



NOMAD SMALL BUSINESS SUITE

Service Desk Pro - Administrator Role Guide

A complete operating guide for Pro's highest internal role, including user and role management, configuration, financial controls, deletion and the WordPress licence boundary.

Edition: 1.1.3

Audience: Service Desk Administrators and WordPress Administrators

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.

- 01 1. Role purpose and access boundary
- 02 2. Sign-in, navigation and account setup
- 03 3. Creating and maintaining Service Desk users
- 04 4. Daily operating routine
- 05 5. Primary workflow
- 06 6. Communication, notes and records
- 07 7. Handover and escalation
- 08 8. Access problems and recovery
- 09 9. Quick reference and review

1. Role purpose and access boundary

The Service Desk Administrator controls the complete Service Desk operation, configuration, users, roles and financial support functions without automatically receiving unrelated WordPress site administration.

Who should receive this access

Assign this role to the trusted owner of the helpdesk configuration and access model. Use a normal Service Desk Administrator account for helpdesk administration; retain the broader WordPress Administrator role for site-level owners who also manage plugins and licensing.

What this role can see

- Every ticket and ticket history
- All customers, organisations and resources
- All internal notes, files, time, events and sign-off
- Operational analytics, exports, billing and quotes
- All Support Desk settings, AI resources and integrations
- All Service Desk users and assigned roles

What this role can do

- Create, edit, assign, reopen and delete tickets
- Manage customers, resources and WordPress user links
- Create users and change Service Desk roles
- Run HR resource/user synchronisation
- Manage billing, financial quotes and settings
- Configure and use embedded Ticket AI

What this role cannot do

- Open the Pro Licence page unless also a WordPress Administrator
- Administer unrelated WordPress plugins, themes or settings
- Change their own Service Desk role from Users & Roles
- Change a WordPress Administrator account through the Service Desk role screen
- Ignore financial, privacy or deletion approval policy

2. Sign-in, navigation and account setup

Start with the correct named account and confirm that the visible workspace matches the assigned access.

First sign-in

1. Sign in with the named Service Desk Administrator account.
2. Confirm landing on Support Desk > Dashboard.
3. Confirm all Service Desk menus except Licence are present.
4. Open Users & Roles and verify the assigned role.
5. Test one settings page, operational ticket and financial control.
6. Confirm unrelated WordPress administration redirects to Support Desk.

Navigation

Area	Availability or purpose
Dashboard / Tickets / Add Ticket	Full operational access
Customers / Resources	Full management and user links
Analytics / Billing	Reports, exports, batches and invoice actions
Users & Roles	Create users and assign roles
Settings / AI	Complete Service Desk configuration
Licence	Available only to WordPress Administrator

Account and resource relationship

The role receives an active staff resource profile and can be assigned to tickets. It remains a restricted Service Desk account unless it also has the WordPress Administrator role. The highest Service Desk role is deliberately not equivalent to site administration.

3. Creating and maintaining Service Desk users

Provision the narrowest appropriate access and verify the result before handing over the account.

Create a user

1. Open Support Desk > Users & Roles.
2. Enter username, email, optional name and optional password.
3. Select the narrowest appropriate role.
4. Choose whether to send the login/set-password email.
5. Create and confirm role/resource result.
6. Test both a permitted and prohibited action.

Change a role

1. Review current tickets and resource responsibility.
2. Choose the new role for another Service Desk user.
3. Select Update.
4. Confirm operational roles have a resource and Reporting Viewer does not.
5. Retest menu, ticket and data visibility.

Protected accounts

The screen cannot change a WordPress Administrator and does not allow the current user to change their own Service Desk role. Use another authorised administrator and the organisation's account process for those cases.

4. Daily operating routine

Use a consistent routine so ownership, communication and audit records remain current.

