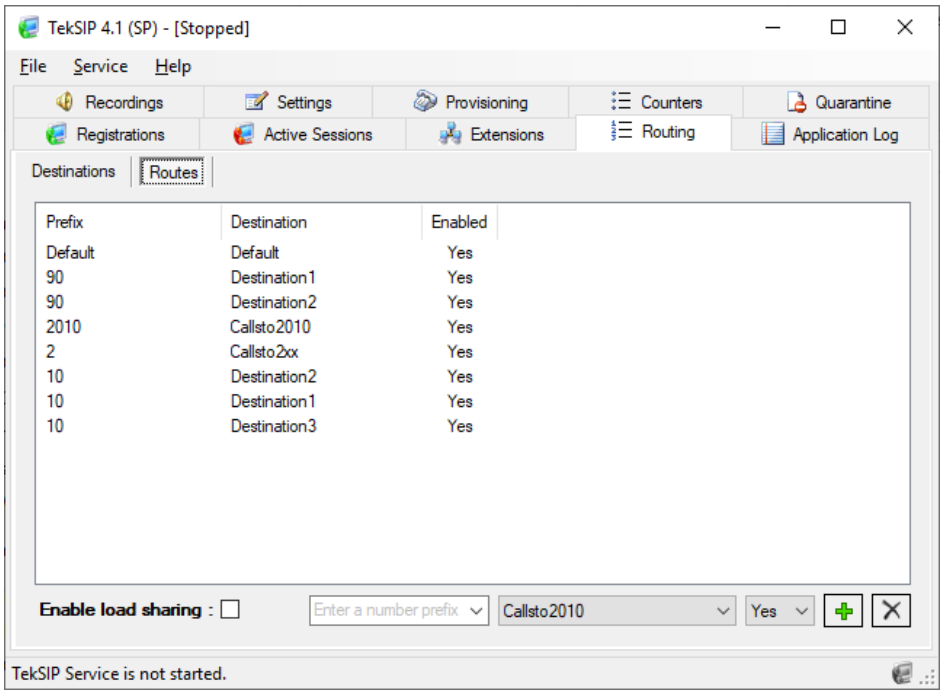


Figure - 11. Routing / Routes Tab

You can enable load sharing between destinations with the same prefix. TekSIP SP license enables you to have hunting for destinations with the same prefix.

TekSIP requests Proxy authentication for the incoming SIP requests from unregistered endpoints. However, SIP requests from the endpoints defined in the routing table are not authenticated if the incoming SIP request is destined to one of the defined endpoints in TekSIP's endpoint database. Enter a prefix and click the "Add Route" button to add a new routing entry. You must edit at least the Gateway entry to be able to commit the changes.

You can specify a separate domain name if the domain name is different to the Gateway IP address or the FQDN. If the configured route requires TCP transport, you can set it by the **Transport** parameter. If you set Remove Prefix = Yes, TekSIP will remove defined prefix from the dialed number. If you set Register = Yes and TekSIP cannot register this route, calls will be routed to the next available matched route.

You can set capacity for a route entry. This enables you to limit the number of calls that can be established for a particular route. TekSIP will select second best matching route entry if the best matching route capacity is used.

TekSIP can send OPTIONS request to remote SIP server / gateway when you disable registration. You need to set OPTIONS Ping = Yes to enable this function. TekSIP will show route entry in blue color when it receives responses to OPTIONS requests in timely manner. OPTIONS sending period can be set using registration timeout parameter of the route profile. Set timeout to zero or set OPTIONS Ping = No if you would like to disable sending OPTIONS requests.

You can force TekSIP to enable media encryption for outgoing calls when RTP proxy is enabled by setting Media Encryption = Yes option in route properties. This is useful when destination systems require SRTP transport mandatory for the media. Currently only `AES_CM_128_HMAC_SHA1_80` crypto suit supported for media encryption for outgoing calls. You can use this option with Direct Trunking to Microsoft Teams[2]. This feature is available with SP license.

