NOMAD SMALL BUSINESS SUITE

Nomad Support Desk Pro - Implementation Guide

A complete Pro deployment guide covering the required Free foundation, licensing, secure attachments, notification events, structured email intake, quote and onsite workflows, PDF reporting, mobile resources, integrations and embedded Ticket AI.

Edition: 1.1.3
Audience: WordPress administrators, implementation partners and support managers

Contents

This guide is based on the verified product package and is written as an operational reference. Use the online version for navigation and this PDF for offline access.

1. Pro architecture and dependency

Deploy Pro as an extension of the required Free foundation while keeping AI ownership clear.

Required architecture

Nomad Support Desk Pro 1.1.3 requires Nomad Support Desk Free to remain installed and active. Free provides the shared foundation; Pro loads the premium runtime and extends the same Service Desk data model.

Component	Requirement	Purpose
Service Desk Free	Required and active	Foundation and shared Service Desk architecture
Service Desk Pro	Required for premium features	Attachments, notifications, templates, quote/onsite workflows and PDF reporting
AI Support Agent	Not required	Separate product; Service Desk AI is embedded in Free and Pro

Pro-only capability map

- Customer and staff ticket attachments
- Secure customer-downloadable files and staff-only files
- Customer email notification events
- WhatsApp connector hooks
- Additional contacts and notification recipients
- Outlook-friendly support email template
- Structured inbound field parsing and inbound attachments
- Quote/proposal requests with Accounting quote integration or fallback PDF
- Onsite site/contact/address fields
- Customer analytics PDF reports
- Pro licence enforcement

Data ownership

Free and Pro operate on the Service Desk's shared records. Activating Pro does not require a ticket migration. Deactivate Pro before Free. Do not delete Free while Pro is active.

Runtime loading model

Both packages remain active, but they do not run two competing desks. Free supplies the dependency and shared foundations; when the Pro runtime is available, the Free bootstrap avoids starting a duplicate operational runtime. Pro therefore presents one Support Desk menu and works with the existing customer, ticket, reply, time, resource, signature, email, event, billing and AI records while adding premium tables and fields.

Treat the pair as one release unit. Record both installed versions, test them together and retain both source ZIPs for rollback. A green WordPress activation state alone is not sufficient; confirm the Pro heading, Licence screen and at least one premium control.

Shared and premium data map

Data area	Foundation	Pro extension
Tickets	Lifecycle, customer, assignment, conversation and totals	Quote, onsite and additional-recipient fields
Files	No managed ticket attachment workflow	Attachment records, visibility and secure download
Communication	Inbound log and core reply flow	Customer event notifications and connector hooks
Commercial	Time, billing batches and Accounting invoice route	Quote records/items, Accounting quote route and fallback PDF
Reporting	On-screen customer/admin measures	Customer PDF report
AI	Embedded settings, resources and analysis	Same engine with Pro ticket context

Dependency change control

- Update and test Free before Pro
- Deactivate Pro before deactivating Free
- Do not remove shared database tables during routine rollback
- Confirm both plugins after site cloning or domain changes
- Keep embedded Ticket AI documentation with Service Desk, not the separate AI Support Agent product

Pro 1.1.3 access-control layer

Pro adds five internal WordPress roles and enforces them across menu registration, direct page access, ticket queries, field rendering and action handlers. WordPress Administrators inherit every Service Desk capability and remain unrestricted. Customer/requester access continues through the separate portal identity relationship rather than an internal Service Desk role.

2. Requirements and readiness

Verify both the technical platform and premium operating decisions.

Technical requirements

Requirement	Value
WordPress	6.0 or later; tested through 6.8
PHP	8.0 or later
Free foundation	Nomad Support Desk Free 0.2.3 active
HTTPS	Required for production portals and file/sign-off links
Outbound mail	Reliable transactional delivery
Storage	Sized for approved attachment volume and retention
Backups	Database and uploads recoverable

Premium policy decisions

- Maximum attachment size and permitted extensions
- Who may upload customer-visible versus staff-only files
- Which customer events send email
- Whether a WhatsApp connector will consume events
- Who receives additional notifications
- Quote numbering, validity and tax defaults
- Accounting quote versus fallback PDF workflow
- Onsite data and sign-off requirements
- PDF report retention

Infrastructure readiness worksheet

Area	Decision or measurement	Owner
PHP/WordPress	Production and staging versions meet minimums	Hosting administrator
Upload path	Writable, backed up and not executable	Hosting/security owner
Limits	PHP and proxy limits exceed approved per-file policy	Hosting administrator
Mail	Transactional sender, SPF/DKIM/DMARC and logs	Mail owner
Licensing	Outbound HTTPS to licensing service and correct production URL	Site administrator
Accounting	Quote/invoice integration availability and product mapping	Finance owner

Area	Decision or measurement	Owner
Retention	Files, reports, messages and sign-off retention	Data owner

Capacity and storage estimate

Estimate attachment storage before enabling uploads: expected tickets per month multiplied by average files per ticket and average file size, then add backup copies and the retention period. Include staging when production files are cloned. Set the application maximum below the lowest effective PHP, web-server and reverse-proxy limit so users receive a controlled validation error instead of an incomplete request.

1. Measure current upload and backup capacity.
2. Set a business maximum per file and reduce allowed extensions.
3. Confirm PHP upload_max_filesize and post_max_size support the policy.
4. Confirm proxy/WAF limits and request timeouts.
5. Test at just below and just above the chosen maximum.

