CallWrapUp Complete Setup Guide

The Official launch manual for agents, managers/admins, and IT

Start with the quick path, then use the screenshot walkthroughs whenever a user gets stuck. Built for clean installation, exact team setup, BYO AI configuration, Manager QA, seat control, and confident first-day rollout.

Fast launch path

Step 1: Install on the real workstation. Step 2: Claim Agent or Manager seat. Step 3: Enter Team / Workgroup ID. Step 4: Validate license. Step 5: Connect approved AI provider. Step 6: Generate a sample wrap. Step 7: Managers/Admins: save team config and run a QA test.

Version 1.1 Managed Desktop Launch Guide

How to Use This Guide

This guide has two layers. The quick path helps a new workstation get running fast. The deeper walkthrough explains every major screen so an agent, manager, admin, or IT lead can recover without guessing.

Setup reminder: The license controls access, the AI key powers generation, and the Team / Workgroup ID keeps each device aligned with the correct team configuration.

Fast path for a first workstation

- Install CallWrapUp from the official installer.
- Choose Agent Seat or Manager Seat during first launch.
- Enter the correct Team / Workgroup ID exactly.
- Validate the license and confirm the role is correct.
- Add the approved AI provider details and run Test configuration.
- Generate one sample wrap and copy it into the ticketing workflow.
- Confirm the generated wrap includes Summary, Key Issue, Resolution, Action Items, and Priority status (Unless using custom format)
- Use Clear after the test wrap & move on to the next call.
- Confirm the device name is readable for Admin seat tracking later.
- Ask the setup owner to verify the workstation appears under the correct seat/team.

Deep path for managers/admins

- Save the Team / Workgroup ID exactly as shown.
- Name devices clearly so seat usage is easy to audit.
- Configure output formatting, writing style, and policy routing.
- Set PIN/recovery controls before exposing Admin features widely.
- Use Manager QA, Enterprise QA Signals, and ROI reporting for proof of value.
- Keep at least two manager/admin devices active or vault recovery codes.
- Import or confirm policy packs before using QA grading for live coaching.
- Review Seat Device Management to confirm no stale or incorrect devices are occupying seats.
- Confirm Billing & Subscriptions is protected behind Admin access.
- Recommend Exporting one sample QA report and one ROI report so leadership reporting is ready before launch.

Table of Contents

Tip: Agents usually need Sections 1-7 and 23. Managers/Admins should review Sections 8-22 before rollout.

1. Before You Install

Do this before opening the installer. A clean setup is faster than a heroic rescue mission later.

You need	Why it matters	Who usually owns it
Windows 10 or Windows 11 workstation	Install on the device the agent, manager, or admin will actually use.	Agent, Manager, or IT
CallWrapUp license key	Unlocks the purchased role, plan, and seat limits.	Purchasing owner or Admin
Team / Workgroup ID	Connects devices to the correct team config and reporting scope. Use the same spelling across devices.	Manager or Admin
AI API key and provider details	Powers wrap generation and QA output. CallWrapUp does not include bundled AI credits.	IT or AI platform owner
Sample transcript	Lets the user test generation immediately after configuration.	Manager, QA lead, or Agent
Password vault / credential store	Stores recovery codes, API keys, and setup records safely.	IT or Admin

Recommended naming convention: Use names authorized users can understand later. Example: Austin Support - Agent01 - Win11, Billing Team - Manager01, or Healthcare QA - Admin Laptop. Avoid unknown device names like DESKTOP-7F9X unless IT requires them.

2. Install the Software

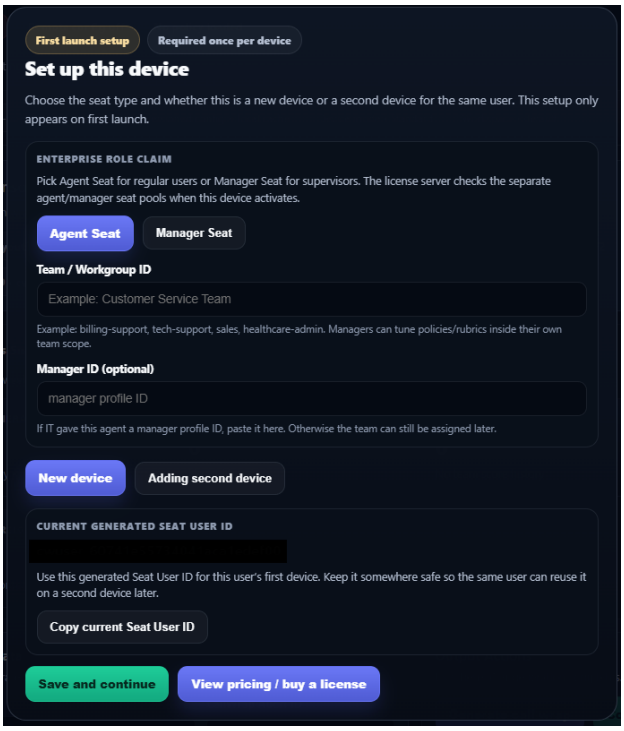
1. Download the official CallWrapUp installer from the approved website or company software portal.
2. Double-click the installer file. If Windows asks for permission, choose Yes.
3. Continue through the installer prompts. Keep the default install path unless IT has a required custom location.
4. When installation finishes, launch CallWrapUp from the Start Menu or desktop shortcut.
5. Do not copy the app folder from another workstation. Each device needs its own seat claim and local setup.

Installer checks:

- Confirm the installer came from the official source or approved company software portal.
- If Windows SmartScreen or security tooling appears, verify the source before continuing.
- Install on the device that will actually use the seat. Do not install on a shared staging device unless that is your intended seat claim.
- Have the license key, Team / Workgroup ID, and AI provider details ready before first launch.

Install tip: To avoid setup delays, gather the license key, Team / Workgroup ID, and approved AI provider details before launching CallWrapUp for the first time..

3. First Launch Role Claim



First-launch setup screen: role claim, Team / Workgroup ID, Manager ID, and generated Seat User ID.

What this screen is doing

1. Choose Agent Seat for a standard user who will paste transcripts and generate wrap notes.
2. Choose Manager Seat for a supervisor/admin who needs QA, team reporting, policy, billing, or admin controls.
3. Enter the Team / Workgroup ID exactly. Uppercase letters, spaces, hyphens, and underscores are accepted.
4. For a first manager/admin device, create the Team / Workgroup ID here and store it in your onboarding record.
5. Copy the generated Seat User ID if your organization tracks second devices or needs a restoration record.
6. Select Save and continue only after the role and team are correct. This setup appears on first launch for that device.

Avoid this mistake: do not create a slightly different team name on another device. Customer Service Team, customerserviceteam, and Customer_Service_Team can behave like different identifiers depending on where they are used.

4. Agent Setup Walkthrough

Agents should have the simplest path: claim the right seat, validate license, connect to managed config, paste transcript, generate, copy, clear.

1. On the first-launch setup screen, select Agent Seat.
2. Type the exact Team / Workgroup ID provided by the manager or admin.
3. Leave Manager ID blank unless your organization specifically uses it for routing.
4. Continue to license validation and enter the license tied to the Agent seat pool.
5. After setup, confirm the Agent tab is visible and Manager/Admin tools are hidden or restricted if kiosk mode is enabled.
6. Paste a sample transcript into the transcript box, click Generate, review the wrap, then click Copy.
7. Use Clear after copying if the organization wants the workstation clean between tickets.