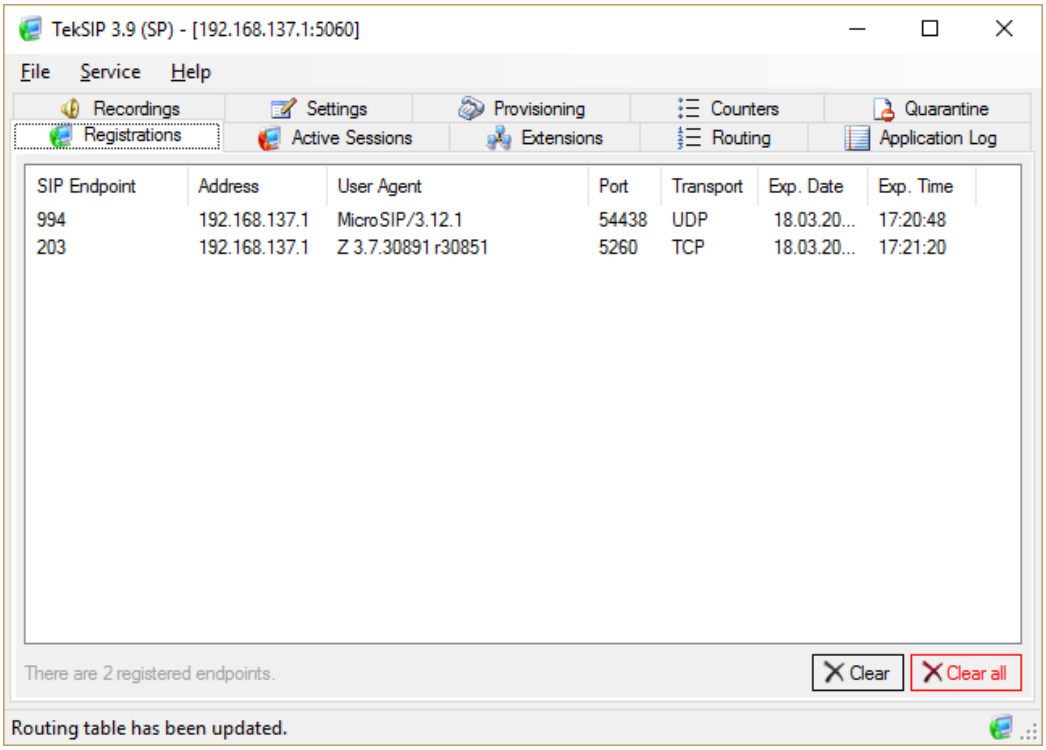


Figure - 12. Registrations Tab

Registrations

You can monitor active registrations through the “Registrations” tab. You can unregister one entry by clicking the [Clear] button, or all entries by clicking the [Clear all] button. If you unregister an entry, the client must re-register itself. If you stop the TekSIP service, all clients must re-register after re-starting the TekSIP service.

Active Sessions

You can monitor Active SIP Sessions through the Active Sessions tab. Sessions can be terminated by clicking the **Clear** or **Clear all** buttons.

[2] https://techcommunity.microsoft.com/t5/Microsoft-Teams-Blog/Direct-Routing-enables-new-enterprise-voice-options-in-Microsoft/ba-p/170450

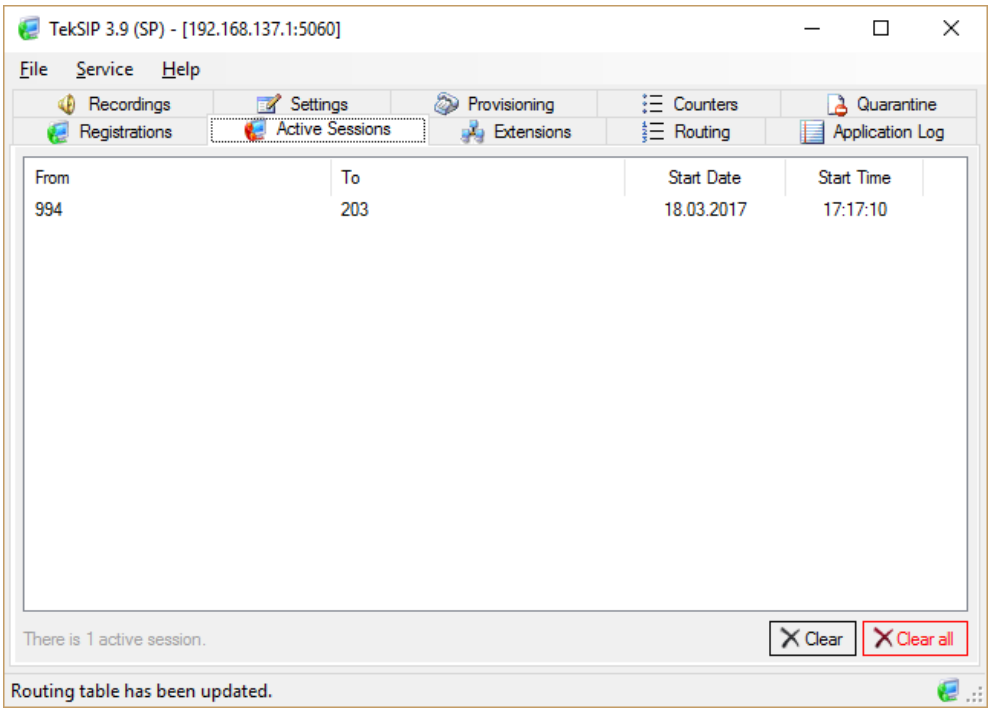


Figure - 13. Active Sessions Tab

Application Log

You can monitor TekSIP service events from the Application Log tab. Active SIP Sessions can be monitored through the Active Sessions tab. The session clearing function just clears entries in the list box. When you clear a session, you just remove the entry in the list box for that SIP session; if there is an active session between listed endpoints, the session stays active.

