SIP Provider

Use SIP technology for chan_sip provider trunks. SIP providers can create and maintain a global `sipfriends` realtime row when **Use Realtime Account** is enabled.

Realtime Account

☑ Use Realtime Account

Transport:	UDP
RTP Encryption (SRTP):	No
Host:	203.0.113.20
Port:	5060
Outbound Proxy:	sip-proxy.example.invalid
Username:	docs_sip_user
Password:	FictionalSecret-2026 [Generate]
From User:	+15551230000
From Domain:	sip.example.invalid
Send RPID:	PAI
Trust RPID:	PAI
Trust Outbound for CallerID Presentation:	Legacy
Qualify:	Yes
Qualify Frequency:	60 secs
Codecs:	
Session Timers:	Accept - Run session-timers only when requested by other UA
Session Expires:	1800
DTMF Mode:	RFC 2833/RFC 4733
Progress inband:	Yes
NAT:	force_rport,comedia
Call response timer (ms) - T1:	500
Call setup timer (ms) - B:	5000
RTP Keepalive:	5
Can Reinvite:	No

SIP realtime account settings with fictional chan_sip trunk values.

Common Realtime Fields

Field	Applies to	Purpose	Fictional example
Use Realtime Account	SIP, PJSIP, IAX2	Creates and maintains the Asterisk realtime peer, endpoint, AOR, auth, or IAX row for the provider.	`checked`
Transport	SIP, PJSIP	SIP signaling transport. For PJSIP this maps to transport objects such as `transport-udp`, `transport-tcp`, or `transport-tls`.	`UDP` or `TLS`
RTP Encryption (SRTP)	SIP, PJSIP	Enables SRTP media encryption when supported by the provider. PJSIP stores this as `media_encryption=sdes`.	`No` for standard UDP SIP, `Yes` for TLS/SRTP trunks
Host	SIP, PJSIP, IAX2	Remote provider address. Use an IP address when inbound realtime matching must identify the carrier by source IP.	`203.0.113.20`
Port	SIP, PJSIP, IAX2	Remote signaling port. Defaults are commonly 5060 for SIP/PJSIP and 4569 for IAX2.	`5060`
Outbound Proxy	SIP, PJSIP	Proxy URI or host used for outbound signaling when required by the carrier.	`sip-proxy.example.invalid`
Username	SIP, PJSIP, IAX2	Authentication username sent to the provider. PJSIP stores this in `ps_auths.username`, chan_sip as `defaultuser`.	`docs_sip_user`
Password	SIP, PJSIP, IAX2	Authentication secret for the provider. Use a unique carrier-supplied or generated secret.	`FictionalSecret-2026`
Qualify	SIP, PJSIP	Enables SIP OPTIONS reachability checks and controls timeout behavior.	`Yes`

Field	Applies to	Purpose	Fictional example
Qualify Frequency	SIP, PJSIP	Interval in seconds between provider reachability checks.	`60 secs`
Codecs	SIP, PJSIP, IAX2	Allowed audio codecs. MiRTA PBX stores `disallow=all` and the selected allow list.	`alaw`, `ulaw`, `g722`
Session Expires	SIP, PJSIP	Maximum SIP session refresh interval in seconds.	`1800`
DTMF Mode	SIP, PJSIP	DTMF signaling method. PJSIP maps RFC 2833 to `rfc4733`.	`RFC 2833/RFC 4733`
RTP Keepalive	SIP, PJSIP	Sends RTP keepalive packets to help keep NAT bindings and media paths active.	`5` seconds

SIP-Only Fields

Field	Applies to	Purpose	Fictional example
From User	SIP only	chan_sip `fromuser` value used in the SIP From header.	`+15551230000`
From Domain	SIP only	chan_sip `fromdomain` value used when the provider requires a specific domain in the From header.	`sip.example.invalid`
Send RPID	SIP only	Controls whether caller identity is sent using Remote-Party-ID, P-Asserted-Identity, or both.	`PAI`
Trust RPID	SIP only	Controls whether inbound Remote-Party-ID or P-Asserted-Identity data is trusted for caller identity.	`PAI`
Trust Outbound for CallerID Presentation	SIP only	Controls how prohibited caller presentation is handled in RPID/PAI headers.	`Legacy`

Field	Applies to	Purpose	Fictional example
Session Timers	SIP only	chan_sip session timer policy: accept remote requests, originate timers, or refuse timers.	`Accept`
Progress inband	SIP only	Controls whether Asterisk generates in-band progress audio before answer.	`Yes`
NAT	SIP only	chan_sip NAT behavior. `force_rport,comedia` is common for symmetric RTP and response routing.	`force_rport,comedia`
Call response timer (ms) - T1	SIP only	Milliseconds to wait for response to SIP messages.	`500`
Call setup timer (ms) - B	SIP only	Maximum milliseconds to wait for call setup before autocongestion when no provisional response arrives.	`5000`
Can Reinvite	SIP only	Allows Asterisk to attempt direct media re-invites. Use No when recording, NAT, or media control should keep Asterisk in the RTP path.	`No`
Allow Transfer	SIP only	chan_sip `allowtransfer`. When enabled, the peer may request SIP REFER transfers.	`No`
Insecure	SIP only	chan_sip authentication matching option. Port, Invite is common for IP-authenticated trunks.	`Port, Invite`

Fictional SIP Example

```
Name: Docs Telecom SIP Trunk
Peer Name: docs_telecom_sip
Technology: SIP
Host: 203.0.113.20
Port: 5060
Username: docs_sip_user
From User: +15551230000
From Domain: sip.example.invalid
NAT: force_rport,comedia
```

```
Insecure: Port, Invite
```

Revision #3
Created 2026-06-13 08:24:36 UTC by Admin
Updated 2026-06-13 08:24:51 UTC by Admin