



Patrol Forge Multiple Company

Customer onboarding and operations handbook

A practical guide for dispatch-company administrators, supervisors, dispatchers, serviced-company teams, officers, and clients

Built for your dispatch operation

This edition focuses only on the customer experience after your dispatch organization has been created. It explains how your team configures companies, gives people the right access, runs CAD, tracks officers, handles emergencies, and maintains accountable records.

Customer Edition 1.0 | Application release 2026.09.19

Patrol Forge LLC | P.O. Box 20431, Albuquerque, NM 87154

<https://multi.patrolforge.com>

Welcome to Patrol Forge Multiple Company

This handbook is written for customers who operate a dispatch center or work for a company served by one. It uses plain operational language and follows the order most customers use when setting up and running the system.

Before you begin

Your written post orders, radio procedures, emergency plan, escalation chain, legal obligations, and continuity plan remain controlling. Patrol Forge helps your team execute and document those procedures; it does not replace them.

What this guide will help you do

- Understand how your dispatch organization and serviced companies are separated.
- Set up company identity, properties, officers, vehicles, clients, SOPs, and access.
- Choose which company changes are blocked, approved first, or applied with notification.
- Use Master CAD and Company CAD without confusing one company for another.
- Create and manage calls, unit status, welfare checks, emergencies, aid, and notifications.
- Use the Officer Portal, GPS sharing, incident reports, Client Portal, reports, and exports.
- Prepare your organization for go-live and troubleshoot common user problems.

Who should read which sections

Customer role	Primary responsibility	Most-used areas
Dispatch Organization Administrator	Configures the dispatch center, companies, access, rules, and oversight.	Organization Settings, users, roles, governance, companies, assignments, audit
Dispatch Supervisor	Oversees active operations and higher-risk decisions.	Master CAD, approvals, emergencies, aid, reports, audit
Dispatcher	Receives calls and coordinates daily field operations.	Master/Company CAD, calls, units, welfare, emergencies, SOPs
Serviced Company Administrator	Maintains the company's authorized records and access.	Company settings, people, properties, vehicles, clients, SOPs, submissions
Serviced Company Supervisor	Works company operations and supervises company resources.	Company CAD, units, resources, incident reports, aid response
Officer / Employee	Shares duty status/GPS, receives operational access, and reports incidents.	Officer GPS, Company CAD reference, SOPs, incident reports, emergency button
Client Portal User	Reviews only the client/property information explicitly granted.	Client Portal

A note about permissions

Your left navigation and available buttons are personalized. If this guide mentions an area you cannot see, your assigned role may not include that capability, you may be in the wrong workspace, or the record may not be in a status that permits the action. Ask your organization's administrator before assuming the feature is missing.

Contents

Welcome to Patrol Forge Multiple Company	2
What this guide will help you do	2
Who should read which sections	2
A note about permissions	2
Contents	3
1. How your account is organized	9
Your Dispatch Organization	9
Your Serviced Companies	9
The three workspace types	9
What company isolation means in daily work	9
2. Accepting your invitation and signing in	11
Accept a new account invitation	11
Normal account types	11
Protect your account	11
If sign-in does not work	11
3. Learning the interface	12
The persistent left navigation	12
Why some items are hidden	12
Items marked Master	12
Notifications and emergency banners	12
Page conflicts and stale forms	12
4. Customer roles and responsibilities	13
Roles do not replace operational policy	13
Built-in roles versus custom roles	13
Least-privilege review questions	13
5. Your recommended customer onboarding sequence	14
Stage 1 - Establish the dispatch center	14
Stage 2 - Define control and responsibility	14
Stage 3 - Build each company workspace	14

Stage 4 - Prove the workflow	14
6. Organization Settings	15
How to save safely	15
What customers cannot change here	15
7. Creating and maintaining Serviced Companies	16
Create a company	16
Choosing a useful company code	16
Archive, delete, and restore	16
Before taking a company out of service	16
8. Dispatch users, roles, and access reviews	17
Invite a dispatch user	17
Manage pending invitations	17
Suspend versus remove	17
Quarterly access review	17
9. Company-change governance and approvals	18
Three governance outcomes	18
How effective rules are chosen	18
Reviewing an approval request	18
What the company user sees	18
10. Setting up company resources in the right order	19
Recommended order for each new company	19
Why order matters	19
Use training data carefully	19
11. Properties, addresses, and maps	20
Create a property	20
Choosing the best marker location	20
How maps identify records	20
12. Officers, employees, and application logins	21
Create a profile	21
Profile identifiers	21
Give an officer application access	21

Important linking rules	21
13. Vehicles, clients, and Client Portal access	22
Vehicles	22
Clients	22
Invite a Client Portal user	22
What clients can and cannot see	22
14. Publishing and using SOPs	23
Create the first published SOP	23
Publish a revision	23
Quick-reference writing guidance	23
Archive an SOP	23
15. Dispatcher assignments	24
Available target types	24
Create an assignment	24
Assignment rules	24
16. Master CAD and Company CAD	25
Master CAD command view	25
Company CAD focused view	25
Refresh timing	25
17. Call intake and call lifecycle	26
Create a call	26
Normal lifecycle	26
Exceptional states	26
Assign responders and dispatchers	26
Notes and closure	26
18. Unit status and vehicle/call linkage	27
Update status from CAD	27
Common status mistakes	27
19. Officer duty and GPS sharing	28
Officer shift start	28
When GPS stops updating	28

How dispatch interprets freshness	28
Shift end	28
20. Welfare checks	29
Start a welfare check	29
Welfare statuses	29
Important limitation	29
21. Officer emergencies	30
Officer activation	30
Dispatcher response sequence	30
Emergency states	30
Audio and visual alerts	30
22. Aid Agreements and Aid Activations	31
Agreement versus activation	31
Create an Aid Agreement	31
Activate aid	31
First-release boundary	31
23. Notifications	32
Use the Notification Center	32
Delivery expectations	32
Notification preferences	32
24. Incident reports	33
Start a draft	33
Review before finalization	33
Write an objective narrative	33
Finalize and print	33
25. Company reports, audit logs, exports, and API tokens	34
Company operational reports	34
Export customer data safely	34
Audit Logs	34
API tokens	34
26. Your plan, capacity, billing, and add-ons	35

What a customer plan may limit	35
Understand an add-on change	35
Billing safety	35
27. Windows app, mobile devices, and offline operation	36
Microsoft Windows application	36
Recommended workstation setup	36
Mobile and tablet use	36
Offline safety	36
28. Daily customer operating checklists	37
Dispatcher shift opening	37
Dispatcher shift closing	37
Officer shift	37
Administrator weekly review	37
29. Practical training scenarios	38
Scenario A - New serviced company	38
Scenario B - Complete call	38
Scenario C - Emergency and aid	38
Scenario D - Governed company change	38
Scenario E - Incident report	38
30. Troubleshooting	39
Send a useful support report	39
31. Security and privacy for customers	40
Every customer user	40
Customer administrators	40
Built-in protections you will notice	40
Your responsibility	40
32. Customer go-live checklist	41
Organization configuration	41
Company data	41
Operational testing	41
33. Quick-reference tables	42

Call priorities42

Core distinctions42

Support information checklist42

1. How your account is organized

The product is designed so one dispatch company can serve many security companies without allowing one customer's data to leak into another customer's operation.



