TekSIP

Installation & Configuration Guide
Version 3.3

Document Revision 3.9

http://www.teksip.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.

TekSIP complies with RFC 3261, RFC 3263, RFC 3311, RFC 3581 and RFC 3891. It supports NAT traversal and ENUM. You can select the IP address to be listened to and the default SIP endpoint for outgoing calls. 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 a 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 runs as a Windows service.

TekSIP also provides a single account proxy. If you have just one provider account and many internal clients, TekSIP proxies all external calls for the provider account. You can also have different provider accounts for different destinations *(Prefixes)*. TekSIP can also register itself to a provider SIP server if needed. You can receive incoming calls with registration. Please see **“Routing”** section for details.

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.

System Requirements

1. A Windows system with at least 1024 MB of RAM.
2. Microsoft.NET Framework v2.0.50727 *(Min.)*
3. 2 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.

Configuration

Run TekSIP Manager from Start Menu / Program Files / TekSIP. TekSIP automatically configures itself at first run. TekSIP selects the first available IPv4 address to listen on and make 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 a 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 Tab

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

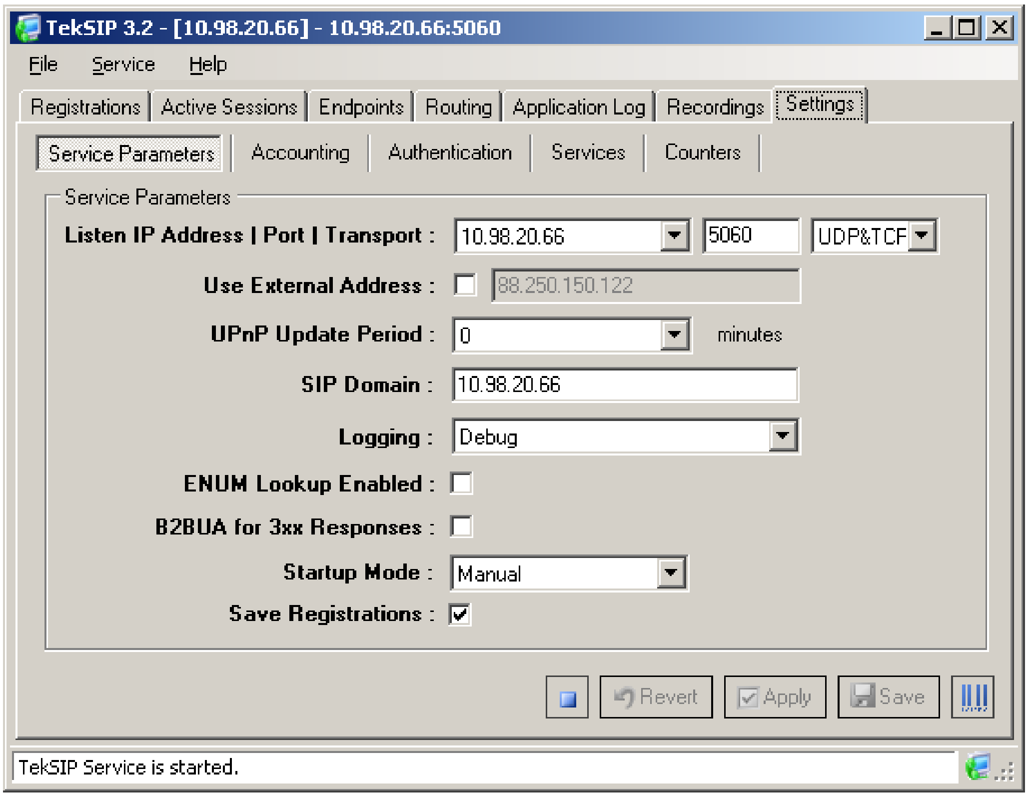

Figure - 1. TekSIP Settings / Service Parameters

Enter the following information for the Service Parameters:

- **Listen IP Address | Port | Transport:** You can select a detected IPv4 address configured on your system. When you change the IP configuration of your system, the IP address list will automatically be updated. You can define a port number to be listened *(Default 5060)*. You can select which transport protocol will be used by TekSIP using the **Transport** parameter. TekSIP uses both UDP and TCP transports by default.
- **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”.

