

DEPLOYMENT AND ADMINISTRATION

Telfron PBX Technical Guide

Architecture features and operating procedures

For IT managers, administrators and technical buyers planning, configuring or maintaining a Telfron PBX deployment.



AI concept illustration. People, equipment and settings are illustrative.

Plan the complete communication workflow

This guide explains how customer PBX services connect with the central workspace, how to organize companies and branches, and how to configure calling, AI, messaging, meetings and industry tools.

Use the customer deployment as your reference

Plan company boundaries, call flows, user permissions, devices and network access together. Use the acceptance checks in this guide to verify the experience from the accounts and endpoints the customer will use.

Reference baseline: PBX 1.6.139, build 202610180002, with the documented October 2026 portal and meeting updates. Android reference release: 1.1.31, version code 33. Record the versions actually installed before making changes.

[Documentation](#) | [Customer workspace](#)

GUIDE NAVIGATION

Using this guide

Use sections 1 to 3 to plan the installation, sections 4 to 19 to configure operational workflows, and sections 20 to 23 to prepare security, maintenance and acceptance. The numbered steps describe the intended order; available controls depend on the account and licence.

Section	Page
01 Architecture and service boundaries	3
02 Capacity and network planning	4
03 Installation and initial setup	5
04 Calling and routing	6
05 Reception and voicemail	7
06 AI receptionist	8
07 WhatsApp workflows	9
08 Social Media and Publishing	10
09 Companies and sites	11
10 Create a company	12
11 Create and manage a site	13
12 Education and campus communication	14
13 Hotel communication workflows	15
14 Devices and Android activation	16
15 User roles and meeting permissions	17
16 Start and share a meeting	18
17 Guest admission and host controls	19
18 Meeting connectivity and diagnostics	20
19 Paging and device provisioning	21
20 Security and data handling	22
21 Backups updates and daily operations	23
22 Licensing and capability scope	24
23 Acceptance and handover	25

Examples use a fictional organization and illustrative numbering. Capacity examples are not licence entitlements. The authoritative values are those shown for the activated installation and the agreed customer proposal.

SECTION 01

Architecture and service boundaries

The customer PBX hosts telephony and application services. The central workspace coordinates connected installations and selected management workflows. A connected installation, a company tenant and a company site are different objects and should be named distinctly.

Layer	Purpose and boundary
Customer PBX	SIP calling, call routing, local administration and the configured meeting service run on the customer installation.
Application services	The current Windows deployment includes SIP and API services, PostgreSQL and Redis. Monitor each service and its storage.
Customer workspace	my.telfron.com manages connected PBXs, company provisioning, licensing and the customer Meet entry point.
Remote console	An authorized portal session can open the PBX through its cloud connection. Access still depends on company and user scope.
External services	SIP carriers, AI providers, WhatsApp connectivity, email and media relay services have separate availability and data flows.

Connection model

The PBX establishes an outbound connection for central management. This does not remove the need to design SIP, media, LAN and branch connectivity. A healthy portal heartbeat is useful evidence of management connectivity; it is not a complete call or media test.

Licence validation and offline operation

Local PBX operation still requires a valid activated licence and a signed entitlement bound to the installation. During a licensing-server outage, cached operation is limited by the configured offline allowance and certificate validity. Contract expiry, any applicable grace period, suspension or revocation can restrict service. Check the displayed licence state and validation status; do not promise indefinite offline operation.

Data location

Distinguish PBX configuration and local records from cloud account metadata, company allocation summaries and external service traffic. AI requests, messaging providers and meeting relays may involve systems outside the customer network. Record those flows in the deployment design.

Example

Example Group has one connected PBX installation. Two independently administered businesses are provisioned as separate company tenants. Each company can then organize its own branches through Sites. A branch on a shared PBX does not imply that a separate PBX server was installed there.

SECTION 02

Capacity and network planning

Size a deployment around concurrent work and retention requirements, not extension count alone. A lightly used directory of many extensions can place different demands on the server from a smaller installation with continuous recording, AI processing and meetings.

Planning input	Record before approval
Users and calls	Users, extensions, expected simultaneous calls, queue peaks and carrier channels.
Meetings	Expected room size, simultaneous meetings, camera usage and screen sharing.
Storage	Recording and voicemail volume, retention periods, backups and free-space threshold.
Automation	AI request volume, knowledge indexing, document processing and messaging activity.
Endpoints	Desk phones, mobile devices, PA endpoints and supported provisioning models.
Availability	Power protection, recovery target, internet dependency and support ownership.