Privacy and communication assessment

- Classify customer-visible and staff-only file content
- Approve which ticket events justify external email
- Define authority for additional recipients
- Decide whether connector events may leave WordPress
- Document when full licence keys or personal information are prohibited
- Set retention and breach-response ownership

3. Installation, activation and licence

Install in dependency order and confirm the licence page before configuration.

Installation order

1. Back up the site.
2. Install and activate Service Desk Free 0.2.3.
3. Upload and activate Service Desk Pro 1.1.3.
4. Open Support Desk > Licence.
5. Confirm the server URL and enter the Pro licence key.
6. Activate the licence and confirm status Active or Valid.
7. Open Support Desk > Dashboard and confirm the heading identifies Pro.

Dependency behaviour

If Free is missing, Pro cancels activation and displays a dependency message. If Free later becomes unavailable, Pro stops loading. This protects the site from running a partial premium runtime.

Do not remove Free	Pro is not a replacement package. Keep both plugins active in production.

Licence troubleshooting

Issue	Check
Licence menu unavailable	Use Support Desk > Licence and confirm administrator capability
Link expired message	Use the current 1.1.3 form; clear cached admin page and submit once
Product mismatch	Catalogue product code must be `small-business-service-desk-pro`
Activation fails	HTTPS, server URL, key status and licensing server reachability
Old key missing	1.1.3 retains the historical local option key; do not manually rename options

Pre-install backup and evidence

1. Export the installed plugin/version list and current Service Desk settings record.
2. Take database and wp-content backups, including any existing Service Desk attachment directory.
3. Verify that the restore process and credentials are available to the maintenance owner.
4. Record current ticket, reply, customer, resource and time-entry counts.
5. Download the exact Free 0.2.3 and Pro 1.1.3 packages into the change record.

Activation verification

Check	Expected result
Plugins screen	Free 0.2.3 and Pro 1.1.3 both Active
Dashboard	One operational Support Desk, identified as Pro
Licence	Support Desk > Licence loads and shows the configured state
Settings	Attachment, notification and quote defaults appear
Ticket edit	Premium file, onsite and quote controls appear
Customer portal	Pro actions render only for authorised customer
AI	Embedded AI menus/settings exist without AI Support Agent

Licence lifecycle

The Licence screen submits the site/server URL, key and the catalogue product code `small-business-service-desk-pro` to the licensing service. Store the key according to the organisation's credential policy and restrict the screen to trusted administrators. Recheck licence state after production-domain changes, cloning, key replacement or licensing-server maintenance.

Staging	Use the licensing terms and available staging allowance; do not assume that copying a production database makes a second site correctly licensed.

Role migration during upgrade

On upgrade, legacy Support Agent accounts are migrated to Service Desk Administrator. Non-administrator users with direct broad Service Desk capability grants but no recognised Service Desk role are migrated to Technician / Resource. Legacy per-user Service Desk overrides are removed so the assigned role becomes the authority.

1. Export the existing WordPress user, role and resource-link inventory before updating.
2. Update the matched Free 0.2.3 and Pro 1.1.3 packages in staging.
3. Open Support Desk > Users & Roles and review every migrated account.
4. Change over-privileged migrated administrators to the appropriate narrower role.
5. Confirm operational roles have active resources and Reporting Viewers do not.
6. Run the ticket-scope and menu tests for each role before production rollout.

4. Upgrade and migration strategy

Protect live ticket operations when moving from Free or an earlier Pro build.

Upgrade sequence

1. Confirm the current installed versions and take a database/files backup.
2. Test the new Free and Pro pair in staging.
3. Update Free first, then Pro.
4. Reactivate/verify the Pro licence if required.
5. Save permalinks and purge caches.
6. Run ticket, attachment, notification, AI, sign-off and billing acceptance tests.

Legacy data importer

The package includes defensive support for legacy Core ticket and reply records. Use the supplied import/demo controls only after a backup and on a verified staging copy. Review counts and spot-check ticket ownership, replies and status mapping.

Migration	Do not repeatedly import the same legacy dataset without checking duplicate-protection behaviour.

Rollback

Deactivate Pro before Free. Restore the previous verified plugin pair without dropping shared Service Desk tables. Recheck licence status, permalinks, cache and scheduled operations.

Staging rehearsal

1. Clone production into an access-controlled staging environment.
2. Disable real inbound forwarding, outbound customer mail and connector delivery.
3. Install the matched Free and Pro versions in the planned order.
4. Run any required schema upgrade once and record resulting table/column checks.
5. Use copied test accounts to validate customer and resource isolation.
6. Complete premium acceptance with controlled files, recipients and quotes.
7. Record duration, defects and the exact production sequence.

Data verification before and after

Record	Verify
Customers	Count and representative email/domain mapping
Tickets/replies	Count plus oldest, newest and complex timeline
Resources	Active state, linked user and assignments
Time/billing	Totals and an existing batch/invoice link
Attachments	Record count, visibility and secure download

Record	Verify
Quotes	Numbering, line items and external Accounting link
AI resources	Active resources and known-answer retrieval

Production rollback trigger

Define the decision before starting. A confirmed cross-customer file exposure, corrupt ticket write, duplicate billing/quote creation, inability to operate the core queue, or unrecoverable activation failure is a rollback trigger. A cosmetic defect with a safe workaround may be handled after launch only with the service owner's approval. Capture logs and counts before restoring the previous matched pair.

