

Administrator Guide

2026



SipLive SBC Manager

Administrator Guide

2026 — Version 12.14

© 2026 SipLive LLC. All rights reserved.

Contents

1	Introduction	6
1.1	What Is SipLive SBC Manager?	6
1.2	Key Capabilities	6
1.3	Licensing	7
2	System Requirements	7
2.1	Server (Per SBC Node)	7
2.2	Browser Support	7
3	Installation	7
3.1	ISO Method (Recommended)	7
3.2	Installation Roles	8
3.3	First Login	8
4	Dashboard	8
4.1	Dashboard Sections	8
5	Network Configuration	9
5.1	Application Settings	9
5.2	OS Network Interfaces	9
6	User Management	10
6.1	Roles	10
6.2	Managing Users	10
6.3	Resetting a Password	10
7	Activation & Licensing	11
7.1	Activating a Device	11
7.2	License States	11
7.3	Daily Check-In	11
7.4	Viewing License Details	11
8	SIP Trunk Configuration	12
8.1	Creating a Trunk	12
8.2	Editing and Disabling Trunks	12
8.3	Carrier Templates	12

9	DID Management	13
9.1	Adding DIDs	13
9.2	Editing DID Routing	13
9.3	Bulk Routing Updates	13
10	Routing Policies	13
10.1	Policy Types	13
10.2	Priority	14
10.3	Failover	14
10.4	Example: NANPA Outbound with Backup	14
10.5	Route Simulation	14
11	Header Manipulation (HMR)	15
11.1	Creating a Rule Set	15
11.2	Assigning Rule Sets	15
11.3	Common HMR Examples	15
11.3.1	Example 1: Normalize Outbound P-Asserted-Identity	15
11.3.2	Example 2: Strip Privacy Header on Outbound	16
11.3.3	Example 3: Add a Custom SIP Header	16
11.3.4	Example 4: Rewrite From Header Domain (Inbound)	16
11.3.5	Example 5: Multi-Rule Set — Teams Direct Routing Normalization	17
12	Fraud Controls	17
12.1	Rule Types	17
13	Config Apply Workflow	18
13.1	Overview	18
13.2	Applying Changes	18
13.3	Scheduling an Apply	18
13.4	Config Versions	18
13.5	Rollback	18
13.6	Approval Workflow	18
14	High Availability	19
14.1	Architecture	19
14.2	Managing HA Nodes	19
14.3	Maintenance Mode	19

14.4 Failover Behavior	19
15 CDR Reporting	20
15.1 Overview	20
15.2 Viewing Call Records	20
15.3 Exporting	20
16 Diagnostics	20
16.1 Packet Capture	20
16.2 Diagnostic Bundle	21
17 Backups	21
17.1 Scheduled Backups	21
17.2 Creating a Manual Backup	21
17.3 Downloading a Backup	21
17.4 Restoring from a Backup	21
17.5 Remote Backup (S3)	22
18 Security	22
18.1 Firewall	22
18.2 TLS / HTTPS	22
18.3 API Tokens	22
18.4 Audit Log	22
19 API Integration	23
19.1 Overview	23
19.2 REST API	23
19.2.1 Key Resource Areas	23
19.3 SOAP API	23
20 Troubleshooting	24
20.1 Dashboard Shows Red or Amber Alerts	24
20.2 Activation Fails	24
20.3 Apply Fails	24
20.4 Cannot Log In to GUI	24
20.5 Packet Capture Shows No Traffic	25
21 Appendix: Permissions Reference	25

22 Support

26

SipLive SBC
CONFIDENTIAL

1 Introduction

1.1 What Is SipLive SBC Manager?

SipLive SBC Manager is a web-based management platform for Asterisk 20+ PJSIP Session Border Controllers. It provides a unified graphical interface for configuring SIP trunks, DID routing, outbound call policies, header manipulation, fraud controls, diagnostics, high availability, backup and recovery — all on a hardened Debian 12 appliance.

Configurations are staged in a database, previewed as a diff, and applied to Asterisk via a controlled reload workflow. Every change is version-controlled with full rollback capability directly from the GUI.