Network requirements

- Provide stable DNS, correct time, a trusted HTTPS endpoint and the required outbound connectivity.
- Review SIP transport, carrier restrictions, NAT behaviour and the configured RTP media range.
- Design interbranch connectivity and access controls for the intended topology; document VPN or other connectivity where used.
- Test media from an external network as well as the LAN, including any relay required by restrictive firewalls.

The administration URL may use HTTPS port 8443 in an installed environment. Use the deployed configuration for actual listener addresses and firewall rules. Do not expose PostgreSQL, Redis or internal API listeners to the public internet as a convenience for administration.

Agree server specifications and a load-test plan with the deployment team. This guide does not assign an untested maximum call count, meeting size or bandwidth figure.

SECTION 03

Installation and initial setup

The current reference installation is a Windows PBX. Use a supported, supplied installation package and confirm its version, source and verification status before deploying it to a customer machine. Android and desktop client releases may have separate version numbers.

1. Confirm the installation owner, licence, company identity, deployment plan and maintenance window.
2. Prepare the server, power, storage, DNS and network access. Record where backups will be stored and who can recover the system.
3. Install or upgrade into the intended folder using the supplied procedure. For an existing installation, preserve customer data and use the supported upgrade or repair route.
4. Check SIP, API, PostgreSQL and Redis service readiness. Open the administration console and confirm the displayed version.
5. Activate the intended installation and confirm it appears under PBX sites in my.teltron.com.
6. Set the company structure before allocating users and extension ranges. Configure user identities and eligible phone extensions separately from AI and PA endpoints.
7. Add the carrier connection and call routes. Make controlled inbound and outbound calls, then verify media and unanswered-call behaviour.
8. Configure only the licensed collaboration and automation services required for this customer. Complete the acceptance checks before handover.

What a successful first check establishes

A loaded dashboard confirms that the web application is accessible. A registered phone confirms a registration path. Neither alone proves two-way audio, carrier routing, voicemail delivery or the correct caller ID. Test each intended workflow independently.

Customer handover record

Record installed versions, service ownership, approved administrator accounts, company and site names, carrier details, endpoint inventory, support contact and backup location. Store credentials in the customer-approved secret store, outside this document.

SECTION 04

Calling and routing

Calling begins with an extension identity, a reachable endpoint and a routing rule. A SIP trunk connects the PBX to a carrier or another supported telephony system. Inbound and outbound rules decide how calls reach their destinations.

Component	Use it when
User extension	A person needs a desk phone, supported softphone or mobile calling identity.
SIP trunk	The organization needs external calls through a configured carrier or peer.
IVR	Callers should choose a department or follow a published menu.
Ring group	A defined set of staff should be alerted according to the configured ringing behaviour.
Call queue	Callers should wait for an available agent and follow an agreed overflow policy.
Time condition	Business hours, holidays or other configured time windows should change the route.

Configure a simple incoming call flow

1. Confirm the incoming carrier number and trunk mapping.
2. Choose the first destination, such as an IVR or receptionist group.
3. Configure the working-hours route and the closed-hours alternative.
4. Set no-answer, busy and overflow destinations. Avoid routing loops.
5. Call the number from outside the PBX and test each menu choice and fallback.

Check outgoing calls

Review permitted destinations, number formatting, carrier caller-ID rules and account permissions. Test an approved external destination and verify audio in both directions. Emergency calling and location behaviour require explicit carrier and deployment validation; do not assume a generic route satisfies them.

SECTION 05

Reception and voicemail



AI concept illustration. People, equipment and settings are illustrative.

The receptionist console supports everyday call handling and visibility across the configured extension directory. Combine that workspace with clear ringing and overflow rules so staff know which calls they own and where unanswered calls go.

Reception workflow

1. Sign in with the intended company account and check that the correct extensions are visible.
2. Receive a controlled incoming call and identify the caller and destination.
3. Test hold, resume and the required transfer workflow with another available staff member.
4. Confirm what the caller hears when the target is busy, unavailable or outside working hours.

Voicemail and greetings

Enable voicemail only where a responsible person will review it. Configure the mailbox, greeting and ringing time, then leave a message from an external call. Verify that the intended user can find and play it. Where configured, staff can record their extension greeting through the telephone voicemail menu.