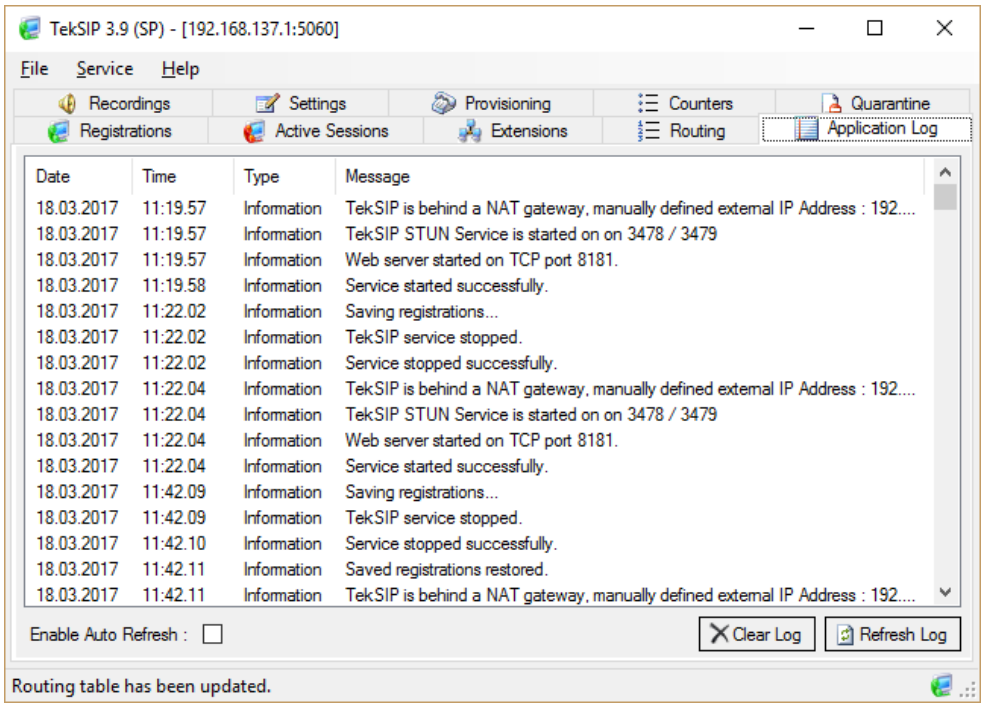


Figure - 14. Application Log Tab

Quarantine

TekSIP monitors failed registration and call attempts from suspicious endpoints and blacklists them if the Settings / Service Parameters / Blacklist IP Endpoints option is set.