Your Dispatch Organization

Your Dispatch Organization is your dispatch center's private top-level workspace. It contains only the serviced companies, dispatch users, assignments, operations, and settings belonging to your organization. Another dispatch company has a different organization and cannot see yours.

Your Serviced Companies

Each security company you dispatch for is a Serviced Company. Its officers, employees, properties, vehicles, clients, SOPs, calls, incidents, and company users stay attached to that company. The system deliberately requires company ownership on operational records.

The three workspace types

Workspace	Use it when	Identity shown
Master CAD	You need an organization-wide view across all companies you dispatch for.	Dispatch Organization plus the home company on every call, unit, alert, and shared resource
Company Workspace	You are working only with one named security company.	Company name, code, color, logo, and written company label
My Assignments	You want the companies, officers, and properties assigned to you personally.	Each assignment's home company and Primary/Secondary responsibility

The safest habit in the system

Before creating, assigning, editing, or closing anything, read the active organization/company label. If it is wrong, switch workspace first.

What company isolation means in daily work

- A Company Workspace normally shows only that company's resources.
- A Master CAD record always identifies its home company using text as well as color.
- An Aid Agreement does not expose another company's roster. Temporary visibility begins only during an authorized activation or emergency.
- A copied or bookmarked record link never silently changes your company context.

- Cross-company or cross-organization record requests return a non-revealing error rather than confirming that the record exists.

2. Accepting your invitation and signing in

Accept a new account invitation

- 1 Open the newest Patrol Forge invitation sent to your email. Older replaced invitations will no longer work.
- 2 Check that the link opens **multi.patrolforge.com**. Do not enter credentials into a look-alike domain.
- 3 Confirm your name and email. If you already have an account with that email, sign in when asked; otherwise create a strong password.
- 4 Complete the invitation before its expiration time. If it has expired, ask the administrator who invited you to resend it.
- 5 After sign-in, select the Dispatch Organization and the workspace your role permits.
- 6 Read the context labels and confirm that the navigation matches your job before doing operational work.

Normal account types

- **Dispatch user invitation:** gives organization-level access with a dispatch role.
- **Officer application invitation:** links one company login to one officer profile and enables Officer Portal functions.
- **Client Portal invitation:** grants access only to an assigned Client record and its permitted properties.

Protect your account

- Use only your own login. Actions are recorded under the signed-in user.
- Never share passwords, invitation links, password-reset links, sessions, or API tokens.
- Use an organization-approved password manager and lock shared workstations when unattended.
- Sign out when using a shared device. Officers should also go off duty before signing out at shift end.

If sign-in does not work

What you see	What it usually means	What to do
Invitation expired or invalid	The link expired, was revoked, or was replaced.	Ask the same administrator to resend the invitation.
Email not accepted	The account was invited under a different email or the address was entered incorrectly.	Use the exact invited email; ask the administrator to verify it.
No organization/company	Membership may be pending, suspended, revoked, or incomplete.	Contact your organization's access administrator.
403/404 after opening a link	You lack capability, are in the wrong context, or the record belongs elsewhere.	Switch workspace and retry through navigation; do not alter the URL.

3. Learning the interface

The persistent left navigation

Navigation group	Customer-facing destinations
Workspace	Master CAD, Company CAD, Client Portal, Officer GPS, Emergencies, My Assignments, Notifications
Company	Officers & Employees, Properties, Vehicles, Clients, SOPs, Reports, Incident Reports, Settings
Operations	Calls, Units, Welfare Checks, Aid Activations
Approvals	Pending Review, Submitted Changes, Change History
Administration	Serviced Companies, Dispatch Users, Assignments, Aid Agreements, Roles & Permissions, Governance Rules, Notifications, Audit Logs, API Access, Organization Settings, Client Access

Why some items are hidden

Navigation is permission-sensitive. Company-only users will not see organization administration. Dispatchers may see operational pages without seeing role or governance configuration. Client users see only the Client Portal. A hidden item is safer than allowing someone to open a page and discover data they should not know exists.

Items marked Master

When you are inside a Company Workspace, certain organization administration links remain visible with a **Master** badge. Selecting one intentionally leaves the company workspace and opens that Master administration destination. This is an explicit switch, not an inferred one.

Notifications and emergency banners

- The notification count shows unread in-app notices for your active organization membership.
- Critical emergency banners stay visible across navigation until the underlying alert state changes.
- The emergency audio control is separate from emergency acknowledgment and response actions.

Page conflicts and stale forms

Many important forms remember the version you opened. If someone else updates the record before you save, the application rejects your stale submission instead of overwriting newer information. Reload, compare the current record, and apply the still-needed change.

4. Customer roles and responsibilities

Customer role	Primary responsibility	Most-used areas
Dispatch Organization Administrator	Configures the dispatch center, companies, access, rules, and oversight.	Organization Settings, users, roles, governance, companies, assignments, audit
Dispatch Supervisor	Oversees active operations and higher-risk decisions.	Master CAD, approvals, emergencies, aid, reports, audit
Dispatcher	Receives calls and coordinates daily field operations.	Master/Company CAD, calls, units, welfare, emergencies, SOPs
Serviced Company Administrator	Maintains the company's authorized records and access.	Company settings, people, properties, vehicles, clients, SOPs, submissions
Serviced Company Supervisor	Works company operations and supervises company resources.	Company CAD, units, resources, incident reports, aid response
Officer / Employee	Shares duty status/GPS, receives operational access, and reports incidents.	Officer GPS, Company CAD reference, SOPs, incident reports, emergency button
Client Portal User	Reviews only the client/property information explicitly granted.	Client Portal

Roles do not replace operational policy

A capability allows a system action; it does not decide when your organization considers that action appropriate. For example, the ability to close aid or finalize an incident report should still be governed by written supervisory policy.

Built-in roles versus custom roles

- Built-in roles provide safe starting bundles for common jobs and cannot be edited.
- Organization administrators may create custom roles when a built-in role is too broad or too narrow.
- Test custom roles with a training account before using them broadly.
- Review high-impact capabilities such as user management, role management, approvals, emergencies, aid closure, exports, and API access separately.