Recordings and follow up

Call history and configured recordings help staff investigate and follow up conversations. Agree which calls are recorded, who can access recordings and how long they are retained. Set any required notices and consent process before enabling production recording.

Callback behaviour

Use the available queue callback or busy-callback workflows where licensed and configured. Test who receives the callback, how it appears to staff, and what happens if the recipient is still unavailable. Do not promise a successful callback solely because a request was queued.

Acceptance example: reception answers a call, holds it, resumes it, transfers it and then verifies the unanswered route on a separate test call. Keep each result with the deployment record.

SECTION 06

AI receptionist

An AI receptionist is a configured call-handling role. It needs a defined task, approved knowledge, connected speech and language services where used, and a clear route to a person. It should not be treated as a substitute for all reception decisions.

1. Define the scope: opening hours, service information, department routing or a specific appointment workflow.
2. Create or select the intended AI receptionist extension. Keep human phone extensions and PA devices in their own roles.
3. Configure the approved AI and speech providers, voice and required languages. Confirm credentials, credit availability and service reachability.
4. Load approved knowledge and review extraction or indexing results. Resolve incomplete or review-required content before relying on it.
5. Set the greeting, transfer destinations, staff handoff and fallback behaviour.
6. Test expected questions, unknown questions, interruptions, language changes and a failed-provider scenario.
7. Review outputs with the business owner and enable the agreed production route.

Monthly AI credits

Eligible plans include a monthly AI credit allowance that resets automatically each calendar month. Free and Basic have no included allowance in the default configuration. Confirm the configured allowance and eligible services against the selected package before use. AI credits are the customer usage unit; provider tokens are measured internally.

Unused included allowance does not accumulate. Purchased credits are a separate balance. Monthly allowance renewal is not automatic paid top-up; automatic paid top-up is currently unavailable. Check remaining credit and any separate provider charges before enabling an AI workflow.

Knowledge and human handoff

Website and document indexing can support the knowledge workflow, but extraction completion does not guarantee that every answer is correct. Use approved FAQs for important facts and make escalation practical when the question falls outside scope. Keep the information owner responsible for changes.

Appointments and sensitive enquiries

For appointment workflows, verify the configured calendar or availability source, caller consent and confirmation behaviour. Do not let a generic demonstration imply that all scheduling systems are connected. Route safeguarding, medical, financial or other consequential decisions to appropriate staff.

Provider access, language performance, data processing and usage charges are part of the customer design. Verify these for the selected deployment rather than assuming all AI processing stays on the PBX.

SECTION 07

WhatsApp workflows

The WhatsApp module provides inbox and automation workflows in the current system. Its connection method, permissions and provider rules determine how a customer can use it. Specify the actual supported connection in the proposal; the presence of a WhatsApp module does not itself establish official Business Platform certification.

Set up a controlled messaging workflow

1. Confirm the business account owner, supported connection method and licence entitlement.
2. Connect the intended account through the supported setup flow and verify its session status.
3. Assign the responsible staff and review which company conversations they may access.
4. Configure the greeting, menu or trigger rules. Leave unwanted AI triggers disabled.
5. If using AI, attach approved knowledge and define staff handoff, unanswered requests and fallback replies.
6. Send a test message from an approved test contact. Verify receipt, reply, staff assignment and the return from automation to human handling.

Example

An admissions enquiry arrives in the configured inbox. An approved automation provides opening hours or a relevant information link. When the person asks for staff, the conversation is handed to the designated team. The team checks its assignment and replies from the correct workspace.

Operational controls

- Monitor connection health and reconnect through the supported procedure when required.
- Review menu behaviour, duplicate handling, reply recovery and appointment confirmations with realistic messages.
- Use consent and opt-out handling appropriate to the communication; review provider restrictions before campaigns.
- Keep message content, attachments and staff access within the agreed retention and privacy policy.

Social publishing, campaigns, live chat and CRM connectors should be scoped separately. Confirm each required channel or connector with a working end-to-end demonstration before including it as a delivered integration.

SECTION 08

Social Media and Publishing

Use Social Publishing to prepare and distribute organizational announcements through connected supported social accounts. This is separate from private WhatsApp inbox conversations and call handling.



AI concept illustration. People, equipment and settings are illustrative.