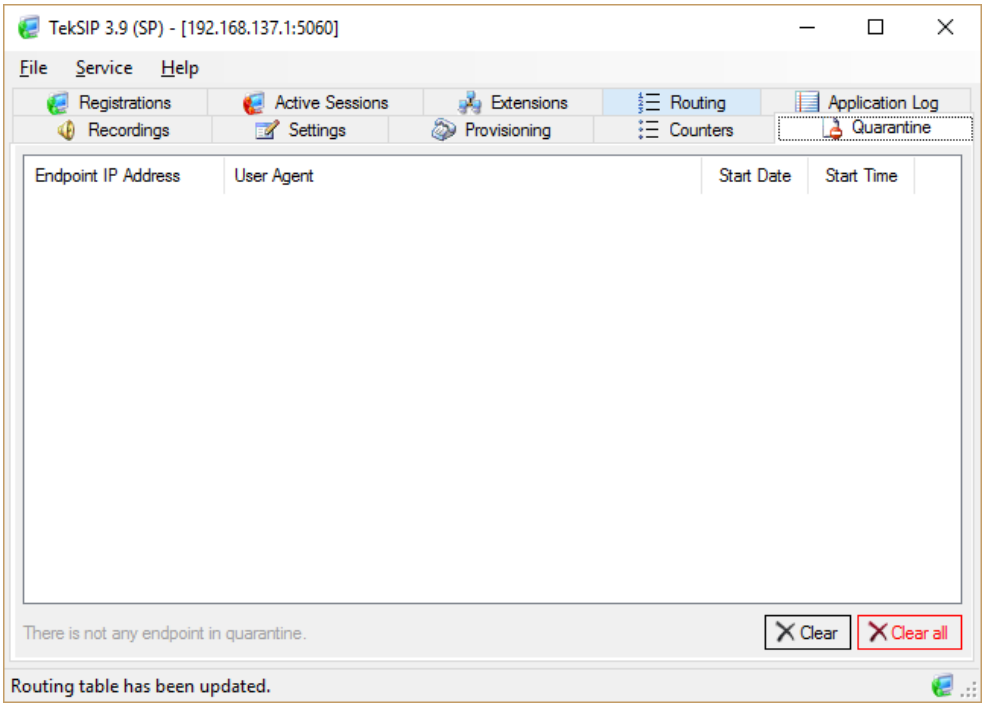


Figure - 15. Quarantine Tab

You can remove blacklisted endpoints from quarantine list if required by clicking either the Clear or Clear all buttons. The quarantine interface is available only in commercial editions of TekSIP.

Starting TekSIP

Click the “Service” menu and select “Start” to run TekSIP after making and saving the necessary configuration. If service starts successfully, you will see the “TekSIP Service is started” message at the bottom left message section of TekSIP Manager. Optionally, you can start/stop TekSIP using the button on the Settings tab. When you make any change(s) in the configuration, TekSIP will ask you if you wish to restart TekSIP to make settings changes active if the TekSIP service is already running.

If the TekSIP service cannot start, please examine the Application Log tab as well as the TekSIP log file under <Application Directory>\Logs, ensuring that you have enabled logging in “Settings/Service Parameters”.

Troubleshooting

TekSIP provides many messages when problems occur. You can see error messages on the TekSIP Status bar or in the log file of the TekSIP service. You can enable logging in the Settings Tab. There are three levels of logging: None, Errors, and Sessions. If you select “Errors”, TekSIP logs just error messages. If you select “Sessions”, both Session and Error messages will be logged. You

have to save or apply settings changes if you change the logging level setting. Log files are located under the <Application Directory>\Logs directory.

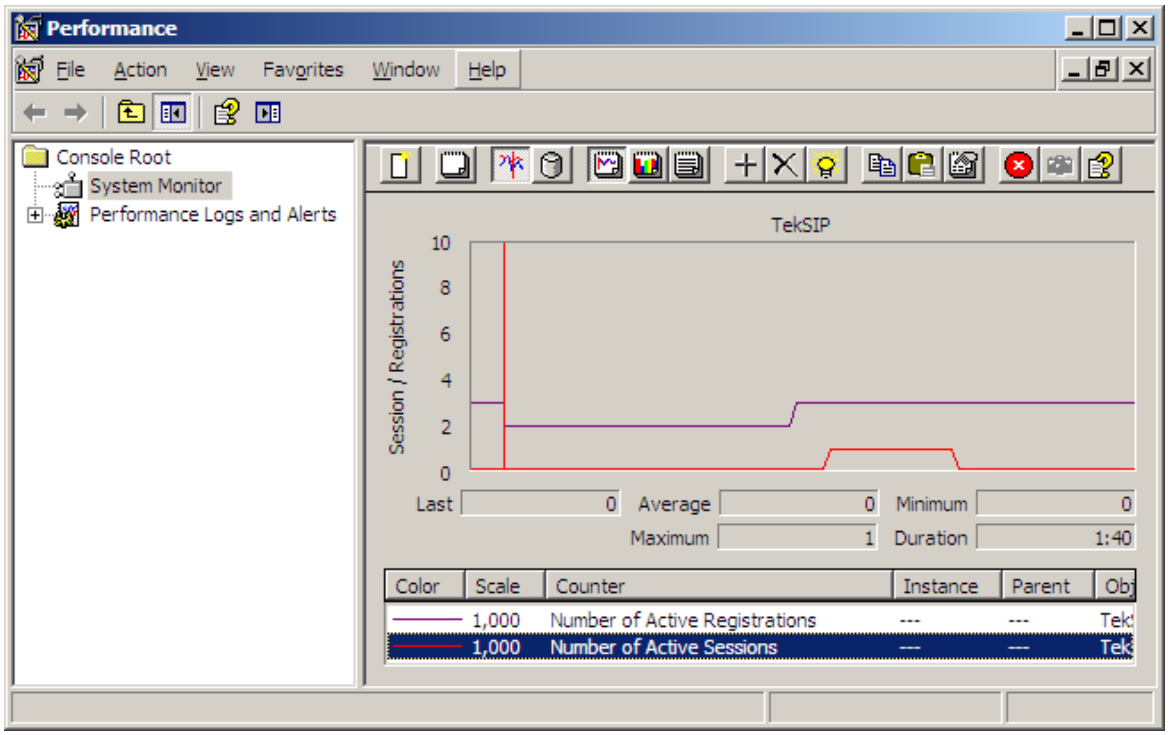


Figure - 16. TekSIP counters on Windows Performance Monitor

TekSIP also utilizes Windows Performance Monitor, providing numerous counters:

- Number of Active Registrations
- Number of Active Sessions (INVITE)
- Number of SIP Requests Received
- Number of SIP Requests Forwarded
- SIP Requests Receive Rate
- Number of Successful Calls
- Number of Failed Calls
- Number of Endpoints in Quarantine
- Number of Requests Received from Banned Endpoints
- Number of RADIUS Authentication Requests Sent
- Number of RADIUS Authentication Replies Received
- Number of RADIUS Authentication Timeouts
- Number of RADIUS Accounting Requests Sent
- Number of RADIUS Accounting Requests Received
- Number of RADIUS Accounting Timeouts

You can add and monitor these counters using Windows Performance Monitor *(Perfmon.exe)*. You can also monitor these counters through TekSIP Manager and the web monitoring interface.

TekSIP Messages

Endpoints could not be loaded.

TekSIP cannot find or read "TekSIP.mdb", which is located under the application directory. Please make sure that this file exists, it is not corrupted, and it is not exclusively opened by another application.

Settings could not be loaded. Initializing with default values.
TekSIP Service is being started with default values.

You get this message at first run of TekSIP if TekSIP cannot find or read TekSIP.ini. TekSIP initializes itself with default settings.

Unable to initialize UDP/TCP thread [5060]

If another application is configured to use the same UDP/TCP port *(5060)* as TekSIP, TekSIP cannot initialize the respective thread.

Default route points to this host

You cannot specify a gateway points to TekSIP.

New setting(s) applied and activated. Check default route.

There is a problem with the IP address or FQDN of the default route.

Cannot apply changes; enter minimum configuration

There is missing configuration data.

Endpoint 'abc' is added, but could not be saved.

There is a problem with the TekSIP database file. It may be opened by another application or the required database tables are missing.

You cannot redirect an endpoint to itself.

You cannot re-direct an endpoint to itself.

Invalid endpoint information or illegal character detected in entries.

Invalid characters found in a SIP username or entry. You can only use numeric characters in SIP username entries. You cannot use a ";" *(Semicolon)* character in password entries.

TekSIP SP Edition

TekSIP SP edition is designed for small to mid-sized telephony service providers. TekSIP SP asks for authorized amount of time for a dialed destination for a particular user to a RADIUS server. TekSIP SP starts a timer for the duration of authorized amount of time if the user is authorized. The call is terminated when the timer expires.

TekSIP SP RADIUS Authentication request contains following RADIUS attributes;

- User-Name *(Phone number in From: header)*
- NAS-IP-Address *(TekSIP Listen IP Address)*
- Called-Station-Id *(Phone number in request header)*
- Calling-Station-Id *(Phone number in From: header)*
- Cisco-h323-conf-id *(Call-Id)*

Following attributes are expected in a RADIUS Access-Accepts for authorization;

- Cisco-h323-credit-time *(Cisco VSA # 102)*
- Cisco-h323-credit-amount *(Cisco VSA # 101)* [Optional]

User session is authorized, and timer is started based on value specified in Cisco-h323-credit-time.

Auto Provisioning for IP Phones

TekSIP supports auto provisioning of IP phones based on SUBSCRIBE / NOTIFY PnP mechanism. PnP Auto Provisioning IP phones send SIP SUBSCRIBES messages to a multicast address *(224.0.1.75)*. TekSIP replies with a SIP NOTIFY message containing the Auto Provisioning Server URL where the phones can request their configuration from.

IP phones from following vendors are supported;

- GrandStream
- Yealink
- Snom
- Aastra

TekSIP displays auto provisioning requests from IP phones on the LAN in provisioning tab;