5. Base Service Desk configuration

Complete the shared Free configuration before enabling premium automation.

Required base setup

- Support email and sender identity
- Inbound endpoint/token and customer matching policy
- Customer and resource records
- Customer, resource and sign-off pages
- CRM status tags
- Accounting service product/rate and billing increment
- Ticket prefix and next number
- Embedded AI settings and approved resources

Portal shortcodes

Shortcode	Pro result
`[nomad_support_portal]`	Full customer portal including Pro actions
`[nomad_support_customer_analytics]`	Customer analytics with PDF download
`[nomad_support_customer_report]`	Pro alias for analytics/reporting
`[nomad_support_agent_portal]`	Assigned-resource portal with Pro files/uploads
`[nomad_support_ticket_signoff]`	Secure sign-off

Base configuration dependency map

Premium feature	Base configuration it depends on
Customer files	Correct customer portal identity and ticket access
Notifications	Support sender, mail delivery and customer email
Structured intake	Inbound endpoint/token and customer matching
Quote	Customer, currency and optional Accounting mapping
Onsite	Ticket assignment and resource mobile portal
PDF report	Customer analytics page and data isolation
Ticket AI	AI settings, approved resources and ticket permissions

Recommended page inventory

1. Confirm the full customer portal page uses `[nomad_support_portal]`.
2. Confirm the resource page uses `[nomad_support_agent_portal]` and is not public navigation content.
3. Confirm the sign-off page uses `[nomad_support_ticket_signoff]`.
4. If a separate report page is required, use the supported customer analytics/report shortcode.

5. Apply normal login protection and authenticated-cache exclusions.
6. Test pages as logged-out, Customer A, Customer B, Resource A and Resource B.

Configuration sequencing rule

Validate the base desk first: customer isolation, assignment, reply visibility, inbound threading, time, sign-off and AI. Then enable one premium area at a time in this order: attachments, customer notifications, structured intake, quotes, onsite fields and PDF reporting. This isolates configuration faults and prevents a notification from distributing a file or field before its visibility policy is verified.

Role-based menu map

Role	Support Desk menus
Service Desk Administrator	Dashboard, Tickets, Add Ticket, Customers, Resources, Analytics, Billing, Users & Roles, Settings and AI management
Service Desk Manager	Dashboard, Tickets, Add Ticket, Customers, Resources and Analytics
Dispatcher / Service Coordinator	Dashboard, Tickets, Add Ticket, Customers and Resources
Technician / Resource	Dashboard and assigned-scope Tickets; assigned-resource portal is recommended
Reporting Viewer	Dashboard, read-only Tickets and Analytics
WordPress Administrator	All Service Desk menus plus Licence and normal WordPress administration

6. Attachment and file security

Control file types, size, visibility and download access.

Configure attachments

1. Open Support Desk > Settings.
2. Enable ticket attachments.
3. Set maximum size per file in MB.
4. Enter only required extensions in the comma-separated allowed list.
5. Save and test one allowed and one blocked file.

Default allowed extensions

The 1.1.3 default is `jpg,jpeg,png,gif,webp,pdf,doc,docx,xls,xlsx,csv,txt,zip`. Reduce this list when the business does not need a type.

Security	An extension allow-list is only one control. Keep WordPress, PHP and the web server patched, scan uploads where available and never execute uploaded files.

Visibility model

File type	Who can access
Customer-visible attachment	Authorised customer and support staff through secure download logic
Staff-only attachment	Authorised support staff/resources only
Reply attachment	Visibility follows whether the reply is public or internal

Storage and retention

- Estimate monthly file volume
- Back up attachment storage with the database
- Define retention by ticket type
- Remove only through approved workflows
- Test restore of a ticket and its file

Upload validation chain

An upload must pass the Pro setting, extension allow-list, configured per-file maximum and server limits before an attachment record is created. Store files through the plugin workflow rather than linking directly into the upload directory. The managed storage area is `nsd-attachments`; secure download logic checks the current user/ticket relationship and the stored customer/staff visibility.

Layer	Control
Business	Permitted purpose, file class and retention

Layer	Control
Application	Attachments enabled, size and extension
Server	PHP/web-server request limits and writable storage
Access	Ticket relationship and visibility flag
Delivery	Secure handler rather than a published file URL
Operations	Malware scanning, backup, restore and deletion process

Visibility acceptance tests

1. Upload a customer-visible file as staff and verify Customer A can download it.
2. Verify Customer B and a logged-out browser cannot download it.
3. Upload a staff-only file and verify Customer A cannot see or download it.
4. Verify an assigned resource can access the staff file for that ticket.
5. Remove the resource assignment and confirm access follows the new assignment.
6. Attach one file to a public reply and another to an internal note; confirm inherited visibility.

File incident and retention procedure

- Stop further sharing when visibility or content is wrong
- Record ticket, attachment, users, time and notification outcome
- Preserve evidence while following the approved incident process
- Remove or restrict through supported controls rather than editing storage directly
- Check whether a notification or copied download already disclosed the file
- Test backup restoration before relying on retention controls

7. Customer notifications and WhatsApp hooks

Enable communication deliberately and prevent duplicate messages.