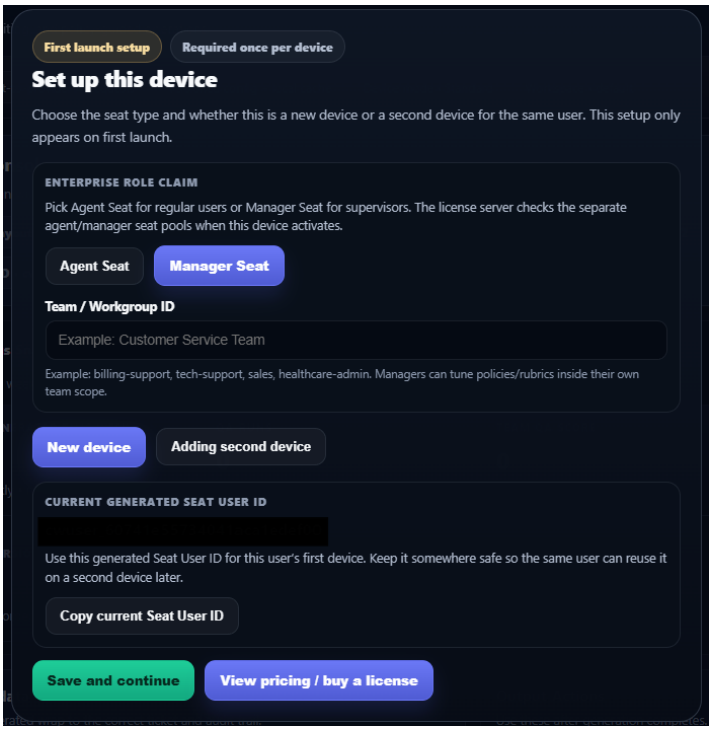
Agent should see

- Agent tab with transcript input.
- Generate, Copy, and Clear controls.
- Seat/device status and config version if enabled.
- Output in the format selected by management.

Agent should not need

- Billing portal access.
- Policy library editing.
- QA grading controls.
- Admin device removal tools.

5. Manager/Admin First Device Setup

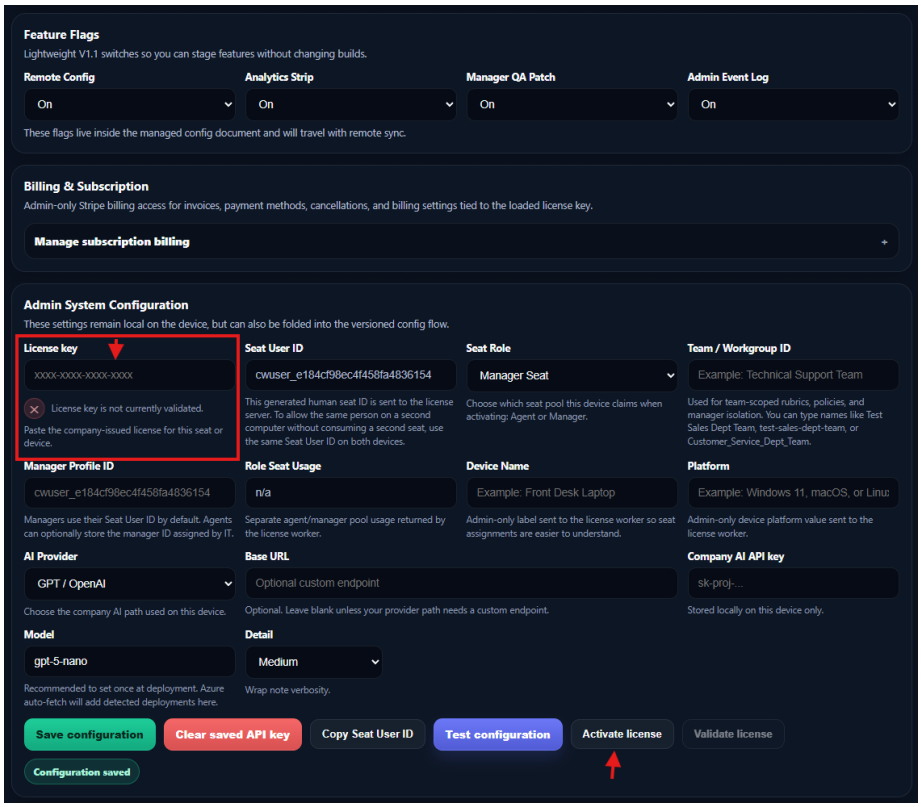


Role claim screen with Manager Seat selected: use this for the first supervisor/admin workstation.

1. Select Manager Seat when the user needs supervisor, QA, reporting, policy, billing, or admin rights.
2. Create or enter the official Team / Workgroup ID. This becomes the team anchor for managed configuration.
3. Copy the current Seat User ID and store it in a secure admin onboarding note.
4. Click Save and continue to proceed to license activation.
5. After activation, open Admin and set device name, platform, provider, and sync behavior.
6. For a second manager device, use the existing Team / Workgroup ID and the correct license/seat pool. Store recovery details in an approved vault.

Best practice: Keep at least two Manager/Admin devices active. If one authorized device loses access, another authorized device can remove, restore, or reassign seats without interrupting team operations.

6. License Activation

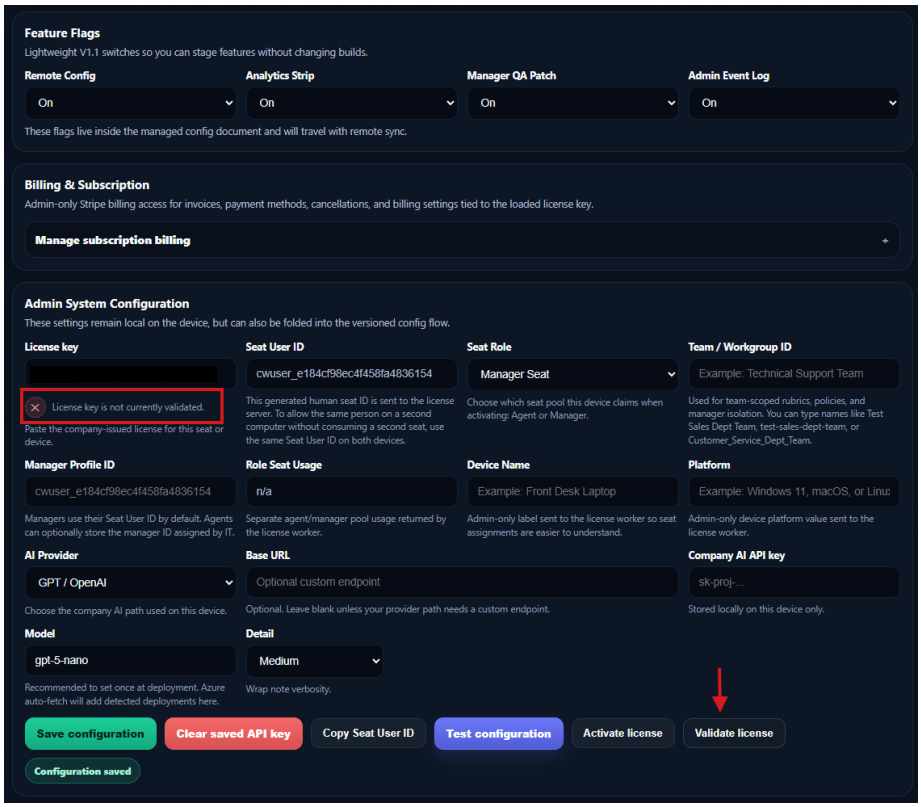


Admin system configuration area: license key, seat role, team/workgroup, device info, and validation controls.

1. Paste the license key exactly as received. Avoid extra spaces before or after the key.
2. Confirm the Seat Role matches the user type: Agent Seat or Manager Seat.
3. Confirm Team / Workgroup ID matches the first-launch team name.
4. Enter a clear Device Name and confirm platform is correct, such as Windows 10 or Windows 11.
5. Select Validate license and wait for success.
6. If validation fails, check internet access, spelling, role mismatch, expired/cancelled status, or whether the device was removed by an admin.

License controls	License does not do this
Unlock roles and seat limits. Validate subscription status. Bind device to the correct team. Keep cancelled or expired access from remaining active.	It does not generate AI output by itself. It does not replace your AI provider key. It does not include bundled AI usage credits. It does not override internal company policy.

7. AI Provider and API Key Setup



Provider setup: choose provider, model, API key, and run the connection test before saving.

