DAEMONCORE // AUTHORIZED ASSESSMENT CONTROL PLANE

FIELDOPS

OPERATOR MANUAL

Signed scope. Pinned targets. Sealed evidence.
Professional assessment operations from one local-first desktop workspace.

PRODUCT	RELEASE	EDITION
DaemonCore Academy	**6.0 Beta 3**	**Latest release**

A LICENSE UNLOCKS THE TOOL. THE ENGAGEMENT AUTHORIZES THE TARGET.

31 AUGUST 2026 // DAEMONCORE APPS

Document control

Field	Value
Document	DaemonCore FieldOps Operator Manual
Product release	DaemonCore Academy 6.0.0-beta.3
Edition	Latest release
Platform	Windows 64-bit; x64 Ubuntu and Debian-family Linux
Publisher	DaemonCore Apps
Classification	Customer documentation
Last revised	31 August 2026

This manual describes the FieldOps functionality shipped with DaemonCore Academy 6.0.0-beta.3, the current Latest release. Product behavior is authoritative when it differs from this document. Preserve an export before upgrading a production workstation and verify release artifacts against the published SHA-256 files.

The product is proprietary commercial software. Possession of this manual or source access does not grant permission to bypass licensing, copy, redistribute, modify, or resell the software. Refer to the license and end-user agreement distributed with the application.

Intended audience

- Authorized security assessors and consultants
- Infrastructure, network, and application security teams
- System owners supervising a controlled assessment
- Reviewers responsible for evidence, findings, and remediation

Conventions

- **FieldOps** means the paid FieldOps Pro workspace inside DaemonCore Academy.
- **Engagement** means a locally stored authorization boundary with exact targets, ports, policy, and dates.
- **Capture** means a diagnostic result sealed with a SHA-256 digest.
- **Permit** means the Ed25519-signed operation permit bound to an engagement.
- **Blocked** means FieldOps rejected an operation before or during execution and recorded the reason.

Contents

1. FieldOps at a glance

FieldOps organizes professional assessment work around one rule: execution must stay inside a declared authorization boundary. Every runnable operation begins with an active FieldOps Pro entitlement, a device-bound operator identity, a signed engagement permit, an exact target, an allowed port where applicable, and a valid testing window.

Core workflow

1. Activate a FieldOps Pro license.
2. Bind the named operator identity to the protected desktop credential context.
3. Create a signed engagement from the written scope or rules of engagement.
4. Collect target and service evidence with diagnostics or campaigns.
5. Review digest-sealed captures in the evidence vault.
6. Promote defensible observations into findings.
7. Retest with a new capture and record the verdict.
8. Export the case file and client-facing report.
9. Close the authorization boundary when work is complete.

Workspace map

Workspace	Primary purpose	Required policy
Diagnostics	Collect focused DNS, TCP, HTTP, TLS, service, and surface evidence	Observe or Validate, depending on operation
Campaigns	Run repeatable assessment profiles across selected authorized targets	Validate or Stress
Assets & evidence	Review observed services, surface drift, captures, and integrity	Any licensed engagement
Findings	Create findings, change disposition, and attach retest evidence	Any licensed engagement
Chaos Engine	Run bounded black-box resilience experiments	Stress
Report / Case file	Export human-readable HTML or machine-readable JSON	Any licensed engagement

OPERATOR NOTE // FieldOps is not an authorization authority, identity-verification service, vulnerability guarantee, exploitation framework, denial-of-service system, or substitute for professional judgment.

2. Installation and first launch

Requirements

- A supported 64-bit Windows installation or x64 Ubuntu/Debian-family desktop
- Permission to install a desktop application
- Network access for initial Lemon Squeezy activation and periodic license validation
- A FieldOps Pro license key for the paid workspace
- Optional: a local Nmap installation or an accessible Docker Engine for deep service inventory

The built-in passive profiler remains available when neither Nmap nor Docker is available. Docker is not required for the standard FieldOps interface, focused diagnostics, evidence management, or reporting.