Email notification events

Pro can notify customers when a ticket is created, updated, replied to, changes status or receives a customer-downloadable file. Enable the setting only after sender identity and mail delivery are verified.

1. Enable customer email notifications.
2. Create a test customer with a controlled mailbox.
3. Trigger each supported event one at a time.
4. Verify subject, ticket number, links and recipient list.
5. Check spam placement and mail logs.

Additional recipients

Structured tickets may include additional contacts and notification emails. Confirm business authority before copying ticket content to extra recipients and keep recipient data current.

Privacy	Do not add recipients merely for convenience; ticket messages may contain confidential customer information.

WhatsApp connector

Pro emits WhatsApp-related event hooks but does not send WhatsApp messages on its own. Install and configure the separate Nomad Support Desk WhatsApp Connector if required, then test opt-in, templates, phone formatting, failure handling and duplicate suppression.

Notification design matrix

Event	Customer value	Implementation check
Ticket created	Receipt and ticket number	Send once to correct customer/approved recipients
Public reply	New support communication	Exclude internal notes
Status change	Next-action visibility	Avoid noisy changes with no explanation
Visible update	Important customer-facing field changed	Confirm event definition and content
Customer file	Secure file now available	File must be customer-visible before send

Recipient and delivery controls

1. Use a controlled customer mailbox and one approved additional recipient.
2. Trigger each event once and record the received message, subject and links.
3. Confirm the main customer and additional addresses receive only authorised content.
4. Remove the additional recipient and repeat an event to confirm it no longer receives mail.
5. Inspect mail logs for one send per intended recipient and event.

6. Test a delivery failure and document the operational alert/retry owner.

Connector event governance

WhatsApp-related hooks are integration points, not a built-in message sender. A connector consuming them must apply consent, template approval, phone normalisation, rate limits, delivery logging and duplicate suppression. Document which plugin or service owns the final message, and ensure disabling customer email does not accidentally imply that connector messages are also disabled unless the connector explicitly follows that setting.

8. Structured inbound email and template

Give email customers a reliable field format while preserving normal threading.

Template deployment

1. Open the customer Support Desk screen.
2. Download the Email Ticket Template.
3. Review the plain-text labels.
4. Provide the template to approved email users.
5. Tell users to keep field labels unchanged and replace only the values.

Structured fields

Field group	Examples
Issue	Subject and description
Product context	Product / Service, Website URL and Licence Key
Commercial	Quote Required
Onsite	Onsite Required, site name, contact, phone and address
Communication	Additional Contacts and Additional Notification Emails

Inbound bridge

The base endpoint fields remain token, sender, subject, body and message ID. Pro can additionally accept uploaded files through `attachments[]` when the bridge supports multipart requests. Enforce the same size and extension policy before forwarding.

Licence-key handling The parser may store a licence-key field on the ticket, but Ticket AI excludes stored licence keys from prepared context. Users should still avoid sending full keys unless operationally necessary.

Template label contract

The plain-text field labels are the parser contract. Users replace values after labels and retain the overall layout. Localised or renamed labels, rich-text transformations and replies that quote a previous blank template can reduce reliable extraction. Keep the original downloadable template as the controlled master and version any organisation-specific instructions outside the labels.

Field parsing acceptance

Test	Expected mapping
Complete template	All product, URL, commercial, onsite and recipient fields saved
Optional fields blank	Ticket creates without placeholder text
Yes/no variants	Quote/onsite values follow documented accepted form
Additional emails	Only valid, authorised addresses saved

Test	Expected mapping
Changed label	Demonstrates the field is not guaranteed; master label restored
Thread reply	Ticket number routes message to existing ticket rather than creating another

Multipart attachment bridge

1. Keep token, sender, subject, text body and message ID mapping from the base endpoint.
2. Use a multipart request and map permitted files into `attachments[]`.
3. Apply size, extension and malware controls before forwarding.
4. Preserve a stable message ID for duplicate suppression.
5. Test one permitted file, one blocked extension, one oversized file and one duplicate delivery.
6. Confirm inbound files receive the intended customer visibility and ticket relationship.

9. Quote and proposal workflow

Route commercial requests to Accounting or a controlled fallback PDF.

Configure quote defaults

- Fallback quote prefix, default NSD-QT
- Next fallback quote number
- Default validity period, 14 days by default
- Default tax rate
- Currency and product/service line mapping

Accounting route

When compatible Accounting Pro quote tables are available, Support Desk can create an Accounting quote from ticket line items. Test customer mapping, product codes, quantities, prices, tax, description and link back to the ticket.

1. Mark or open the ticket's quote request.
2. Review the customer and requested work.
3. Add line items.
4. Create the Accounting quote.
5. Open it in Accounting and verify totals and customer data.

Fallback route

Without Accounting Pro, or when staff deliberately selects the fallback, Service Desk creates an internal quote/proposal record and downloadable PDF. Verify numbering, validity, tax and line items before sending it.

Commercial control	A support diagnosis is not automatically an approved quotation. Use the business's normal approval authority.

Quote data model and numbering

Pro stores internal quote headers and line items when using the fallback route, and stores ticket references to the resulting commercial record. Configure the fallback prefix and next number before creating live documents. Do not move the next number backwards or reuse a cancelled number merely to remove a gap; uniqueness and traceability are more important than a continuous sequence.