Prepare and publish a post

1. Confirm the account owner, supported platform connection and staff publishing permissions.
2. Open Social Publishing and prepare the post text, target accounts and supported media.
3. Save a draft for review or select immediate publication or a scheduled date and time. Confirm the displayed time zone.
4. Check the selected destinations and content, then submit the intended publishing action.
5. Review publication status for each destination. Resolve reported account, media or provider errors before retrying.

Acceptance checks

Use an approved test account or post. Check draft saving, the scheduled time, the resulting publication and its status. Confirm account permissions and platform-specific media requirements for every channel included in the customer scope.

Connected channels and formats depend on the platform, account permissions and provider requirements. A provider name in a menu is not evidence that the customer account is connected.

SECTION 09

Companies and sites

Use a company tenant to represent an organization that needs its own scoped administration and resources. Use a Site to represent a branch, building or location inside that company. Use PBX sites in the central workspace to identify connected PBX installations.

Object	Represents	Managed through
Connected PBX	A running customer installation with an activation and management connection.	PBX sites in my.telfron.com.
Company tenant	A separately scoped business with assigned capacity and an extension range.	Companies in my.telfron.com.
Company site	A branch or location belonging to one company.	Sites in the selected company PBX console.

When to create a company

Create another company when separate ownership, users, administration and resource boundaries are needed. Central provisioning replaces company creation from the customer PBX dashboard. Keep the company count and resource allocations within the installation licence and use non-overlapping extension ranges. The licence company limit is separate from its user, extension and concurrent-call limits.

When to create a site

Create a site when the same company needs another location. A site can organize extension and trunk associations and location details. Creating a site does not by itself install a remote PBX, establish a VPN or prove that a phone can register from that branch.

School group example

Example Education Group operates two independently administered schools. Provision each school as a company tenant. Within School A, use sites for the main campus and annex. If two buildings share one administration and resource boundary, they may belong to the same company as separate sites.

Tenant isolation and branch organization serve different purposes. Test that staff see only authorized company resources, and test branch connectivity separately from the company creation workflow.

SECTION 10

Create a company

Create companies through my.telfron.com using an authorized account. Start with an online, activated PBX, an available licensed company slot and sufficient resource capacity. Record the proposed allocation before submitting a production company.

1. Open PBX sites and identify the intended installation. Check its status, installed version and last-seen information.
2. Open Companies and synchronize the intended PBX. Review the companies and allocations already present.
3. Select Create company. Enter its name and a unique company address; add the optional custom domain and company code only when required.
4. Check the licensed maximum company count, then allocate users, extensions and concurrent calls within the remaining installation capacity.
5. Choose an extension range that does not overlap an existing company range. Review the values with the responsible administrator.
6. Submit the request and wait for provisioning to complete on the PBX. If it remains pending or fails, inspect the reported result before submitting again.
7. Open the intended company, verify its identity and allocation, then create its first site and configure users and calling services.

Example field	Illustrative value	Review point
Company name	Example Company	Recognizable to its administrators.
Company address	example-company	Unique within the supported addressing scheme.
Users and extensions	10 users and 10 extensions	Fits remaining licensed allocation.
Concurrent calls	2	Matches the intended allocation and carrier design.
Extension range	3000 to 3099	Does not overlap another company.

The example is not a default package or a capacity recommendation. Do not lower another company allocation just to make room without an approved capacity decision. Archiving or changing a company is a separate administrative action. Archived companies can retain users and extensions that still consume installation capacity; archiving alone does not guarantee that allocation is available for reuse. Company limits must not be reduced below current usage.

SECTION 11

Create and manage a site

Sites belong to a company. Confirm the selected company before adding or editing a branch. Use consistent names and codes so reception teams and administrators can distinguish locations.

1. Open the intended company PBX console, then select Phone System and Sites.
2. Select Create Site. Enter the site name, unique code and a short description of its purpose.
3. Choose the site type and intended status. Set a primary site only when that is the correct company location.
4. Enter applicable address and location details. Complete the network or remote connection fields only with approved deployment values.
5. Review the completed form and create the site. Reopen it to confirm the saved values.
6. Associate the intended extensions, trunks and relevant configuration. Verify those associations from the correct company context.
7. Check the site view or statistics, then test registration, calling and media from the real branch network.

Completed example

For Example Company, use North Branch with site code NORTH and a description such as North office for Example Company. Add its real address in production. Use the actual network design rather than copying a VPN address or remote URL from a demonstration.