Install on Windows

1. Download `DaemonCore-Academy-Setup.exe` from the official release channel.
2. Close any running DaemonCore Academy window.
3. Run the installer and follow the Windows prompts.
4. Launch **DaemonCore Academy** from the Start menu or desktop shortcut.
5. Confirm the footer displays `6.0.0-beta.3` and `WINDOWS` before starting paid work.

The current Windows installer is not Authenticode-signed. Windows may show **Unknown Publisher**. Download only from the official release and verify `DaemonCore-Academy-Setup.exe` against `SHA256SUMS-windows.txt` before running it. Do not deploy it through a managed production fleet as a trusted signed package.

Install on Linux

Use the AppImage for a portable launch, or the Debian package for an installed desktop entry. The first beta support matrix covers x64 Ubuntu and Debian-family desktops; compatible derivatives may work but remain outside that matrix.

1. Download either `DaemonCore-Academy-6.0.0-beta.3.AppImage` or `DaemonCore-Academy-6.0.0-beta.3.deb` from the tagged release.
2. Verify the selected package against `SHA256SUMS-linux.txt`.
3. For AppImage, run `chmod +x DaemonCore-Academy-6.0.0-beta.3.AppImage`, then launch it as the desktop user.
4. For Debian packages, run `sudo apt install ./DaemonCore-Academy-6.0.0-beta.3.deb`.
5. Confirm the footer displays `6.0.0-beta.3` and `LINUX`.

Never launch DaemonCore with `--no-sandbox`, as root, or with `--password-store=basic`.

Upgrade

Close the app before upgrading. The Windows installer replaces the prior version, Debian packages upgrade in place, and AppImage users replace the old file manually. Operator progress, licensing metadata, identity material, engagements, captures, findings, and audit records remain in the per-user application-data directory.

Before a material upgrade, export active case files and finish running campaigns or Chaos Engine experiments. Beta.3 consistently uses the version-independent `daemoncore-academy` data directory and retains it during Windows upgrades. When an affected earlier build has only a browser-fallback operator record, beta.3 migrates it automatically without replacing an existing durable profile.

3. Activate FieldOps Pro

Academy training content is available without a paid license. FieldOps is the commercial gate.