Line and total acceptance

Field	Test
Customer	Matches ticket and destination commercial record
Product/code	Recognised by Accounting or clearly described in fallback
Description	Defines scope and exclusions sufficiently
Quantity/unit price	Units and decimal precision produce expected subtotal
Tax	Approved rate and calculation

Field	Test
Currency	Matches customer and commercial policy
Validity	Issue/expiry dates follow configured default and approval

Accounting and fallback decision

1. Detect whether compatible Accounting Pro quote tables and customer mapping are available.
2. Use the Accounting route when the organisation controls quotes there.
3. Use forced fallback only for an approved exception or when Accounting is unavailable.
4. Create once and open the resulting quote before repeating any action.
5. Compare line totals, tax, customer, numbering and ticket link.
6. Keep customer acceptance and conversion in the approved commercial workflow.

10. Onsite workflow and sign-off

Capture the details technicians need before travelling and the evidence required after work.

Onsite fields

- Onsite Required
- Site name
- Site contact name
- Site contact phone
- Site address

Implementation test

1. Create a ticket with Onsite Required selected.
2. Populate site details.
3. Assign a mobile resource.
4. Confirm the fields are readable on the resource portal at phone width.
5. Complete work, add notes/time and capture customer sign-off.
6. Verify the stored signature and closure behaviour.

Operational safety

Site details support scheduling but do not replace the organisation's travel, lone-worker, access or health-and-safety procedures. Keep those procedures in the relevant business system.

Onsite field validation

Field	Validation rule
Onsite Required	Selected only when physical attendance is part of the request
Site name	Unambiguous location name
Contact	Authorised person expected at site
Phone	Usable format for the operating region
Address	Complete arrival information without unrelated personal data
Assignment	Named active resource who can access the mobile ticket

Mobile field and workflow test

1. Test at 320px width and on a representative mobile browser.
2. Confirm site details wrap and remain readable without horizontal loss.
3. Use contact/copy actions and verify the intended value.
4. Add an internal site-preparation note and a public arrival update.
5. Upload each visibility class, log time and save with intermittent-network awareness.
6. Capture sign-off and confirm the signature is stored against the correct ticket.

Onsite record boundary

The ticket should contain information needed to deliver and evidence the service, but it is not the organisation's complete workforce-safety, travel or facility-access system. Link or reference those controlled procedures without copying sensitive personal or security information unnecessarily into the ticket.

11. Customer analytics PDF reporting

Enable and test secure customer report downloads.

Report access

The Pro customer analytics screen adds a PDF download. Access is tied to the authorised customer context; test that changing URLs or using another customer account cannot expose a report.

1. Open the customer analytics page as Customer A.
2. Download the report and verify ticket metrics and identity.
3. Repeat as Customer B.
4. Attempt access while logged out.
5. Check filename, date, page layout and privacy.

Report limitations

The PDF reflects Service Desk data at generation time. It is an operational support report, not a financial statement, contractual SLA certificate or substitute for reading individual tickets.

Report contents and data sources

The customer PDF is generated from the current authorised customer context and Service Desk measures. It can summarise ticket volume, status and service timing for the available reporting scope. Its quality depends on customer matching, lifecycle timestamps and complete ticket use; it does not reconstruct work performed only in email or another system.

Report security matrix

Test context	Expected result
Customer A	Only Customer A report and metrics
Customer B	Only Customer B report and metrics
Logged out	No report data
Altered URL/parameters	No cross-customer report
Cached authenticated page	No shared cached report response
Expired session	Authentication required again

Layout and records test

1. Use customers with short and long names and enough tickets for multiple pages.
2. Confirm headings, tables, totals, dates and page breaks remain readable.
3. Check PDF metadata and filename for appropriate information exposure.
4. Compare representative figures with the on-screen analytics and source tickets.
5. Define who may store, email or retain the downloaded report.

12. Embedded Ticket AI in Pro

Configure the same Service Desk-owned engine with premium ticket context and files.

Independence

Service Desk Pro 1.1.3 embeds its own AI configuration, resource retrieval and ticket-analysis controller. AI Support Agent is not a dependency and is not required for licence or runtime operation.

Correct architecture	Do not install AI Support Agent merely to make Ticket AI work in Service Desk Pro.

Implementation

1. Configure Support Desk > AI Settings.
2. Add approved manuals, notes, URLs, PDFs, text/code files or plugin ZIPs under AI Resources.
3. Test knowledge-only matching without an API key.
4. If approved, add the API key and test generated answers.
5. Enable live web research only after privacy/cost approval.
6. Run an admin ticket test and an assigned-resource test.
7. Verify sources, insertion actions, rate limiting and audit events.

Context protection

- Customer identity fields excluded
- Stored licence keys excluded
- Common secrets redacted
- Untrusted resource/web instructions do not override the assistant role
- Outputs distinguish evidence from hypotheses
- Risky actions require verification warnings

AI configuration reference

Control	Pro implementation decision
Enabled	Which roles and portals receive AI controls
Answer generation	Whether an external API may synthesise text
API endpoint/key/model	Approved provider, credential owner and supported model
Temperature	Low variation for support work
Matched resources	Relevance/performance balance, normally tested around 6-8
Pre-ticket assistant	Customer guidance and privacy notice
Web research	Public-web need, cost and data policy

Premium context and file boundary

Ticket analysis uses the authorised ticket's text context. Stored customer identity and licence-key fields are excluded, and common secret patterns are redacted. Ticket attachments are not a reason to assume every file is safe or suitable for AI context; establish a reviewed process for extracting or adding approved knowledge to AI Resources instead of treating customer uploads as trusted instructions.