1. Open the Admin provider/settings area.
2. Choose the approved AI provider: OpenAI, Google Gemini, Azure OpenAI, Anthropic Claude, or Custom provider if your organization has a private endpoint.
3. Paste the API key or endpoint details exactly as provided by IT or the AI platform owner.
4. Select the model your organization has approved and your AI account can access.
5. Click Test configuration. A successful test means provider, key, model, and network access are working together.
6. Click Save Configuration or Save Full Config after the test passes.

Setup note: The license activates the software, while the API key enables AI-powered wrap generation and QA output. Both are required for CallWrapUp to function properly.

8. Provider Verification and Safe BYO AI Notes

Use this page as the provider check instead of leaving the provider table stranded on its own. Before testing, confirm that the provider account, model, and network path are all valid.

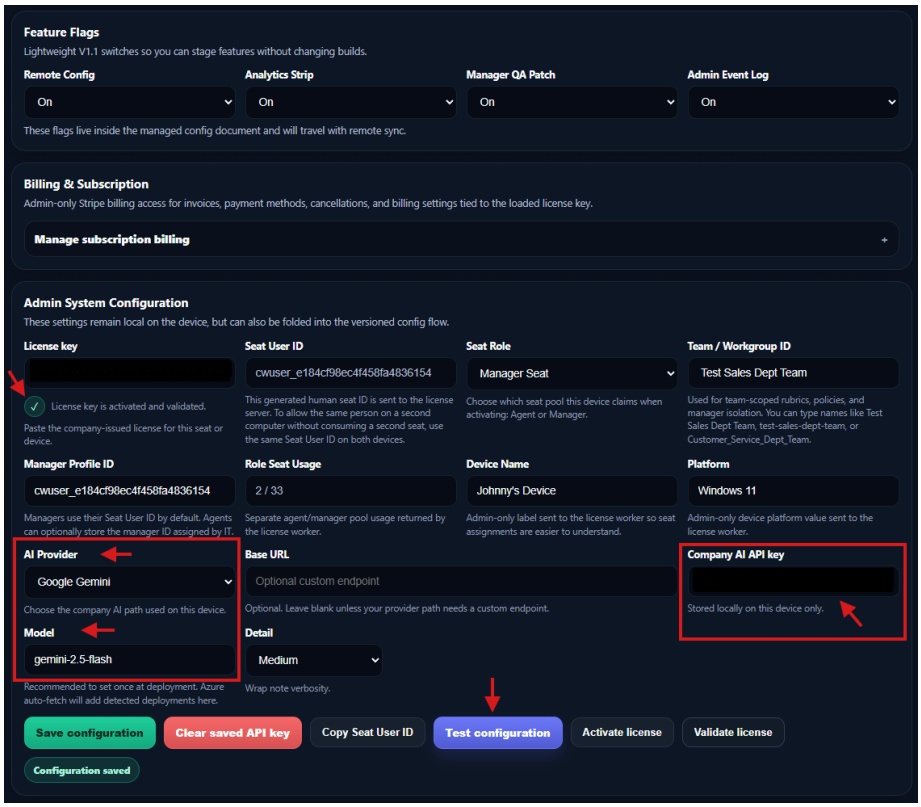
Provider	What to check before testing
OpenAI	API key is active, billing/usage is enabled, and the selected model is available to the account.
Google Gemini	Gemini/Google AI key is active and the selected model is allowed on the account.
Azure OpenAI	Endpoint, deployment name, API version, and key are correct. Deployment name is not always the same as model name.
Anthropic Claude	API key is active, selected Claude model is available, and organization policy allows usage.
Custom provider	Base URL, headers, routing path, authentication, and model field match the internal endpoint requirements.

Approved BYO AI Setup Notes

- Only use organization-authorized AI keys. Do not use personal keys for company data unless policy allows it.
- Confirm whether transcripts may be sent to the selected provider under your organization’s data policy.
- If the provider test passes but output still fails, check model access, rate limits, organization restrictions, and endpoint formatting.
- If secure local storage is unavailable on a workstation, follow your organization’s approved device-security process before launch.

Launch validation: A successful provider test confirms that the AI connection is working. Before sending the setup to live users, generate one sample wrap, run one sample QA audit if applicable, and confirm the output meets your organization’s quality expectations.

9. Admin System Configuration

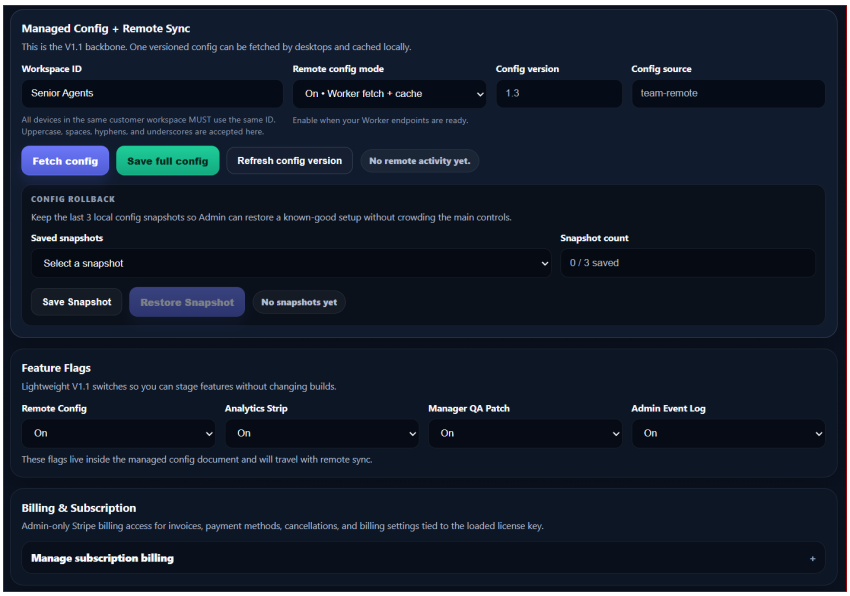


Admin configuration view: provider, model, team ID, device, company AI key, billing, and feature flags.

1. Use Team / Workgroup ID as the main team identifier for role, policy, QA, and managed configuration behavior. This ID MUST be the same for all workstations, in order for proper teams to be connected/seperate team connections to avoid mix up)
2. Use Device Name to make seat/device management readable later.
3. Use Company AI key only for organization-approved AI credentials.
4. Use Test configuration before saving so the workstation does not look ready while the provider is actually failing.
5. Use Save Configuration for local/admin changes and Save Full Config when you want the managed setup stored for team sync.
6. Use Fetch Config on other devices to pull the latest managed settings.

Final check on this screen: Confirm the license is valid, the role is correct, the team is correct, the provider is correct, the model is selected, the connection test passed, and the configuration has been saved.

10. Managed Config + Remote Sync



Managed Config + Remote Sync, local snapshots, feature flags, and billing area.

1. Set the Workspace ID for the customer workspace. All devices in the same customer workspace should use the same ID.
2. Enable remote config when you want desktops to fetch the latest team settings from the license/config backend.
3. Use Fetch Config to pull the current version onto a device.
4. Use Save Full Config to publish the current admin configuration for the team/workspace.
5. Use local snapshots before major changes so you can roll back if a template or policy experiment goes sideways.
6. Keep feature flags staged and deliberate. They travel inside managed config, so a small switch can become team-wide.

Control	Use it when	Success looks like
Fetch Config	A device needs the latest team settings.	Config version updates and settings match admin setup.
Save Full Config	Admin wants to publish provider/output/policy/sync settings.	Team devices can fetch the new config version.
Save Snapshot	Before changing templates, policies, provider, or feature flags.	Snapshot appears in rollback list, up to the local limit.
Restore Snapshot	A change broke output quality or workflow.	Known-good local configuration is restored.

11. Billing and Seat Changes

Billing & Subscriptions should stay behind Admin access. It controls invoices, payment methods, cancellations, billing settings, and seat upgrades or downgrades tied to the loaded license key.

