NOMAD SMALL BUSINESS SUITE

Service Desk - Customer / Requester Portal Guide

A detailed portal guide covering account access, ticket submission, organisation scope, public communication, customer files, visits, quotes, sign-off, privacy and escalation.

Edition: Free 0.2.3 / Pro 1.1.3
Audience: Customers, authorised organisation requesters and portal 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.

1. Role purpose and access boundary

The Customer / Requester Portal keeps external access separate from internal Service Desk roles. It lets an authenticated requester create and follow authorised tickets without exposing staff-only work, other organisations, internal analytics or configuration.

Who should receive this access

Provide portal access only to a verified requester linked to the correct Service Desk customer or organisation. Organisation-wide visibility must be authorised by the customer's own access policy; otherwise keep the requester limited to their own submitted tickets.

What this role can see

- Tickets submitted by the requester
- Tickets for the requester's organisation where that broader access is authorised and configured
- Ticket number, subject, description, lifecycle status and public conversation
- Assigned technician name where the portal exposes it
- Customer-visible attachments
- Onsite/visit information stored for the customer workflow
- Quotes or proposals requiring customer attention where Pro and the workflow provide them
- Signature and sign-off requests

What this role can do

- Create a support request
- Review authorised tickets
- Send a public reply
- Provide requested information
- Upload customer-visible supporting files where attachments are enabled
- Download customer-visible files
- Review a quote or proposal through the provided action
- Review work and complete the provided sign-off process
- Ask the Service Desk to correct account or organisation access

What this role cannot do

- See internal notes
- See staff-only or technician-only attachments
- See another customer or unauthorised organisation's tickets
- See technician workload or performance
- See staff analytics, internal escalation details or audit records
- Assign staff or change internal ownership
- Change Service Desk settings, integrations, roles or credentials

- Use an internal Service Desk WordPress role

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. Use the organisation's approved portal link.
2. Sign in with the named customer/requester account.
3. Confirm the displayed identity and organisation.
4. Review the visible ticket list and confirm every ticket is expected.
5. Open a controlled ticket and confirm only public replies and customer-visible files appear.
6. Report any unknown ticket, organisation, internal note or staff-only file immediately without forwarding it.

Navigation

Area	Availability or purpose
Portal home / tickets	Own or authorised organisation tickets
Create request	Submit a new support ticket
Ticket conversation	Public replies and customer-visible files
Visit / quote / sign-off	Shown only when the ticket and Pro workflow require it
Internal administration	Never available
Staff analytics and settings	Never available

Account and resource relationship

Portal access is based on the authenticated WordPress user and its linked Service Desk customer/organisation relationship. It is separate from Service Desk Agent, Administrator, Manager, Dispatcher, Technician and Reporting Viewer roles. A requester should not be assigned an internal role to solve a portal-access problem.

3. Daily operating routine

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

Start of day or session

- Open the approved portal URL
- Check identity and organisation
- Review new Service Desk replies or status changes
- Check requests for information, quote action, visit details or sign-off
- Use one ticket for each continuing issue

During the day

- Reply on the existing ticket
- Answer the exact information request
- Upload only relevant and sanitised files
- Keep visit/contact details current
- Record the ticket number when contacting support through another channel

End of day or session

- Confirm replies and files appear on the correct ticket
- Note the current status and next-action owner
- Avoid creating a duplicate for an existing issue
- Remove downloaded sensitive files from shared devices
- Sign out on shared or public devices

4. Primary workflow

Submit one complete request, keep all updates on its public conversation and complete any customer action securely.

Customer ticket procedure

1. Search the portal for an existing ticket about the same issue.
2. Create a request only when no existing ticket should be continued.
3. Enter a clear subject, description, affected product/service and business impact.
4. Add contact, site, quote or onsite information only when relevant.
5. Attach a sanitised customer-visible file and explain what it shows.
6. Submit once and retain the ticket number.
7. Use the public reply area for updates and requested information.
8. Review the resolution, quote or visit result and complete sign-off only when it matches the work.

Decision and quality rules

- Continue an existing issue on its existing ticket
- Never place passwords, access tokens or unnecessary private information in a ticket
- A public reply is visible to authorised customer and staff users
- Only upload a file the intended customer audience may receive
- Do not approve a quote or sign-off until the details match the agreed work
- Report unexpected access immediately

5. 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
New request	Clear issue, impact, affected service, environment and desired outcome
Public reply	Requested answer, current result and any timing constraint
Attachment	Purpose, safe contents and relationship to the issue
Onsite details	Current site, contact, access and scheduling information
Quote/sign-off	Correct ticket, reviewed scope/result and authorised customer decision

Visibility rules

Content	This role's access or responsibility
Own/authorised organisation tickets	Visible according to the linked customer relationship
Public replies	Visible
Customer-visible attachments	Visible/downloadable through authorised controls
Internal notes and staff files	Hidden
Other customers, staff analytics and workload	Hidden
Settings, roles and credentials	Hidden

Information protection

- Use a named account and protect its password
- Do not include credentials or full licence keys unless the approved process explicitly requires them
- Remove unrelated people and data from screenshots
- Check that an attachment belongs to the correct ticket
- Do not forward portal links or downloaded files to unauthorised recipients
- Report incorrect organisation or ticket visibility immediately

6. Handover and escalation

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

Escalate when

- The visible identity or organisation is wrong
- An unknown ticket or another customer's data appears
- An internal note or staff-only file is visible
- A public reply or customer file cannot be accessed
- A visit, quote or sign-off does not match the request
- The portal is unavailable or login recovery fails

Handover procedure

1. Record the ticket number and portal account email.
2. Describe the expected and actual result.
3. State the page/action and time.
4. Provide a sanitised screenshot only when necessary.
5. Do not send passwords, tokens or unrelated ticket content.
6. Confirm the Service Desk owner and next update channel.

Escalation evidence

- Ticket number
- Account email and expected organisation
- Page/action and timestamp
- Exact non-secret message
- Browser/device type
- Sanitised screenshot if approved

7. Access problems and recovery

Identify expected restrictions before treating them as faults.

Access troubleshooting

Problem	Check or action
No tickets appear	Confirm the correct account and customer/organisation link
A submitted ticket is missing	Refresh once, check confirmation and give Support the ticket number
Cannot upload a file	Check that attachments are enabled, extension/size is allowed and the file is safe
Download is denied	Confirm the account is authorised and the file is customer-visible
Quote/sign-off action missing	Confirm Pro is active and the ticket currently requires that customer action
Unknown ticket appears	Stop viewing and report a possible access issue immediately

Do not bypass the role model

- Do not create an internal WordPress role for a customer
- Do not use another person's customer account
- Do not alter ticket or download URLs
- Do not repeatedly submit when the result is uncertain
- Do not send sensitive attachments through an unapproved fallback channel

8. Quick reference and review

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

Role checklist

- Named requester account
- Correct customer/organisation link
- Expected ticket scope
- Public content only
- Create/reply/file flow tested
- Quote/visit/sign-off tested where used
- Privacy escalation route known

Periodic review

1. Confirm the requester still belongs to the customer/organisation.
2. Confirm own-ticket or organisation-wide scope remains appropriate.
3. Review recent portal access and customer-visible files.
4. Disable leavers and remove unnecessary organisation authority.
5. Repeat cross-customer and internal-content isolation tests.

Related master documentation

- Service Desk Free Detailed User Guide
- Service Desk Pro Detailed User Guide
- Service Desk Free Implementation Guide
- Service Desk Pro Implementation Guide