

Initial Configuration

Start here for installation, first access, tenant creation, provider setup, routing profile setup, tenant completion, mobile use, and shared interface controls.

- [Presentation](#)
- [Installation](#)
- [Initial Configuration](#)
 - [Log In and Select a Tenant](#)
 - [Create a Tenant](#)
 - [Configure a Provider](#)
 - [Configure a Routing Profile](#)
 - [Complete the Tenant configuration](#)
- [Use on mobile device](#)
- [Use multiselect](#)

Presentation

MiRTA PBX is a cloud PBX platform built on Asterisk for VoIP providers, hosted PBX operators, call centers, and enterprises that need centralized voice services, tenant separation, and scalable operations.

This manual is the operational entry point for administrators, tenant managers, support teams, and integrators working with MiRTA PBX in production environments.

What MiRTA PBX Provides

- **Cloud PBX delivery:** run hosted PBX services from a centralized platform designed for provider and enterprise voice operations.
- **Multitenant management:** keep customer environments logically separated while sharing a common service platform.
- **Realtime configuration:** store configuration and tenant state in the database so Asterisk can retrieve data dynamically where supported.
- **HA-ready architecture:** operate Asterisk nodes as a pool and scale capacity by adding nodes around shared database-backed configuration.
- **Call flow and routing tools:** manage DIDs, extensions, routing profiles, IVRs, conditions, feature codes, queues, and custom destinations.
- **Provisioning and endpoint operations:** automate phone configuration with generic templates and provisioning workflows.
- **Contact center features:** build queue strategies, callbacks, reporting, monitoring, switchboard workflows, and agent-facing operations.
- **Media, AI, and collaboration integrations:** manage recordings and prompts, use TTS/STT services, support WebRTC softphone workflows, and integrate with modern voice experiences where configured.
- **Security and abuse prevention:** use operational controls such as call limits, fraud mitigation, GeoIP filtering, User-Agent validation, and Fail2ban integration patterns.

Who This Manual Is For

- **Platform administrators** who install, upgrade, monitor, secure, and scale MiRTA PBX.
- **Tenant administrators** who configure extensions, DIDs, call routing, IVRs, queues, voicemail, and user-facing features.

- **Support engineers** who troubleshoot registrations, call failures, media issues, queues, provisioning, and tenant configuration.
- **Integrators** who connect MiRTA PBX to billing, CRM, storage, monitoring, APIs, TTS/STT, Microsoft Teams, WebRTC, or AI-assisted workflows.

Core Concepts

Concept	Meaning
Tenant	A logically separated customer or organization environment with its own PBX configuration and operational behavior.
Asterisk node	A call-processing server that participates in a single-node or clustered MiRTA PBX deployment.
Realtime configuration	A database-backed model where configuration can be read dynamically by Asterisk instead of relying only on static flat files and reloads.
Routing profile	A set of outbound routing rules, restrictions, provider choices, and number transformations.
Destination	A target in the call flow, such as an extension, IVR, queue, voicemail, hunt list, custom destination, or external route.
Provisioning template	A reusable template used to generate phone configuration files for supported endpoint workflows.
Switchboard	A real-time operator panel for monitoring calls and queues and performing assisted call actions where enabled.

Manual Roadmap

The manual should grow around the way operators actually use MiRTA PBX:

1. **Architecture and deployment:** platform topology, web layer, database, Asterisk nodes, clustering, DNS/SIP/RTP design, and HA considerations.
2. **Administration:** licensing, nodes, system settings, users, permissions, defaults, monitoring, backups, upgrades, and maintenance.
3. **Tenant setup:** tenants, extensions, DIDs, voicemail, media files, phone books, provisioning, feature codes, and tenant defaults.
4. **Call flow design:** destinations, conditions, calendars, IVRs, hunt lists, queues, routing profiles, caller ID manipulation, and custom logic.
5. **Contact center operations:** queues, agent behavior, callbacks, switchboard, wallboards, recordings, reports, and statistics.

6. **Security and fraud control:** registration hardening, call limits, GeoIP, Fail2ban, TLS, network exposure, and abuse response.
7. **Integrations:** APIs, database integrations, billing, CRM, storage backends, TTS/STT, WebRTC, Microsoft Teams, SMS, fax, and AI workflows.
8. **Troubleshooting:** SIP registration, one-way audio, failed calls, logs, Asterisk diagnostics, provisioning failures, queues, fax, voicemail, and performance.

First Steps for New Administrators

1. Understand the deployment topology: single node or clustered, database location, SIP/RTP routing, and tenant boundaries.
2. Review global settings before creating tenants, especially security, language, media, recording, provisioning, and WebRTC-related defaults.
3. Create or verify the tenant, then configure extensions, DIDs, outbound routing, voicemail, media files, and required feature codes.
4. Test inbound calls, outbound calls, internal calls, voicemail, failover behavior, and emergency or restricted dialing paths before production use.
5. Enable monitoring, backups, log review, and fraud controls before exposing services broadly on the public Internet.

Source Material

- [MiRTA PBX home page](#)
- [MiRTA PBX architecture overview](#)
- [MiRTA PBX feature overview](#)
- [MiRTA PBX licensing overview](#)
- Legacy public documentation is being migrated into these BookStack manuals.

Created: 2026-06-02. Source review: public website plus local codebase location

`/var/www/html/mirtapbx`.

Installation

This page reorganizes the MiRTA PBX installation flow into an operational checklist. Use it as a starting point, then adapt paths, hostnames, IP addresses, package versions, and credentials to the server being installed.

Scope and Prerequisites

The legacy installation notes describe an automatic installer that has been proven on CentOS Stream 9 64-bit. Even with the installer, several manual configuration steps are still required after the base packages are installed.