AI acceptance scenarios

1. Run a known-answer query against one active versioned AI resource.
2. Deactivate that resource and confirm it is no longer a valid source.
3. Test an administrator and an assigned resource on the same ticket.
4. Test an unassigned resource and confirm access is denied.
5. Insert a proposed public reply, edit it and verify only the final saved text reaches the timeline.
6. Exercise the configured rate limit and confirm a controlled response.
7. Review the Service Desk event/audit record for the completed analysis.

13. Full acceptance test

Validate the complete Free plus Pro stack before launch.

Premium test matrix

Area	Required result
Dependency	Pro loads only while Free is active
Licence	Active/valid state survives refresh
Attachments	Allowed upload works; blocked type/size fails; visibility enforced
Email	Each enabled event sends once to correct recipients
Structured intake	Template fields and optional files map correctly
Quote	Accounting and fallback route totals are correct
Onsite	Resource sees site details on mobile
PDF report	Correct customer can download; others cannot
AI	Admin and assigned resource analysis works without AI Support Agent
Sign-off	Signature attaches to the correct ticket
Billing	Batch and invoice integration remain correct

Non-functional checks

- 320px mobile workflow
- Authenticated page cache exclusions
- File storage backup/restore
- Wordfence and REST compatibility
- Mail deliverability
- Reasonable response time with representative ticket volume
- No PHP warnings in logs

Test identities and fixtures

Use separate Administrator, Support Manager, Resource A, Resource B, Customer A and Customer B accounts. Prepare tickets with public/internal replies, both attachment visibilities, additional recipients, quote and onsite fields, time entries and a sign-off. Use controlled mailboxes and non-sensitive files so a failed privacy test cannot expose real customer information.

End-to-end business scenarios

Scenario	Required path
Portal request	Customer creates with file; staff replies; resource works; sign-off closes

Scenario	Required path
Structured email	Template maps fields/file; number threads reply; duplicate is suppressed
Commercial request	Quote-required ticket produces verified Accounting or fallback document
Onsite request	Site fields reach assigned resource; time/file/sign-off saved
Reporting	Customer downloads own multi-page PDF; another user is denied
AI-assisted triage	Approved resource cited; draft edited; audit event stored

Acceptance evidence pack

- Environment and version inventory
- Account/role matrix and isolation results
- Screenshots or logs without secrets
- Mail event and recipient results
- Attachment visibility/download tests
- Quote and PDF samples marked as test
- Known defects, owners, workarounds and go-live decision

Role isolation matrix

Function	Administrator	Manager	Dispatcher	Technician	Reporting Viewer
Ticket scope	All	All	All operational	Assigned only	All, read-only
Create tickets	Yes	Yes	Yes	No	No
Update ticket/status	Yes	Yes	Yes	Assigned only	No
Assign resources	Yes	Yes	Yes	No	No
Customer records	View/manage	View/manage	View	No global list	Masked in ticket views
Resource records	View/manage/link users	View/manage operations	View availability	Own link only	No
Internal notes	View/add	View/add	View/add coordination notes	Assigned tickets	Hidden
Ticket files	View/upload	View/upload	View; no upload	Assigned tickets; upload	Customer-visible only; staff files hidden
Time and sign-off	Yes	Yes	No	Assigned tickets	No
Ticket AI	Yes	Yes	No	Assigned tickets	No
Analytics/export	Yes	Operational	No analytics menu	No	Read-only operational
Billing/rates/financial quotes	Yes	No	No	No	No

Function	Administrator	Manager	Dispatcher	Technician	Reporting Viewer
Settings/AI resources	Yes	No	No	No	No
Users and roles	Yes	No	No	No	No
Permanent ticket deletion	Yes	No	No	No	No
Plugin Licence page	WordPress Administrator only	No	No	No	No

Direct-access and action tests

1. Sign in separately as every role; never validate the entire matrix as a WordPress Administrator.
2. Confirm login redirects to Support Desk and unrelated WordPress menus are absent.
3. Paste an unrelated wp-admin URL and confirm the user is redirected.
4. Paste a hidden Service Desk page URL and confirm its required capability is enforced.
5. As Technician A, attempt Technician B's ticket URL and action submission; both must be denied.
6. As Reporting Viewer, attempt edit, reply, upload, time, sign-off and AI actions; all must be denied.
7. Confirm customer contact, internal notes, staff files and financial information are hidden where the role matrix requires it.

14. Launch and operations

Move to production with clear ownership and rollback controls.

Launch sequence

1. Freeze configuration changes.
2. Take a verified backup.
3. Install Free, then Pro, then activate the licence.
4. Apply reviewed settings.
5. Publish portal links.
6. Enable inbound forwarding.
7. Enable notifications after mail verification.
8. Enable AI web research last, if approved.
9. Monitor the first live tickets and files.

Routine review

- Licence status and server reachability
- Attachment storage and retention
- Failed or duplicate notifications
- Additional-recipient accuracy
- Quote numbering and approvals
- Unbilled time
- Inactive resources
- AI resource freshness and API costs
- Customer report access tests after major updates

Rollback order

1. Pause inbound and outbound automation.
2. Deactivate Pro first.
3. Restore the previous verified Pro and Free files as a matched pair.
4. Verify the licence and shared data.
5. Clear caches, save permalinks and run smoke tests.