1.2 Key Capabilities

- **Trunk management** — IP or credential-based SIP trunks with per-trunk codec, capacity, and security settings
- **DID routing** — Inbound number inventory with per-DID trunk assignment and failover
- **Routing policies** — Destination and source prefix routing with priority-ordered failover
- **Header manipulation (HMR)** — Reusable rule sets for normalizing SIP headers on inbound and outbound calls
- **Fraud controls** — Destination-based allow/block rules applied before Asterisk config is generated
- **Config versioning** — Staged apply with diff preview, approval workflows, scheduling, and one-click rollback
- **High availability** — Active/active dual-node model with shared MariaDB and per-node apply agent
- **CDR reporting** — Call history, duration, and disposition reporting with search and export
- **Diagnostics** — Bounded packet capture, PCAP download, and protocol analysis from the browser
- **Backups** — Scheduled and on-demand backups with optional S3 remote sync and one-click restore
- **REST & SOAP API** — Full programmatic surface for external provisioning systems
- **Activation & licensing** — Device registration with SipLive licensing server and call-capacity enforcement

1.3 Licensing

SipLive SBC Manager is dual-licensed:

- **AGPL-3.0** — Free for open source and personal use
- **Commercial License** — Required for proprietary products, managed services, or OEM deployments

Contact licensing@siplive.net for commercial licensing inquiries.

2 System Requirements

2.1 Server (Per SBC Node)

Component	Minimum	Recommended
OS	Debian 12 (Bookworm)	Debian 12 (Bookworm)
CPU	2 vCPU	4+ vCPU
RAM	4 GB	8 GB
Disk	40 GB	80 GB SSD
Network	1 NIC	2 NIC (management + SIP)

2.2 Browser Support

Any modern browser with JavaScript enabled — Chrome, Firefox, Edge, and Safari are all supported.

3 Installation

3.1 ISO Method (Recommended)

The SipLive SBC Manager ISO installs a complete Debian 12 base system with all required packages bundled offline. No internet connection is needed after the initial boot.

1. Download `SIPLive.SBC.*.iso` from SipLive
2. Boot the target server from the ISO (physical media or VM)
3. At the boot menu select **Automated SBC base install**

4. The installer runs unattended — the Debian base OS installs and the machine reboots automatically
5. Log in as **root** with the password provided by SipLive
6. A setup wizard launches automatically on first login to guide you through the remaining configuration

3.2 Installation Roles

During setup you will be prompted to choose a deployment role:

Role	Description
Standalone	All-in-one: web GUI, Asterisk, and database on a single server. Ideal for single-site deployments.
SBC Node	Web GUI and Asterisk only; connects to a remote database node. Used in HA deployments.
Database Node	Database only; serves one or more SBC nodes in an HA cluster.

3.3 First Login

After installation completes, open a browser and navigate to <https://<server-ip>>. Log in with the default credentials:

Account	Default
Email	admin@example.com
Password	ChangeMeNow!

Change this password immediately via **Security** → **Users**.

4 Dashboard

The dashboard is the landing page after login. It provides a live overview of the SBC environment.

4.1 Dashboard Sections

- **Node Health** — Heartbeat status and last-seen time for each registered SBC node
- **Apply Status** — Whether each node's Asterisk config is current or has pending changes

- **Call Capacity** — Licensed maximum vs. current concurrent call count
- **Backup Health** — Age and status of the most recent backup
- **Recent Alerts** — Operations alerts (stale nodes, failed applies, backup warnings)
- **Recent Apply History** — Last several apply and rollback operations with outcome

A green indicator on all panels means the system is healthy. Any warning or error state is highlighted in amber or red with a brief description.

5 Network Configuration

5.1 Application Settings

Go to **Settings** → **Network** to configure this node's identity within SBC Manager.

Field	Description
Node Name	Display name shown in the GUI and dashboard
Node ID	Lowercase identifier used in configuration (letters, numbers, hyphens, underscores only)
Management IP	IP address used for web GUI access and cluster communication
SIP IP	Public IP used for SIP and RTP traffic
Web URL	Full URL of the web GUI (e.g., <code>https://sbc.example.com</code>)

Click **Save application settings** to apply. This updates the application configuration only — Asterisk is not affected.