Requirement	What to Prepare
Server access	Root shell access to a fresh server, with network access to download packages and MiRTA PBX updates.
Hostname	A meaningful hostname for the PBX node. Do not leave the system hostname set to a generic localhost value.
License details	The MiRTA PBX name and key values supplied for the installation.
Network plan	The node private IP address, public IP address when NAT is used, local network range, and any additional cluster node IP addresses.
Database plan	A local database for a single node, or a shared/replicated database design for a cluster.

Prepare the Server

1. Copy the MiRTA PBX installer script to `/usr/local/src` on the new server.
2. Install any missing download tools needed to retrieve packages or the installer.
3. Confirm the server hostname and change it before continuing if it is still generic.
4. Move to `/usr/local/src` and run the installer in kernel mode.
5. Reboot the server so the latest kernel is active.
6. Return to `/usr/local/src` and run the installer normally.

```
cd /usr/local/src
./installMirtaPBX.sh Kernel
```

```
reboot
cd /usr/local/src
./installMirtaPBX.sh
```

When the installer completes without blocking errors, Asterisk and VoIPmonitor should be compiled and installed. The MiRTA PBX SSH key is installed automatically during the kernel check, installation, or upgrade phase.

Configure the Application and Database

1. Open the MiRTA PBX application directory. The exact path can vary by operating system and installation layout.
2. Edit the database configuration include file and enter the supplied MiRTA PBX name and key values.
3. Run the protected application upgrade utility to download the latest MiRTA PBX version.
4. Run the database upgrade utility.
5. Convert the database content to UTF-8.
6. Convert the database tables to InnoDB.
7. Run the upgrade check utility.

```
cd /var/www/html/pbx
vi include/db.inc.php
cd protected
php manualUpgrade.php
cd ..
php dodbupgrade
cd protected
php convert_to_utf8.php
php convert_to_innoDB.php
cd ..
php checkupgrade.php now
```

The first database upgrade can produce warnings and notices while the schema is being aligned. Review blocking errors, but do not treat every notice as a failed installation.

If the upgrade check reports that the system timezone is not configured, set the correct `date.timezone` value in the PHP runtime configuration and run the check again.

Configure the Local Asterisk Node

Configure Asterisk so the PBX node can reach itself and, later, any other cluster nodes. The node peer name should match the short server name used by the operating system and by the PBX node record.

SIP Peer

Add a peer entry for the local node in the SIP configuration. Replace the peer name, secret, and host address with values for the server being installed.

```
[IC-PBX01]
context=fromotherpbx
type=friend
defaultuser=IC-PBX01
secret=<strong-random-secret>
host=<node-ip-address>
qualify=yes
insecure=port,invite
```

If the server uses a private IP address behind NAT, add the public IP address and local network range to the SIP general configuration.

```
externip=<public-ip-address>
localnet=<private-network>/<mask>
```

Reload the SIP configuration and verify that the local peer is reachable before continuing.

Manager Interface

Add the local node IP address to the Asterisk manager configuration. Use a strong manager secret, deny access by default, permit localhost and the node IP address, then reload the manager interface.

For clustered systems, repeat the same manager access pattern for each node that must communicate with the PBX services.

Device State

In the Asterisk AGI configuration area, create the device-state configuration from the sample file and list the IP addresses for every server that belongs to the cluster. A single-node installation should still list the local node IP address.

Complete the First Web Configuration

1. Log in to the MiRTA PBX web interface using the temporary administrator credentials supplied for the installation.
2. Open **Admin > Settings**.
3. Set the International Prefix, Trunk Prefix, License Key, VoIPmonitor retention, and Call History retention.
4. Enable the options needed for the installation, such as extension status display, administrator visibility across tenants, and at least one DID selection format.
5. Save the settings.
6. Run the web interface upgrade action.
7. Log out and log in again so database upgrade changes are applied to the session.
8. Open **Admin > PBX Nodes** and add the PBX node.
9. Set the node **Peer Name** to match the operating system node name.
10. Change the administrator password immediately.
11. Reboot the server and confirm the services return correctly.

Cluster Installations

A cluster installation follows the same base process as a single-node installation, then adds node-to-node consistency and database sharing requirements.

Area	Cluster Requirement
SIP and manager configuration	Enter the peer and manager access information for all nodes. Keep the configuration consistent on each node, except for node-specific public IP settings.
Realtime registrations	Confirm the node-specific SIP registration view created when PBX nodes are added, then enable the matching registration view for the node being configured.

Area	Cluster Requirement
Application settings	Enable SIP registration view usage in both the web application configuration and the AGI configuration area.
Device state	List every cluster node IP address in the device-state configuration.
Database	All nodes must share a common database. Multi-master replication is preferred over a single central database server.
Scheduled jobs	Daily housekeeping, cost computation, and fax mailbox checks should run only once in the cluster. Disable duplicate scheduled jobs on the other nodes.

Optional Services

Additional Daemons

A normal installation configures the device-state sender and receiver daemons for automatic startup. Additional daemons should be enabled only when the related feature is required.

WebRTC and Switchboard

To use the browser phone or Switchboard features, configure Apache for secure WebSocket traffic, enable the required WebRTC settings on the extension, and complete the related values in **Admin > Settings**.

The Switchboard uses extension credentials. The extension user must have permission to use the Switchboard, and the extension should be configured with Opus, encryption, and WebRTC support when using the embedded phone.

Only one SIP module can handle WebSocket connections on a single Asterisk server. If both chan_sip and PJSIP WebRTC extensions are needed, use separate nodes or a clearly defined module assignment. In a cluster, one node can serve chan_sip WebRTC extensions while another serves PJSIP WebRTC extensions.