- **UPnP Update Period:** You can specify the period for querying the UPnP Internet Access Gateway. Set to "0" to disable UPnP support.
- **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.
- **Logging:** 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.
- **ENUM Lookup Enabled:** TekSIP can resolve numbers in incoming SIP requests to an ENUM entry if it exists. If TekSIP can not 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. Visit http://en.wikipedia.org/wiki/Electronic_Numbering for detailed information on ENUM.
- **B2BUA for 3xx Responses:** 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.
- **Startup Mode:** Set TekSIP service startup mode: Manual or Automatic. You can also disable the service startup.
- **Save Registrations:** In order to keep the endpoint registrations while restarting, set this option.

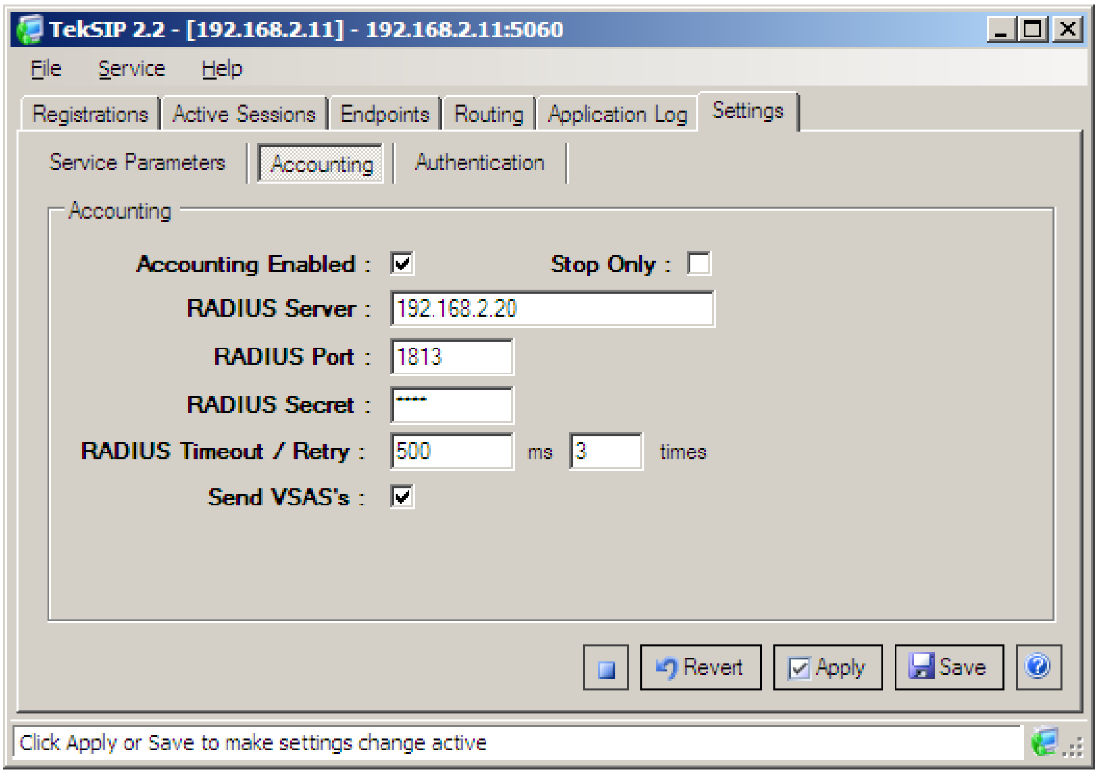

Figure - 2. TekSIP Settings / Accounting

Enter following information for Accounting:

- **Accounting Enabled:** TekSIP supports RADIUS accounting. RADIUS accounting is disabled by default. Click “Accounting Enabled” to enable RADIUS accounting.
- **Stop Only:** If you prefer to send only RADIUS Accounting stop messages to the RADIUS server, select this option.
- **RADIUS Server:** Enter a valid IPv4 address for the RADIUS server.
- **RADIUS Port:** Enter the UDP port number of the RADIUS server. 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-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)