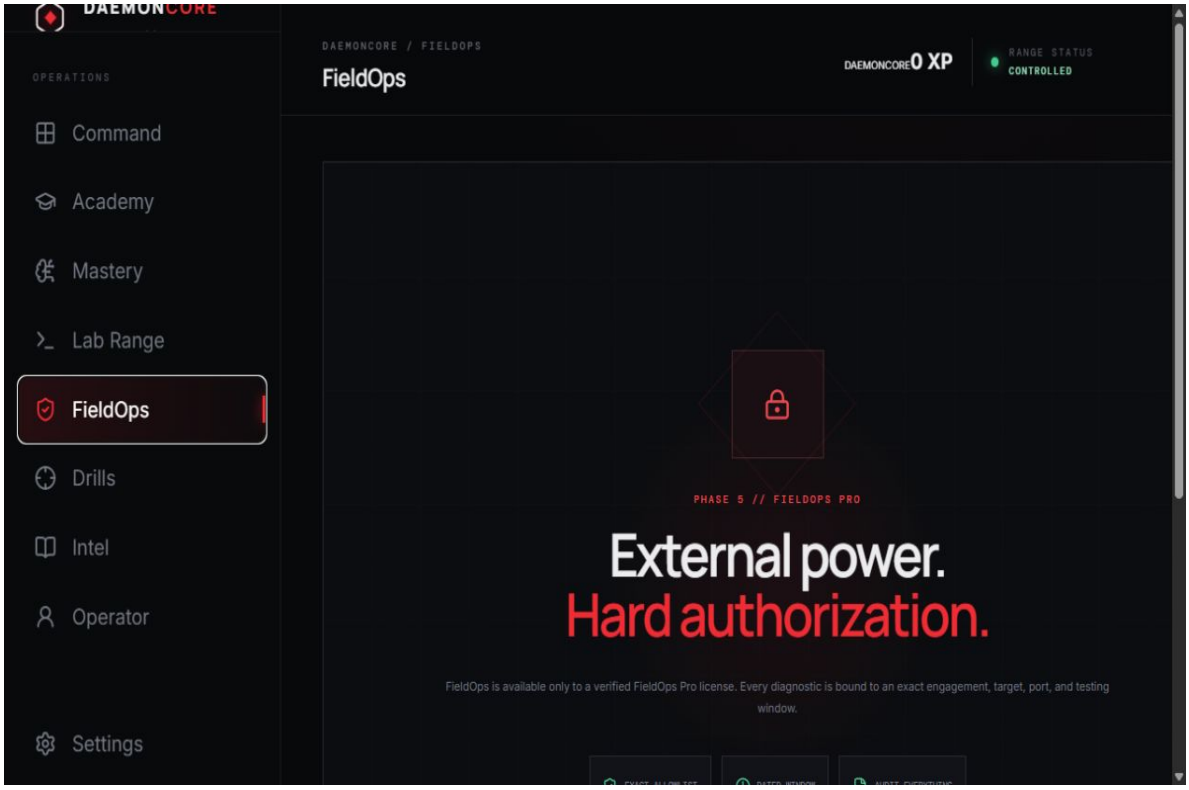
Activate a purchased license

1. Open **Settings**.
2. Locate the commercial licensing section.
3. Enter the license key from the Lemon Squeezy receipt.
4. Enter the checkout email if requested.
5. Give the installation a recognizable device name.
6. Select **Activate**.
7. Confirm the tier reads **FieldOps Pro** and the entitlement is active.

The license key is protected with operating-system credential storage. On Linux, FieldOps activation requires an unlocked GNOME Keyring or KWallet backend; the app blocks protected writes when Electron reports `basic_text`. The interface retains a masked key, license instance, tier, product metadata, validation time, and grace deadline.

Offline grace

After successful validation, FieldOps permits up to 14 days of offline grace when the license service cannot be reached. Grace is not a permanent offline license. Connect and validate before the grace deadline to avoid interruption.



FieldOps Pro gate before commercial activation

Move a license to another device

1. Connect the current device to the internet.

2. Open Settings and deactivate the installation.
3. Install DaemonCore Academy on the replacement device.
4. Activate the license with a new device name.

Deactivation removes the protected license key from the current device. It does not delete engagement evidence.

Activation failures

Message or state	Meaning	Operator action
Different store	The key was issued by another Lemon Squeezy store	Verify the purchase source
Product not recognized	The key does not map to the FieldOps variant	Contact the seller with the order details
Email mismatch	Supplied email differs from the purchase email	Use the checkout email
Secure storage unavailable	The operating system cannot protect the license secret	Verify Windows credential services or unlock GNOME Keyring/KWallet
Offline expired	Validation failed beyond the grace deadline	Restore connectivity and validate
Tampered	Cached entitlement integrity failed	Connect and run license validation again

4. Bind the operator identity

FieldOps requires a named, device-bound operator identity before it permits engagement creation or execution.

Enroll

1. Open **FieldOps** after license activation.
2. Select **Bind operator**.
3. Enter the operator's full name, organization, professional email, and role.
4. Review the displayed information.
5. Save the identity.

FieldOps generates an Ed25519 key pair on the device. The private key is encrypted with operating-system credential storage. The public-key fingerprint and named identity are embedded in permits and signed receipts. The private key is never included in exports.

What the signature proves

The signature can demonstrate that a record was signed by the same device-held key and that signed content has not changed since signing. It does not independently verify that the typed person, organization, approving authority, or authorization claim is truthful.

Protect the identity

- Use a dedicated desktop account protected by strong authentication.
- Do not share an operating-system profile between operators.
- Do not copy protected application-data files between devices.
- Treat a device compromise as a signing-key compromise.
- Preserve exports before rebuilding or retiring the workstation.

OPERATOR NOTE // Updating the displayed operator details reuses the existing device key when it remains accessible. Review identity details before issuing each new permit.

5. Understand the authorization model

The authorization model separates entitlement, attribution, and target authorization. All three must be satisfied.