Interpret status carefully

A site marked Active is an administrative state. Displayed extension counts or a health label are useful operational information, but they do not independently prove live phone registration, two-way audio or a complete network path. Make those checks at the endpoint.

Keep branch management within its scope

Use a separate company when administration or data boundaries must be independent. Use another site for a location within the same company. If a branch needs its own PBX installation, record that installation separately under the central PBX management view.

SECTION 12

Education and campus communication

Map the school caller journey before creating departments and campus locations. Use the company and site structure to reflect the intended administration, then connect the relevant reception and communication workflows.



AI concept illustration. People, equipment and settings are illustrative.

Configure a school communication workflow

1. Identify reception, admissions, accounts and other call destinations, including working hours and holiday routes.
2. Use separate companies for independently administered schools. Create Sites for campuses or buildings within each company.
3. Associate the intended staff extensions and define reception, queue and no-answer behaviour.
4. If using AI or WhatsApp, approve the knowledge, owner, scope and staff handoff for routine enquiries.
5. Assign meeting permissions for staff and configure the required paging zones on compatible endpoints.
6. Test a parent enquiry from outside the PBX, including an unavailable department and the selected fallback.

Verify the campus experience

Check each real campus network, the correct company directory, staff access and announcement coverage. Use approved test content for Social Publishing. Keep student information and personal enquiries within the agreed access and retention rules.

SECTION 13

Hotel communication workflows

Use the hotel workspace to connect reception calling with room-related telephone tasks. Confirm the hotel entitlement on the activated licence first. The current PBX interface applies an Enterprise-level access rule; the package name alone does not confirm hotel availability. Establish ownership of room records, service requests and housekeeping updates before daily use.



AI concept illustration. People, equipment and settings are illustrative.

Hotel tool	Operational purpose
Rooms and status	Maintain the room view used by reception.
Wake up calls	Schedule guest wake-up calls and review their outcomes.
Service requests and menu	Record and organize room-related requests for the responsible team.
Housekeeping status	Coordinate room-related status with reception.
Call records and rates	Review room telephone activity and configured charges.
Dashboard and reporting	Review the hotel operational information available to the account.

Test a room workflow

1. Confirm the intended room record, assigned telephone and responsible reception account.
2. Schedule an approved test wake-up call and verify both the room endpoint and the recorded outcome.
3. Record a test service request and housekeeping update, then check the responsible team and front-desk views.
4. Make a controlled room call and verify its record and any configured rate or charge.

Confirm any external hotel or property-management integration for the exact deployment. The hotel modules do not by themselves establish connectivity with an external PMS.

SECTION 14

Devices and Android activation

A person should use an eligible User Extension for phone and mobile access. AI receptionists, PA endpoints and other service extensions have different roles and should not be provisioned as a personal softphone merely because they have an extension number.

Android activation

1. Create or select the intended User Extension and verify its company, assigned person and enabled status.
2. In extension settings, configure mobile access, ringing behaviour and the required meeting permission.
3. Generate the supported activation invitation or QR code for that extension. Treat the activation material as sensitive access information.
4. Install the supplied current Telfron Android application and complete activation with the intended account or QR workflow.
5. Review the assigned extension and meeting permission shown during activation. Grant only the required Android permissions.
6. Test outgoing and incoming calls, locked-screen behaviour, notification actions and the selected ringing mode on the actual handset.

Ringing choice	Intended use
Desk phone	Calls should alert the desk endpoint.
Mobile	The enabled mobile application is the intended endpoint.
Both	Desk and mobile should participate in the configured ringing behaviour.
Desk then mobile	Try the desk first, then the mobile after the configured delay.
Automatic	Use the system supported automatic selection behaviour.

The Android reference release is 1.1.31, code 33. Use the current supplied download method; a working public Play Store listing should be confirmed before directing customers to it. Test deep links from email on supported phones and retain a browser joining option where appropriate.

SECTION 15

User roles and meeting permissions

PBX administration, room host assignment and an extension meeting permission are related controls. A person does not receive hosting access just by entering a room UUID, choosing a display name or using the same email in another application.