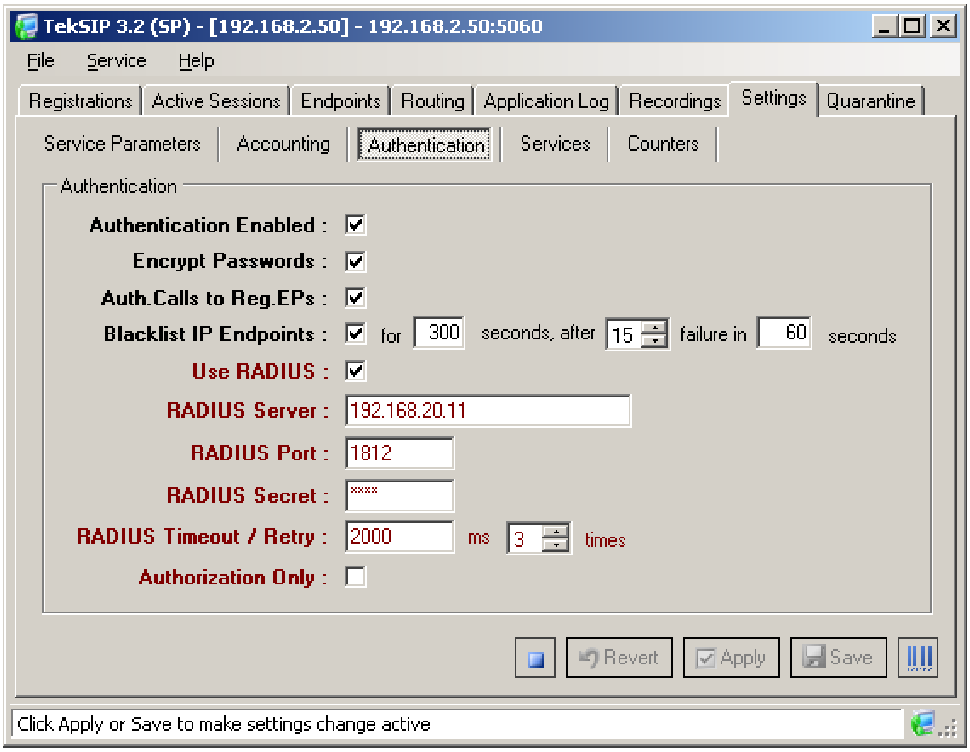

Figure - 3. TekSIP Settings / Authentication

Enter following information for Authentication:

- **Authentication Enabled:** SIP endpoint authentication is enabled by default. If you do not want to authenticate SIP registration and SIP requests, uncheck this option.
- **Encrypt Passwords:** Set this option to keep the endpoint passwords in encrypted form in TekSIP.mdb.
- **Auth.Calls to Reg.EPs:** You can enable authentication for incoming calls to registered endpoints by settings this option.
- **Blacklist IP Endpoints:** If selected, TekSIP monitors failed registration and call attempts from suspicious endpoints and blacklists them.
- **Use RADIUS:** 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 Server:** Enter a valid IPv4 address for the RADIUS server.
- **RADIUS Port:** Enter the UDP port number of the RADIUS server. 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.
- **Authorization Only:** When you set this option TekRADIUS only request authorization parameters from the RADIUS server *(Maximum allowed session time for the call e.g.)*. This parameter is available only in SP edition of TekSIP.

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:

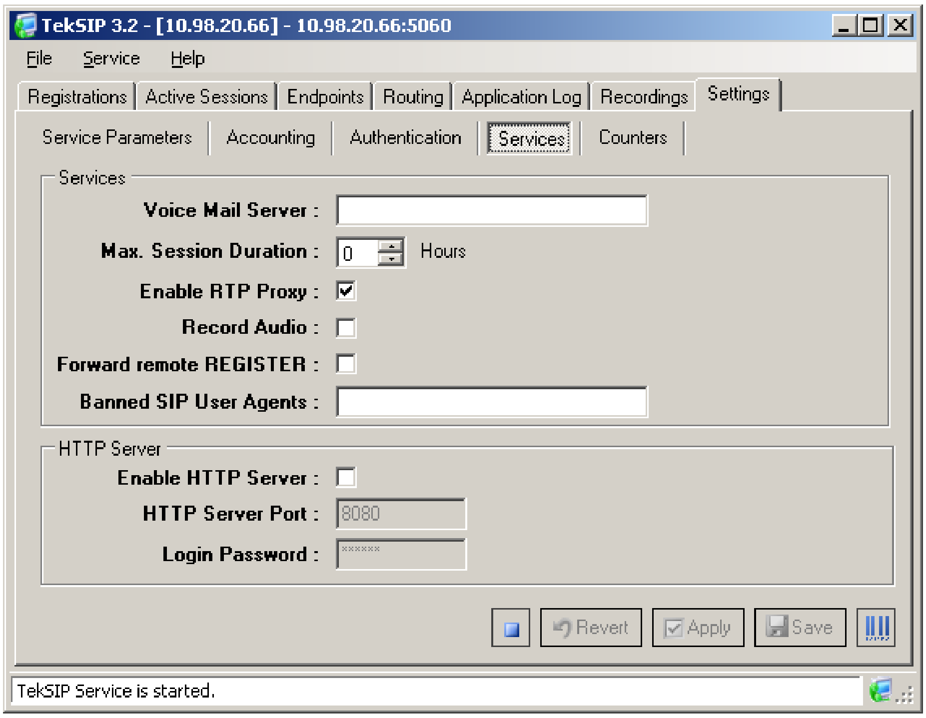

Figure - 4. TekSIP Settings / Services tab.

You can set which calls for a specific endpoint should be re-directed to the voice mail server at the Endpoints tab.

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 processes REGISTER, SUBSCRIBE and PUBLISH requests locally by default. If you would like to forward such requests to remote SIP servers based Request URI check **Forward Remote REGISTER** option.

You can also ban specific user agents. Multiple user agent identifiers can be concatenated with semicolons “;”.

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

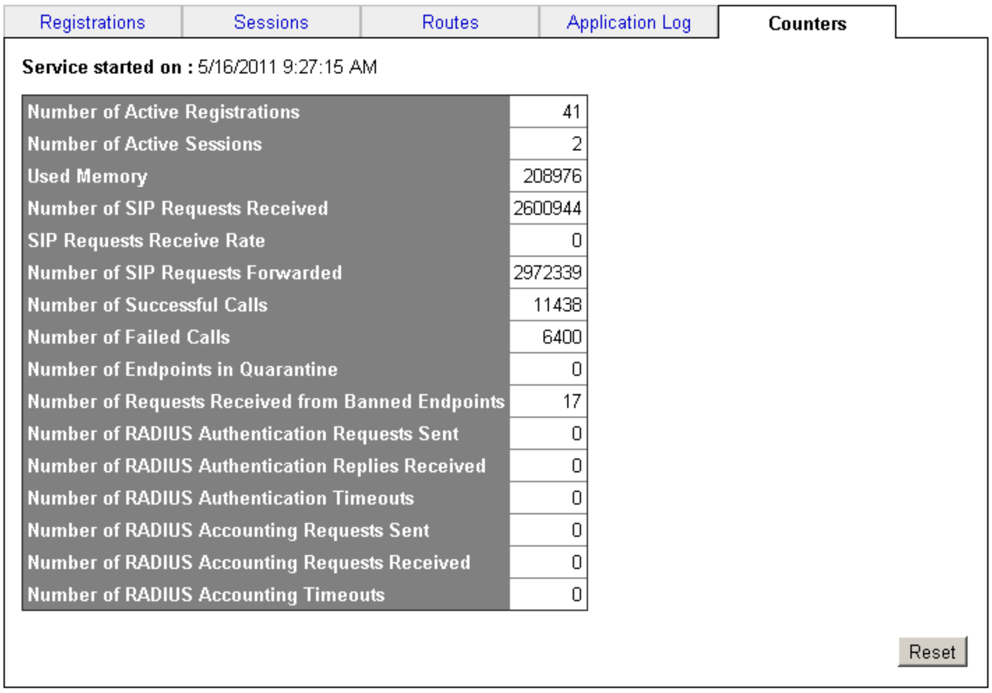

Figure - 5. HTTP Interface

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.

Endpoints

You can define the SIP endpoints using the “Endpoints” 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 endpoint to another endpoint when it’s unavailable *(Off-line, busy…)*, select the endpoint to be used as an alternative endpoint, 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 endpoint. All SIP endpoint data is stored in TekSIP.mdb which is located under the application directory. TekSIP clears expired registrations automatically.