Least-privilege review questions

- Does this person need organization-wide access or only one company?
- Do they need to view data, manage it, or only submit changes for approval?
- Should they respond to emergencies, manage resolution, or only activate an officer emergency?
- Do they need to export data or create API tokens?
- Who will remove or suspend access when their job changes?

Do not use one shared dispatcher account

Shared accounts remove individual accountability and make access removal difficult. Invite each dispatcher separately and assign the appropriate role.

5. Your recommended customer onboarding sequence

Stage 1 - Establish the dispatch center

- 1 Complete Organization Settings, including timezone, contacts, welfare/aid defaults, and map center.
- 2 Create every initial Serviced Company with a unique code, recognizable color, correct timezone, and logo.
- 3 Invite your administrators and supervisors first. Confirm they can sign in before inviting the full team.
- 4 Review built-in roles and create only the custom roles you actually need.

Stage 2 - Define control and responsibility

- 1 Configure governance defaults for company-managed changes.
- 2 Apply company-specific and field-specific exceptions where required by contract or risk.
- 3 Create dispatcher Primary/Secondary assignments for companies, officers, and properties.
- 4 Create Aid Agreements, but activate them only during a controlled test or real authorized need.

Stage 3 - Build each company workspace

- 1 Add clients and properties; verify map coordinates and property instructions.
- 2 Add officers/employees and vehicles; review identifiers and status.
- 3 Publish current SOP quick references and full procedures.
- 4 Invite/link officer logins and client users only after the records they need are correct.

Stage 4 - Prove the workflow

- 1 Create a training call from intake through closure.
- 2 Put an officer on duty, confirm GPS, change status, assign a call, and complete a welfare check.
- 3 Run a controlled emergency drill including sound, acknowledgment, response ownership, resolution, and closure.
- 4 Run an aid drill showing exactly which resources appear and disappear.
- 5 Create, review, finalize, and print a training incident report.
- 6 Confirm notifications, email delivery, reports, exports, and audit history.

6. Organization Settings

Organization Settings are available in Master context to authorized customer administrators. These settings affect your dispatch operation, not the Patrol Forge platform as a whole.

Setting	What to enter	Where it appears or matters
Display name	The name dispatchers and customers recognize.	Workspace identity and customer-facing organization labels
Timezone	The dispatch center's primary IANA timezone.	Organization-level timestamps and audit presentation
Operations contact	Responsible name, email, and phone.	Administrative contact; contact details are encrypted
Mailing address	Dispatch-center business address.	Organization record and administrative reference
Welfare default	Normal interval from 1 to 480 minutes.	Prefills new welfare checks
Aid default	Normal duration from 15 to 720 minutes.	Prefills manual and qualifying automated aid activations
Map center/zoom	Latitude, longitude, and preferred zoom.	Fallback view when no authorized mapped records exist

How to save safely

- 1 Enter Master context and open **Administration > Organization Settings**.
- 2 Review the current version and existing values before editing.
- 3 Enter both latitude and longitude together if setting a map center.
- 4 Save once and confirm the success message and updated values.
- 5 If a stale-version message appears, reload and compare before resubmitting.

What customers cannot change here

The organization workspace slug, platform service status, subscription assignment, billing configuration, and organization deletion/restoration are not customer Organization Settings. Contact Patrol Forge when those platform-owned items need attention.

7. Creating and maintaining Serviced Companies

Create a company

- 1 Enter Master context and open **Administration > Serviced Companies**.
- 2 Choose **Add serviced company** and enter the display/legal names, short company code, timezone, and status.
- 3 Choose a brand color that remains readable and distinct from your other companies.
- 4 Upload an optional PNG, JPEG, or WebP logo no larger than 2 MB.
- 5 Save, then enter the new Company Workspace and verify its name, code, color, logo, and text label throughout the shell.
- 6 Complete company data and governance before inviting company users.

Choosing a useful company code

Use a short code dispatchers can recognize under pressure, such as a familiar abbreviation. Avoid codes that differ only by punctuation or one easily misheard character. Codes are intended to help identification, not replace the full company name.

Archive, delete, and restore

The customer interface may call the action Delete, but company removal is recoverable soft deletion. The company leaves active service and normal workspace access while protected operational and audit history remains. Restoration is explicit. Permanent purge is intentionally unavailable because calls, emergencies, incidents, governance, and security history may need retention.

Before taking a company out of service

- Resolve or hand off active calls, emergencies, aid activations, and welfare checks.
- End officer duty/GPS sessions and review outstanding incident reports.
- Revoke or suspend company users and client access as appropriate.
- Export only the records your policy requires and store them securely.
- Document the business reason and effective date outside the free-text fields that hold sensitive operational data.

8. Dispatch users, roles, and access reviews

Invite a dispatch user

- 1 In Master context, open **Administration > Dispatch Users**.
- 2 Enter the user's real name and work email.
- 3 Select the organization role that grants only the capabilities needed.
- 4 Send the invitation and confirm its pending state.
- 5 Ask the user to complete sign-in and verify Master/Company access with training data.

Manage pending invitations

Resending or replacing an invitation invalidates the older link. Revoke an invitation when the wrong email or role was used, the person no longer needs access, or the invitation was exposed.

Suspend versus remove

Suspension immediately prevents the membership from resolving into an active organization context while preserving history. Administrators cannot suspend themselves or the final active user who can manage dispatch users. Use suspension promptly for leave, termination, or suspected compromise.

Quarterly access review

- 1 List active users, suspended users, pending invitations, and company-only memberships.
- 2 Verify each user's supervisor, job function, role, and company need.
- 3 Review custom roles and high-impact capabilities.
- 4 Review officer-profile links, Client Portal access, and API tokens.
- 5 Suspend or revoke anything not affirmatively required and record the review according to your policy.

Protect the last administrator

The system blocks changes that would leave your organization without an active user who can manage access. Always maintain at least two trained access administrators when staffing allows.

9. Company-change governance and approvals

Governance lets your dispatch center decide how much control each serviced company receives over its own people, properties, vehicles, clients, profile, and SOPs.

Three governance outcomes

Mode	Customer experience	When to use
Not allowed	The company user cannot submit the action in the application.	Dispatch retains exclusive control or the contract does not permit self-service.
Approval required	The user submits a proposed revision; live data stays unchanged until approval.	Changes need dispatch review before becoming operational.
Direct change with notification	The change applies immediately; dispatch receives a recorded notification.	Trusted low-risk updates can be made without delay.