Identity or setting	Hosting behaviour
User extension with Join only	The assigned user may join when room admission permits; it does not grant permission to start a host-required room.
User extension with Can host meetings	Enables hosting eligibility; the user also needs the appropriate room or administrator access.
Administrator without an extension assignment	Existing administrative room access is retained within the administrator company scope.
Administrator with an assigned extension	The assigned extension policy still applies. A restricted or non-user assignment can block hosting.
AI or PA extension	Not an eligible user extension for granting Can host meetings.
Company portal account	Host access also depends on company membership, entitlement, PBX availability and the assigned extension policy where applicable.

Grant access deliberately

1. Confirm the actual account, company and active extension assignments.
2. For a human user extension, choose Can host meetings or Join only according to the agreed role.
3. If the user needs explicit room hosting rights, assign the intended room through its host management control.
4. Verify the effective access from that same account on both PBX and customer workspace where applicable.

If a human administrator is linked to an AI receptionist, correct the account assignment with approval. Do not convert the AI extension into a phone or bypass meeting checks to hide the underlying mismatch. Preserve the AI call route while resolving the user identity.

SECTION 16

Start and share a meeting

Use the customer Meet page for a simple host workflow. The host should have the required account rights, an eligible licence and an online meeting gateway. Guests use the invitation link rather than PBX administration access.

1. Sign in to my.telfron.com with the intended company account and open Telfron Meet.
2. Check that the meeting gateway is online and the intended room is displayed. Refresh status if needed.
3. Select Start Meeting. Review the device choices and enter the display name on the prejoin screen.
4. Join as host. If devices are unavailable, use the supported listen-only option to enter without camera or microphone.
5. Return to the Meet workspace or use the meeting control to copy the intended room link.
6. Share the copied invitation using your usual email or messaging application. For time-limited access, use a secure invitation where configured.
7. When guests arrive, admit them if approval is enabled. Check their audio and video before starting the discussion.

Permanent room link or secure invitation

A permanent link is convenient for recurring communication, but it must be managed through the room access policy. A secure invitation can have an expiry and can be revoked through invitation management. Confirm the displayed expiry rather than assuming it is suitable for every event.

Starting from the PBX

In Conferences, select the intended room. The prejoin screen refreshes current server permission. An authorized host sees Start Meeting. A guest in a host-required room sees Waiting for host until a host is present; the page checks again automatically.

Starting a room and joining its media are separate operations. A copied link alone does not prove that the host has connected. Test the guest path after the host has entered.



AI concept illustration. People, equipment and settings are illustrative.

SECTION 17

Guest admission and host controls

Room access controls determine who may enter and when. Configure them before distributing invitations, then verify the actual guest experience from a separate supported browser or device.

Control	What to verify
Guest access policy	The intended permanent-link or secure-invitation route is allowed.
Host-required entry	A guest waits while no host is present and can proceed when the host arrives.
Host approval	The request appears in People and the host can approve or deny it.
Lock new entry	New guests are blocked as intended while the existing meeting remains usable.
PIN where configured	The guest must satisfy the room PIN policy without learning it from an unauthorized directory response.
End for everyone	The host confirms the action and all participants are disconnected from that meeting session.

During the meeting

Use the microphone, camera, Share, People and Chat controls as available. People provides participant and host actions. Mute all, room locking and ending the meeting are privileged operations. A guest display name must not be used as proof that the person is a host.

Leaving and ending are different

Leave meeting removes your participant. End for everyone is a host action that disconnects the current meeting participants. Use the latter only when the meeting should finish, and check the confirmation before applying it.

A short admission test

1. Open a guest session before the host; confirm the waiting behaviour.
2. Start the meeting with an authorized host and submit a guest request.
3. Deny one request, then submit and approve another test request.
4. Check guest controls, lock entry, leave the guest and end the host test session.

SECTION 18

Meeting connectivity and diagnostics

A successful sign-in or participant tile is only one part of meeting validation. Signalling, permission checks, media transport, device access and playback must all work for a complete meeting experience.

Audio video and screen sharing

- Allow microphone and camera access only for the intended meeting site or application. A phone or PC without a camera can use a supported audio or listen-only mode.
- Use two separate endpoints to test audio in both directions. Check mute, playback output and headset selection.
- Test camera frames in both directions where cameras exist. An avatar or a connection badge is not camera evidence.
- Share a nonsensitive test window, change its content and confirm changing frames at the other endpoint. Then stop sharing.
- Repeat an external-network test. Restrictive NAT or firewalls may require an available media relay.