Layer	Question answered	Enforcement
Entitlement	Is this installation licensed for FieldOps?	Lemon Squeezy tier validation and protected local cache
Attribution	Which device-bound operator initiated the work?	Ed25519 operator identity and signed receipts
Authorization	What may be tested, where, and when?	Signed engagement permit and runtime checks

Policy ladder

Observe

Permits focused posture and identity evidence: DNS resolution, TCP reachability, HTTP response evidence, HTTP security posture, TLS identity, service profiles, and the bounded HTTP resilience baseline.

Validate

Includes Observe and adds broader inventory and assessment operations: DNS record profiles, allowed-port surveys, complete target baselines, deep service inventory, bounded web mapping, and assessment campaigns.

Stress

Includes Observe and Validate and permits the bounded Chaos Engine resilience profiles. Stress must be explicitly selected in the signed engagement.

Network boundary

External mode accepts public addresses only. FieldOps blocks private, loopback, link-local, multicast, reserved, documentation, carrier-grade NAT, and mixed-boundary resolution results.

Internal mode accepts RFC1918 IPv4 or IPv6 unique-local addresses only. Resolution must remain entirely inside that private boundary.

Scope rules

- Between 1 and 100 exact targets
- Between 1 and 128 exact TCP ports
- No CIDR ranges or wildcard targets
- Valid TCP ports from 1 through 65535
- A testing window no longer than one year
- Named approving authority and professional email
- Written authorization or rules-of-engagement reference
- Explicit operator attestation

Hostnames are resolved at execution time and the selected address is pinned for the operation. HTTP requests connect to the pinned address while retaining the authorized host identity. Redirects are not followed.

6. Create and manage an engagement

Prepare the scope

Before opening FieldOps, have the following available:

- Signed statement of work, permission letter, or rules of engagement
- Engagement and client names
- Approving authority name and professional email
- Exact public or internal targets
- Exact permitted TCP ports
- Authorized start and end timestamps
- Required operation policy: Observe, Validate, or Stress

Create the permit

1. Select **New engagement**.
2. Enter the engagement name and client or system owner.
3. Enter the approving authority and email.
4. Select the minimum policy needed for the work.
5. Select External or Internal network mode.
6. Enter the authorization or ROE reference.
7. Enter exact targets separated by spaces, commas, or new lines.
8. Enter allowed TCP ports.
9. Set the validity window.
10. Read and select the authorization attestation.
11. Select **Sign and open engagement**.

The issued permit binds the operator identity, approving authority, client, ROE reference, policy, boundary, targets, ports, and validity window. Altering a bound field invalidates execution.

During the engagement

- Work only from the engagement matching the written authorization.
- Confirm the active testing window before every campaign or resilience run.
- Use the audit ledger to investigate blocked operations.
- Export case files at meaningful milestones.
- Create a new engagement when scope changes; do not treat an old permit as editable authorization.

Close the scope

Select **Close scope** only after running work has settled. FieldOps refuses closure while a campaign or Chaos Engine experiment is active. Closure permanently blocks new diagnostics under that engagement while retaining evidence, findings, dispositions, reports, and the ledger.

7. Run focused diagnostics

Open an active engagement and select **Diagnostics**. Choose an operation, authorized target, and authorized port when required. HTTP operations also accept a path beginning with / and no control characters.

Diagnostic catalog

Operation	Evidence collected	Policy / hard boundary
DNS resolution	Boundary-checked address records	Observe
TCP reachability	Connection result and latency	Observe; one declared port
HTTP response evidence	HEAD status and bounded headers	Observe; no redirect or body download
HTTP security posture	Response controls, cookie flags, implementation disclosure	Observe; one HEAD request
TLS identity and cipher	Protocol, cipher, certificate identity, lifetime, validation state	Observe; one handshake
HTTP resilience baseline	Ten sequential HEAD samples	Observe; concurrency 1, at least 500 ms apart
Service profile	Server-first banner, protocol identity, optional HTTP/TLS context	Observe; 2 KB banner cap
DNS record profile	Address, MX, NS, TXT, CAA, and SOA evidence	Validate; bounded record counts
Allowed-port survey	State and latency for declared ports	Validate; 128 ports, concurrency 4
Complete target baseline	DNS, declared ports, HTTP posture, TLS identity, prior-baseline comparison	Validate; up to eight observed web services
Deep service inventory	Service and version evidence for declared ports	Validate; pinned IP and fixed argument profile
Bounded web map	Fixed control-plane path survey	Validate; eight sequential HEAD requests

Deep service inventory engines

FieldOps selects one of three paths:

1. Local Nmap, when an accessible installation responds to the version probe.
2. Docker Desktop on Windows or an accessible Docker Engine on Linux with the pinned Nmap image.
3. The built-in passive profiler when neither external engine is available.