If the server is behind NAT, configure RTP/STUN support and map the private IP address to the public IP address for ICE candidates.

Asterisk Versions and ODBC

The legacy notes describe version-specific behavior for Asterisk and ODBC libraries. When installing a non-default Asterisk version, verify the required ODBC driver version and add the required maximum connection setting to each ODBC handle.

If call history records show character encoding problems, review the MySQL ODBC driver version and use the ANSI driver required by the installation notes. Upgrade database server versions carefully and only when required.

Queue Rules

If queue rules were not enabled by the installer, activate queue-rule realtime mapping in Asterisk and reload the related realtime configuration module.

Final Checklist

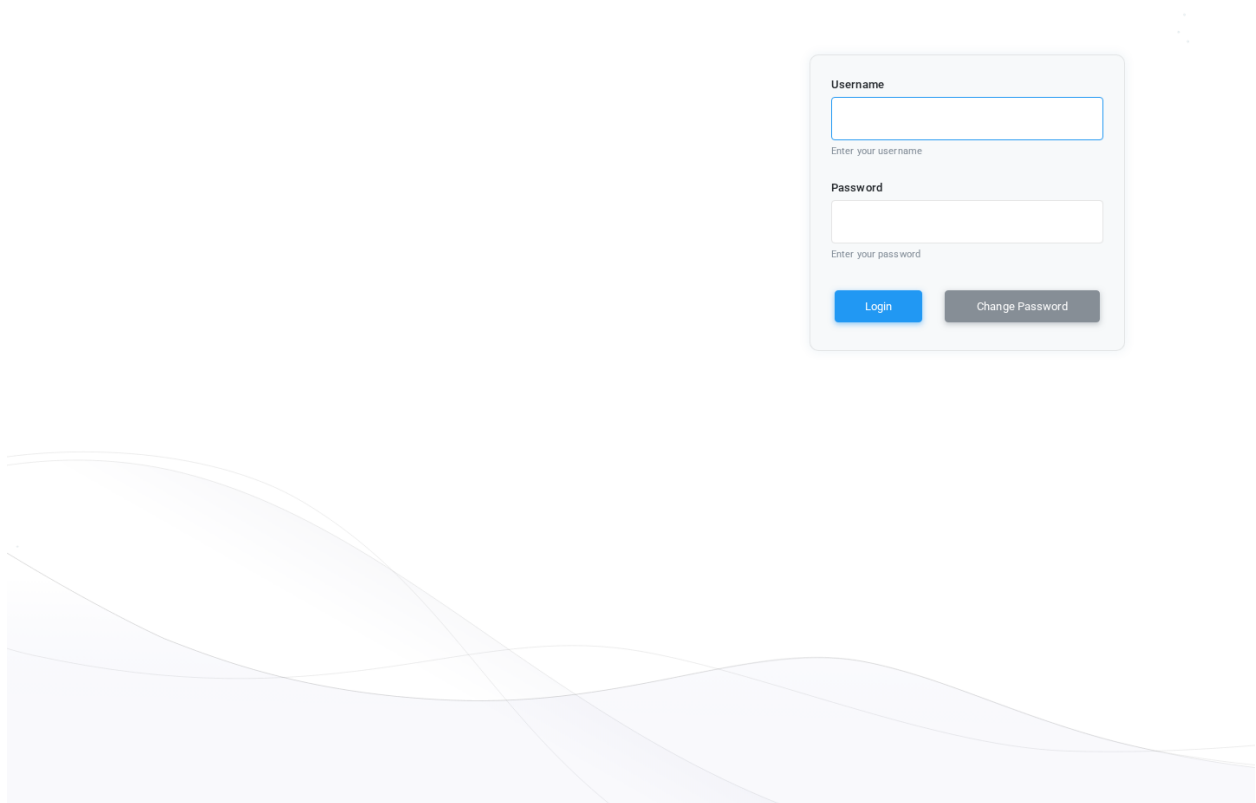
- The server hostname is correct and matches the PBX node peer name.
- The MiRTA PBX name, key, and license settings are saved.
- The database has been upgraded, converted, and checked.
- The local SIP peer is reachable from Asterisk.
- The Asterisk manager interface permits the required local or cluster node addresses.
- The PBX node exists in the web interface.
- The administrator password has been changed.
- The server has been rebooted and services return cleanly.

Initial Configuration

Initial setup and navigation tasks.

Log In and Select a Tenant

Use the MiRTA PBX web interface to sign in, then select the tenant whose configuration you want to manage.



MiRTA PBX login page.