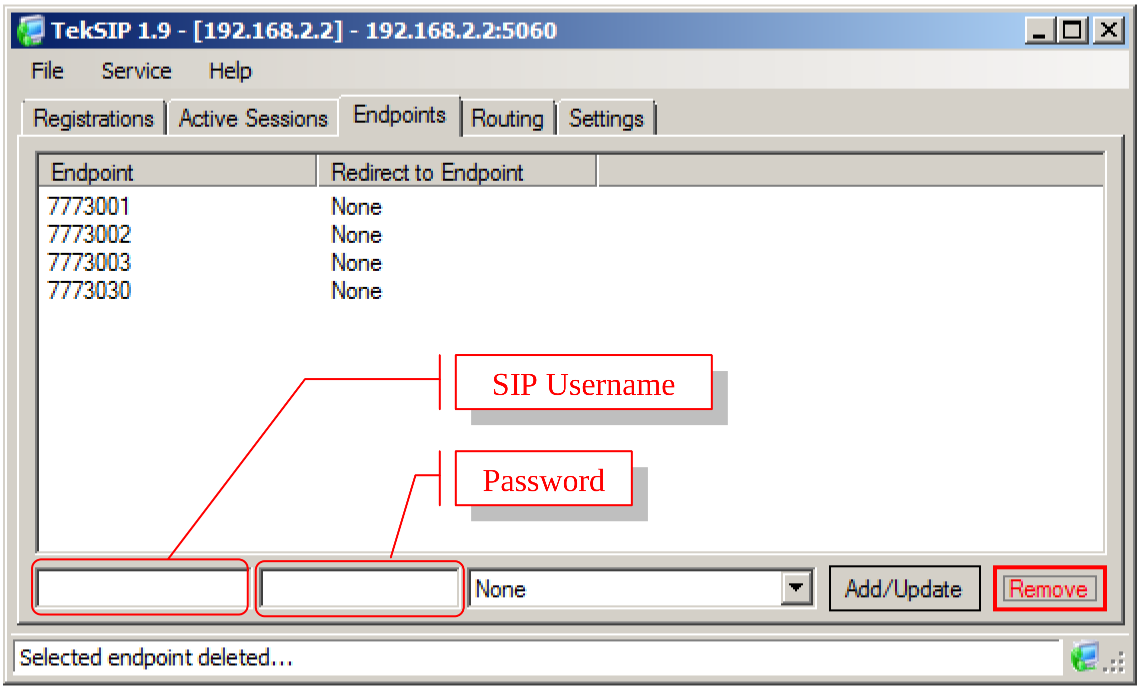

Figure - 6. Endpoints Tab

Routing

You can define static routes to SIP endpoints through the "Routing" tab. Enter a phone number prefix to bottom leftmost textbox, enter the endpoint IP address to the textbox to the right of the prefix entry. You can also enter the SIP port *(Default 5060)* used by the SIP Endpoint and the Endpoint type *(Default SIP UA)*.

You can also have a default route entry as shown the figure below. TekSIP chooses the longest match prefix route. 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 particular routing entry. If authentication is not required, you can leave the username and password fields blank.

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.