5.2 OS Network Interfaces

The **Server Network Interfaces** section lists every detected network adapter and allows you to configure each one directly from the GUI.

For each interface you can set:

- IP address
- Prefix length (subnet mask)
- Gateway (set on exactly one interface to define the default route)

- DNS servers

Click **Apply & restart** <interface> to write the configuration and restart that adapter immediately.

Note: Applying changes to the interface you are currently connected through will restart it and redirect your browser to the new IP address. Verify the gateway is correct before applying — an incorrect gateway can cause loss of access.

6 User Management

6.1 Roles

Access is controlled by roles with granular permission sets. Two roles are created at installation:

Role	Access Level
admin	Full access to all features
read-only	View-only access across all sections

Custom roles with any combination of permissions can be created under **Security** → **Roles**.

6.2 Managing Users

Go to **Security** → **Users** to view, add, edit, or disable user accounts.

To add a new user click **New User** and provide:

- Display name
- Email address (used as the login username)
- Role assignment
- Initial password

Users can be enabled or disabled without deleting them. Disabled users cannot log in but their history and settings are preserved.

6.3 Resetting a Password

Go to **Security** → **Users**, select the user, and click **Reset Password**. A new password can be set directly from the edit form.

7 Activation & Licensing

7.1 Activating a Device

Go to **Security** → **Activation** and click **Activate Now**. The device contacts the SipLive licensing server, registers its identity, and receives a license GUID. Activation is required to unlock full call capacity.

7.2 License States

State	Behavior
Unactivated	Limited to trial maximum (default: 5 concurrent calls). A red banner is shown on all pages.
Active	Full licensed call capacity. No banner.
Grace	Check-in has been failing. A warning banner is shown. Calls are not yet limited.
Suspended	Contact SipLive support at support@siplive.net
Revoked	Contact SipLive support at support@siplive.net

7.3 Daily Check-In

Once activated, the device automatically checks in with the SipLive licensing server once daily. If check-in fails, the device enters **Grace** state and a warning banner appears in the GUI.

To trigger an immediate check-in go to **Security** → **Activation** and click **Check In Now**.

7.4 Viewing License Details

Security → **Activation** displays:

- Current license status
 - License GUID
 - Registered MAC address and hostname
 - Activation date and time
 - Last successful check-in
 - Licensed concurrent call limit
-

8 SIP Trunk Configuration

8.1 Creating a Trunk

Go to **Trunks** → **New Trunk**. Fill in the trunk details:

Field	Description
Name	Internal label for this trunk
Direction	Inbound, Outbound, or Bidirectional
Authentication	IP-based or Username/Password
Host	Remote SIP peer hostname or IP address
Allowed IPs	Source IP addresses permitted for inbound calls on this trunk
Codecs	Ordered list of audio codecs (drag to reorder priority)
Max Channels	Maximum simultaneous calls on this trunk (0 = unlimited)

Click **Save** to stage the trunk. Go to **Apply** to push the change to Asterisk.

8.2 Editing and Disabling Trunks

From the **Trunks** list, click any trunk to edit it. To temporarily take a trunk out of service without deleting it, toggle the **Enabled** switch and apply.

8.3 Carrier Templates

Trunks → **Carrier Templates** provides pre-built configurations for the most common carriers and use cases:

- Microsoft Teams Direct Routing
- Bandwidth
- SIPLive
- Telnyx
- Twilio Elastic SIP Trunking
- Skyetel
- Flowroute
- Generic PBX
- Generic TLS carrier

Select a template to see recommended settings, firewall requirements, codec guidance, and security notes. Templates can be applied when creating a new trunk via the **New Endpoint Wizard**, or applied to an existing trunk from the template detail page.

9 DID Management

9.1 Adding DIDs

Go to **DIDs** → **New DID** to add a single number, or **DIDs** → **Import** to bulk-import from a CSV file.