Log in

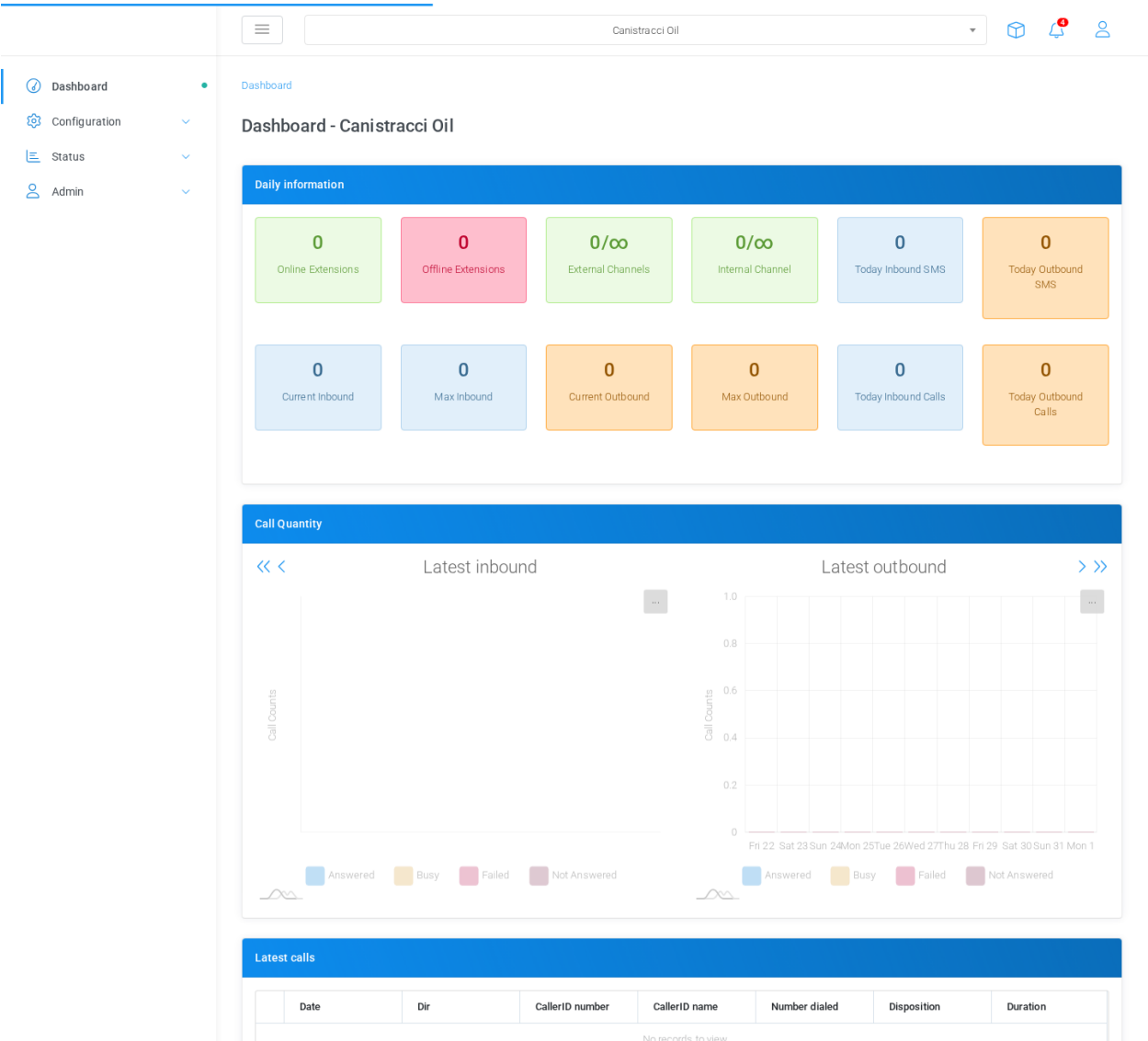
1. Open the MiRTA PBX web address provided by your administrator.
2. Enter your **Username** and **Password**.
3. Select **Login**.

If your account requires a second authentication step, complete the security-code prompt before continuing.

Select the tenant after login

If your user is enabled for more than one tenant, MiRTA PBX can show a **Tenant select** dialog immediately after login. Select the tenant you want to work on, then select **Connect**.

Only tenants authorized for your user account are shown. If the expected tenant is missing, ask an administrator to check your user-to-tenant assignments.



The selected tenant is shown in the top bar.

Change the current tenant

After login, the current tenant is shown in the selector in the top bar. To work on a different tenant, open this selector and choose the tenant from the list. MiRTA PBX reloads the work area using the selected tenant.

Dashboard

Configuration

Status

Admin

Canistracci Oil

Canistracci Oil

Daily information

0Online Extensions

0Offline Extensions

0/∞External Channels

0/∞Internal Channel

0Today Inbound SMS

0Today Outbound SMS

0Current Inbound

0Max Inbound

0Current Outbound

0Max Outbound

0Today Inbound Calls

0Today Outbound Calls

Call Quantity

Latest inbound

Latest outbound

Latest calls

Date	Dir	CallerID number	CallerID name	Number dialed	Disposition	Duration
No records to view						

Open the top-bar tenant selector to switch tenant.

The selected tenant controls the records shown and the configuration changes you make. Before editing extensions, DIDs, routing, media files, or other tenant-level settings, verify that the top-bar selector shows the correct tenant.

When the selector is not available

If you do not see the tenant selector, your account may be enabled for only one tenant, or your permissions may limit tenant switching. Continue using the tenant assigned at login, or contact an administrator if you need access to another tenant.

Create a Tenant

Create a tenant before adding tenant-specific extensions, DIDs, routing, media, and user permissions. A tenant is the top-level container for a customer's PBX configuration.

Information

Name:

Code:

☒ Allow onnet calls from this tenant

☒ Allow onnet calls to this tenant

☒ Allow any Caller ID usage when dialing out

☐ Block any outbound call with wrong Caller ID

☐ Allow incoming Caller ID usage when dialing out

☐ Allow incoming Caller ID with prefix usage when dialing out

☒ Allow any Caller ID usage when dialing out an emergency number

☐ Force recording for emergency calls

☐ Force using a pincode for onnet calls

☐ Allow transcript for recorded calls

☐ Allow summary for recorded calls

☐ Allow sentiment and emotion analysis for recorded calls

Alert email:

Emergency recording email:

Default timezone:

Use server default



Routing profile:

No outbound calls



Call campaign routing profile:

Use tenant default routing profile



New tenant form filled with Kartoon Cars and tenant code KARTOON.