The bridge passes an already resolved IP address and declared port list as separate arguments. It does not pass a hostname, free-form flags, or shell text. External engine failures are recorded in the evidence and the native profiler is used where possible.

Read the result

Every successful diagnostic produces a capture ID, operation type, target, optional port and path, resolved addresses, elapsed time, result payload, timestamp, and SHA-256 digest. Review the raw result before promoting it. A successful connection or missing header is evidence, not automatically a vulnerability.

Repeat a surface baseline

Run **Complete target baseline** again to compare the latest address set, exposed ports, DNS control-plane records, HTTP posture, response behavior, server disclosure, and TLS certificate fingerprint with the prior sealed surface capture. FieldOps marks baseline established, no change, or drift detected and records each material change.

8. Operate assessment campaigns

Campaigns coordinate repeatable Validate-level modules across selected authorized targets.

Profiles

Profile	Modules	Best use
Service Inventory	Deep service inventory	Build or refresh the authorized service record
Change Verification	DNS profile and surface baseline	Compare present posture with prior evidence
Complete Assessment	DNS profile, deep inventory, and surface baseline	Build the broadest shipped evidence set

Start a campaign

1. Open **Campaigns** in an active Validate or Stress engagement.
2. Name the campaign.
3. Select the profile.
4. Select one or more targets from the engagement allowlist.
5. Confirm the campaign attestation.
6. Select **Launch assessment campaign**.

Only one assessment campaign may be active at a time. Campaigns cannot run while a Chaos Engine experiment or manual diagnostic is active.

Control behavior

- **Pause** requests a safe pause after the current module finishes.
- **Resume** continues pending work and can requeue failed tasks after an interruption.
- **Cancel safely** lets the active module settle before closing the campaign.
- **Completed with errors** retains successful evidence and exposes failed tasks for review or retry.
- A desktop restart marks running work interrupted and returns the active task to pending.

The job ledger records each target/module task, state, linked capture, start and finish time, and bounded failure detail.

9. Work with assets and sealed evidence

The **Assets & evidence** workspace turns individual diagnostics into a durable engagement record.

Asset intelligence

Each authorized target is shown as pending, observed, baselined, or drifted. FieldOps derives observed ports from current surface evidence or earlier inventory captures and displays the latest signal time.

Evidence vault

Captures are stored locally and verified against their SHA-256 digest. The vault displays the operation, target, port or path, digest, timestamp, and duration. When capture integrity fails, promotion controls are disabled.

Evidence handling practices

- Preserve the original case-file export before transforming data for another system.
- Record the engagement, capture ID, and digest in external tickets or reports.
- Do not overstate what a HEAD request, banner, certificate, or connection attempt proves.
- Use a new capture for every remediation retest.
- Investigate an integrity failure before continuing review.

OPERATOR NOTE // SHA-256 integrity detects changes to retained capture content. It does not prove that the assessed system returned truthful information or that the local workstation was uncompromised at collection time.

10. Create, disposition, and retest findings

FieldOps requires sealed evidence before a finding can be created.

Create a finding

1. Select **Promote to finding** from a diagnostic result or evidence row.
2. Confirm the sealed capture.
3. Write a specific title.
4. Select informational, low, medium, high, or critical severity.
5. Describe the observed condition and what the evidence proves.
6. Describe the bounded technical or business impact.
7. Give a specific remediation and measurable closure condition.
8. Select **Seal finding**.

The title must be specific and the observation must contain meaningful evidence. The target is inherited from the capture.