1. Open Admin > Billing & Subscriptions.
2. Use Manage billing / invoices for Stripe portal tasks: invoices, payment methods, cancellations, and billing details.
3. Use the seat upgrade checkout only when adding Agent or Manager seats.
4. Before removing paid seats, remove unused devices first so the available seat count is truly free.
5. Confirm which team/workgroup added seats should apply to, especially on Enterprise plans.
6. After checkout or portal changes, validate the license again or fetch config so the app reflects the latest plan state.

Use billing portal for

- Invoices and receipts.
- Payment method updates.
- Cancellation settings.
- Billing profile details.

Use seat checkout for

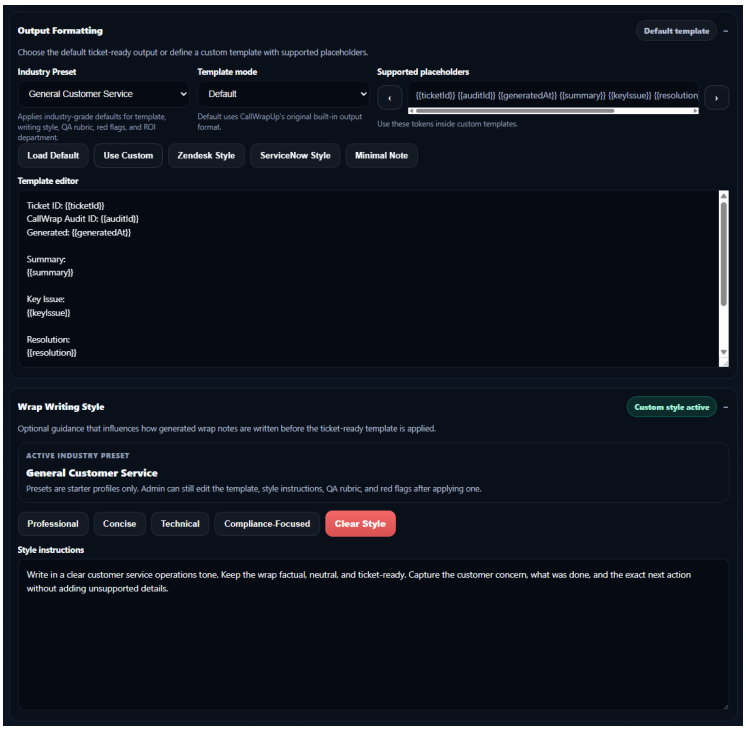
- Adding Agent seats.
- Adding Manager seats.
- Applying seats to the same license/team.
- Updating subscription quantity through checkout.

Seat removal rule: A seat that is still occupied by a device cannot be cleanly removed. Remove or restore devices first, then reduce unused seats.

Seat change examples

Scenario	Correct action
Adding two agents	Use seat upgrade checkout, select Agent seats, then apply to the correct team/workgroup.
Removing one unused manager seat	Confirm no device occupies that manager seat, remove stale devices if needed, then reduce unused seat quantity.
Invoice or card update only	Use Manage billing / invoices. Do not use seat checkout.

12. Output Formatting + Wrap Writing Style



Output Formatting and Wrap Writing Style: industry presets, template mode, supported placeholders, and style controls.

1. Choose the Industry Preset closest to the workflow: Customer Service, Technical Support, Finance Support, Healthcare Administration, Sales, or Custom where available.
2. Leave Template Mode on Default for the built-in CallWrapUp output structure.
3. Use Custom mode only when management wants internal wording, special section names, or enterprise-specific wrap structure.
4. When editing custom templates, keep supported placeholder tokens in the template so generated content lands in the correct place.
5. Choose a Wrap Writing Style such as Professional, Concise, Technical, or Compliance-Focused.
6. Save the config and test one transcript before rolling the new format to the whole team.

Output quality tip: Generic summaries are easy. Consistent operational wraps come from a complete transcript, the right model, the right template, and a writing style that matches the department.

13. Template Quality Gate

Use this page before publishing a custom template. A template can look polished and still create bad notes if the placeholders are missing or the wording encourages guessing.

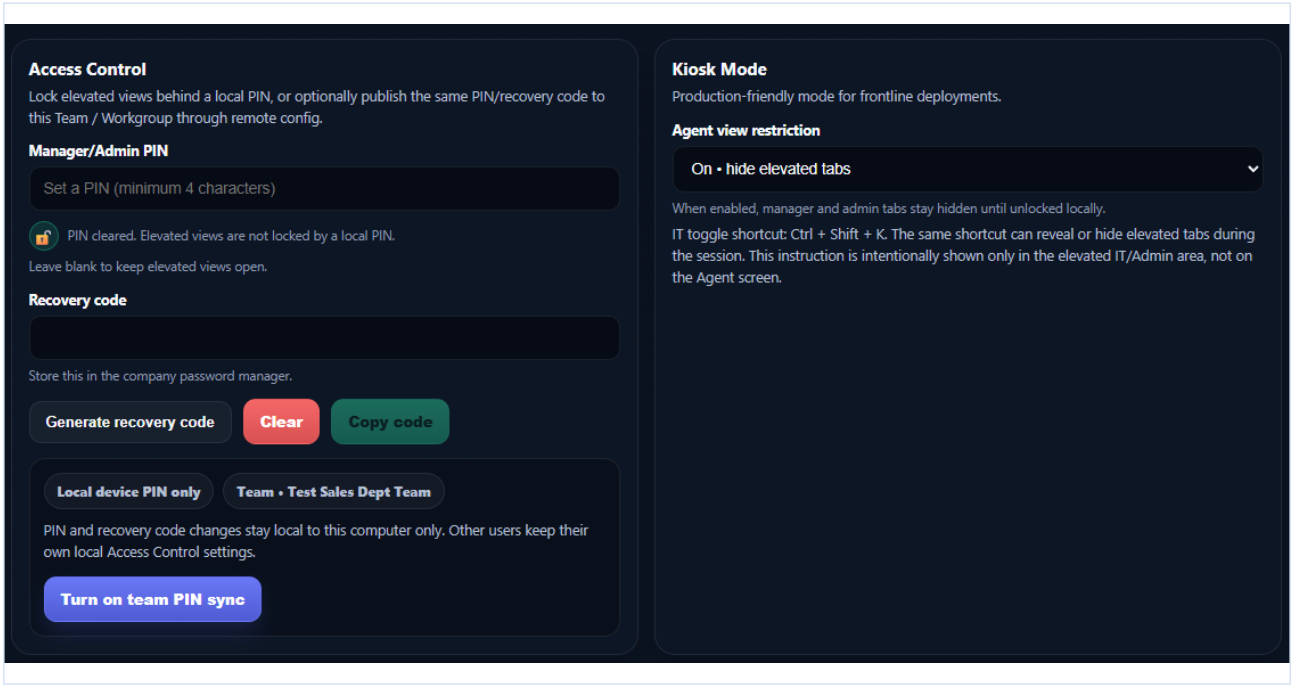
Check	What to verify	Why it matters
Placeholders	Supported placeholder tokens remain in the template.	The generated content lands in the correct sections.
Outcome language	Template allows resolved, unresolved, escalated, pending callback, or customer follow-up outcomes.	Prevents false resolution wording.
Action items	Template asks for specific next steps and responsible party when available.	Makes the wrap useful after the call ends.
Risk wording	Compliance or escalation language does not claim approval unless the transcript supports it.	Protects manager QA and audit integrity.
Test transcript	Run one clean transcript and one messy transcript before publishing.	Confirms output works under real-world conditions.

Recommended first template test

1. Use a transcript with a clear issue, troubleshooting steps, and final outcome.
2. Generate the wrap with the new template.
3. Check Summary, Key Issue, Resolution, Action Items, and Priority.
4. Run a QA audit against the generated wrap if Manager tools are active.
5. Adjust template wording only after reviewing evidence, not after one unusual transcript.

If the output sounds too short, then it is recommended to Check transcript details, model strength, writing style, and template wording first.

14. Access Control + Kiosk Mode



Access Control and Kiosk Mode: manager/admin PIN, recovery code, tab visibility, and role lock behavior.