Open the tenant form

1. Log in with an administrator account that can add tenants.
2. Open **Admin > Tenants**.
3. Select **Add** or **New** to open **Define Tenant**.

Enter name and code

1. In **Name**, enter **Kartoon Cars**.
2. In **Code**, enter **KARTOON**.
3. Review the defaults for calling, routing, parking, billing, limits, and storage.
4. Select **Save**.

The tenant code must be unique. Use an alphabetic code such as **KARTOON**. Avoid numbers, spaces, hyphens, and underscores unless your deployment has a specific reason to use them.

Why the code matters

MiRTA PBX uses the tenant code when creating extension usernames. The username format is:

```
<extension username>-<tenant code>
```

For example, with tenant code **KARTOON**, an extension username **201** becomes **201-KARTOON**. This keeps usernames unique across tenants even when two tenants use the same extension numbers.

After a tenant has been saved, the code field becomes read-only in the tenant form. Use the **Change** button beside the code only when you intentionally need to rename the tenant code, because extension usernames and related references depend on it.

Configure a Provider

A provider represents a trunk or external service used by MiRTA PBX for outbound calls, inbound call handling, SMS delivery, or other carrier-side functions. The screenshots on this page use fictional values and should be replaced with the values supplied by the carrier or service provider.

Open the Provider List

Open **Admin > Providers**. The list shows each configured provider, its peer name, technology, host, penalty, status, current inbound and outbound channel counters, and available actions.

Providers

New ProviderDelete Selected

Docs Demo SIP Provider

Show 10 entries

	Name	Peer Name	Tech	Host	Penalty	Status	# IN	# OUT	Actions
☐	Docs Demo SIP Provider	docs_demo_sip_provider	SIP	dynamic	99	×			ⓘ

Showing 1 to 1 of 1 entries (filtered from 9 total entries)

Previous1Next

Provider list filtered to the documentation example provider.

Select **New Provider** to create a carrier trunk or SMS gateway. Existing providers can be opened from the provider name or peer name links.

Information

Start with the provider identity. Use a descriptive **Name** that operators recognize, and use a stable **Peer Name** that matches the SIP peer, PJSIP endpoint, IAX peer, local route, or SMS gateway identifier used by the system. Choose the technology and set the status.

Name:

Example Telecom SIP Trunk

Peer Name:

example_telecom_sip

Technology:

SIP

Status:

Enabled

Provider Information block filled with fictional SIP trunk values.

- **Enabled** allows inbound and outbound use.
- **Disabled** keeps the provider configured but unavailable.
- **Only Inbound** hides outbound routing options and is useful when the carrier should only deliver calls into the PBX.

Outbound Calls

Use outbound settings to normalize calls before sending them to the provider. Additional headers can be sent to SIP, PJSIP, IAX2, or SMS providers. Digits to add and digits to remove are applied during outbound routing. Caller ID presentation, caller ID modification, and caller ID regex control which caller identity the provider receives.

Outbound Calls

Additional Header (1):

X-Account-Code: docs-demo

+

CallerID Presentation:

Auto Privacy, CallerID not screened

▼

Digits to Add:

+1

Number of digits to Remove:

1

CallerID Modifications:

No Modifications

▼

CallerID allowed regex:

^\\+1555[0-9]{7}\$

Max outbound channels:

12

Penalty:

10

☒ Ignore SIP Cause codes

☒ Ignore BUSY

Outbound Calls block with fictional caller ID and routing controls.

CallerID and **CallerID Name** force the caller identity for every call using the provider. Leave them blank when the caller ID should come from the extension and normal caller ID rules.

Max outbound channels limits concurrent outbound calls through the provider. **Penalty** is used by routing decisions and round-robin selection. The ignore options let routing continue to another provider when the current provider returns SIP cause codes or a BUSY status that should not stop the route search.

Inbound Calls

Inbound options normalize numbers before DID matching. Use these fields only when the carrier sends the destination number in a format that does not match the DIDs configured in the tenants.

Inbound Calls

Inbound Digits to Add:

+1

Inbound Number of digits to Remove:

0

DID Modifications:

No Modifications

Same provider IN and OUT:

Yes

☐ Allow custom extensions

☒ Normalize number

Get number from:

SIP To: Header

Variable name (1):

USR-ProviderName

Variable value (1):

Example Telecom

Variable name (2):

USR-SupportTier

Variable value (2):

Gold

Variable name (3):

USR-

Variable value (3):

Inbound Calls block with fictional DID normalization and user variables.

DID Modifications can rewrite inbound numbers before matching. **Same provider IN and OUT** controls whether a call that arrived from this provider may also leave through the same provider. The variable fields create user variables prefixed with `USR-`, which can later be used by routing logic and dialplan actions.

Realtime Account

For SIP, PJSIP, and IAX2 providers, enable **Use Realtime Account** when the provider should be represented by realtime Asterisk configuration. The fictional example below uses documentation IP and domain values.

Realtime Account

☒ Use Realtime Account

Transport: UDP

RTP Encryption (SRTP): No

Host: 203.0.113.20

Port: 5060

Outbound Proxy: sip-proxy.example.net

Username: example_user

Password: FictionalSecret-2026 Generate

From User: +15551230000

From Domain: sip.example.net

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: No

Call response timer (ms) - T1: 500

Call setup timer (ms) - B: 5000

RTP Keepalive: 5

Can Reinvite: No

Realtime Account block with fictional SIP registration and media settings.

Use **Host** and **Port** for the provider address. For inbound calls, an IP address is preferred because Asterisk realtime matching cannot always rely on a hostname. Username, password, From User, From Domain, RPID/PAI handling, qualify settings, codecs, DTMF mode, NAT, timers, and RTP keepalive should match the carrier interconnection requirements.