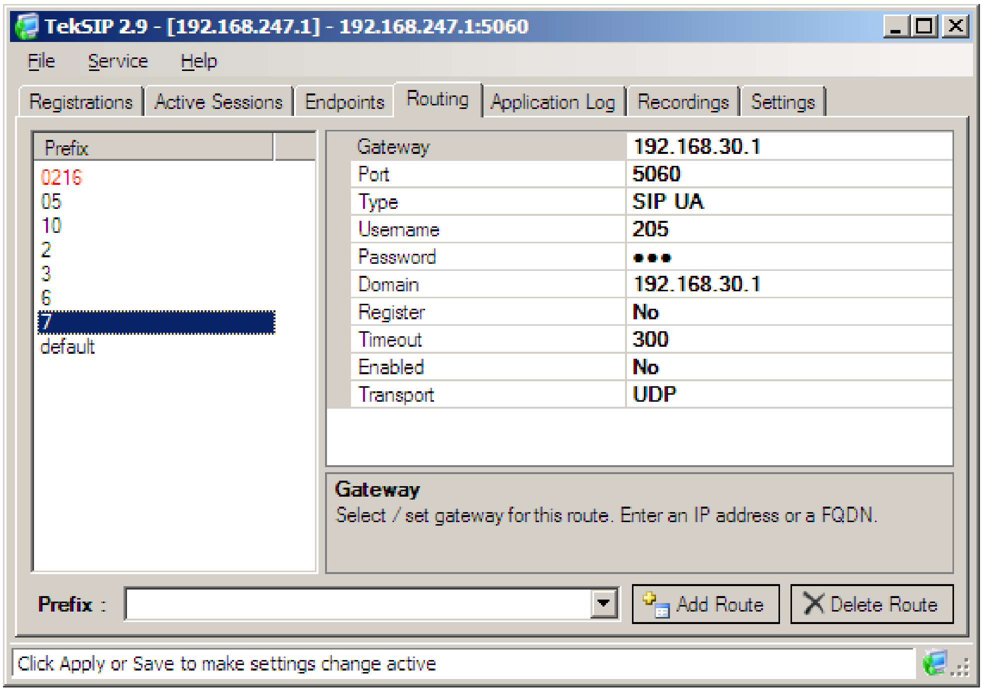

Figure - 7. Routing Tab

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.

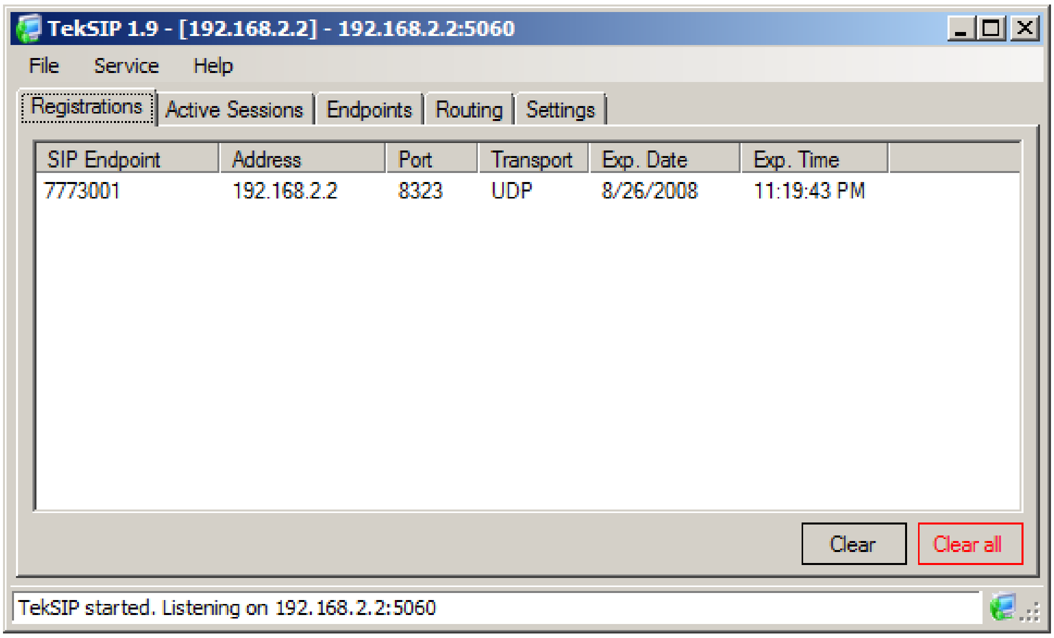

Figure - 8. Registrations Tab

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.