Each DID requires:

- Phone number (E.164 format recommended, e.g., +15125550100)
- Primary inbound trunk
- Optional failover trunk

9.2 Editing DID Routing

Click any DID from the **DIDs** list to update its trunk assignment or failover trunk. Changes are staged and require an Apply to take effect in Asterisk.

9.3 Bulk Routing Updates

Use **DIDs** → **Bulk Update** to reassign routing across many numbers at once — useful when migrating a block of numbers to a new trunk.

10 Routing Policies

Routing policies control how calls are matched and where they are sent. Go to **Routes** to manage them.

10.1 Policy Types

Type	Description
Destination	Matches the dialed number by prefix and routes to a specified trunk
Source	Matches the calling number by prefix

10.2 Priority

Multiple policies can match the same call. The policy with the **lowest priority number** wins. Use gaps between priority values (e.g., 100, 200, 300) to leave room for future insertions without renumbering.

10.3 Failover

If the primary trunk on the winning policy is unavailable, the next matching policy is tried automatically — providing built-in call failover without additional configuration.

10.4 Example: NANPA Outbound with Backup

Priority	Policy Name	Prefix	Trunk
10	Emergency — 911	911	carrier-primary
10	Emergency — 988	988	carrier-primary
100	Outbound NANPA — Primary	1	carrier-primary
200	Outbound NANPA — Backup	1	carrier-backup

In this example, 911 and 988 always go to the primary carrier at highest priority. All other NANPA calls try the primary carrier first, then automatically fall back to the backup carrier.

10.5 Route Simulation

Go to **Routes** → **Simulate** to test routing decisions without originating a real call. Enter a source number and destination number to see which policy wins, which trunk is selected, and which transforms are applied.

11 Header Manipulation (HMR)

Header manipulation rule sets (HMR) rewrite, remove, or add SIP headers on calls passing through the SBC. Go to **HMR** to manage rule sets.

11.1 Creating a Rule Set

1. Go to **HMR** → **New Rule Set**
2. Set the name and direction (Inbound or Outbound)
3. Add rules — each rule specifies:
 - **Header** (e.g., P-Asserted-Identity)
 - **Action** (rewrite, remove, or add)
 - **Match pattern** (regular expression)
 - **Replacement value** (supports regex capture groups, e.g., \$1)
 - **Priority** (execution order within the set; lower runs first)

11.2 Assigning Rule Sets

A rule set can be assigned to one or more trunks or routes from the rule set's detail page. The same set can be reused across multiple assignments — edit once, updated everywhere.

11.3 Common HMR Examples

The following examples illustrate typical use cases. Each would be added as a rule within a rule set.

11.3.1 Example 1: Normalize Outbound P-Asserted-Identity

Rewrites the caller identity header to present a consistent domain to the carrier, regardless of how the PBX sends it.

Field	Value
Header	P-Asserted-Identity
Action	Rewrite
Match pattern	<code>^sip:(.*)@.*</code>
Replacement	<code>sip:\$1@siplive.com</code>

Before: P-Asserted-Identity: sip:15125550100@192.168.1.10

After: P-Asserted-Identity: sip:15125550100@siplive.com

11.3.2 Example 2: Strip Privacy Header on Outbound

Removes the **Privacy** header before sending calls to a carrier that does not support it.

Field	Value
Header	Privacy
Action	Remove
Match pattern	.*
Replacement	<i>(leave blank)</i>

11.3.3 Example 3: Add a Custom SIP Header

Inserts a carrier-required account code header on all outbound calls.

Field	Value
Header	X-Carrier-Account
Action	Add
Match pattern	<i>(leave blank — add unconditionally)</i>
Replacement	ACCT-10294

11.3.4 Example 4: Rewrite From Header Domain (Inbound)

Normalizes inbound calls arriving with a carrier-specific domain so internal systems see a consistent format.

Field	Value
Header	From
Action	Rewrite
Match pattern	^"?(.*?)"?\s*<sip:(.*)@carrier\.example\.com>
Replacement	"\$1" <sip:\$2@sbc.example.com>

Before: From: "John Smith" <sip:15125550199@carrier.example.com>

After: From: "John Smith" <sip:15125550199@sbc.example.com>

11.3.5 Example 5: Multi-Rule Set — Teams Direct Routing Normalization

This example shows a complete rule set with multiple rules applied in priority order to prepare inbound calls from Microsoft Teams for delivery to a PBX.