SMS Provider Options

When the technology is **SMS**, the outbound section changes to SMS delivery settings. Choose the SMS protocol and complete the fields required by the provider. The JSON Web URL example shows a fictional REST endpoint and a JSON body built from MiRTA PBX SMS variables.

Outbound Calls

Additional Header (1):	X-Account-Code: docs-demo	⊕
Additional Header (2):		⊕
Additional Header (3):		⊕
Additional Header (4):		⊕
Additional Header (5):		⊕
Additional Header (6):		
Digits to Add:	+1	
Number of digits to Remove:	1	
CallerID Modifications:	No Modifications ▼	
CallerID allowed regex:	^\+1555[0-9]{7}\$	
Max outbound channels:	12	
Penalty:	10	
SMS Protocol:	Web URL (JSON) ▼	
SMS URL/AGI Script Name:	https://sms.example.net/v1/messages	
HTTP Content Type:	application/json	
User:	docs-demo-user	
Password:	FictionalSmsSecret	
JSON data:	<pre>sender.number:\${SMSSOURCENUM} receiver.number:\${SMSDESTNUM} message.text:\${SMSTEXT}</pre>	
☒ Ignore SIP Cause codes		
☒ Ignore BUSY		

SMS provider options shown with fictional JSON Web URL values.

Common SMS variables include `${SMSTEXT}`, `${SMSDESTNUM}`, `${SMSSOURCENUM}`, and `${SMSNAME}`. For JSON payloads, dot notation in the field name creates nested JSON objects.

Save and Test

1. Save the provider only after replacing the fictional values with production values from the carrier.
2. Confirm the provider appears in the provider list.
3. Create or update a routing profile so outbound calls can select the provider.
4. Use provider status, channel counters, and call history to validate registration, dialing, inbound DID matching, and caller ID presentation.

Configure a Routing Profile

A routing profile groups routing rules. Tenants, extensions, campaigns, fax features, and SMS features can use routing profiles to decide which provider or route should be used for an outbound destination.

Create the Routing Profile

1. Open **Admin > Routing Profiles**.
2. Select the add action.
3. Enter a name, such as **Docs Demo Voice Routing**.
4. Enter a short description explaining when this profile should be used.
5. Select the type: Voice, SMS, or FAX.
6. Save the profile.

Add Routes

After the profile exists, add routing rules for the destinations that should use it. A typical voice profile starts with emergency, national, mobile, international, and fallback rules. Each rule should point to one or more providers and should be specific enough to avoid accidental matches.

Routing Profile Types

Type	Use
Voice	Outbound voice calls and normal extension dialing.
SMS	Outbound SMS routing through SMS-capable providers.
FAX	Outbound fax routing where fax provider handling must be separated from voice routing.

Test Routing

Use a limited test pattern and a known test number before assigning the profile to production tenants. Confirm which provider is selected, whether digit manipulation is correct, and whether caller ID rules match carrier requirements.

Complete the Tenant configuration

After the tenant exists and the routing profile has been created, complete the tenant configuration so the tenant can place billable outbound calls using the intended profile.

Assign the Routing Profile

1. Open **Admin > Tenants**.
2. Edit the tenant.
3. In the tenant information area, select the default routing profile for voice calls.
4. If needed, select a separate call-campaign routing profile, fax routing profile, and SMS routing profile.
5. Review the tenant limits before saving, especially channels, extensions, DIDs, media files, queues, and campaigns.
6. Save the tenant.

Move the Tenant to Post Paid

1. In the tenant billing section, find the payment type field.
2. Change the payment type from **Prepaid** to **Post Paid**.
3. Confirm the tenant has the expected call rate, billing code, and cost-limit settings.
4. Save the tenant and reopen it to verify the new value.

Post Paid tenants are not stopped by prepaid balance exhaustion in the same way as prepaid tenants. Use cost warnings, cost limits, route cost limits, and call limits when the tenant still requires spending protection.

Final Check

- The tenant is enabled.
- The default routing profile is assigned.

- The tenant is set to Post Paid.
- The billing code and call rate are correct.
- Outbound and emergency caller ID policies have been reviewed.
- The tenant channel limits are appropriate for production traffic.

Use on mobile device

MiRTA PBX is a web application and can also be used from a mobile phone browser. Use the same MiRTA PBX address, username, password, and tenant selection process that you use on a desktop browser.

Login

Username

Enter your username

Password

Enter your password

Login

Change Password

MiRTA PBX login page on a mobile phone viewport.

Log in from a phone

1. Open the MiRTA PBX web address in the phone browser.
2. Enter your **Username** and **Password**.
3. Select **Login**.
4. If your account requires a second authentication step, complete it before continuing.

Dashboard

Dashboard - Canistracci Oil

Daily information

2

Online Extensions

8

Offline Extensions

0/∞

External Channels

MiRTA PBX after login on a mobile phone viewport.

Work with the mobile layout

After login, the same tenant-aware interface is available on the phone. The selected tenant remains visible in the header area, and the page content adapts to the narrower screen.

Before changing configuration, verify that the selected tenant is correct. Any page opened from the mobile interface uses the tenant currently selected in the header.



Dashboard



Configuration



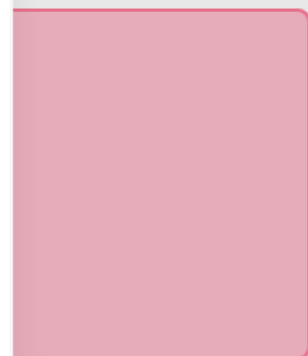
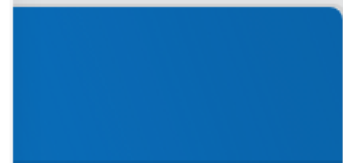
Status



Admin



il



Mobile navigation drawer opened from the header menu icon.