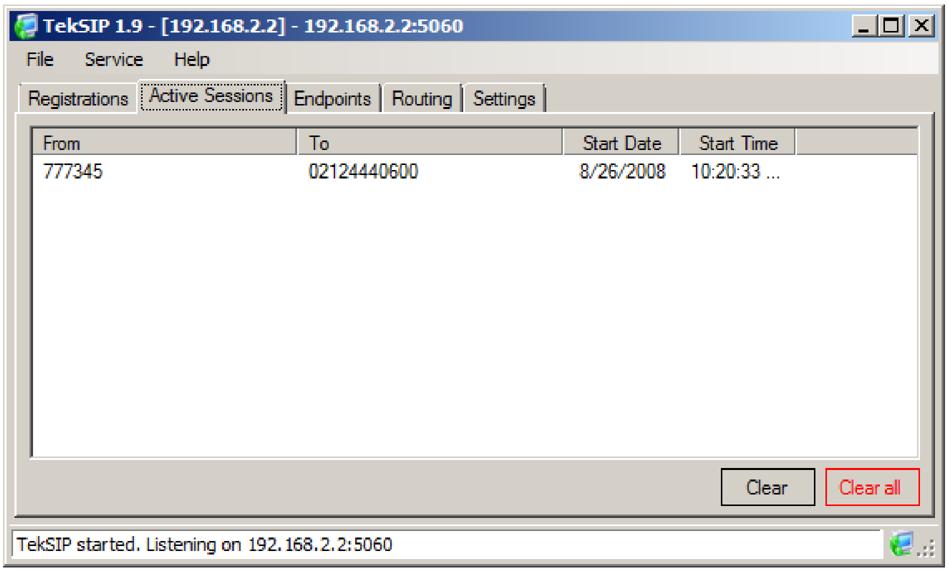

Figure - 9. Active Sessions Tab

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 clear entries in the list box. When you clear a session you just remove the entry in the list box for that particular SIP session; if there is an active session between listed endpoints, the session stays active.