Priority	Header	Action	Match Pattern	Replacement
10	P-Asserted-Identity	Rewrite	<code>^sip:(.*)@.*</code>	<code>sip:\$1@pbx.example.com</code>
20	Contact	Rewrite	<code>^<sip:(.*)@.*></code>	<code><sip:\$1@sbc.example.com></code>
30	X-MS-Teams-Team-ID	Remove	<code>.*</code>	
40	X-MS-SBC	Remove	<code>.*</code>	

Rules execute in ascending priority order. The **P-Asserted-Identity** rewrite runs first, then **Contact**, then the two Microsoft-specific headers are stripped before the call reaches the PBX.

12 Fraud Controls

Destination fraud rules allow or block outbound calls to specific number patterns before Asterisk configuration is generated. Go to **Fraud** to manage rules.

12.1 Rule Types

Type	Description
Block	Reject calls to the matching destination prefix
Allow	Explicitly permit calls (overrides a broader block rule)

Rules are evaluated longest-prefix first. A more specific allow rule will always override a broader block. Changes to fraud rules take effect after the next Apply.

13 Config Apply Workflow

13.1 Overview

Changes to trunks, routes, DIDs, HMR rule sets, or fraud rules are staged in the database and do not affect live Asterisk behavior until you apply them. This staged workflow allows you to batch changes, preview them, and apply at a time of your choosing.

13.2 Applying Changes

1. After making changes, go to **Apply**
2. Review the diff — every added, modified, and removed config element is shown
3. Click **Apply Now** to push the changes immediately, or use **Schedule Apply** for a maintenance window
4. The apply agent writes generated Asterisk config files and reloads Asterisk
5. The result (success or failure) is recorded in the apply history

13.3 Scheduling an Apply

Click **Schedule Apply** and choose a future date and time. The apply will execute automatically at that time. Scheduled applies are visible in the apply queue and can be cancelled before they run.

13.4 Config Versions

Every apply creates a numbered config version. Go to **Apply → History** to browse past versions, view the full generated config for any version, and compare versions.

13.5 Rollback

If a change causes issues, go to **Apply → History**, find the last known-good version, and click **Rollback**. The prior config is queued for immediate apply and Asterisk is reloaded to that state.

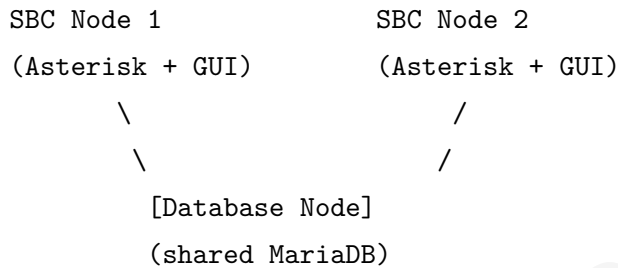
13.6 Approval Workflow

If your role configuration requires approval before applying, a pending apply will appear in the queue for an authorized user to review and approve or reject before it executes.

14 High Availability

14.1 Architecture

SipLive SBC Manager supports an active/active dual-node HA model. Both SBC nodes share a common database and operate independently — each manages its own Asterisk instance and apply agent.



The dashboard shows the health, heartbeat, and apply state of both nodes simultaneously.

14.2 Managing HA Nodes

Go to **Settings** → **HA / Replication** to view and manage cluster nodes. From this page you can:

- Register a new node in the cluster
- View each node's connection status and last heartbeat
- Put a node into **maintenance mode** before upgrades or reboots
- Remove a decommissioned node

14.3 Maintenance Mode

When a node is in maintenance mode its apply agent is paused and the dashboard shows it as intentionally offline. Other nodes continue serving calls normally. Clear maintenance mode from **Settings** → **HA / Replication** when the node is ready to return to service.

14.4 Failover Behavior

If one SBC node becomes unreachable, the other continues serving calls using its last-applied Asterisk configuration. No manual intervention is required — PJSIP endpoints on both nodes are symmetric.