How effective rules are chosen

- 1 The system first looks for a company-specific field rule.
- 2 Then it looks for a company-specific action rule.
- 3 Then it checks the organization field default and organization action default.
- 4 If several changed fields resolve differently, the strictest mode governs the entire request.
- 5 If no rule exists, the action is denied by default.

Reviewing an approval request

- 1 In Master context, open **Approvals > Pending Review**.
- 2 Verify the requesting company, requester, resource, action, reason, and submission time.
- 3 Compare the before values with every proposed value. Consider operational, contractual, and privacy impact.
- 4 Approve, reject, or request correction. You cannot decide your own request.
- 5 Give a useful comment for rejection or correction. Avoid placing unrelated sensitive information in the comment.
- 6 If approval reports a conflict, open the live record, compare the newer state, and ask for a corrected submission when appropriate.

What the company user sees

Company users follow their requests under **Submitted Changes** and **Change History**. Approval-required submissions never silently alter the live record. Direct changes apply immediately and create history plus dispatch notification.

10. Setting up company resources in the right order

Recommended order for each new company

- 1 Confirm Company Settings, identity, and governance.
- 2 Create Client records when properties will be client-owned.
- 3 Create Properties and verify address/map coordinates.
- 4 Create Officers & Employees with unique company identifiers.
- 5 Create Vehicles and verify operating status.
- 6 Publish SOPs and quick-reference procedures.
- 7 Create dispatcher assignments for the company, its officers, and high-priority properties.
- 8 Invite/link officer logins and Client Portal users only after the underlying records are ready.

Why order matters

Properties can link to existing clients, officer accounts link to existing officer profiles, and operational units use existing officers, vehicles, and calls. Building the durable company records first makes later forms easier and reduces incorrect or duplicate records.

Use training data carefully

- Label training companies/records clearly and keep them out of live operational queues.
- Never use a real person's private information in demonstrations unless policy expressly permits it.
- Remove or archive training resources before production use so dispatchers do not assign them accidentally.

11. Properties, addresses, and maps

Create a property

- 1 Enter the correct Company Workspace and open **Company > Properties**.
- 2 Choose Add property and enter the official property name, status, address, and any permitted company-specific details.
- 3 Link the Client record when the property is owned/managed for a specific client.
- 4 Run address lookup. Review the returned position rather than assuming it is correct.
- 5 Click the map or drag the marker to the precise operational entrance/dispatch location when needed.
- 6 Save and reopen the property to verify address, coordinates, company identity, and client link.

Choosing the best marker location

- Use the location your dispatchers and officers need operationally: main gate, lobby, loading entrance, guardhouse, or designated response point.
- Document unusual access directions in the approved property/SOP fields rather than relying only on a map pin.
- If a large property has several critical locations, follow your organization's record and naming policy instead of placing an ambiguous center point.

How maps identify records

Map element	Meaning
Square marker	Active property with saved coordinates
Circle marker	On-duty officer with an active GPS session and accepted location
Company color	Visual aid matching the home company
Written company label	Authoritative company identity; do not rely on color alone
Layer control	Allows authorized users to show/hide property or officer marker layers

Map location is operational assistance

A pin or GPS report is not proof that a person is at an exact location. Review accuracy, report age, site conditions, and radio confirmation.

12. Officers, employees, and application logins

Create a profile

- 1 Open the correct Company Workspace and select **Officers & Employees**.
- 2 Choose Officer or Employee profile type.
- 3 Enter legal/preferred names and the company employee/badge numbers.
- 4 Choose Active, Leave, or Inactive employment status and enter relevant dates.
- 5 Add only the permitted contact and administrative information. Sensitive contact fields are encrypted.
- 6 Save and verify that the profile appears only in the correct company roster.

Profile identifiers

Employee and badge numbers must be unique inside that Serviced Company. Another company may use the same value. Do not invent a global identifier or reuse an old employee's number unless company policy permits it and the operational impact has been reviewed.

Give an officer application access

- 1 Open the saved officer profile and locate **Officer application login**.
- 2 Send a secure invitation to the officer's exact email, or link one existing eligible same-company login.
- 3 Confirm the invitation is pending and resend/revoke it only through that panel.
- 4 After acceptance, confirm the profile shows exactly one linked login and the Officer / Employee role.
- 5 Have the officer sign in, enter the correct Company Workspace, open Officer GPS, and complete a supervised duty/GPS test.

Important linking rules

- Creating an officer profile alone does not create a password or allow portal access.
- One officer profile links to exactly one eligible company login.
- A login already linked to another officer in that company cannot be reused.
- Suspended/revoked access is not silently reactivated by linking.
- Removing the profile link immediately prevents that login from resolving as the officer for GPS reporting.

13. Vehicles, clients, and Client Portal access

Vehicles

Vehicle records stay inside one company and can be linked to active operational units. Use the company's recognized unit/fleet identifiers and keep status current so dispatchers do not assign an unavailable vehicle.

- 1 Open **Company > Vehicles** in the correct workspace.
- 2 Create the vehicle with the identifiers and status your dispatchers recognize.
- 3 Review the record before making it available for operational-unit selection.
- 4 Change status promptly when the vehicle is out of service or returned to service.

Clients

A Client record represents the customer associated with one or more properties. Linking a property to a client is limited to the same Dispatch Organization and Serviced Company.

Invite a Client Portal user

- 1 Create and verify the Client record and its active properties.
- 2 Open **Administration > Client Access** in that Company Workspace.
- 3 Invite the person's email and select the exact Client access record.
- 4 Ask the recipient to accept the invitation and verify the portal with the administrator.
- 5 Revoke access immediately when the relationship ends or the person changes duties.

What clients can and cannot see

Client Portal includes	Client Portal excludes
Assigned Client identity and active-property summaries	CAD calls, welfare checks, and emergency records
Only records explicitly authorized by active access	Officers/employees, vehicles, SOPs, assignments, and other clients

14. Publishing and using SOPs

Create the first published SOP

- 1 Enter the Company Workspace and open **Company > SOPs**.
- 2 Enter a unique company SOP code, clear title, and category.
- 3 Write a short Quick Reference containing the information dispatch needs first.
- 4 Enter the complete procedure, optional effective date, and revision summary.
- 5 Submit the publication. The result is applied directly, routed for approval, or blocked according to governance.
- 6 After publication, open the dispatcher view and verify the quick reference, full procedure, version number, and effective date.

Publish a revision

A revision creates the next numbered immutable version; it does not overwrite the previous published content. Explain the operational difference in the revision summary. Dispatchers should use the current published version and treat superseded versions only as history.