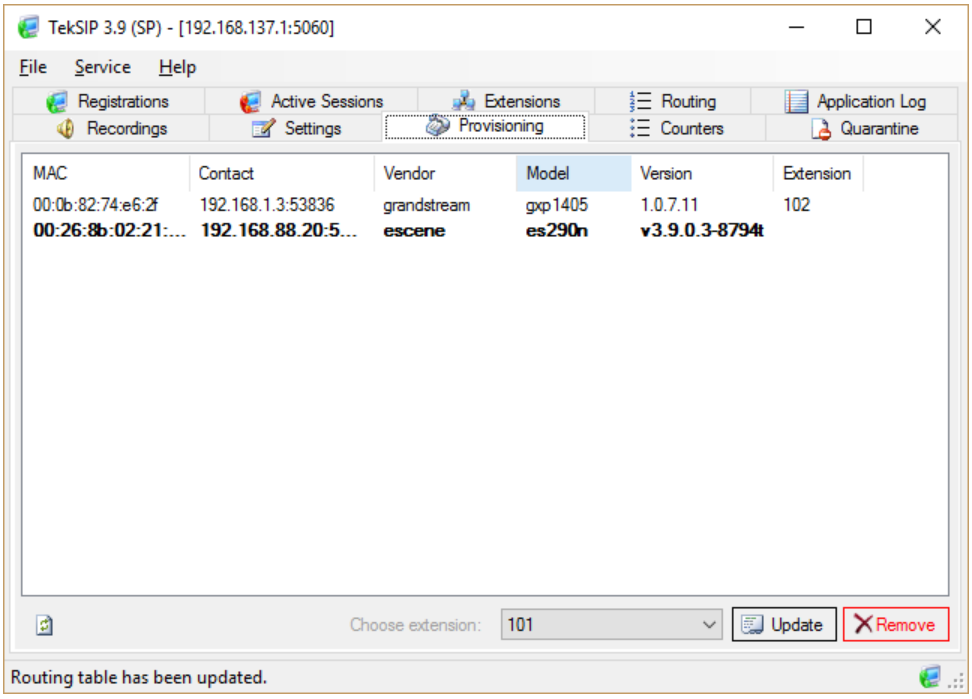


Figure - 18. TekSIP Manager Provisioning tab

New provisioning requests are shown as **bold** and provisioning requestes from unknown vendors are shown in red. Select new provisioning request, choose an extension and click Update button to send a NOTIFY message contaning configuration URL to the IP phone. You can also change configuration of provisioned phones already.

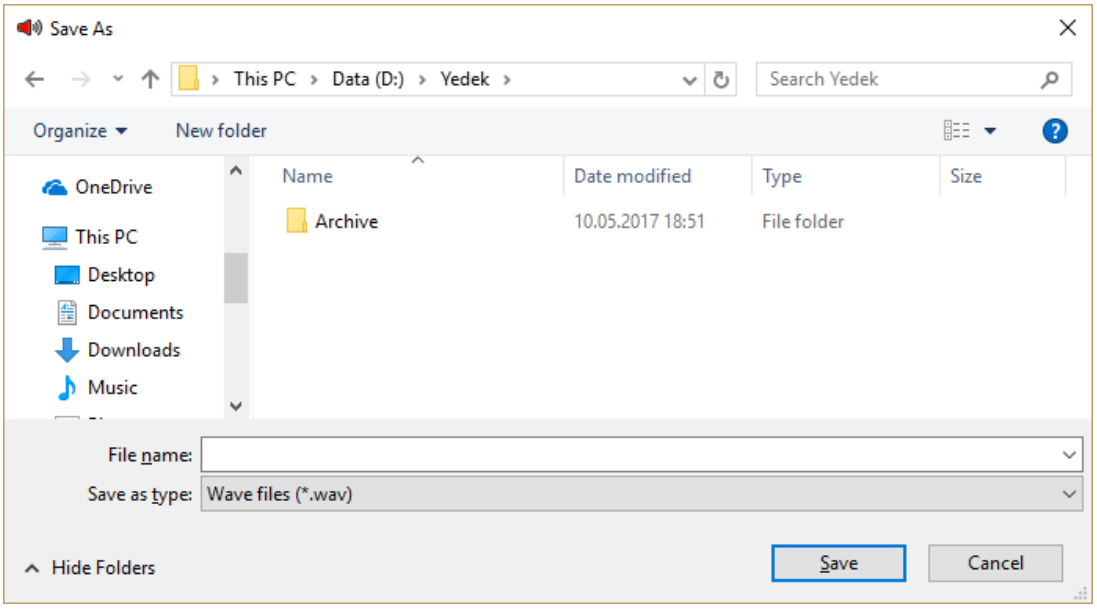
TekSIP configuration file contains a SIP account profile. TekSIP configuration file also contains time zone and day light saving time information. TekSIP defaults web console admin password to the account password for the IP phone. You can open IP phones administrative web console by double cliecking provisioing entry.

You must enable HTTP Server at Settings / Services for configuration file delivery to the IP phones.

How to Record a Custom Audio Message

You can use Windows Sound Recorder to record a custom audio prompt. You can use TekRecorder to record audio files compatible with TekSIP.

Click the record button to start recording. Click the record button again after finishing. Select "File/Save As" option from File menu.



Audio file will be saved in "8000 Hz; 16 Bit; Mono" format. You can download TekRecorder from KaplanSoft website download section.

HTTP API

TekSIP provides a JSON based HTTP REST API when the HTTP interface is enabled.