15 CDR Reporting

15.1 Overview

SipLive SBC Manager imports Asterisk call detail records automatically every five minutes and makes them available in the reporting interface.

15.2 Viewing Call Records

Go to **Reports** → **CDR** to view the call history. Records can be filtered by:

- Date and time range
- Caller ID
- Destination number
- Trunk (source or destination)
- Disposition (Answered, No Answer, Busy)

15.3 Exporting

Use the **Export CSV** button on the CDR page to download the current filtered result set as a spreadsheet-compatible CSV file.

16 Diagnostics

16.1 Packet Capture

Go to **Diagnostics** → **Packet Capture** to start a live capture from the browser.

Field	Description
Interface	The network adapter to capture on
Filter	Traffic filter expression (e.g., <code>port 5060</code> for SIP only)
Duration	Maximum capture length in seconds

Once the capture completes, a protocol summary is displayed inline and the `.pcap` file can be downloaded for analysis in Wireshark or any compatible tool.

16.2 Diagnostic Bundle

Go to **Diagnostics** → **Download Bundle** to generate a sanitized bundle of captures, logs, and a config summary. This bundle can be sent to SipLive support to assist with troubleshooting.

17 Backups

17.1 Scheduled Backups

SipLive SBC Manager creates automatic backups on a configurable schedule. Go to **Settings** → **Backup Schedule** to set:

- Frequency (daily, weekly, or hourly)
- Time of day
- How many backups to retain locally

Each backup contains a full database snapshot, the generated Asterisk configuration, and the application environment settings.

17.2 Creating a Manual Backup

Go to **Backups** and click **Create backup now**. The backup is created immediately and appears in the local inventory below.

17.3 Downloading a Backup

From the **Backups** page, click **Download** next to any backup in the local inventory to save it to your computer.

17.4 Restoring from a Backup

On the **Backups** page, use the **Upload & Restore** form to upload a backup ZIP from your computer. The restore process replaces the current database and Asterisk configuration with the backup contents. Application credentials are preserved automatically so the system keeps working after restore.

Important: Restore replaces all current data. Verify the backup is from a compatible version before restoring.

17.5 Remote Backup (S3)

Go to **Settings** → **Remote Storage** to configure an S3-compatible bucket. Once configured, every backup is automatically pushed to the remote bucket after it is created locally. Remote backups appear in a separate section of the **Backups** page and can be restored directly from there.

18 Security

18.1 Firewall

The SBC Manager firewall controls which IP addresses can reach the management interface, SIP ports, and RTP range. Go to **Settings** → **Firewall** to view and manage firewall rules.

Add management IP addresses to the allowlist here rather than opening broad network ranges. SIP and RTP ports are controlled separately from the management web interface rules.

18.2 TLS / HTTPS

Go to **Settings** → **TLS** to configure HTTPS:

- **Let's Encrypt** — Automated certificate issuance and renewal using your domain name
- **Manual** — Upload your own certificate and private key

Once TLS is configured, HTTP connections are automatically redirected to HTTPS.

18.3 API Tokens

Go to **Security** → **API Tokens** to manage tokens for external system integration. Each token is scoped to one or more resource areas (trunks, routes, DIDs, operations, etc.) so that integrations only have access to what they need.

Tokens are shown only once at creation time — copy and store them securely.

18.4 Audit Log

Every configuration change, apply, login, and user management action is recorded automatically. Go to **Security** → **Audit Log** to search and review activity by user, action type, or date range.

19 API Integration

19.1 Overview

SipLive SBC Manager exposes a full REST API and a SOAP API for integration with external provisioning systems, carrier portals, and automation tools.

API tokens are managed under **Security** → **API Tokens** in the GUI.