1. Set a Manager/Admin PIN if elevated settings should be protected on the workstation.
2. Generate a recovery code immediately after setting a PIN.
3. Store recovery codes in an approved password manager or IT credential vault.
4. Enable Team PIN sync only when you want the team to inherit the same elevated-access restriction.
5. Use Kiosk Mode to hide Manager/Admin tabs on Agent workstations.
6. Use the IT shortcut CTRL + SHIFT + K only for authorized show/hide review of restricted tabs.

Safe setup

- PIN created and tested.
- Recovery code generated.
- Recovery code stored outside the app.
- At least two manager/admin devices active.

Risky setup

- PIN created but no recovery code saved.
- Only one manager device exists.
- Admin tab exposed on agent computers.
- Recovery code stored in the same unsafe location as the device.

15. PIN and Recovery Code Responsibility

This section was restored and expanded because it belongs in the guide. PIN and recovery-code handling is not just a convenience item. It is the emergency keyring for Manager and Admin access.

Normal recovery path

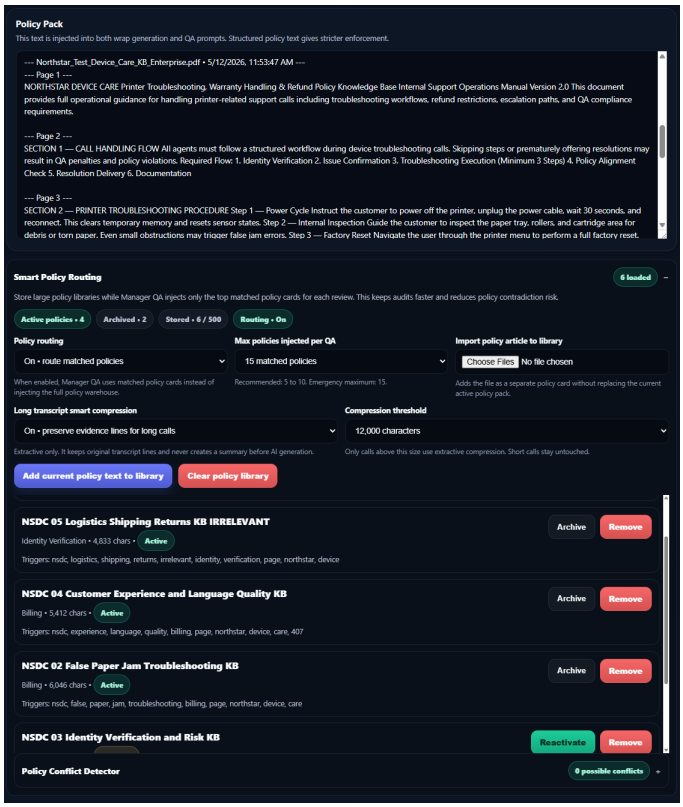
1. If a manager forgets the PIN, use the saved recovery code to regain elevated access.
2. After access is restored, set a new PIN if needed and generate a new recovery code.
3. Store the new recovery code in the approved vault and remove the old recovery note from circulation.
4. Confirm at least one other Manager/Admin device remains active.

If the PIN and recovery code are both lost

1. Use another active Manager/Admin device to open Admin > Seat Device Management.
2. Remove or replace the affected device so it returns to setup on the next validation/sync check.
3. Reinstall or reauthorize the workstation under the correct Manager seat if needed.
4. If no active Manager/Admin device remains and no recovery code exists, the organization may need to add a temporary Manager seat or request a paid recovery setup option.
5. Temporary recovery seats and recovery setup charges should be treated as non-refundable administrative recovery work unless your billing policy says otherwise.

Best practice: Keep at least two Manager/Admin devices active or store recovery codes in an IT-approved password vault. A single locked manager laptop should never become the whole primary device.

16. Policy Pack + Smart Policy Routing



Policy Pack and Smart Policy Routing: active policy cards, confidence thresholds, routing controls, and policy library actions.

1. Import policy articles as text-based PDF, TXT, MD, or JSON when possible.
2. Use manual import when online URL fetching is blocked by CORS or organization security controls.
3. Keep policy routing enabled so the Manager tab can match the best policy cards instead of dumping the entire library into every audit.
4. Set max policies to a practical range, commonly 5 to 15, to balance accuracy and speed.
5. Use the Policy Conflict Detector to catch mismatched verification windows, escalation rules, or contradictory policy language.
6. Archive policies that should not be active, instead of deleting useful historical material too quickly.
7. Keep long transcript smart compression enabled for large transcripts so QA remains usable without losing original transcript structure.

Policy Hygiene Rule: Do not upload ten versions of the same procedure as a conflict detector will start notifying you of possible conflicts being detected in your procedures. Keep one approved version active whenever possible.

17. Policy Hygiene + Smart Compression

This page expands the policy section so admins know what to do before importing a large library. Policy routing is powerful, but clean input wins battles quietly.

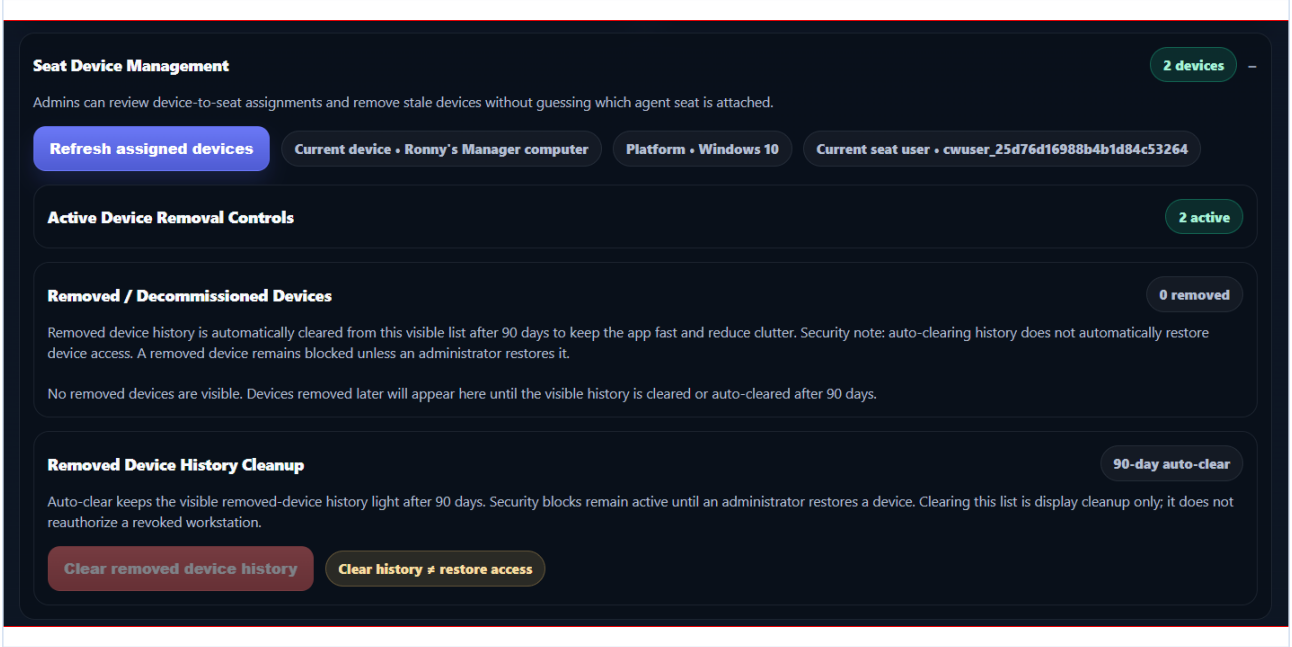
Admin task	Recommended action
Before importing policies	Remove duplicates, outdated articles, and drafts that should not influence QA.
When a policy changes	Archive the old version or clearly mark it inactive before adding the replacement.
When audits feel slow	Reduce max routed policies, archive duplicates, and keep smart compression enabled.
When QA flags contradictions	Review conflicting policy cards first. The issue may be the knowledge base, not the agent.
When URL import fails	Use manual import with text-based PDF, TXT, MD, or JSON. CORS/security controls commonly block URL fetching.