Quick-reference writing guidance

- Put immediate contact/escalation order, verification questions, and time-sensitive actions first.
- Use short headings and numbered actions that are readable while handling a call.
- Separate normal procedure from emergency exceptions.
- Name the company/property context explicitly when confusion could create risk.
- Do not place passwords, alarm codes, or secrets in fields not approved for that information.

Archive an SOP

Archiving removes the SOP from the default published roster but preserves all versions and history. Confirm replacement guidance is published before archiving an SOP dispatchers still need.

15. Dispatcher assignments

Assignments identify responsibility without limiting an authorized dispatcher's organization-wide Master CAD visibility.

Available target types

Target	Example	Use
Serviced Company	Primary dispatcher for Company Alpha	Overall responsibility for that company's queue
Officer	Secondary dispatcher for Officer 214	Special attention or shared responsibility for one officer
Property	Primary dispatcher for Central Mall	Dedicated responsibility for a site or contract

Create an assignment

- 1 Enter Master context and open **Administration > Assignments**.
- 2 Select the Serviced Company first. Officer and property choices then come only from that company.
- 3 Select the eligible active dispatcher and target type/record.
- 4 Choose Primary or Secondary responsibility.
- 5 Save and verify the home company, dispatcher, target, and responsibility in the roster.
- 6 Ask the dispatcher to open **My Assignments** and verify the card and company-workspace link.

Assignment rules

- A target may have only one Primary dispatcher and multiple Secondary dispatchers.
- The same dispatcher cannot be assigned to the same target twice.
- Targets and dispatcher identity cannot be changed in place; remove and recreate when needed.
- Responsibility changes and removals create immutable audit history.

16. Master CAD and Company CAD

Master CAD command view

- Organization identity and LIVE operating state.
- Counters for active calls, available units, on-duty units, active companies, and open emergencies.
- Emergency focus card linked to the highest-priority open event.
- Company coverage badges and a company-labeled, priority-sorted dispatch queue.
- Organization-wide activity/aid feed and a live property/officer map.
- Embedded unit-status controls for authorized dispatchers.

Company CAD focused view

- The selected company's calls, active properties, officers, and on-duty units.
- The same combined property/officer map, but limited to the active company.
- Only explicitly shared officers from an active, unexpired aid activation; their home company remains visible.
- Shared aid officers are read-only in the receiving company's CAD.

Refresh timing

Information	Normal refresh behavior	Operator responsibility
Emergency alerts	Approximately every 3 seconds	Acknowledge and respond; refresh alone does not change status
CAD state	Approximately every 5 seconds	Reload after a conflict and verify before retrying
Officer locations	Approximately every 10 seconds	Check report age/accuracy and confirm by radio when necessary

Company identity under pressure

Say the company name aloud during high-risk call assignment, emergency response, and aid coordination. Color supports identification but must never be the only cue.

17. Call intake and call lifecycle

Create a call

- 1 Confirm the workspace and home company before opening the intake form.
- 2 Enter the call type and priority based on your organization's written criteria.
- 3 Select a same-company property when applicable, or enter the operational location.
- 4 Enter caller contact/details only when needed and permitted. Sensitive intake fields are encrypted.
- 5 Verify the map marker and move it when the returned address location is not operationally correct.
- 6 Save and verify the generated call number, company, priority, location, and New status.

Normal lifecycle

New -> Queued -> Assigned -> Dispatched -> En Route -> On Scene -> Cleared -> Closed

Exceptional states

Status	Use
Pending Information	Required information is missing or awaiting verification.
Holding	The call is intentionally paused while remaining active.
Canceled	The call will not be completed; a reason is required.
Transferred	Responsibility moved according to procedure; treated as terminal until reopened.
Reopened	A previously cleared/closed/canceled/transferred matter requires renewed work; a reason is required.

Assign responders and dispatchers

- 1 Move a New call to Queued before assigning operational resources.
- 2 Choose eligible officers from the same company and authorized dispatch users.
- 3 The first assignment can advance a queued call to Assigned.
- 4 Release an assignment when it is no longer active; release preserves history.
- 5 Never use a visible aid resource as if it belonged to the receiving company; follow the supported aid workflow and retain home-company identity.

Notes and closure

Call notes are append-only. Write factual, time-relevant information and correct a mistake with a new note rather than trying to erase history. Closing, canceling, and reopening require a reason. Confirm assignments are released and the final disposition is documented before closure.

18. Unit status and vehicle/call linkage

Unit status	When to use	System requirement
Off Duty	Shift ended or unit removed from operation	Clears vehicle/call; dispatch change requires reason
Available	On duty and ready	No active call required
Assigned	Committed to an active call	Active same-company call required
En Route	Traveling to the assigned call	Active same-company call required
On Scene	At the assigned call	Active same-company call required
Busy	Working but not available	Reason required; call link cleared
On Break	Temporarily unavailable	Call link cleared
Unavailable	Cannot accept work	Reason required

Update status from CAD

- 1 Find the officer in Master or Company CAD and verify the home company.
- 2 Expand the status form and review the current version.
- 3 Choose the new status.
- 4 Choose an eligible same-company vehicle and call when appropriate.
- 5 Enter the required operational reason.
- 6 Save and confirm the status, links, timestamp, and immutable history entry.

Common status mistakes

- Leaving an officer On Scene after the call is cleared.
- Leaving a vehicle linked after going Off Duty.
- Using Busy instead of assigning the correct active call.
- Changing an assisting aid officer in the receiving company workspace; those officers are read-only there.
- Retrying a stale form without reloading and reviewing the intervening change.

19. Officer duty and GPS sharing

Officer shift start

- 1 Sign in with the linked officer account and enter the correct Company Workspace.
- 2 Open **Officer GPS** and confirm your officer identity/company.
- 3 Press **Go on duty**. The unit becomes Available and a GPS-sharing session begins.
- 4 When the browser asks, allow precise location for the site/app.
- 5 Keep the page available and verify the screen reports active sharing.
- 6 Use the organization's radio check or dispatch confirmation process at shift start.

When GPS stops updating

- 1 Confirm the officer is still on duty and signed in.
- 2 Open the Officer GPS page and check the permission/status message.
- 3 Use **Restart GPS** and grant location again.
- 4 Disable device/browser power restrictions only when permitted by organization policy.
- 5 Tell dispatch when location is unavailable; do not allow a map to imply coverage that is not present.

How dispatch interprets freshness

State	Default threshold	Meaning
Current	Within 120 seconds	A recent accepted location is available.
Stale	More than 120 seconds	The last point is aging and should be treated cautiously.
Offline	More than 300 seconds	The officer is on duty but no longer reporting a current location.
Not mapped	No usable report/session	The unit may be on duty, but the system does not invent a position.

