Configuring SIP Stacks

Viewing and Editing General Settings for SIP Stacks

Procedure

Step 1 Choose **Configure > SIP Stack > General Settings**.

The system displays the SIP Stack Settings page with the SIP General Settings tab highlighted. It lists the general SIP settings.

Step 2 Update the values as described in Table 1.

Table 1 SIP Stack General Settings

Parameter	Description
SIP Message	
SIP Header Compaction	Whether or not to enable SIP header compaction. When enabled, compact header forms are used for the following SIP headers: • Call-ID • Contact • Content-Encoding • Content-Length • Content-Type • From • Subject • To • Via When header compaction is disabled, complete SIP headers are used in all outgoing messages, regardless of the header format.
SIP Message Logging	Whether or not to enable the logging of all incoming and outgoing SIP messages. **Note** Turning on SIP logging has a significant performance impact on Cisco Unified SIP Proxy.
SIP Statistics	Whether to display statistics for active SIP queues.
Period Time	(Optional, only available if you check SIP Statistics) Determines how often to collect the peg-logging statistics.
Reset Time	(Optional, only available if you check SIP Statistics) Determines how often to reset the peg-logging statistics.

Table 1 SIP Stack General Settings (continued)

Parameter	Description
Max Forwards	Specifies the maximum number of times that a request can be forwarded to another server. Each time a request is received by a server, this value is decremented by one. (If the request does not have a Max Forwards header, one is added.) When the value reaches zero, the server responds with a 483 (too many hops) response and terminates the transaction. You can use the Max Forwards header field to detect forwarding loops within a network. The allowed values are 0 to 255. The default value is 70. **Note** We recommend that you set this command to a value greater than or equal to 10, and less than or equal to 100.
Overload	
Reject	Configures the server to send a 503 (Server Unavailable) response when the server is overloaded.
Retry After	(Optional, only available if you choose Reject) The number of seconds sent in the SIP Retry-After header field of the 503 (Server Unavailable) response, which indicates when the sender can attempt the transaction again. If not specified, the 503 (Server Unavailable) response does not contain a Retry-After header field. The minimum value allowed is 0. The default value is 0.
Redirect	Configures the server to send a 300 (Redirect) response when the server is overloaded.
IP Address	(Optional, only available if you choose Redirect) The redirect interface host name or IP address sent in the SIP Contact header field. Subsequent requests will be redirected to the server at this address.
Port	(Optional, only available if you choose Redirect) The port of the redirect host. The valid range is from 1024 to 65535. The default is 5060.
Transport Type	(Optional, only available if you choose Redirect) The transport protocol used by the redirect host. Can be UDP, TCP, or TLS.
DNS Settings	
DNS SRV Lookups	Configures SIP DNS SRV lookup commands.

Table 1 SIP Stack General Settings (continued)

Parameter	Description
DNS NAPTR Lookups	Enables the use of DNS NAPTR for domain hostname/IP address mapping.
TCP Settings	
Idle Connection Timeout	Configures the amount of idle time that is allowed to pass before sending a keep-alive probe.
Maximum Connections	Configures the maximum number of TCP/TLS connections. When the maximum number of TCP/TLS connections is reached, passive (incoming) connections are not accepted, and additional active (outgoing) connections can be made.
TLS Settings	
TLS Settings	Enables the use of SIP Transport Layer Security (TLS) connections with other SIP entities, providing secure communication over the Internet. Can be either enabled or disabled.
TLS Setup Connection Timeout	It is the time specified in Cisco Unified SIP Proxy by the user to establish connection with the trusted peer. The default value is 1 second. The range of values is 1 to 60 seconds.

Step 3 Click **Update**.

Related Topics

Back to the Configuring SIP Stacks menu page

Adding and Deleting an Alias FQDN

Procedure

Step 1 Choose **Configure > SIP Stack > Alias FQDNs**.

The system displays the Alias FQDNs page with the Alias FQDNs tab highlighted.

Step 2 To add an alias FQDN, do the following:

a. Enter a name.

b. Click **Add Alias**.

Step 3 To delete an alias FQDN, do the following:

a. Check the check box next to the name of the alias FQDN to delete.

b. Click **Remove**.

Related Topics

Back to the Configuring SIP Stacks menu page

Adding and Deleting a Trusted Peer

This procedure creates one or more SIP TLS trusted peers. The establishment of TLS connections fails unless the identity of the remote side matches the identifier of a configured trusted peer. If there are no trusted peers configured, the connection is accepted as long as the TLS handshake succeeds.

Procedure

Step 1 Choose **Configure > SIP Stack > TLS Trusted Peers**.

The system displays the TLS Trusted Peers page with the TLS Trusted Peers tab highlighted.

Step 2 To add a TLS trusted peer, do the following:

a. Enter a name.

b. Click **Add Trusted Peer**.

Step 3 To delete a TLS trusted peer, do the following:

a. Check the check box next to the name of the TLS trusted peer to delete.

b. Click **Remove**.

Related Topics

Back to the Configuring SIP Stacks menu page