Symptom	First checks
Waiting for the meeting host	Confirm a host is connected; inspect the same account hosting rights and extension assignments.
Gateway offline or reconnecting	Refresh status; verify the PBX services, outbound connection and licence state.
Connected without sound	Check device permission, mute, playback, audio output and media transport.
No camera picture	Check actual camera availability, camera selection, permission and remote received frames.
Shared window does not move	Confirm the intended source was selected and received frames are updating.
Link opens the wrong place	Check the installed Android version, verified link handling and the fallback route.

A host-required guest conflict is an admission state, not automatically a microphone fault. Permission and navigation tests do not establish large-meeting capacity or media quality; those need their own acceptance evidence.

SECTION 19

Paging and device provisioning



AI concept illustration. People, equipment and settings are illustrative.

Paging sends an announcement to configured endpoints or groups. Intercom and PA roles depend on the device capabilities and the selected call behaviour. Keep these identities separate from user phones and AI receptionist extensions.

Prepare a paging zone

1. Select supported endpoints and confirm their audio, power and network requirements.
2. Create the intended PA or intercom extension role and configure supported paging or auto-answer behaviour.
3. Build a group for the required area, such as a building, floor or warehouse zone.
4. Review who may initiate announcements and which endpoints the group includes.
5. Make an approved test announcement at a suitable time. Check target coverage, intelligibility, call cleanup and the behaviour of unrelated endpoints.

Device provisioning

Use Devices and Provisioning to manage supported devices, configuration profiles and firmware workflows. Confirm the exact manufacturer and model compatibility before generating a profile or initiating an upgrade. Discovery or an inventory row alone does not prove that a device accepted its configuration.

Firmware maintenance

Record the current firmware and configuration, review the supplied image and model match, schedule the maintenance and verify the endpoint after it returns. Preserve customer-specific settings and use the supported rollback route when one exists.

Deployment boundaries

Paging requires actual endpoint support. Ordinary Android devices should not be advertised as unattended PA speakers unless that feature has been implemented and validated for the intended deployment. This guide does not claim that general paging is a certified emergency or life-safety system.

SECTION 20

Security and data handling

Security is a combination of account scope, endpoint configuration, network design and operating practice. Document the protections configured for the customer rather than implying that a feature name establishes certification or regulatory compliance.

Identity and authorization

- Use named accounts and the intended company scope. Review administrator, staff and room-host assignments.
- Keep phone, AI and PA extension roles accurate. Review active extension associations when resolving unexpected access behaviour.
- Protect activation QR codes, meeting capabilities, SIP credentials and remote-session links as access material.
- Use supported session controls and remove obsolete account or device access through the administration workflow.

Data and network controls

- Use trusted HTTPS for browser and portal access. Review SIP and media encryption separately for the carrier and endpoint paths.
- Restrict administration and internal database or cache services to the intended networks and authorized access routes.
- Define who may read recordings, voicemail, messages and knowledge documents. Agree retention and deletion procedures.
- Review cloud and third-party processing for AI, messaging, email and media relay use. Agree the appropriate notices and processing terms.

Evidence and review

Use available audit records, application logs and controlled access tests to verify changes. Keep credentials and personal conversations out of exported diagnostics and public documentation. Check the retention and access controls of backup and diagnostic storage as well as the live application.

Tenant isolation should be verified with accounts from different companies. An administrator should see only the resources allowed by the intended scope. Do not describe a deployment as certified, fully encrypted in every path or fully local without supporting evidence for that specific claim.

SECTION 21

Backups updates and daily operations

Operate the PBX with defined responsibility for availability, storage, backups and controlled updates. Portal online status, local service readiness and end-to-end calling are separate checks.

Daily checks

- Review SIP and application service readiness, carrier status and a sample of endpoint registration.
- Check active incidents, failed automation, messaging connectivity and pending administrative actions.
- Monitor free disk space, recording and voicemail growth, knowledge indexing and backup completion.
- Check the cloud last-seen time when remote administration or Meet depends on it.

Back up for recovery

Back up the database, required configuration, customer media and any other state named by the supported procedure. Protect secrets and define who may restore them. Keep an appropriate copy away from the live server and test restoration in a controlled environment. A backup job reporting success is not proof that recovery works.

Apply a controlled update

1. Confirm package source, version, verification status and the applicable release notes.
2. Verify sufficient space and a usable backup. Preserve the existing installation path and customer-specific configuration.
3. Schedule the change when calls, conferences, paging and relevant background work are idle.
4. Apply the supported upgrade or repair procedure and check service readiness.
5. Test calling and the customer critical workflows, then record the result and rollback location.