Controlled production cutover

1. Approve the staging result and freeze settings/content changes.
2. Pause inbound forwarding and connector delivery.
3. Take and verify final database and file backups.
4. Install/update Free, then Pro, and verify the licence.
5. Apply settings and clear authenticated/page caches.

6. Run role, ticket, file, mail, AI and report smoke tests.
7. Resume automations one at a time and observe the first live event.

Operational monitoring

Frequency	Review
Daily	Failed uploads/downloads, duplicate or failed mail, unassigned work and quote/onsite commitments
Weekly	Licence, storage growth, additional recipients, inactive resources, AI failures and unbilled time
Monthly	Cross-customer file/report tests, extension policy, retention, AI resources, quote numbering and restore test
After update	Dependency pair, licence, portals, files, notifications, structured intake, quote, report, AI and sign-off

Handover ownership

- Service owner for status and notification policy
- Website owner for plugin pair, licence, pages and cache
- Security/data owner for files, recipients, AI and retention
- Mail/connector owner for delivery and duplicate control
- Finance owner for rates, tax, quotes, batches and invoices
- Support manager for resources, queue and acceptance training

15. Implementation troubleshooting

Use focused evidence for premium deployment faults.

Common faults

Symptom	Primary check
Pro will not activate	Free plugin active and PHP 8.0+
Licence resets	Server URL, catalogue code, key status and caching
File upload blocked	Enabled setting, size, extension, PHP/web-server limits
Customer cannot download	Customer mapping, file visibility and secure token
Duplicate emails	Event hook/connector duplication and mail retry
Template fields ignored	Labels changed or plain-text body missing
Quote uses fallback	Accounting Pro tables/columns not detected or fallback forced
PDF report unavailable	Pro licence/runtime and analytics shortcode
AI asks for another plugin	Wrong/outdated documentation; 1.1.3 has embedded AI

Diagnostic sequence

1. Reproduce with the affected role and record ticket/file/quote ID and time.
2. Confirm both plugin versions, Pro licence state and PHP/WordPress versions.
3. Check whether the base Free workflow works before testing the premium layer.
4. Inspect PHP, browser network, mail, bridge or connector logs for the specific event.
5. Repeat in staging while isolating cache, firewall or integration controls one at a time.
6. Apply one reversible correction and rerun the relevant acceptance scenario.

Premium failure evidence

Area	Evidence
Licence	Server URL, product code, status, timestamp and non-secret response
Attachment	Ticket, file name/type/size, visibility, user role and HTTP result
Notification	Event, recipients, message ID, mail result and duplicate count
Structured intake	Message ID, preserved labels, mapped fields and endpoint response
Quote	Ticket, route, customer/product IDs, totals and resulting record ID
Report	Customer account, date scope, request result and page issue
AI	Mode, model, source, ticket role, event time and error

Do-not-do list

- Do not deactivate or delete Free while Pro is active
- Do not publish attachment storage URLs
- Do not repeatedly press send/create after an uncertain mail, quote or invoice response
- Do not rename structured template labels without parser changes and tests
- Do not solve a licence problem by installing AI Support Agent
- Do not edit Service Desk IDs or numbering directly in the database
- Do not share logs containing licence keys, inbound tokens or private files

16. Implementation handover and technical reference

Complete deployment with a durable record of premium configuration, ownership and interfaces.

Premium handover pack

- Free and Pro package versions and checksums
- Production/staging URLs and licence owner
- Attachment setting, storage, backup, scanning and retention record
- Notification-event matrix and approved recipient rules
- Inbound bridge/template mapping and secret rotation owner
- Connector inventory and delivery-failure procedure
- Quote numbering, tax, validity and Accounting/fallback decision
- Onsite and sign-off operating policy
- Customer report access/retention policy
- AI settings, provider owner and approved resource register
- Acceptance evidence, known issues and rollback runbook

Premium table and field reference

Area	Pro-owned data
Attachments	File metadata, ticket/reply relationship, visibility and storage reference
Quotes	Quote header, numbering, validity, totals, route and line items
Ticket extension	Quote requirement, onsite requirement/site details and additional recipients
Licence	Local licence configuration/state tied to the Pro catalogue product
Reports	Generated output based on authorised live Service Desk data

Final readiness sign-off

1. Confirm the service, technical, security, mail and finance owners have reviewed their controls.
2. Confirm all four documentation routes and downloadable manuals are available to the intended audience.
3. Confirm support staff can identify customer-visible versus internal content.
4. Schedule the first storage, recipient, report-isolation and restore reviews.
5. Record the go-live approval and the matched rollback package location.

17. Detailed premium acceptance scripts

Run these scripts with controlled accounts and evidence before approving production use.

Attachment and visibility script

1. As a manager, upload one customer-visible PDF and one staff-only text file to Customer A's ticket.
2. As Customer A, verify only the visible PDF is listed and downloadable.
3. As Customer B, test the copied secure link and confirm access is denied.
4. As Resource A assigned to the ticket, verify both files are available as permitted.
5. As Resource B unassigned to the ticket, confirm the staff-only download is denied.
6. Remove Resource A's assignment and verify its access changes accordingly.
7. Inspect logs and ensure no direct public storage URL was exposed.