Long transcript smart compression

- Keep it enabled for large call/chat/email transcripts.
- It helps preserve the original transcript structure instead of forcing a pre-summary before AI generation.
- Use the compression threshold based on the expected transcript size, commonly in the 8,000 to 22,000 character range when your setup supports it.
- For very large transcripts, Smart Policy Routing is usually faster and cleaner than sending every policy into every QA run.

Manager expectation: A long transcript plus a large policy library may take longer. That is normal. Use routing, sensible policy limits, and clean policy data to keep QA practical.

18. Seat Device Management



Seat Device Management: active seats, removed devices, restore controls, and history cleanup.

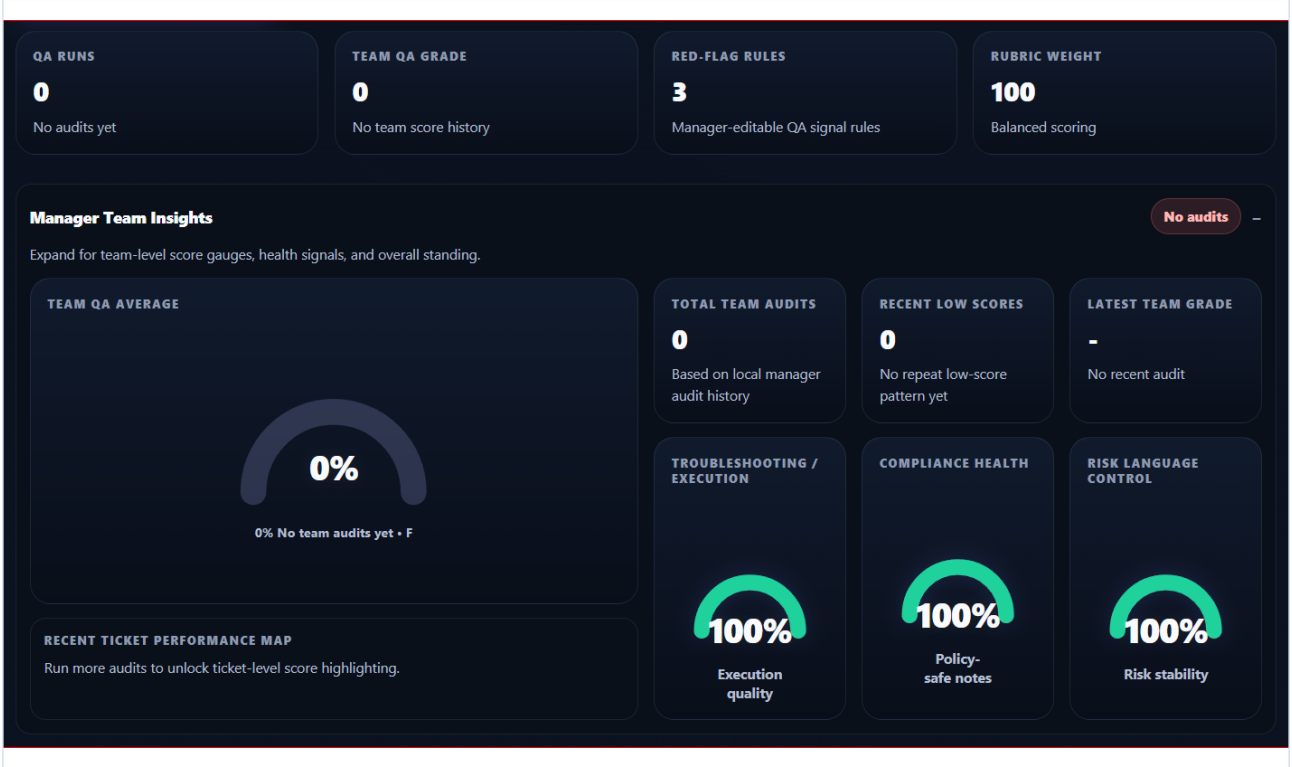
1. Open Admin > Seat Device Management to see which devices are occupying purchased seats.
2. Use clear device names to identify who owns each workstation.
3. Remove stale or incorrect devices to free a seat.
4. Understand that removing a device revokes that workstation until an admin restores or re-adds it.
5. Use removed device history for audit visibility, but remember clearing the list is display cleanup only.
6. Security blocks remain active until the device is restored or properly reauthorized.

Important: Please note that removing a device is not for cosmetic purposes. The removed app should return to setup on its next validation/sync check. This is the correct behavior.

Before removing a device

- Confirm the user no longer needs access on that workstation.
- Confirm whether it is an Agent or Manager seat. Do not remove the wrong elevated device during a recovery situation.
- Copy or record the device name, seat user ID, and reason for removal if your organization tracks audit history.

19. Manager Team Insights



Manager Team Insights: audit volume, score gauges, risk language control, compliance health, and coaching patterns.

1. Open the Manager tab after the team has generated wraps or QA audits.
2. Review total audits, latest score, low/high score movement, troubleshooting quality, compliance health, and risk language control.
3. Use recent audit trend patterns to identify repeated weak spots.
4. Use coaching recommendations as a starting point, not as a replacement for supervisor judgment.
5. Export QA or ROI reports when leadership needs a clean performance story.
6. Refresh or fetch config when team names, role scope, or latest activity appears outdated.

Manager rhythm: Use Team Insights for patterns, Audit Intake for evidence, Enterprise QA Signals for risk, and Coaching Recommendations for action.

20. Enterprise Team Scope + ROI Ledger

Enterprise Team Scope and the Real-Time Usage & Savings Ledger help managers verify the team they are looking at and translate usage into leadership-friendly value.

Enterprise Team Scope

- Confirms the current role claim, Team / Workgroup ID, workspace scope, manager profile, and team members returned by the license backend.
- Shows how agent activity contributes to team usage, coaching visibility, and operational reporting.
- If team members look incorrect, validate the license, confirm Team / Workgroup ID spelling, fetch config, and verify the seat belongs to the right license/team.

Operational Value / ROI Report

- Shows wraps generated, estimated time saved, labor-value assumptions, and productivity impact.
- Use the CFO/ROI export when leadership wants proof of saved time and labor value, not just a screenshot.
- Treat ROI as a transparent estimate based on configured assumptions. Keep assumptions realistic for the department.