Dispositions

Status	Meaning
Open	The condition requires owner review or action
Accepted risk	The owner accepts the documented condition
Resolved	A later evidence-backed review records closure
False positive	Review determined the original interpretation was incorrect

Retest

Run a fresh diagnostic under the same engagement, then select that new capture in the finding. Record **Still present** or **Verified fixed**. FieldOps appends the retest, adds the capture to the finding evidence set, updates status, and preserves the history.

Do not mark a finding fixed solely because a configuration change was reported. The retest capture should measure the original closure condition.

11. Run Chaos Engine resilience experiments

Chaos Engine performs bounded black-box HTTP resilience sampling. It is available only inside an active **Stress** permit and requires a run-specific authorization confirmation.

Profiles

Profile	Arrival pattern	Purpose
Baseline	One request per second	Establish steady-state behavior
Controlled ramp	Gradually increases to the declared ceiling	Observe the first point of degradation
Traffic spike	Low baseline, short peak, then low rate	Observe stabilization after a brief peak
Bounded soak	Holds the declared ceiling	Observe accumulating latency or errors

Hard caps

- 10 to 60 seconds per run
- 1 to 4 requests per second
- No more than 240 requests
- Concurrency no greater than 4
- One exact target, declared port, and path
- Automatic stop when the configured p95 latency or error-rate boundary is exceeded
- Operator emergency stop
- Recovery sampling and resilience score after the load phase

Run an experiment

1. Confirm the written authorization explicitly covers the planned resilience test.
2. Open **Chaos Engine** in the matching Stress engagement.
3. Select the profile, target, port, path, duration, and request ceiling.
4. Set p95 latency and error-rate abort thresholds appropriate to the service SLO.
5. Confirm the run-specific attestation.
6. Select **Arm and execute**.
7. Watch request count, p95 latency, error rate, phase, progress, and outcome.
8. Use **Emergency stop** if the service behaves unexpectedly.
9. Review recovery evidence and the final score before reporting conclusions.

OPERATOR NOTE // Chaos Engine is not a DDoS tool and must not be represented as one. Its shipped caps are intentionally bounded. Use a dedicated, separately governed performance-testing platform when a larger approved workload is required.

12. Export a case file or professional report

JSON case file

Select **Case file** from the engagement header. The export contains:

- Export schema and timestamp
- Overall audit, capture, and signature integrity verdicts
- Public operator identity metadata
- Engagement and signed permit
- Campaigns and task states
- Diagnostic captures and digests
- Findings, evidence links, dispositions, and retests
- Chaos Engine run history
- Engagement audit entries

The JSON export is intended for archival, machine processing, review, and later verification. Preserve an original copy.

Printable HTML report

Select **Report** to export a standalone HTML assessment record. The report includes engagement and authorization metadata, named operator and approving authority, policy and integrity verdict, campaign summary, service inventory, surface change intelligence, and reviewed findings.

Open the HTML file in a modern browser to review it, then print or save to PDF if required by the client workflow. Inspect the result before delivery; FieldOps does not replace a human technical and editorial review.

Release checklist

- Verify the client and authorization reference.
- Confirm signature, capture, and audit integrity show verified.
- Remove unsupported or overstated conclusions.
- Confirm severity and remediation language with the evidence.
- Verify retest verdicts use later captures.
- Review the report for sensitive operational data.
- Deliver through an approved encrypted channel.

13. Understand integrity and attribution

Capture integrity

Each capture digest covers the retained capture content excluding the digest field itself. The application recalculates every digest when producing the integrity verdict.

Audit integrity

Audit entries include the prior hash for the same engagement. The resulting SHA-256 chain exposes edited, removed, or reordered records within the retained ledger window.

Signature integrity

Signed permits and operation receipts are verified against the public key embedded in the Ed25519 signature envelope. The application also verifies that the engagement still matches the signed permit.

Attribution limits

Device-key attribution is not nonrepudiation by itself. A reviewer should also validate written authorization, workstation custody, operator account controls, system time, export custody, and delivery records.

Verdict	Recommended response
All verified	Continue review while preserving ordinary chain-of-custody controls
Capture integrity failed	Stop promotion and investigate local record changes
Audit integrity failed	Treat the activity history as incomplete or altered
Signature integrity failed	Do not rely on the permit or signed receipt until revalidated

14. Data lifecycle and recovery

FieldOps is local-first. It does not require an Academy account or automatically synchronize engagement data to a DaemonCore cloud service.