19.2 REST API

All REST endpoints are under `/api/v1/`. Requests are authenticated with a Bearer token:

Authorization: Bearer <token>

19.2.1 Key Resource Areas

Area	Base Path	Description
Trunks	<code>/api/v1/trunks</code>	Create, read, update SIP trunks
DIDs	<code>/api/v1/dids</code>	Manage DID inventory and routing
Routes	<code>/api/v1/routes</code>	Manage routing policies
HMR	<code>/api/v1/hmr</code>	Manage header manipulation rule sets
Fraud	<code>/api/v1/fraud-rules</code>	Manage destination fraud rules
Operations	<code>/api/v1/ops/</code>	Stage versions, queue apply/rollback, view history
Backups	<code>/api/v1/backups</code>	Trigger and download backups
Endpoints	<code>/api/v1/endpoints/provision</code>	Full NAP provisioning in one call
Route Simulation	<code>/api/v1/route-simulate/batch</code>	Batch routing decision test (up to 200 calls)

Full endpoint documentation is available in the API reference guide.

19.3 SOAP API

A SOAP interface is available at `/soap/v1` for legacy provisioning systems. It provides equivalent coverage to the REST API. The WSDL is available at `/soap/v1?wsdl`.

20 Troubleshooting

20.1 Dashboard Shows Red or Amber Alerts

Alert	Cause	Resolution
Node heartbeat stale	SBC node agent is not running or network is down	Check the node's network connectivity and service status from Settings → HA / Replication
Apply needed	Staged changes have not been applied	Go to Apply and apply or discard pending changes
Backup overdue	No backup has been created within the retention window	Go to Backups and create a manual backup, then verify the backup schedule under Settings → Backup Schedule
Device not activated	Activation has not been completed	Go to Security → Activation and click Activate Now

20.2 Activation Fails

- Verify the server has outbound internet access to <https://sbc.siplive.net>
- Check that the server's clock is accurate (TLS validation requires correct time)
- Contact support@siplive.net if the issue persists

20.3 Apply Fails

Go to **Apply** → **History** and click the failed apply to view the detailed error message. Common causes:

- Asterisk is not running on the target node
- A trunk or route references a deleted dependency
- Generated config has a syntax error (shown in the apply output)

If the error is unclear, use **Diagnostics** → **Download Bundle** and send it to SipLive support.

20.4 Cannot Log In to GUI

- Verify the correct email and password are being used
- Check that the user account is enabled under **Security** → **Users**
- Use the password reset option on the login page

20.5 Packet Capture Shows No Traffic

- Verify the correct interface is selected — SIP traffic is typically on the SIP IP interface, not the management interface
- Confirm the filter expression is correct (e.g., `udp port 5060` for standard SIP)
- Verify SIP traffic is actually arriving at the server using the firewall rules under **Settings** → **Firewall**

21 Appendix: Permissions Reference

The following permission tokens can be assigned to custom roles:

Permission	Access Granted
<code>dashboard.view</code>	View the main dashboard
<code>trunks.view</code>	View SIP trunk list and details
<code>trunks.manage</code>	Create, edit, and delete trunks
<code>dids.view</code>	View DID inventory
<code>dids.manage</code>	Create, edit, and delete DIDs
<code>routes.view</code>	View routing policies
<code>routes.manage</code>	Create, edit, and delete routing policies
<code>hmr.view</code>	View HMR rule sets
<code>hmr.manage</code>	Create, edit, and delete HMR rule sets
<code>fraud.view</code>	View fraud control rules
<code>fraud.manage</code>	Create, edit, and delete fraud rules
<code>apply.preview</code>	View config diffs and apply previews
<code>apply.run</code>	Execute applies, rollbacks, and scheduling
<code>cdr.view</code>	View and export CDR records
<code>diagnostics.view</code>	View packet captures and bundles
<code>diagnostics.manage</code>	Start packet captures
<code>backups.view</code>	View and download backups
<code>backups.manage</code>	Create and restore backups
<code>settings.manage</code>	Access all Settings pages
<code>users.manage</code>	Create and manage user accounts
<code>roles.manage</code>	Create and manage roles
<code>audit.view</code>	View the audit log

Permission	Access Granted
<code>api.manage</code>	Create and revoke API tokens

22 Support

General Support	support@siplive.net
Commercial Licensing	licensing@siplive.net
Website	https://siplive.net

© 2026 SipLive LLC. All rights reserved.

SipLive SBC Manager is dual-licensed under AGPL-3.0 and the SipLive Commercial License.