Open the navigation menu

On a phone, the left navigation is hidden until it is needed. Select the menu icon in the header to open the navigation drawer, then choose the same sections you use on desktop, such as **Configuration**, **Status**, or **Admin**.



Extensions

-

Canistracci

New SIP peer

Bulk SIP peers

Custom Extension

Virtual Extension

Oil

☐	Nun	Nan	Des	Tec	Use	Pas
	☐ x	☐ x	☐ x	☐ x	☐ x	☐ x
☐	100	Alex R	Demo	SIP	100-C	Demo
☐	101	Bella S	Demo	PJSIP	101-C	Demo
☐	102	Casey	Demo	SIP	102-C	Demo
☐	103	Drew H	Demo	PJSIP	103-C	Demo
☐	104	Eva Br	Demo	SIP	104-C	Demo
☐	105	Finn C	Demo	PJSIP	105-C	Demo
☐	106	Gia Pa	Demo	CUSTO	106-C	

Extensions configuration page displayed on a mobile phone viewport.

Use configuration pages

Configuration pages can be opened and edited from the mobile interface. Forms, buttons, filters, and tables remain available, although wide tables may require horizontal scrolling or a desktop browser for longer editing sessions.

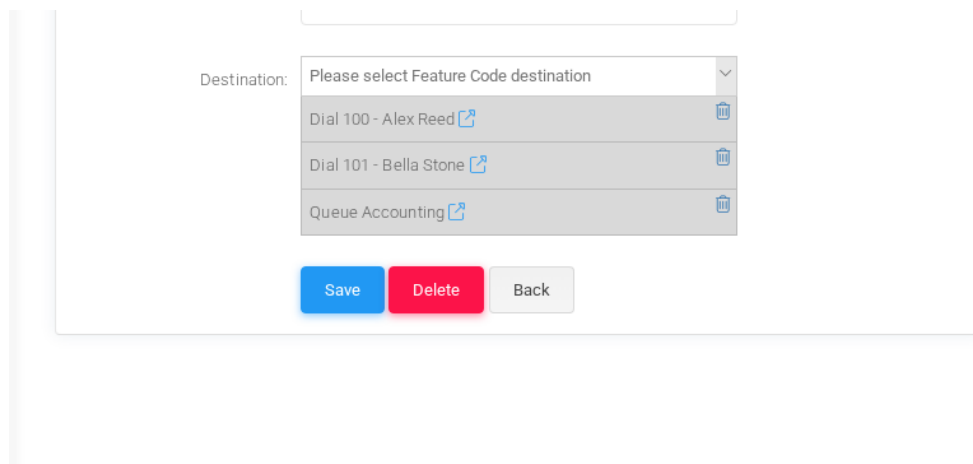
Recommended use

Use case	Recommendation
Quick checks	Use the phone interface to check tenant selection, status pages, recent records, and simple configuration values.
Small changes	Use the phone interface for short edits when the required fields are visible and easy to review.
Large changes	Use a desktop browser for long forms, large grids, bulk actions, or changes that require comparing many fields.

Use multiselect

MiRTA PBX uses multiselect fields when a form can hold more than one related object. Common examples include destination lists, extension lists, media files, queues, allowed providers, and report fields.

The example below uses a **Destination** field. The same control behavior applies to other multiselect fields, although the available object types depend on the field you are editing.

A screenshot of a web form showing a 'Destination' multiselect field. The field is labeled 'Destination:' and has a dropdown menu open. The dropdown menu contains the text 'Please select Feature Code destination' and a list of three items: 'Dial 100 - Alex Reed', 'Dial 101 - Bella Stone', and 'Queue Accounting'. Each item has a small blue icon to its right. Below the dropdown menu are three buttons: 'Save' (blue), 'Delete' (red), and 'Back' (gray).

Destination multiselect field with two extensions and the Accounting queue selected.