Shift end

Press **Go off duty** to end duty and close the GPS session, then sign out when appropriate. Signing out also closes an active sharing session. The release uses foreground browser tracking, not native iOS/Android background tracking.

20. Welfare checks

Start a welfare check

- 1 Confirm the unit is on duty and the officer/company identity is correct.
- 2 Open Welfare Checks in Master or Company context.
- 3 Start a timer using the organization default or a permitted value from 1 to 480 minutes.
- 4 Add only the operational note needed for the check.
- 5 Confirm the due time and ensure responsibility is clear during shift handoff.

Welfare statuses

Status	Dispatcher action
Pending	Monitor until response, cancellation, or due time.
Overdue	Use the approved contact/escalation procedure immediately.
Responded	Record the response and factual outcome.
Canceled	Use only when the check no longer applies; preserve the reason/history.

Important limitation

Overdue, Needs Assistance, and Unable to Contact conditions are operationally important, but a welfare record does not automatically create, acknowledge, or close an Emergency Event. Dispatch must follow written escalation procedures and use the emergency workflow when appropriate.

One active timer per unit

The system allows one active welfare check for an on-duty unit. Resolve or cancel the current check before starting a replacement.

21. Officer emergencies

Officer activation

- 1 Use the high-contrast emergency control above duty/GPS controls or the fixed mobile emergency bar.
- 2 Press the action and confirm a second time. Add a short factual message if circumstances allow.
- 3 The system derives officer/company from the signed-in linked account; it does not ask the officer to choose an identity.
- 4 The latest accepted location/accuracy/time is copied as emergency evidence when available.
- 5 Critical alerts are sent to authorized dispatch users and eligible aid may activate.
- 6 Continue the company's radio/phone/emergency procedure. The on-screen state confirms the alert was sent but does not guarantee every recipient heard audio.

Dispatcher response sequence

- 1 Read the officer name, home company, event time, message, and latest-location age/accuracy.
- 2 Open the Emergency Event from the persistent banner or CAD emergency card.
- 3 Acknowledge the event. This records that an authorized user has seen it.
- 4 Claim/assign response ownership so responsibility is explicit.
- 5 Record factual response actions and follow the organization's radio, call, supervisor, and outside-agency procedures.
- 6 Coordinate authorized aid and verify each shared resource's home company.
- 7 Mark Resolved when the immediate condition is addressed; an authorized supervisor completes closure after final review.

Emergency states

State	Meaning
Active - unacknowledged	Alert is open and has not been operationally acknowledged.
Acknowledged	Alert was seen; response ownership/action may still be required.
Response in progress	Active response has an accountable owner.
Resolved - awaiting closure	Immediate condition addressed; final review remains.
Closed	Supervisor-authorized final state; action history remains immutable.

Audio and visual alerts

- Enable/test emergency audio at every workstation at shift start. Browsers require user interaction before sound can play.
- The siren repeats, the tab title flashes, and supported devices may vibrate for current alerts.
- Silencing audio affects only that browser tab/current alerts. It never acknowledges, resolves, or closes an emergency.
- Navigation and page refresh do not remove an open emergency banner.

Five separate actions

Notification acknowledgment, emergency acknowledgment, sound silence, emergency resolution, and emergency closure are not interchangeable.

22. Aid Agreements and Aid Activations

Agreement versus activation

Record	Purpose	Visibility effect
Aid Agreement	Defines which same-organization companies may assist and what categories may be shared.	None by itself
Aid Activation	Authorizes temporary assistance for a reason and duration.	Only explicitly eligible/selected resources during the active window
Emergency sharing	Shares the affected officer and eligible responders when an emergency qualifies.	Limited to the open emergency/activation scope

Create an Aid Agreement

- 1 Enter Master context and open **Administration > Aid Agreements**.
- 2 Choose the requesting and assisting companies inside your Dispatch Organization.
- 3 Choose one-way or permitted direction and the categories allowed by policy.
- 4 Set effective/expiration dates and status.
- 5 Save and verify both companies, direction, categories, and dates.
- 6 Remember: saving the agreement does not expose either company's resources.

Activate aid

- 1 Open Aid Activations from the authorized operations context.
- 2 Choose an active agreement and enter the approved reason/duration.
- 3 Select only the resources needed. Do not share an entire roster when a limited response is sufficient.
- 4 Confirm each shared resource retains its home company label.
- 5 Monitor expiration and extend only under authorized supervisory policy.
- 6 Close the activation as soon as the need ends. Visibility is removed at closure or expiry.

First-release boundary

Aid is available only between Served Companies inside the same Dispatch Organization. It does not create access to a company served by another dispatch company.

23. Notifications

Priority	Examples	Normal customer experience
Critical	Emergency activation, overdue emergency acknowledgment	Persistent in-app item requiring per-recipient acknowledgment plus immediate queued email
Urgent	Aid activation/extension, overdue welfare check	Immediate in-app and email by default
Normal	Emergency/aid resolution or closure	Immediate in-app and email by default
Informational	Assignments and governance activity	Immediate in-app when enabled and eligible for hourly email digest

Use the Notification Center

- 1 Open Notifications from the left navigation and review unread items by priority/time.
- 2 Open the source record for operational action rather than treating notification text as the complete record.
- 3 Acknowledge or mark the notification according to its controls.
- 4 Complete the separate operational action on the emergency, aid, welfare, assignment, or governance record.

Delivery expectations

Email is queued. A functioning queue worker and mail configuration are required. Routine digests depend on the scheduler. The in-app center remains the authoritative customer workspace for current notifications when email delivery is delayed.

Notification preferences

Critical notices cannot be turned off. Routine company/governance notifications may follow immediate, digest, or permitted disabled behavior according to the available preferences. Do not disable a notice required by contract or policy.

24. Incident reports

Start a draft

- 1 Enter the correct Company Workspace and open **Company > Incident Reports**.
- 2 Create a draft and optionally link a same-company Property and CAD Call.
- 3 Complete occurrence date/time/location and reporting information.
- 4 Enter offense/incident details and suspected-use indicators when applicable.
- 5 Complete up to three person entries using Person Code, Entity Type, and Injury Code dropdowns.
- 6 Enter vehicle information, narrative, actions taken, and reporting/assisting/approving officer details.
- 7 Save the draft and verify the version event was recorded.

Review before finalization

- Confirm the company, property, and call links.
- Verify names, dates/times, addresses, person codes, injury codes, and vehicle details.
- Read the narrative chronologically and separate observations from statements.
- Confirm actions taken, notifications, evidence/property handling, and disposition.
- Verify the correct reporting, assisting, and approving officer information.
- Follow your organization's supervisory approval policy before finalizing.