Start of day or session

- Review access, mail, file and integration failures
- Review urgent/unassigned tickets and resource capacity
- Check quote, billing and onsite exceptions
- Confirm no unexpected role or resource changes

During the day

- Approve or perform high-risk Service Desk changes
- Support managers and dispatchers with access issues
- Review financial and deletion requests
- Maintain AI resources and settings under policy

End of day or session

- Review destructive/financial actions
- Confirm unresolved security or access issues have an owner
- Check failed automations and handovers
- Record configuration changes

5. Primary workflow

Administer the desk while separating routine operations from restricted configuration and commercial decisions.

Administrative control procedure

1. Confirm the request and authorised owner.
2. Identify the smallest capability or setting involved.
3. Record the current configuration or access state.
4. Back up before material configuration or update work.
5. Apply the narrowest reversible change.
6. Test with the affected non-administrator role.
7. Record result, approver and rollback information.
8. Review access again after the change.

Decision and quality rules

- Use the narrowest role that covers actual duties
- Do not solve Service Desk access by granting WordPress Administrator
- Review before permanent deletion or financial creation
- Licence activation remains a WordPress Administrator task
- Test permissions as the affected role, not only as Administrator

6. Communication, notes and records

Create records that another authorised person can understand without relying on memory or a separate email.

Record standards

Record	Required content
Role change	User, old/new role, reason, approver and test result
Settings change	Old/new value, owner, date, test and rollback
Deletion	Ticket, retention approval, reason and resulting audit evidence
Financial action	Ticket/batch/quote, totals, approver and destination ID
Incident	Scope, affected roles/data, containment and owner

Visibility rules

Content	This role's access or responsibility
All Service Desk data	Visible
Billing/rates/financial PDFs	Visible and manageable
Users and roles	Visible and manageable
Service Desk settings/AI resources	Visible and manageable
Licence/site administration	Hidden unless also WordPress Administrator

Information protection

- Use named administrator accounts
- Review additional recipients and file visibility
- Keep tokens and licence keys out of diagnostic evidence
- Record destructive and financial approvals
- Retain role-review evidence

7. Handover and escalation

Escalate work with enough verified context for the next authorised role to act safely.

Escalate when

- Licence or plugin installation requires WordPress Administrator
- Hosting/database access is required
- A privacy or cross-customer exposure is suspected
- Accounting or licensing response is uncertain
- Policy approval is required for deletion or data export

Handover procedure

1. Record the affected function and current state.
2. Identify users, tickets and integrations in scope.
3. Preserve relevant logs without secrets.
4. State containment or rollback already performed.
5. Assign the correct site, finance, security or service owner.
6. Confirm the next acceptance test.

Escalation evidence

- User and role
- Ticket/resource/quote IDs
- Configuration area and timestamp
- Exact non-secret response
- Plugin/WordPress/PHP versions
- Approval and expected result

8. Access problems and recovery

Identify expected restrictions before treating them as faults.

Access troubleshooting

Problem	Check or action
Licence menu missing	Expected unless the account is also WordPress Administrator
User role cannot be changed	Own role and WordPress Administrator accounts are protected
Resource link wrong	Review role and update through Users & Roles or authorised resource controls
Manager sees rate	Retest with a clean manager account; rates require billing capability
Direct URL opens unexpectedly	Recheck role/capabilities and active Pro runtime

Do not bypass the role model

- Do not add direct capabilities to individual users
- Do not edit role or resource IDs in the database
- Do not share administrator accounts
- Do not publish storage or secure download URLs
- Do not retry uncertain quote/invoice creation without checking the destination

9. Quick reference and review

Use this checklist during onboarding, supervision and periodic access review.

Role checklist

- Named trusted account
- Service Desk Administrator role
- Active staff resource
- Full Service Desk menus except Licence
- Unrelated WordPress pages blocked
- User/role and financial test completed
- Access review scheduled

Periodic review

1. Review all Service Desk and WordPress Administrators.
2. Confirm role, resource and current duties.
3. Review recent role, settings, deletion and financial actions.
4. Downgrade or disable unnecessary access.
5. Repeat cross-role isolation and direct URL tests.

Related master documentation

- Service Desk Pro Implementation Guide
- Service Desk Pro Detailed User Guide
- All Pro role guides
- Customer / Requester Portal Guide