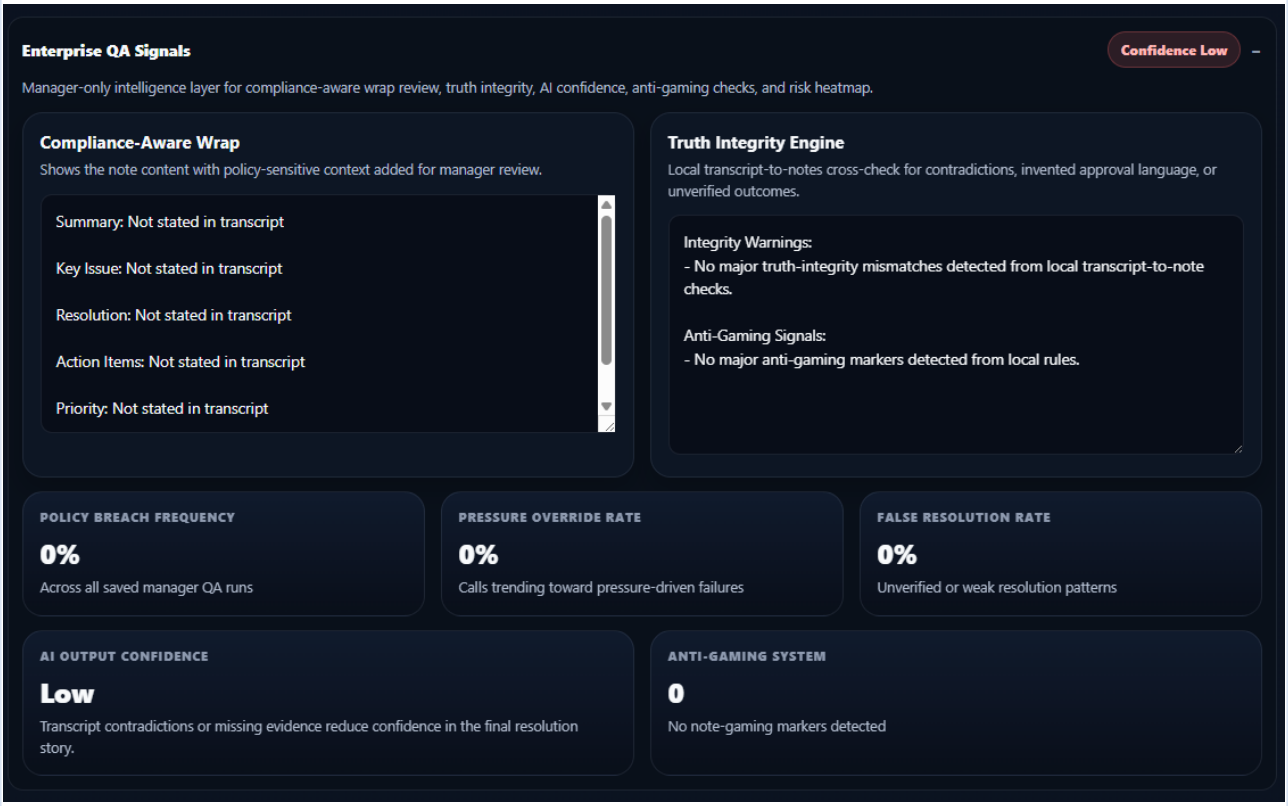
Signal	Manager use
Wraps generated	Shows adoption and repeated value.
Time saved	Connects faster wrap completion to operational efficiency.
Labor value	Gives leadership a dollar-value story using transparent assumptions.
QA health	Pairs productivity with quality instead of speed alone.
Risk visibility	Shows where coaching, policy clarity, or escalation behavior needs attention.

Leadership angle: CallWrapUp connects frontline efficiency to leadership visibility. Faster wraps reduce after-call work, QA signals reveal process gaps, ROI reporting shows measurable value, and managers gain evidence before coaching decisions are made.

Enterprise config deployment note

When managers modify Manager Red Flag Risk rules or the QA Rubric Editor, use this safe deployment path:
1. In Enterprise Team Scope, select Save Team Config, then Load Team Config first.
2. Open the Admin tab and confirm the changes appear under QA Rubric + Red-Flag Governance.
3. If everything looks correct, select Save Full Config to save/confirm the managed configuration.
4. Give the sync a little time to deploy and reflect across the team's agent devices.
To make another change later, repeat these same steps before publishing again.

21. Enterprise QA Signals

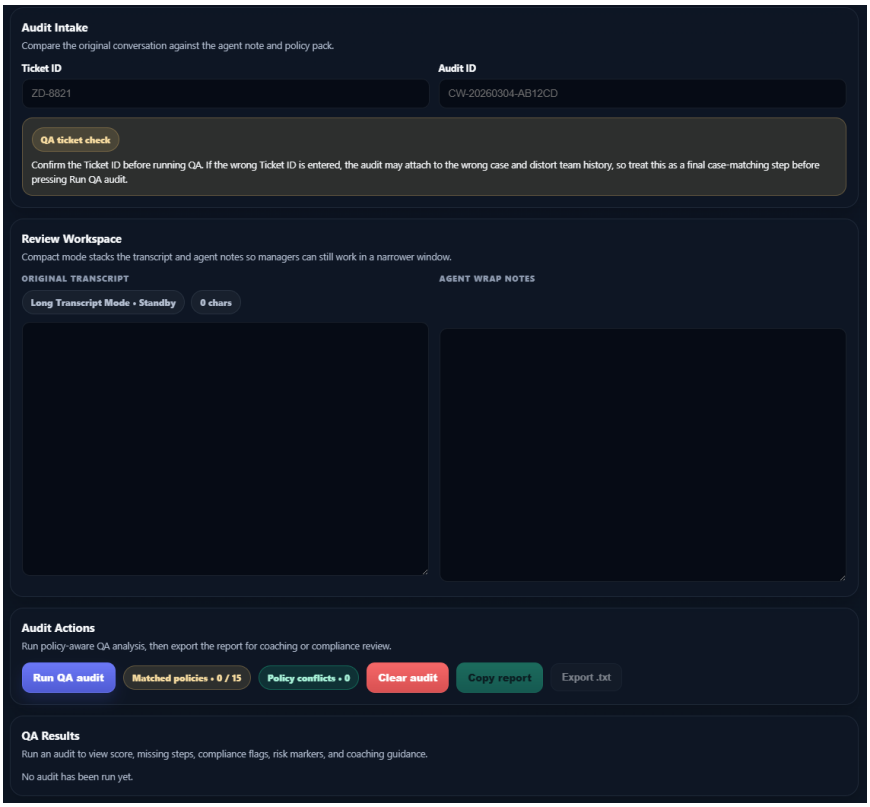


Enterprise QA Signals: compliance-aware wrap review, truth integrity, confidence level, and risk indicators.

1. Use Enterprise QA Signals after a QA audit or when reviewing sensitive wrap output.
2. Read the Compliance-Aware Wrap to see how the note behaves with policy-sensitive context.
3. Check the Truth Integrity Engine for contradictions, invented approval language, or unverified outcomes.
4. Review Policy Breach Frequency, Pressure Override Rate, False Resolution Rate, and AI Output Confidence.
5. Treat low confidence or risk flags as review prompts. They do not automatically mean an agent acted in bad faith.
6. Use findings to improve training, templates, policy clarity, or escalation behavior.

Why this matters: CallWrapUp helps managers compare final wrap notes against the original transcript, making it easier to confirm accuracy, identify unsupported claims, and strengthen QA review quality.

22. Audit Intake + QA Grading



Audit Intake and QA Review workspace: ticket ID, generated wrap, original transcript, audit actions, and QA result area.

1. Enter the ticket ID so the audit can be connected to your internal record.
2. Paste the agent-generated wrap into the wrap review area.
3. Paste the original transcript into the transcript review area.
4. Click Run QA audit to grade the wrap against the active rubric, policy pack, and safety rails.
5. Review the score, findings, risk flags, and coaching recommendations.
6. Export the audit report if your organization stores QA records externally.
7. Click Clear audit before starting the next review.

Speed tip: Large transcripts plus large policy libraries at times take longer. Smart Policy Routing helps keep QA targeted by selecting the most relevant policies instead of forcing the full library into every review.

23. Agent Daily Workflow

This is the daily copy-paste path agents should remember. It is intentionally simple.

1. Copy the customer interaction transcript from your approved platform.
2. Paste it into the CallWrapUp transcript box.
3. Confirm the ticket ID or reference is present when your workflow requires it.
4. Click Generate and keep the window open while CallWrapUp works.
5. Review the generated Summary, Key Issue, Resolution, Action Items, and Priority.
6. Click Copy and paste the result into the ticketing/CRM system.
7. Click Clear after the note is saved if your organization requires clean workstation handling.

Good transcript input	Weak transcript input
Includes customer issue, troubleshooting steps, customer responses, result, and next action.	Only says "customer called about printer" with no steps or outcome.
Keeps the actual call/chat/email content intact.	Contains mostly browser chrome, menus, or irrelevant page text.
Includes resolution status: resolved, unresolved, escalated, pending callback, or customer follow-up.	Leaves the outcome unclear and forces the AI to guess.

Agent standard: Paste the customer interaction, troubleshooting steps, outcome, and next action whenever available. Avoid unrelated browser text or system clutter so CallWrapUp can generate a cleaner, more accurate wrap note.

24. Manager Weekly Workflow

1. Fetch the latest team config so the Manager tab is aligned with admin settings.
2. Run a small QA sample across different agents and issue types.
3. Review Enterprise QA Signals for truth integrity, risk language, false resolution patterns, and pressure-driven failures.
4. Review Team Insights for score trends, compliance health, troubleshooting quality, and repeated weak spots.
5. Export QA reports for coaching records when needed.
6. Export the CFO/ROI report when leadership needs time-saved and labor-value visibility.
7. Adjust templates, writing style, policy routing, or coaching focus based on actual evidence.