Stored locally

- Protected license key and entitlement metadata
- Protected operator signing key and public identity record
- Engagements and permits
- Campaigns and task state
- Captures, findings, retests, and Chaos Engine runs
- Audit ledger

Records are written using temporary-file replacement to reduce partial-write risk. Running campaigns become interrupted after an unexpected desktop stop and can be resumed while the engagement remains valid. Running Chaos Engine experiments become interrupted and are not silently restarted.

The authoritative desktop record remains outside the installation directory and is mirrored to browser storage as a recovery copy. On Windows, the durable record is beneath `%APPDATA%\daemoncore-academy`; on Linux, it is beneath the desktop user's configuration root in `daemoncore-academy`. Upgrading or uninstalling program files does not intentionally remove this record. A cleanup utility, manual directory deletion, or operating-system profile removal can still destroy local data.

Backup

Use FieldOps case-file exports as the supported portable engagement archive. Keep copies in an approved evidence repository. Application-data backups may depend on the original operating-system account, device protection context, and Linux keyring and should not be treated as a portable license or signing-key transfer.

Retention

Define retention before the engagement begins. Case files can contain hostnames, addresses, service details, headers, certificate identity, findings, operator identity, and authorization metadata. Handle them as sensitive customer evidence.

15. Troubleshooting

Diagnostic is blocked

Check, in order:

1. Confirm FieldOps Pro is active or in grace and the selected engagement is active.
2. Confirm the current time is inside the signed validity window.
3. Confirm the policy permits the operation and the exact target and port are allowlisted.
4. Confirm DNS resolution stays inside the selected public or private boundary.
5. Confirm no campaign, diagnostic, or Chaos Engine run conflicts with the operation.

The activity ledger records the blocked reason when an engagement was identified.

Deep inventory reports no engine

- Confirm Nmap is installed and available to the desktop process, or
- Start Docker Desktop on Windows, or confirm `docker version` succeeds as the same unprivileged desktop user on Linux, then retry.

If neither engine is available, FieldOps normally records the adapter notice and uses the built-in passive profiler.

HTTPS operation fails

FieldOps verifies certificates for HTTP HEAD operations and does not follow redirects. Confirm the authorized hostname, selected TLS option, port, certificate chain, and server-name configuration. The separate TLS identity operation can still collect certificate context with validation state for analysis.

License is locked after account, device, or keyring changes

The protected key may be tied to the original credential context. Restore access to that account or keyring, or deactivate/reactivate when possible. Contact the seller if an instance cannot be released.

Operator identity is missing after restart or upgrade

1. Confirm the footer shows `6.0.0-beta.3` or newer.
2. Reopen the installed application shortcut rather than rerunning the setup file.
3. Confirm the per-user `daemoncore-academy` application-data directory was not deleted or redirected.
4. Allow the first beta.3 launch to complete recovery migration when no durable profile exists.
5. Do not reactivate, reenroll, import, or delete data until the original directory and latest case-file export have been preserved for support review.

Campaign was interrupted

Open Campaigns, inspect completed and failed tasks, confirm the permit remains within its validity window, and select **Resume failed or pending**.

Integrity failure appears

Stop creating findings or distributing exports. Preserve the affected files and a fresh case-file export, document the workstation state, and compare against an earlier trusted export. Do not “repair” evidence by editing local JSON.

16. Standard operating procedures

Pre-engagement checklist

- Verify FieldOps version and license state.
- Confirm operator identity and device custody.
- Read the signed authorization and translate it into exact targets and ports.
- Select the minimum required policy.
- Confirm internal versus external boundary.
- Record the approving authority and validity window.
- Agree on abort contacts and thresholds for Stress work.
- Confirm evidence handling and retention.

Daily start

1. Confirm system time and network path.
2. Validate license status when connectivity is available.
3. Confirm the engagement window and written authorization remain active.
4. Review the prior activity ledger and unresolved campaign state.
5. Export a milestone case file before high-value work.

