

PJSIP Provider

Use PJSIP technology for res_pjsip provider trunks. MiRTA PBX maintains related `ps_endpoints`, `ps_aors`, `ps_auths`, and `ps_endpoint_id_ips` rows when realtime is enabled.

Realtime Account

☒ Use Realtime Account

Transport: TLS

RTP Encryption (SRTP): Yes

Host: 198.51.100.30

Port: 5061

Outbound Proxy: sip:edge.example.invalid\transport=tls

Username: docs_pjsip_user

Password: FictionalSecret-2026 Generate

From User:

From Domain:

Send RPID: PAI

Trust RPID: Yes

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: No

Call response timer (ms) - T1: 500

Call setup timer (ms) - B: 5000

RTP Keepalive: 10

Can Reinvite: No

PJSIP realtime account settings with fictional res_pjsip 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.	<code>checked</code>
Transport	SIP, PJSIP	SIP signaling transport. For PJSIP this maps to transport objects such as <code>transport-udp</code> , <code>transport-tcp</code> , or <code>transport-tls</code> .	<code>UDP</code> or <code>TLS</code>
RTP Encryption (SRTP)	SIP, PJSIP	Enables SRTP media encryption when supported by the provider. PJSIP stores this as <code>media_encryption=sdes</code> .	<code>No</code> for standard UDP SIP, <code>Yes</code> 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.	<code>203.0.113.20</code>
Port	SIP, PJSIP, IAX2	Remote signaling port. Defaults are commonly 5060 for SIP/PJSIP and 4569 for IAX2.	<code>5060</code>
Outbound Proxy	SIP, PJSIP	Proxy URI or host used for outbound signaling when required by the carrier.	<code>sip-proxy.example.invalid</code>
Username	SIP, PJSIP, IAX2	Authentication username sent to the provider. PJSIP stores this in <code>ps_auths.username</code> , <code>chan_sip</code> as <code>defaultuser</code> .	<code>docs_sip_user</code>
Password	SIP, PJSIP, IAX2	Authentication secret for the provider. Use a unique carrier-supplied or generated secret.	<code>FictionalSecret-2026</code>
Qualify	SIP, PJSIP	Enables SIP OPTIONS reachability checks and controls timeout behavior.	<code>Yes</code>

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

PJSIP-Specific Fields

Field	Applies to	Purpose	Fictional example
Transport	PJSIP only	Maps to the selected PJSIP transport object. Use TLS when the carrier requires encrypted signaling.	TLS
Host and Port	PJSIP only	Used to build the AOR contact and, when Host is an IP address, the endpoint identify match.	198.51.100.30:5061
Username and Password	PJSIP only	Stored in ps_auths. If username is empty, MiRTA PBX does not attach username/password auth.	docs_pjsip_user
Outbound Proxy	PJSIP only	PJSIP outbound proxy string for the endpoint.	sip:edge.example.invalid;transport=tls
Send RPID	PJSIP only	Maps to PJSIP send_rpid and send_pai.	PAI
Direct Media	PJSIP only	Allows PJSIP to attempt direct RTP. Disable when NAT, recording, transcoding, or media control requires Asterisk in the RTP path.	No

Field	Applies to	Purpose	Fictional example
Allow Transfer	PJSIP only	PJSIP <code>allow_transfer</code> . When enabled, the endpoint may request SIP REFER transfers.	No
RTP Encryption (SRTP)	PJSIP only	Stores <code>media_encryption=sdes</code> when enabled.	Yes
Qualify Frequency and Timeout	PJSIP only	Stored on the AOR as <code>qualify_frequency</code> and <code>qualify_timeout</code> .	60 secs
Support Path	PJSIP only	Enables Path support on the provider AOR for REGISTER requests and Route support for other requests. The value is stored as <code>ps_aors.support_path</code> ; System default leaves it unset. Enable Yes only for registrations received through a trusted SIP proxy.	No

Fictional PJSIP Example

Name: Docs Telecom PJSIP Trunk

Peer Name: docs_telecom_pjsip

Technology: PJSIP

Transport: TLS

RTP Encryption: Yes

Host: 198.51.100.30

Port: 5061

Outbound Proxy: sip:edge.example.invalid;transport=tls

Send RPID: PAI

Direct Media: No

Allow Transfer: No