Recommended weekly rhythm

Day or cadence	Manager action
Monday	Fetch config, check team scope, review previous week trends.
Midweek	Run a small QA sample across issue types and agents.
Friday	Export QA or ROI summaries if leadership needs the story.
Any time risk appears	Use Enterprise QA Signals and original transcript evidence before coaching.

Coaching guidance: CallWrapUp helps managers identify documentation gaps, process friction, and recurring coaching opportunities using evidence from actual customer interactions. It is designed to support fair, consistent, and actionable coaching conversations.

25. First Sample Wrap Test

Before declaring launch complete, run a controlled sample. This prevents a setup from being technically valid but operationally awkward.

1. Use a realistic sample transcript with a customer issue, agent troubleshooting, customer response, and final status.
2. Generate a wrap using the selected provider and current output style.
3. Confirm the output includes Summary, Key Issue, Resolution, Action Items, and Priority unless your custom template intentionally changes those names.
4. Copy the result into a test ticket or internal note location.
5. Clear the transcript box after testing if clean-workstation handling is required.
6. If Manager tools are active, paste the generated wrap and original transcript into Audit Intake and run one QA audit.
7. Review the QA score, Enterprise QA Signals, and coaching notes to confirm the whole workflow works from agent to manager.

Pass/fail launch criteria

Check	Pass condition
License	Valid and role matches user.
Provider	Test configuration passes and sample wrap generates.
Output	Wrap is structured, useful, and not generic filler.
Team sync	Fetched config matches admin settings on the test device.
Manager QA	Audit runs and produces a useful score/findings when Manager plan is active.
Security	PIN/recovery setup matches organization policy.

26. Troubleshooting Playbook

Problem	Likely cause	Fix
License will not validate	Typo, expired/cancelled license, wrong role, no internet, removed device, team mismatch.	Re-paste key, confirm role and Team / Workgroup ID, check subscription, validate internet, or restore device.
API test fails	Wrong provider, bad key, unavailable model, missing endpoint/region/API version, network block.	Confirm provider details with IT, choose an approved model, and test again.
App opens but no output generates	Transcript box empty, API test failed, selected model unavailable, or provider account blocked.	Paste transcript, run Test configuration, verify model access, then generate again.
Manager/Admin features missing	Agent role, hidden tabs, kiosk mode, wrong license, or role lock.	Confirm license role, use authorized shortcut if appropriate, or reassign proper Manager seat.
Output too short or generic	Transcript lacks detail, model too weak, template too vague, style too concise.	Use fuller transcript, stronger approved model, more detailed template, or different style.

Support note: before escalating a setup issue, capture the role, device name, Team / Workgroup ID, license validation status, provider selected, model selected, and exact error text.

27. Recovery Scenarios

Scenario	What to check	What to do
Team names do not match	Different Team / Workgroup ID spelling across devices.	Standardize team spelling, save/fetch config again, and validate license.
Seats appear full	Old devices still occupy seats.	Remove stale devices in Admin > Seat Device Management, then validate/fetch again.
Policy routing feels slow	Too many active policies or large transcripts.	Enable Smart Policy Routing, reduce max policies, archive duplicates, keep compression enabled.
User lost PIN only	Recovery code exists or another manager device is active.	Use recovery code, or use another Manager/Admin device to remove/replace affected device.
User lost PIN and recovery code	No recovery code available.	Use another active Manager/Admin device if available. If none exists, temporary Manager seat or paid recovery setup may be required.
Removed device still appears in history	History list is display/audit record.	Clearing visible history does not restore access. Restore or reauthorize the device if needed.

Escalation packet

When requesting setup or technical support, include the details below so the issue can be reviewed quickly and accurately.

- Screenshot of the error message or failed screen.
- Current license validation status and selected role claim.
- Team / Workgroup ID and Workspace ID exactly as entered.
- Device name, platform, and whether the workstation is the first or second device for that user.
- Provider, model, endpoint details, and Test configuration result.
- Do not include secret API keys, full credentials, private tokens, or sensitive customer transcripts in general support notes.
- Support goal: Provide enough setup context for the issue to be diagnosed clearly, without exposing sensitive information.

28. FAQ

Does CallWrapUp come with AI included?

No. CallWrapUp uses a bring-your-own-AI setup. Your organization provides the AI key and pays the AI provider directly.

Do I need both a license key and an API key?

Yes. The license unlocks the software. The API key allows AI generation and QA output.

Can one company use different AI providers?

Yes, if deployment rules and internal policy allow it. Many teams standardize on one provider for consistency.

Can agents use the software without manager tools?

Yes. Role-based access, kiosk mode, and PIN controls can keep manager/admin tools hidden or restricted.

Does CallWrapUp store customer transcripts on a server?

The intended design is desktop-first, with transcript handling on the workstation and organization-owned AI provider routing. Users should still follow internal data-handling policy.

What happens if the subscription is cancelled or expires?

License-controlled features can lock based on validation rules, plan status, and grace settings.

What should we test right after install?

Validate the license, test provider connection, generate one sample wrap, copy it into a test ticket, and run one manager QA audit if applicable.

What if a manager forgets the PIN?

Use the recovery code or another active manager/admin device to remove or replace the affected device. If all elevated access is lost and no recovery code exists, recovery may require a temporary manager seat or paid recovery setup.

Can this be used outside call centers?

Yes. It can fit support, healthcare administration, finance support, sales, internal help desk, operations, and other transcript-heavy workflows.

How long should basic setup take?

Most users can finish basic setup in a few minutes once they have the installer, license key, Team / Workgroup ID, and AI provider details ready.

29. First-Day Launch Checklist

Check	Owner	Done
Installer completed successfully on each workstation.	Agent/Manager/IT	
Correct role selected: Agent Seat or Manager Seat.	Setup owner	
Team / Workgroup ID typed exactly and recorded.	Manager/Admin	
License validated successfully.	Setup owner	
Device name and platform entered clearly.	Setup owner	
AI provider selected and model chosen.	IT/Admin	
API key/endpoint saved and Test configuration passed.	IT/Admin	
Save Configuration / Save Full Config completed.	Admin	
One sample wrap generated and copied successfully.	Agent/Manager	
Manager/Admin access confirmed if applicable.	Manager/Admin	
PIN and recovery code stored if access control is enabled.	Admin/IT	
Policy pack imported or confirmed not needed for launch.	Manager/Admin	
One QA audit run successfully if Manager plan is active.	Manager/QA lead	
Seat Device Management reviewed for stale/incorrect devices.	Admin	
Team knows where to paste transcripts and where to paste final wraps.	Manager	

Final launch note: CallWrapUp is designed to support repeatable documentation and QA workflows. When agents follow a simple daily process, managers review evidence-based QA, and admins keep configuration clean, the organization gains faster wraps, stronger visibility, and clearer operational reporting.

30. One-Page Setup Command Card

1. Install CallWrapUp on the real workstation.
2. Choose Agent Seat or Manager Seat.
3. Enter Team / Workgroup ID exactly.
4. Validate license.
5. Enter AI provider details and run Test configuration.
6. Save Configuration or Save Full Config.
7. Generate a sample wrap.
8. Managers/Admins: configure output, policy, access control, and device management.
9. Run one QA audit and one ROI/report export test before declaring launch ready.

The tiny checklist that prevents giant headaches: license valid, provider test passed, team name exact, device named clearly, recovery code stored, sample wrap generated, sample QA audit complete.

Keep this visible during rollout

Role	First thing to confirm
Agent	Can paste transcript, generate wrap, copy result, and clear workspace.
Manager	Can run QA audit, see Team Insights, and export needed reports.
Admin	Can validate license, save/fetch config, manage seats, and protect access.
IT	Can verify provider key/endpoint, device naming, and recovery-code storage.

Last Setup reminder: CallWrapUp requires three items to work correctly: a valid license, an approved AI provider key, and the correct Team / Workgroup ID.