Evidence-to-finding review

1. Verify capture integrity.
2. Read the raw result and identify what it proves.
3. Separate observation from inference.
4. Reproduce when safe and useful.
5. Write bounded impact.
6. Give a measurable remediation.
7. Attach the correct capture and seal the finding.

Closeout

1. Finish, cancel, or document interrupted work.
2. Run required retests and record verdicts.
3. Review finding dispositions.
4. Verify all three integrity verdicts.
5. Export JSON and HTML deliverables.
6. Review and securely deliver the report.
7. Close the engagement boundary.
8. Apply the agreed retention schedule.

Disconnected or air-gapped workstation

FieldOps can continue local review, findings work, reporting, and authorized diagnostics that do not require public name resolution or internet services while the installation remains inside its 14-day offline license grace. Air-gapped operation does not disable entitlement, permit, policy, target, port, time-window, or integrity checks.

1. Validate the license while connected, then record the displayed grace deadline.
2. Preinstall and test required local tools and Docker images before disconnecting; FieldOps does not fetch them across an air gap.
3. Export an initial case file and record its SHA-256 in the engagement evidence log.
4. Confirm system time, operator identity, signed permit, exact targets, ports, and testing window after entering the disconnected environment.
5. Keep case files and printable reports on approved encrypted removable media using the engagement's transfer procedure.
6. Do not copy the protected application-data directory as a substitute for a case-file export.
7. Before the grace deadline, reconnect through an approved path and validate, or stop FieldOps work until validation can occur.

OPERATOR NOTE // An isolated network can still contain production dependencies and sensitive systems. Air-gapped does not mean authorized, low-impact, or safe by default.

17. Product limits and responsible operation

FieldOps 6.0.0-beta.3 provides scoped diagnostics and evidence workflow. It does not claim complete vulnerability coverage and does not replace specialist platforms for interception, packet capture, credentialed vulnerability management, exploitation, source review, cloud-provider APIs, wireless testing, malware analysis, or large-scale performance engineering.

Shipped safety boundaries

- Exact host and TCP-port allowlists
- Public-only or private-only address resolution per engagement
- Permit validity-window enforcement
- Signed policy-level enforcement
- No HTTP redirect following
- HEAD-only HTTP posture and web-map behavior
- Fixed diagnostic and resilience caps
- Single active execution domains to avoid conflicting workloads
- Automatic SLO abort and emergency stop for Chaos Engine
- Recorded blocked actions

These controls reduce accidental scope expansion. They do not make an unauthorized test lawful or safe.

Operator responsibility

The operator must understand the target, authorization, expected load, third-party dependencies, incident contacts, data sensitivity, and applicable law. Stop immediately when actual service behavior differs materially from the approved plan.

18. Quick-reference appendix

Numeric limits

Control	Shipped limit
Targets per engagement	100 exact hosts
TCP ports per engagement	128 exact ports
Engagement window	Maximum 366 days
Port-survey concurrency	4
Surface web services	8
Web-map requests	8 sequential HEAD requests
Service banner	2 KB retained
Baseline samples	10 HEAD requests, concurrency 1
Manual diagnostic spacing	750 ms minimum between launches
Captures retained	2,000 local records
Findings retained	1,000 local records
Campaigns retained	200 local records
Chaos runs retained	100 local records
Audit entries retained	1,000 local records
Chaos duration	10-60 seconds
Chaos ceiling	1-4 requests/second
Chaos maximum	240 requests, concurrency no greater than 4
Offline license grace	14 days after successful validation

Status reference

Area	Common states
License	Unlicensed, active, grace, invalid, offline expired, locked, tampered
Engagement	Active, closed
Campaign	Queued, running, pause requested, paused, cancelling, cancelled, interrupted, completed, completed with errors, failed
Finding	Open, accepted risk, resolved, false positive
Chaos run	Queued, running, recovering, aborting, aborted, interrupted, completed, degraded, failed

Support package

When requesting support, provide the application version, operating-system and distribution version, package type, exact visible error, operation type, and whether Nmap or Docker is available. Remove customer secrets and unnecessary target information. Never send a license key, private application-data file, or protected signing-key material.