Types

```
Enum OperationTypes As Integer
      None = 0
      AddDestination = 1
      RemoveDestination = 2
      ListDestination = 3
      AddRoute = 4
      RemoveRoute = 5
      ListRoute = 6
      ListSession = 7
      TerminateSession = 8
      ReadLogs = 9
      ClearLogs = 10
      ReadCounters = 11
      ClearCounters = 12
      AddExtension = 13
      RemoveExtension = 14
      ListExtension = 15
      ListRegistration = 16
      TerminateRegistration = 17
      ListQuarantineEntry = 18
      RemoveQuarantineEntry = 19
      AddIPFilter = 20
      RemoveIPFilter = 21
      ListIPFilter = 22
End Enum
```

```
Enum DestinationTypes As Integer
      UA = 1
      Proxy = 2
      Extension = 3
End Enum

Enum Transports As Integer
      None = 0
      UDP = 1
      TCP = 2
      TLS = 3
      WS = 4
      WSS = 5
End Enum
```

Functions

Add Destination [POST /routing]

Request

```
{
    "APIPassword": "1234",
    "OperationType": "AddDestination",
    "Username": "",
    "AuthUsername": "",
    "Password": "",
    "Register": false,
    "Timeout": 3600,
    "Domain": "192.168.3.1",
    "Gateway": "192.168.3.1",
    "Port": 5060, "Transport": 1,
    "Capacity": 500,
    "Ping": false, "Enabled": true,
    "RemovePrefix": false,
    "MediaEncryption": false,
    "AddPrefix": "",
    "TranslationProfile": "Default",
    "Type": 2,
    "Name": "Proxy2"
}
```

Response

```
{
    "Operation": 1,
    "Success": true,
    "Message": "Destination is added"
}
```

Delete Destination [POST /routing]

Request

```
{
  "APIPassword": "1234",
  "OperationType": 2,
  "Data": {
      "Name": "Proxy2"
  }
}
```

Response

```
{
  "Operation": 2,
  "Success": true,
  "Message": "Destination entry 'Proxy2' is deleted."
}
```

List Destinations [POST /routing]

Request

```
{
  "APIPassword": "1234",
  "OperationType": 3
}
```

```
{
    "APIPassword": "1234",
    "OperationType": 3,
    "Data": {
        "Name": "Proxy"
    }
}
```

Response

```
[
    "94777552555",
    "Deneme",
    "Deneme 3",
    "Deneme2",
    "EP",
    "Proxy",
    "Vaio"
]
```

```
{
    "Username": "",
    "AuthUsername": "",
    "Password": "",
    "Register": false,
    "Timeout": 3600,
    "Domain": "192.168.1.1",
    "Gateway": "192.168.1.1",
    "Port": 5060,
    "Transport": 1,
    "Capacity": 500,
    "Ping": false,
    "Enabled": true,
    "RemovePrefix": false,
    "MediaEncryption": false,
    "AddPrefix": "",
    "TranslationProfile": "Default",
    "Type": 2,
    "Name": "Proxy"
}
```

Add Route [POST /routing]

Request

```
{
  "APIPassword": "1234",
  "OperationType": "AddRoute",
  "Prefix": "2000",
  "Destination": "X",
  "Enabled": true
}
```

Response

```
{
  "Operation": 4,
  "Success": false,
  "Message": "Specified destionation does not exist."
}
```

```
{
  "Operation": 4,
  "Success": true,
  "Message": "Route entry is added for prefix '2000'."
}
```

Delete Route [POST /routing]

Request

```
{
    "APIPassword": "1234",
    "OperationType": 5,
    "Data": {
        "Prefix": "tset"
    }
}
```

Response

```
{
    "Operation": 5,
    "Success": true,
    "Message": "Route entry is deleted"
}
```

List Routes [POST /routing]

Request

```
{
    "APIPassword": "1234",
    "OperationType": 6
}
```

Response

```
[
    {
        "Order": 0,
        "Prefix": "15199132345",
        "Destination": "94777552555",
        "Enabled": true
    },
    {
        "Order": 1,
        "Prefix": "tset",
        "Destination": "94777552555",
        "Enabled": true
    }
]
```

List Sessions [POST /sessions]

Request

```
{
  "APIPassword": "1234",
  "OperationType": 7
}
```

Response

```
[
    {
      "SessionId": "741223cc78ee4f4eb18ed8c6884712e2",
      "From": "102",
      "To": "999",
      "Established": "/Date(1681556605365)/"
    },
    {
      "SessionId": "671823cc78ee4f4eb18ed8c6884712e1",
      "From": "103",
      "To": "998",
      "Established": "/Date(1681556615965)/"
    }
]
```

Terminate Session [POST /sessions]

Request

```
{
  "APIPassword": "1234",
  "OperationType": 8,
  "Data": {
      "SessionId": "a4c4f7"
    }
}
```

Response

```
{
  "Operation": 8,
  "Success": true,
  "Message": "Hung up active call - (a4c4f7)"
}
```

Add Extension [POST /extensions]