Write an objective narrative

- Describe who, what, when, where, and how using direct, factual language.
- Attribute statements: identify who said what rather than presenting every statement as observed fact.
- Avoid unsupported medical diagnoses, legal conclusions, motives, or character judgments.
- Use a correction in the next draft version; do not hide a substantive change.
- Do not include passwords, tokens, full payment data, or unrelated personal information.

Finalize and print

- 1 Open the reviewed draft and confirm no one else changed it.
- 2 Choose Finalize and complete the confirmation.
- 3 The report becomes read-only and cannot be deleted.
- 4 Open the printable view and use the browser's Print / Save as PDF function when an authorized copy is required.
- 5 Store and share copies only through approved secure methods.

Finalization is permanent

Do not finalize a report simply to see how it prints. Use a training report for practice and complete your review before finalization.

25. Company reports, audit logs, exports, and API tokens

Company operational reports

Reports summarize the selected company's calls, emergency events, welfare checks, aid activations, and current unit statuses. The default range is the latest 30 company-calendar days; the maximum inclusive range is 366 days.

Export customer data safely

- 1 Enter the correct Company Workspace and choose the authorized report/date filters.
- 2 Select calls, emergencies, welfare checks, or aid activations for CSV export.
- 3 If more than 50,000 rows match, narrow the date range.
- 4 Download only to an approved managed device/location.
- 5 Review recipients and use approved encrypted sharing. Delete local copies according to retention policy.

Exports intentionally exclude highly sensitive narratives and details such as caller names/phones, emergency summaries/action notes, welfare notes, and aid reasons. Formula-like cell beginnings are escaped to reduce spreadsheet execution risk.

Audit Logs

Authorized customer administrators use Master-context Audit Logs to review immutable organization activity by date, company, event type, outcome, actor, IP address, reference, and organization-timezone timestamp. Operational timelines remain on their CAD/emergency/aid/welfare/governance records.

API tokens

- Tokens are personal, expiring, hashed, and bound to the authorized Dispatch Organization context.
- The plain token is displayed only when created. Copy it directly into an approved secret manager.
- Never send a raw token through email/chat, place it in screenshots, or commit it to source control.
- Revoke unused or suspected tokens immediately. Plan/API limits may block new token issuance without affecting CAD access.

26. Your plan, capacity, billing, and add-ons

What a customer plan may limit

- Number of active Serviced Companies.
- Dispatch users, including pending invitations.
- Officers per Serviced Company.
- New API-token issuance and other plan entitlements.

A reached or inactive limit blocks creation of new covered resources. It does not disable your existing CAD, emergency, aid, notification, or data access.

Understand an add-on change

- 1 Review your current plan, included capacity, current usage, and recurring price.
- 2 Enter the additional company/officer/capacity amount you need.
- 3 Review the exact recurring price change before confirming.
- 4 Read the next-tier warning. Compare total add-on pricing with the next plan tier before purchase.
- 5 Confirm proration, taxes, credits, and billing interval when shown by the payment provider.

Example

A Starter plan at \$89.99 plus two additional serviced-company units at \$2.50 each becomes \$94.99 for that billing interval before applicable taxes, credits, proration, or provider adjustments.

Billing safety

- Patrol Forge uses hosted payment-provider pages; do not put full card details into application notes or support messages.
- Payment failure, cancellation, or processor outage does not automatically disable operational CAD or emergency access.
- Contact your organization's billing contact or Patrol Forge for subscription/plan ownership questions.

27. Windows app, mobile devices, and offline operation

Microsoft Windows application

The Windows app is a Progressive Web App that opens Patrol Forge in a dedicated application window and receives most feature changes from the hosted service without a new installation.

Microsoft Store: apps.microsoft.com/detail/9mzdnd1ltsvd

Recommended workstation setup

- Use a supported, updated Windows device and browser/webview.
- Allow emergency audio and test it at shift start.
- Use a dedicated work profile/device according to your security policy.
- Prevent sleep/volume settings from silently disabling critical alerting where policy permits.
- Keep the network connection monitored and know the offline continuity plan.

Mobile and tablet use

Pages adapt to iPhone, iPad, Android phones/tablets, and desktop screens. Officers should keep the GPS page available while on duty. Mobile operating systems may pause a foreground website when the screen locks or the page is suspended.

Offline safety

The app intentionally does not cache authenticated pages, CAD calls, GPS locations, emergency data, sessions, or forms for offline operation. When the server cannot be reached, the installed app shows a static offline safety screen instead of potentially outdated operational data.

If the service is unreachable

Move immediately to your approved radio/telephone/paper continuity plan. Do not assume a form, status change, acknowledgment, or emergency action was saved without confirmation.

28. Daily customer operating checklists

Dispatcher shift opening

- Sign in with your own account and confirm the Dispatch Organization.
- Open Master CAD and confirm expected companies, calls, units, and company labels.
- Enable/test emergency audio, workstation volume, flashing title, and supported vibration.
- Review open emergencies, active aid, overdue welfare checks, active calls, and notifications.
- Review My Assignments and the approved shift handoff.
- Check the map and identify on-duty officers with stale/offline/no GPS.
- Open frequently used company SOP quick references.

Dispatcher shift closing

- Confirm each open emergency/aid activation has an owner and documented state.
- Review overdue welfare checks, holding/pending calls, and incorrect unit status.
- Release inactive assignments and complete permitted notes/dispositions.
- Hand off unresolved work through the approved procedure.
- Sign out or lock the workstation.

Officer shift

- Sign in, select the correct company, go on duty, and grant location.
- Confirm active GPS sharing and complete the required radio check.
- Use Restart GPS and tell dispatch if updates stop.
- Know the emergency-button location and the radio/phone fallback procedure.
- Complete incident-report drafts accurately and finalize only under policy.
- Go off duty and sign out at shift end.

Administrator weekly review

- Review users, pending invitations, company memberships, roles, and portal/profile links.
- Review governance requests, conflicts, notifications, and audit exceptions.
- Review plan usage and tier/add-on warnings before adding resources.
- Confirm operational emails/digests are arriving and report background-service concerns to Patrol Forge.
- Run a safe training emergency/aid scenario and record any policy/training changes.

29. Practical training scenarios

Scenario A - New serviced company

- 1 Create a clearly labeled training company with identity/branding.
- 2 Set governance, add one client/property/officer/vehicle, publish an SOP, and create an assignment.
- 3 Invite a company administrator and officer; verify each sees only the intended areas.
- 4 Archive the training company only after the instructor confirms all objectives.

Scenario B - Complete call

- 1 Create a Normal training call at a mapped property.
- 2 Queue, assign, dispatch, move the officer En Route and On Scene, and append factual notes.
- 3 Start/respond to a welfare check, clear the officer, release assignments, and close with reason.
- 4 Review all call and unit history with the trainee.