Notification and structured-email script

1. Enable only one notification event and use controlled primary/additional mailboxes.
2. Trigger the event once and confirm subject, number, content, links and exact recipients.
3. Verify an internal note produces no customer message.
4. Submit the unchanged structured template with product, quote, onsite and recipient fields.
5. Confirm each value maps to the intended ticket field.
6. Reply with the ticket number and confirm threading; resend the same message ID and confirm duplicate suppression.
7. Repeat after removing the additional recipient and confirm delivery changes.

Commercial, onsite and reporting script

1. Create a quote-required ticket with two line items, tax and an approved currency.
2. Run the Accounting route when available and verify customer, lines, totals and ticket link.
3. Run an approved fallback case and inspect every page of the PDF.
4. Create an onsite ticket, verify site fields as an assigned mobile resource and add both file visibilities.
5. Log time, record completion and capture sign-off against the same ticket.
6. Download Customer A's analytics PDF and compare representative figures with source tickets.
7. Attempt the report as Customer B and logged out; both cross-customer attempts must fail.

Embedded AI and recovery script

1. Ask a known question using a single approved resource and confirm its citation.
2. Run ticket analysis as an administrator, assigned Resource A and unassigned Resource B.
3. Confirm Resource B is denied and the authorised completions create audit events.
4. Insert a reply draft, remove an unsupported statement and save the corrected text.
5. Disable web research and confirm the internet-only choice is no longer usable as configured.
6. Restore the original setting and document the tested API/model/resource versions.

18. Roles, user creation and access governance

Implement the Pro role model, provision restricted users and verify least-privilege access.

Implemented role matrix

Function	Administrator	Manager	Dispatcher	Technician	Reporting Viewer
Ticket scope	All	All	All operational	Assigned only	All, read-only
Create tickets	Yes	Yes	Yes	No	No
Update ticket/status	Yes	Yes	Yes	Assigned only	No
Assign resources	Yes	Yes	Yes	No	No
Customer records	View/manage	View/manage	View	No global list	Masked in ticket views
Resource records	View/manage/link users	View/manage operations	View availability	Own link only	No
Internal notes	View/add	View/add	View/add coordination notes	Assigned tickets	Hidden
Ticket files	View/upload	View/upload	View; no upload	Assigned tickets; upload	Customer-visible only; staff files hidden
Time and sign-off	Yes	Yes	No	Assigned tickets	No
Ticket AI	Yes	Yes	No	Assigned tickets	No
Analytics/export	Yes	Operational	No analytics menu	No	Read-only operational
Billing/rates/financial quotes	Yes	No	No	No	No
Settings/AI resources	Yes	No	No	No	No
Users and roles	Yes	No	No	No	No
Permanent ticket deletion	Yes	No	No	No	No
Plugin Licence page	WordPress Administrator only	No	No	No	No

Create a Pro Service Desk user

1. Sign in as a WordPress Administrator or Service Desk Administrator.
2. Open Support Desk > Users & Roles.
3. Enter the required username and email and optional first/last name.
4. Enter an initial password, or leave Password blank for secure generation.
5. Choose the narrowest role that covers the person's actual responsibilities.
6. Leave the login/set-password email selected only when outbound WordPress mail is working.
7. Create the user and confirm the role and resource-link result in the user table.

8. Test menu access, ticket scope, hidden data and at least one permitted and prohibited action.

Resource-link behaviour

Assigned role	Resource result
Service Desk Administrator	Active staff resource created or reactivated
Service Desk Manager	Active staff resource created or reactivated
Dispatcher / Service Coordinator	Active staff resource created or reactivated
Technician / Resource	Active technician resource created or reactivated
Reporting Viewer	No assignable resource; an existing linked resource is deactivated

Change an existing role

1. Open Support Desk > Users & Roles.
2. Find the named Service Desk account and review current assignments.
3. Reassign work first when the new role will lose assigned-ticket responsibility.
4. Choose the new approved role and select Update.
5. Confirm the role and resource state changed.
6. Sign in as the affected user and repeat access tests.

Safeguards	The screen does not change WordPress Administrator accounts and does not allow a user to change their own Service Desk role.

Administrator and Manager resource boundaries

Only the Service Desk Administrator or WordPress Administrator can create Service Desk users, assign roles, change linked WordPress users or run HR-to-technician user synchronisation. A Service Desk Manager can maintain operational resource information such as display/contact details, capacity, availability and active state, but cannot change WordPress user links, roles, rates or billing access.

Restricted WordPress administration

All non-administrator Service Desk-role users land on the Support Desk dashboard. Unrelated WordPress top-level menus are removed, direct attempts to open unapproved administration pages redirect to Support Desk, and the front-end admin bar is hidden. Page actions remain protected by capability, nonce and ticket-scope checks.

Licence boundary

The Service Desk Administrator is the highest role inside the desk, but the Pro Licence page deliberately requires WordPress Administrator access. Do not grant a site-wide Administrator role merely to allow normal helpdesk administration; retain licence activation with the site owner or authorised WordPress administrator.

Periodic access review

- Named user, current job function and assigned Service Desk role
- Resource link, active state and current ticket assignments
- Additional recipients and downloaded-file handling where applicable

- Accounts that should be downgraded, disabled or offboarded
- WordPress Administrators who inherit Service Desk access
- Evidence from representative permitted and prohibited action tests