PBX services, web assets, central portal and Android applications can have different update paths. Record the versions actually deployed instead of assuming that a single installer includes every later web or mobile update.

SECTION 22

Licensing and capability scope

Use the active signed licence and its effective feature flags as the authority for a customer installation. The published catalogue below is a baseline checked on 20 October 2026. Administrator overrides, existing licence terms and custom contracts can change the effective entitlement.

Plan	Calling and meetings	AI mobile and branch access
Free	Core calling. Call queues, recording and video Meet disabled.	AI, WhatsApp, mobile app access and multi-site disabled.
Basic	Call queues, recording, reporting and video Meet enabled.	AI, WhatsApp, mobile app access and multi-site disabled.
Professional	Call queues, recording, reporting and video Meet enabled.	AI, WhatsApp, mobile app access and multi-site enabled.
Education AI	Call queues, recording, reporting and video Meet enabled.	AI, WhatsApp, mobile app access and multi-site enabled.
Enterprise AI	Call queues, recording, reporting and video Meet enabled.	AI, WhatsApp, mobile app access and multi-site enabled.

Check limits and permissions separately

A feature entitlement does not assign staff permission. Meet hosts still need the correct company, user-extension and room rights, plus an online gateway. Android access needs an eligible extension and compatible device. Company creation needs an available licensed company slot as well as sufficient users, extensions and concurrent-call allocations.

AI allowance and additional usage

Eligible plans include monthly AI credits that reset each calendar month. Confirm the configured allowance and eligible services; Free and Basic have none by default. Included credits do not accumulate. Purchased credits are separate, and automatic paid top-up is currently unavailable. Additional provider charges depend on the service configuration.

Confirm module specific availability

Hotel tools require a confirmed hotel entitlement. The current PBX interface uses an Enterprise-level access rule; verify the activated licence before committing hotel functionality. Social Publishing currently sits within the WhatsApp workspace, while paging uses contact-centre access in the PBX interface. Confirm these access dependencies, supported devices and connected accounts for the deployment.

Licence lifecycle and commercial scope

Record the installation activation, licence expiry, validation state and configured offline allowance. Local operation is subject to the signed entitlement and applicable grace policy. Keep licence fees separate from carrier calls, hardware, connectivity, additional AI usage and agreed support services. Confirm renewal terms and support commitments in the customer agreement.

[Published licensing catalogue](#)

Published package names and defaults are a reference, not a replacement for the entitlement issued to an individual installation. Custom plans and overrides require explicit confirmation.

SECTION 23

Acceptance and handover

Accept the deployment using the same accounts, devices and networks the customer will use. Record the expected outcome, actual result and responsible owner for each check. Resolve failed critical checks before enabling the affected production workflow.

Area	Required evidence
Calling	Incoming and outgoing calls, correct routing and caller ID, two-way audio and fallback paths.
Reception	Hold, resume, transfer, queue or group behaviour, voicemail and authorized recording access.
Company boundaries	Correct company identity, allocation and cross-company access checks.
Branches	Saved site details, endpoint association and actual branch calling or media checks.
AI and WhatsApp	Approved answers, unknown enquiry, staff handoff, failed-provider fallback and message handling.
Social Publishing	Approved test publication, scheduled time, target account and reported status.
Hotel	Room endpoint, wake-up outcome, service request, housekeeping status and call record.
Paging	Authorized source, selected zone, received announcement and call cleanup.
Meet	Host and Join-only access, waiting, approval and denial, chat, two-way media and changing screen-share frames.
Android	Activation identity, permission display, incoming and locked-screen calls, network change and link handling.
Operations	Backup and restore evidence, monitoring ownership, update plan and support escalation.

Handover package

Provide the approved architecture, inventory, call-flow plan, company and site allocation record, access responsibilities, acceptance results, backup procedure and support route. Keep credentials in the agreed secret store. Set an owner and review date for changes to AI knowledge and business hours.

Documentation and support

docs.telfron.com - product walkthroughs and administration guidance.

my.telfron.com - customer workspace and connected installation management.

support@telfron.com - deployment and support enquiries.

Tenant means a company scope. Site means a location within a company. SIP handles call signalling; RTP carries telephony media. A meeting host manages room access; a Join-only participant enters subject to that room policy.