Scenario C - Emergency and aid

- 1 Enable/test audio, put a training officer on duty, and confirm GPS.
- 2 Activate the officer emergency in a controlled exercise.
- 3 Dispatcher identifies company/location, acknowledges, claims, records action, and coordinates eligible aid.
- 4 Verify only selected assisting resources appear with home-company identity.
- 5 Resolve and supervisor-close the emergency; close aid and verify temporary visibility disappears.

Scenario D - Governed company change

- 1 Set one field to approval required and another to direct with notification.
- 2 Submit the approval-required change as a company user and verify live data is unchanged.
- 3 Review/approve as a different authorized dispatch user and verify the live update/history.
- 4 Submit a direct change and verify immediate application plus dispatch notification.

Scenario E - Incident report

- 1 Create a training draft linked to the training property/call.
- 2 Add three different person entries/codes and a vehicle, narrative, and actions.
- 3 Save a correction, review the version history, finalize, and print to PDF.
- 4 Verify the finalized report cannot be changed or deleted.

30. Troubleshooting

Problem	Try first	Escalate when
Wrong/missing company data	Confirm organization and switch workspace explicitly.	Correct context still lacks authorized records.
Menu/button missing	Check workspace, role/capability, record status, and plan limit.	Administrator confirms it should be available.
409 Conflict	Reload and review the current record/history before retrying.	Conflict repeats or the correct state is unclear.
Property pin wrong	Correct address, rerun lookup, then click/drag marker and save.	Coordinates will not persist or maps fail broadly.
Officer not on map	Check on-duty state, linked login, GPS session, permission, and report age.	Restart GPS fails after device/browser checks.
Emergency sound absent	Enable/test audio, raise device/browser volume, keep visual alerts open.	Multiple workstations fail or policy needs another alert channel.
Invitation email delayed	Verify address/pending state and wait for queued delivery.	Multiple invitations remain undelivered.
Notification/digest delayed	Check in-app center and collect time/notification reference.	Routine delivery remains delayed or critical email fails.
Cannot connect	Use the continuity plan; stop resubmitting forms.	Network/service outage affects operations.
Unexpected access	Stop, preserve safe details, sign out if needed.	Always report immediately as a security incident.

Send a useful support report

- Date, time, and timezone.
- Your customer role and the organization/company label shown.
- Page and action attempted; exact safe error text/status.
- X-Request-Id when displayed.
- Whether the issue affects one user/device or multiple users.
- For GPS: device/browser, permission, duty state, and last-update time.

Never include secrets

Do not send passwords, invitation/reset links, raw API tokens, payment data, private narratives, caller details, or unnecessary personal information in screenshots or support messages.

31. Security and privacy for customers

Every customer user

- Confirm company context before every operational action.
- Use individual accounts and protect credentials.
- Collect and record only information needed for a legitimate operational purpose.
- Share exports/printed reports only with authorized recipients through approved methods.
- Report unexpected access, records, or company visibility immediately.

Customer administrators

- Use least privilege and review access on a schedule.
- Suspend access promptly when duties change or employment ends.
- Use governance rules that match contracts and operational risk.
- Review audit history, exports, client access, officer links, and API tokens.
- Keep company names/codes/colors distinct enough to reduce dispatch confusion.

Built-in protections you will notice

Protection	Customer-facing effect
Explicit workspace context	A record link does not silently switch companies.
Tenant/company boundaries	Foreign records return non-revealing failures.
Encrypted sensitive fields	Selected contacts, narratives, locations, notes, and notifications are encrypted at rest.
Immutable histories	Operational and administrative actions remain accountable.
Version checks	Stale pages cannot silently overwrite newer critical work.
Private storage	Protected files are delivered through authorization rather than public links.

Your responsibility

Customer security also depends on trained users, correct company setup, managed devices, current browsers, accurate permissions, reliable internet/radio plans, and tested emergency/offline procedures.

32. Customer go-live checklist

Organization configuration

- Organization name, timezone, contacts, address, welfare/aid defaults, and map center are correct.
- Every serviced company has the correct name, code, timezone, color, logo, and active status.
- Roles, custom roles, governance defaults/overrides, notifications, and aid agreements are approved.
- Plan capacity is sufficient for companies, users, officers, and required API access.

Company data

- Clients and properties are correct; every operational property marker is verified.
- Officers/employees and vehicles are current and free of obvious duplicates.
- Officer application links and Client Portal access have been tested.
- Current SOP quick references/full procedures are published and superseded guidance archived.
- Dispatcher Primary/Secondary assignments are complete.

Operational testing

- Dispatchers completed a full call lifecycle, unit status changes, and welfare checks.
- Officer on/off-duty and GPS freshness/offline behavior were verified on intended devices.
- Emergency siren, persistent banner, acknowledgment, ownership, action history, resolution, and closure were tested.
- Aid activation exposed only selected resources and removed them at closure/expiry.
- Notifications, company reports, CSV exports, audit logs, and incident-report finalization/printing were tested.
- Offline continuity and security incident reporting procedures were practiced.

Customer acceptance

Go live only when the software workflow and your human response procedures have both been tested. Record who approved the setup, who completed training, and when the next access/emergency drill will occur.

33. Quick-reference tables

Call priorities

Priority	Operational meaning
Critical	Highest urgency under your dispatch center's written criteria.
Urgent	Immediate attention required.
High	Elevated above normal work.
Normal	Standard operational response.
Routine	Low-urgency or scheduled work.

Core distinctions

Do not confuse	With	Difference
Master CAD	Company CAD	All your serviced companies versus one selected company.
Responsibility	Visibility	Assignments identify ownership of work; they do not automatically hide other authorized records.
Aid Agreement	Aid Activation	Permission framework versus temporary live sharing.
Notification acknowledgment	Emergency acknowledgment	Recipient notice state versus the emergency's operational state.
Silence	Acknowledge	Stops audio in one tab versus records that the emergency was seen.
Resolve	Close	Immediate condition addressed versus final supervisory completion.
Draft incident report	Final report	Editable versioned work versus permanent read-only record.
On duty	GPS current	Unit is working versus a recent accepted location exists.

Support information checklist

- Time/timezone, user role, organization/company context.
- Page/action/error and X-Request-Id.
- One user/device or widespread impact.
- No passwords, tokens, private narratives, or payment data.

Patrol Forge LLC

P.O. Box 20431
Albuquerque, NM 87154
multi.patrolforge.com

This handbook describes customer-accessible behavior in the release identified on the cover. Your organization's roles, governance, plan, written policies, and later software updates may change the choices visible to an individual user.