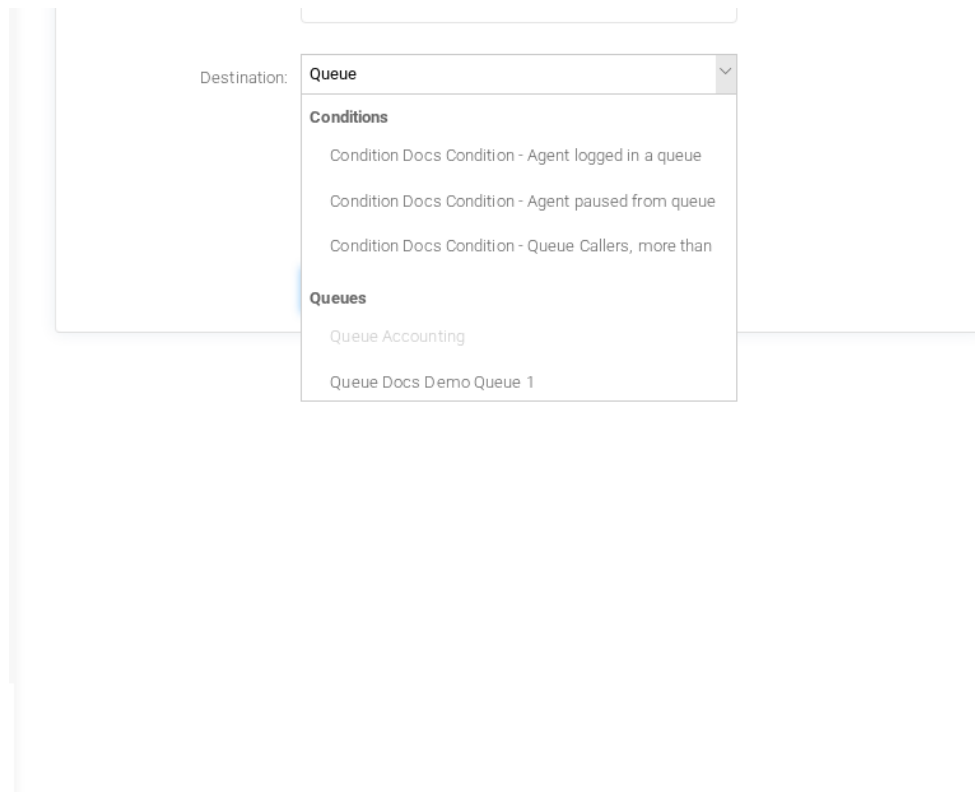
Select Items

Select the field, or the arrow at the right side of the field, to open the list of available values. Values are grouped by object type, such as Extensions, Queues, Conditions, or IVRs.

Select an item from the list to add it to the chosen items under the input. In the example, the field contains two extension destinations and the Accounting queue. When an arrow icon is shown beside a selected item, select it to open the edit page for that referenced object.

Search Items

Start typing in the multiselect input to filter the available values. The search is field-specific: a Destination field searches destination objects, while another multiselect field may search extensions, media files, providers, or another object type.



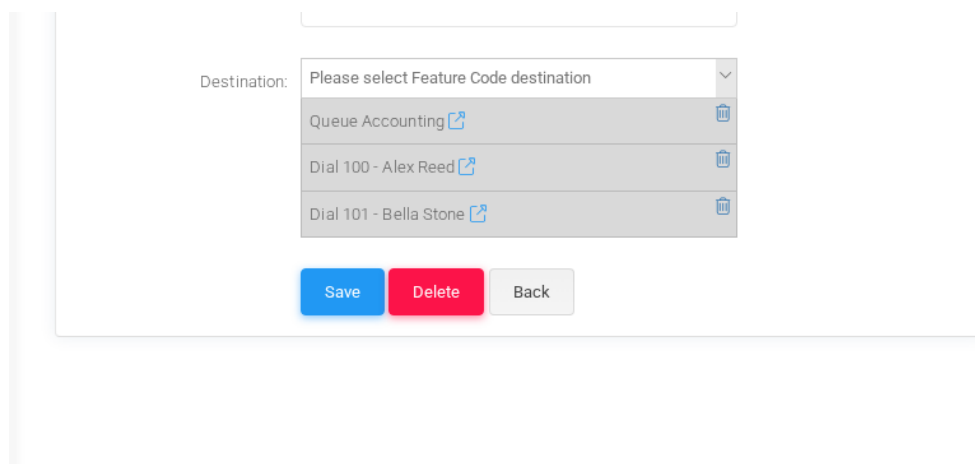
Filtering the Destination field by typing Queue in the multiselect search input.

The example searches for **Queue**. Matching results are grouped by type, so you can distinguish a queue from a condition, special action, or another object whose label also contains the search term.

If the expected item is not returned, verify that you are working in the correct tenant and that the object exists in a type accepted by the current field.

Rearrange Items

Selected items can be reordered by dragging a chosen item up or down in the selected list. When the field represents an ordered sequence, MiRTA PBX saves the items in the displayed order.

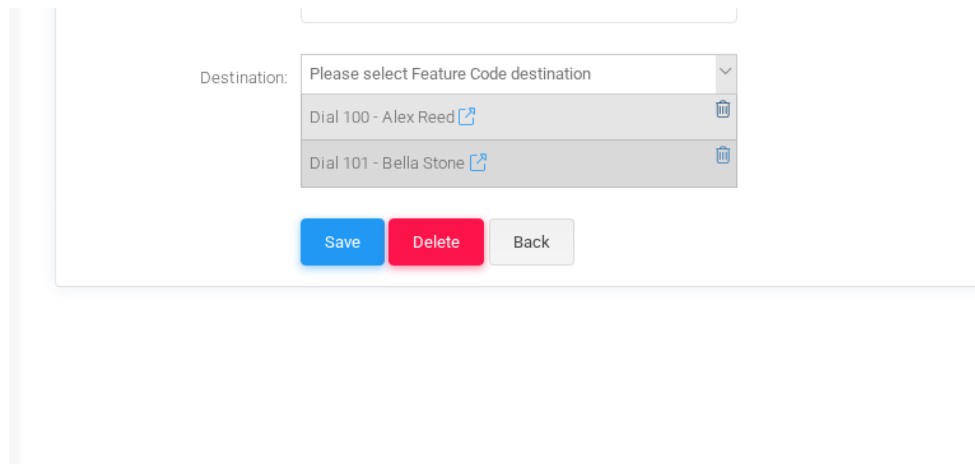


Selected destinations reordered so the Accounting queue is first.

In the example, **Queue Accounting** has been moved before the two extension destinations. Use this ordering for fallback paths, destination chains, ordered report columns, or any other multiselect field where the order changes the result.

Remove Items

Select the trash icon at the right side of a chosen item to remove it from the field. This removes the relationship from the current form only; it does not delete the destination, extension, queue, media file, or other referenced object.



Destination: Please select Feature Code destination

Dial 100 - Alex Reed	
Dial 101 - Bella Stone	

[Save](#) [Delete](#) [Back](#)

The Accounting queue removed from the selected destinations.

After selecting, rearranging, or removing values, save the form to apply the change. If you leave the page without saving, the multiselect changes are discarded like any other unsaved form edit.