Request

```
{
"APIPassword": "1234",
"OperationType": 13,
"Username": "Tester",
"Password": "1234",
"AllowExternalCalls": false,
"RecordCalls": false,
"Prefix": "",
"Redirection": "",
"Enabled": true
}
```

Response

```
{
 "Operation": 13,
 "Success": true,
 "Message": "'Tester' added. Calls will be redirected
             to '100' when it's off-line."
}
```

Delete Extension [POST /extensions]

Request

```
{
  "APIPassword": "1234",
  "OperationType": 14,
  "Data": {
      "ExtensionId": "Tester"
    }
}
```

Response

```
{
  "Operation": 14,
  "Success": false,
  "Message": "Extension 'Tester' is deleted"
}
```

List Extension [POST /extensions]

Request

```
{
  "APIPassword": "1234",
  "OperationType": 15,
  "Data": {
      "ExtensionId": "Tester"
    }
}
```

```
{
  "APIPassword": "1234",
  "OperationType": 15
}
```

Response

```
{
    "Username": "Tester",
    "Password": "1234",
    "Redirection": "100",
    "AllowExternalCalls": false,
    "RecordCalls": false,
    "Prefix": "",
    "ExternalRoute": "None",
    "Enabled": true,
    "APIPassword": null,
    "OperationType": 0,
    "Data": null
}
```

```
[
    "1000",
    "101",
    "102",
    "103",
    "998",
    "999",
    "Tester"
]
```

List Registrations [POST /registrations]

Request

```
{
  "APIPassword": "1234",
  "OperationType": 16
}
```

Response

```
[
    {
        "EndpointId": "102",
        "UserAgent": "MicroSIP/3.21.3",
        "IPAddress": "192.168.1.51",
        "Port": 63793,
        "Transport": 1,
        "Expires": "/Date(1681732056378)/",
        "Status": "online"
    },
    {
        "EndpointId": "999",
        "UserAgent": "TekIVR/v2.7.4",
        "IPAddress": "192.168.1.51",
        "Port": 50765,
        "Transport": 2,
        "Expires": "/Date(1681735364682)/",
        "Status": "online"
    }
]
```

Terminate Registrations [POST /registrations]

Request

```
{
  "APIPassword": "1234",
  "OperationType": 17,
  "Data": {
      "ExtensionId": "999"
  }
}
```

Response

```
{
  "Operation": 17,
  "Success": false,
  "Message": "Registration for 999 is cleared "
}
```

Terminate Registration [POST /registrations]

Request

```
{
  "APIPassword": "1234",
  "OperationType": 17,
  "Data": {
      "ExtensionId": "999"
  }
}
```

Response

```
{
  "Operation": 17,
  "Success": false,
  "Message": "Registration for 999 is cleared "
}
```

Read Logs [POST /log]

Request

```
{
    "APIPassword": "1234",
    "OperationType": 9
}
```

Response

```
[
    {
        "EntryDateTime": "/Date(1681727315000)/",
        "Type": "Information",
        "Message": "TekSIP Service is being stopped."
    },
    {
        "EntryDateTime": "/Date(1681727315000)/",
        "Type": "Information",
        "Message": "TekSIP service is stopped."
    }
]
```

Clear Logs [POST /log]

Request

```
{
    "APIPassword": "1234",
    "OperationType": 10
}
```

Response

```
{
    "Operation": 10,
    "Success": true,
    "Message": "Application log is cleared"
}
```

Read Counters [POST /counters]

Request

```
{
    "APIPassword": "1234",
    "OperationType": 11
}
```

Response

```
[
    [
    {
        "Name": "Number of Active Registrations",
        "Value": "1"
    },
    :
    {
        "Name": "Number of RADIUS Accounting Timeouts",
        "Value": "0"
    }
]
```

Clear Counters [POST /counters]

Request

```
{
    "APIPassword": "1234",
    "OperationType": 12
}
```

Response

```
{
    "Operation": 12,
    "Success": true,
    "Message": "Counters are cleared"
}
```

Read Quarantine Entries [POST /quarantine]

Request

```
{
    "APIPassword": "1234",
    "OperationType": 18
}
```

Response

```
[
    {
        "EntryDateTime": "/Date(1681727315000)/",
        "Address": "1921.68.1.1",
        "UserAgent": "Test"
    }
]
```

Clear Quarantine Entries [POST /quarantine]

Request

```
{
 "APIPassword": "1234",
 "OperationType": 19,
 "Data": {
   "Address": "192.168.1.1"
 }
}
```

Response

```
{
 "Operation": 19,
 "Success": true,
 "Message": "Quarantine entry '192.168.1.1' is
             cleared"
}
```

```
{
 "APIPassword": "1234",
 "OperationType": 19
}
```

```
{
 "Operation": 19,
 "Success": true,
 "Message": "Quarantine table is cleared."
}
```

Index