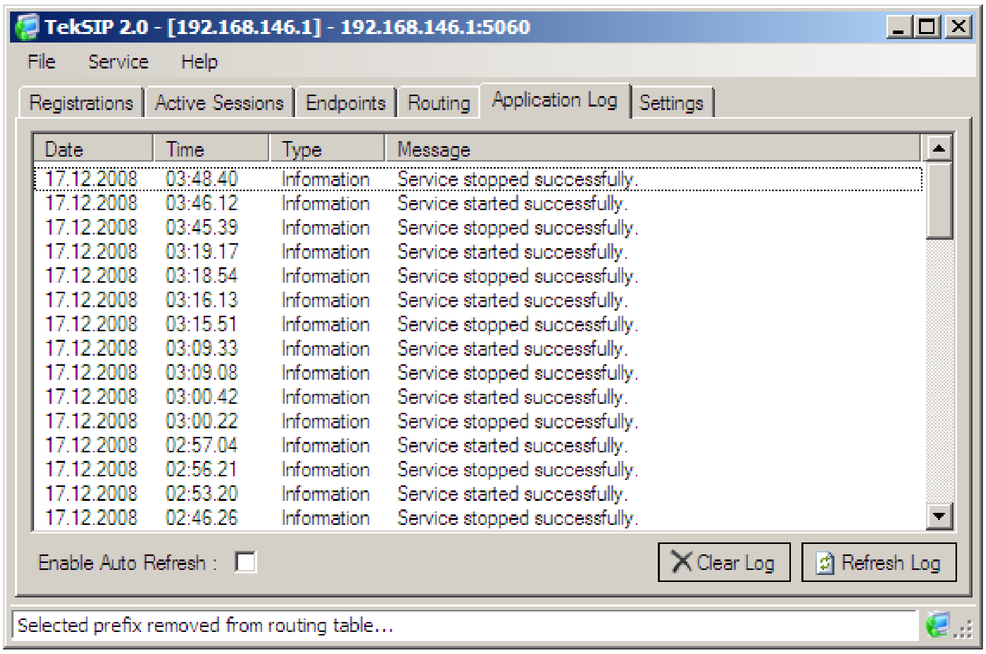

Figure - 10. Application Log Tab

Quarantine

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

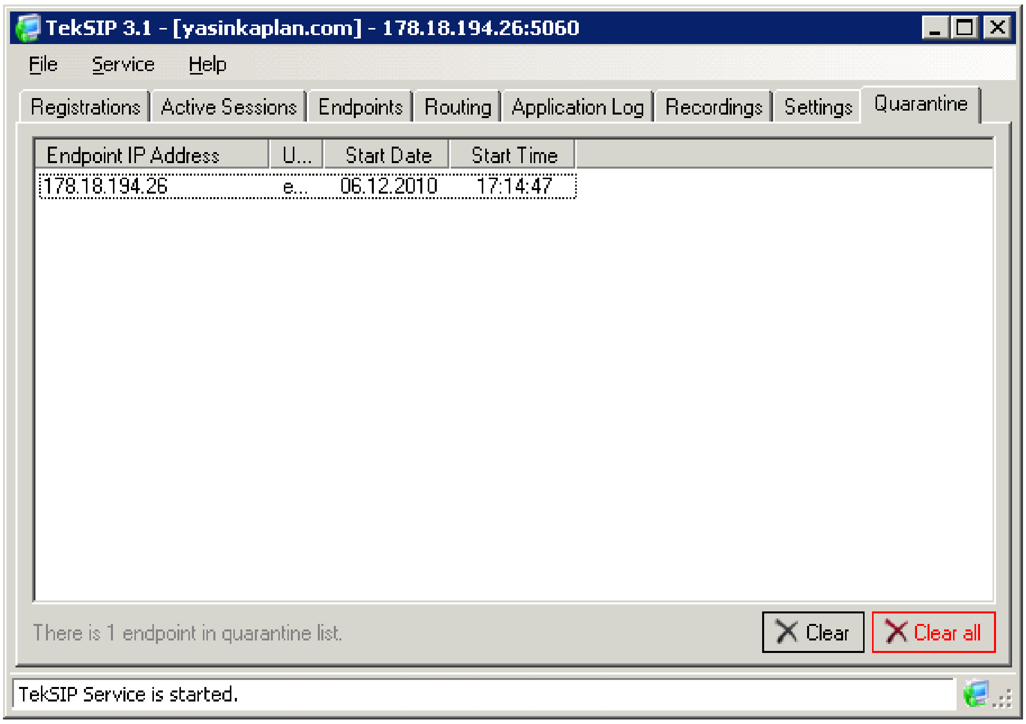

Figure - 11. Application Log Tab

You can remove black listed 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.

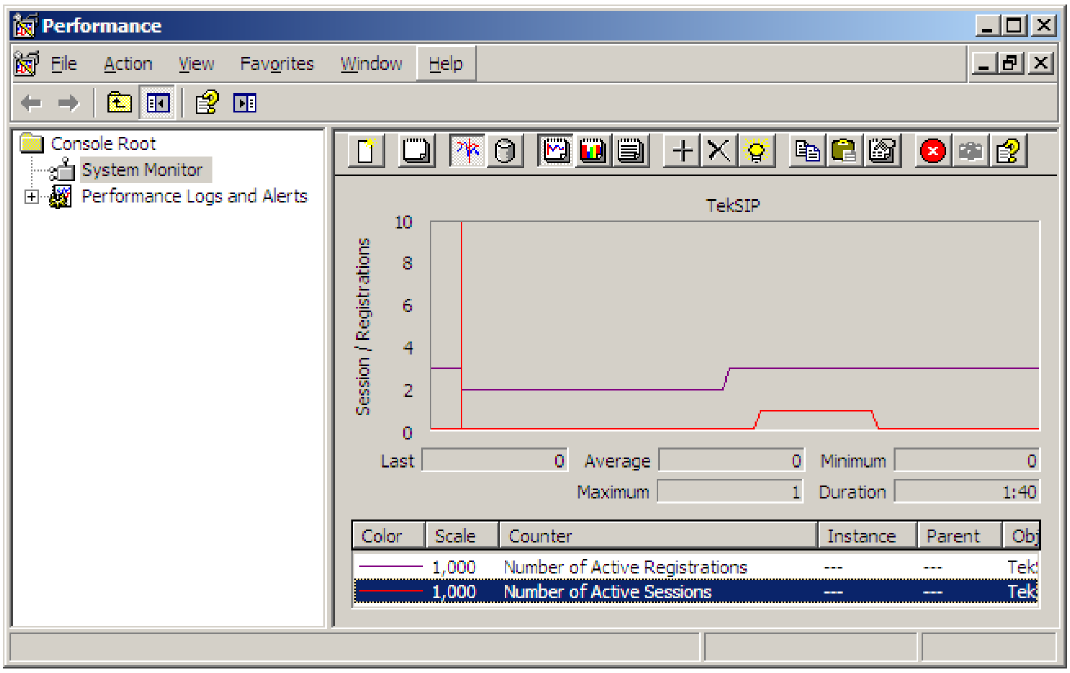

Figure - 12. TekSIP counters on Windows Performance Monitor

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

`TekSIP started. Listening on x.x.x.x.`

This message notifies that the TekSIP service is started.

Listened IP Address is being changed from x.x.x.x to y.y.y.y.

TekSIP has detected a change in system's IP configuration and automatically changed the listened IP address. You might change or remove the IP address configured for listening.

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 exits, 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 on : x.x.x.x

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 [x.x.x.x: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 the listened IP address as the default route.

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

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

Can not apply changes; enter minimum configuration

There is missing configuration data.

Endpoint 'abc' added, but could not saved.

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

You can not redirect an endpoint to itself.

You can not 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.