SENTINEL AUTHORITY

ODDC Certification Guide

Complete Applicant Roadmap

Version 1.0 — February 2026 — Confidential

ODDC (ODD Conformance Determination) provides independent, third-party attestation that autonomous systems operate within formally declared boundaries with non-bypassable enforcement. This guide walks applicants through the complete certification process from initial inquiry to ongoing conformance monitoring.

Field	Details
Document	ODDC Certification Guide v1.0
Classification	Confidential — Applicant Distribution
Effective Date	February 2026
Owner	Sentinel Authority — Conformance Operations
Contact	conformance@sentinelauthority.org

CONTENTS

Table of Contents

Section page numbers will populate when the Table of Contents field is updated in Word.

OVERVIEW

Executive Summary

Operational Design Domain Conformance (ODDC) is an independent certification that proves an autonomous system operates within its declared boundaries and enforces fail-closed behavior when it does not. Unlike traditional compliance frameworks that rely on design-time documentation and periodic audits, ODDC requires continuous, real-time enforcement verified through a 72-hour live conformance test.

The certification is built on three pillars. First, the applicant declares a precise Operational Design Domain (ODD) defining exactly where, when, and how the system is designed to operate. Second, the ENVELO enforcement agent monitors every declared parameter at runtime and triggers an immediate, non-bypassable shutdown if any boundary is violated. Third, the CAT-72 test generates a cryptographic, tamper-evident evidentiary record proving 72 continuous hours of in-bounds operation.

ODDC certification takes approximately 6–10 weeks from first contact to certificate issuance, depending on system complexity and revision cycles. The base assessment fee is $12,000 per system, with $6,000 annual maintenance for continued monitoring and registry listing.

Who This Document Is For

- Engineering teams responsible for deploying the ENVELO agent and configuring telemetry
- Product and compliance leaders managing the certification timeline
- Executives evaluating ODDC as a trust and safety differentiator
- Legal and regulatory affairs teams preparing for autonomous systems oversight

How to Use This Document

This guide is structured in seven sequential phases. Each phase includes what the applicant is responsible for, what Sentinel is responsible for, what deliverables are required, what the outcome is, and how long it takes. Phase 4 (ENVELO Deployment) contains a complete step-by-step technical walkthrough with platform-specific commands, configuration examples, and troubleshooting references. A quick-start checklist is provided at the end of the document for teams that want a printable task list.

Certification at a Glance

Phase	Duration	Owner	Key Deliverable
1. Inquiry & Eligibility	1–2 weeks	Applicant	System overview, eligibility confirmation
2. Formal Application	1 week	Applicant	Application, ODD spec, tolerances, signed agreement
3. ODD Specification Review	2–3 weeks	Sentinel	ODD acceptance or revision requests
4. ENVELO Deployment	1–2 weeks	Applicant	Agent active, pre-flight passed, portal green
5. CAT-72 Execution	72 hours min	Automated	72h evidentiary telemetry record

6. Determination & Attestation	1–2 weeks	Sentinel	Certificate, report, registry entry
7. Continued Monitoring	Ongoing	Both	Annual review, continuous enforcement

REFERENCE

Glossary of Terms

The following terms are used throughout this document and in all Sentinel Authority communications.

Term	Definition
ODDC	Operational Design Domain Conformance — the certification standard administered by Sentinel Authority
ODD	Operational Design Domain — the formally declared set of conditions under which an autonomous system is designed to operate
ENVELO	Enforced Non-Violable Execution-Limit Override — the runtime enforcement agent deployed alongside your system
CAT-72	Conformance Assessment Test (72-hour) — the mandatory 72-hour continuous operation test
Five Gates	The five requirements for conformance: ODD specification, proven behavior, ENVELO enforcement, cryptographic audit, drift protocol
Fail-closed	Safety behavior where the system halts on boundary violation rather than continuing in a degraded state
Interlock	An ENVELO enforcement action that halts or constrains system operation when a boundary violation is detected
Tolerance	Declared acceptable range for each ODD parameter — locked at application and used as pass/fail criteria
Case ID	Unique identifier (format: ODDC-YYYY-NNNNN) assigned when application is accepted
Conformance Engineer	Assigned Sentinel Authority point of contact for your certification engagement
Attestation	Formal conformance determination issued after successful completion of all Five Gates
Drift	Gradual deviation of system behavior toward or beyond declared ODD boundary edges over time
Telemetry	Boundary-state data transmitted from ENVELO to Sentinel — numeric parameter values and timestamps only
Hash-chain	Cryptographic linking mechanism where each telemetry record references the previous, ensuring tamper evidence

GOVERNANCE

Roles & Responsibilities (RACI)

R = Responsible (does the work) | A = Accountable (approves) | C = Consulted | I = Informed

Activity	Applicant	Sentinel	Exec Sponsor
Initial inquiry	R	I	I
System overview submission	R	I	A
Eligibility determination	I	R/A	I
Application form completion	R	C	A
ODD specification authoring	R	C	I
Tolerance declaration	R/A	C	I
Conformance agreement signing	R	I	A
ODD specification review	C	R/A	I
ENVELO deployment	R	C	I
Pre-flight validation	R	C	I
CAT-72 initiation	R	I	A
CAT-72 monitoring	I	R	I
Evidence review & determination	I	R/A	I
Certificate issuance	I	R	I
Ongoing ENVELO maintenance	R	I	I
Material change reporting	R/A	I	I
Annual surveillance review	C	R/A	I
Suspension/reinstatement	I	R/A	A

PHASE 1

Inquiry & Eligibility

Timeline: 1–2 weeks | **Owner:** Applicant

Before formal application, Sentinel conducts a preliminary assessment to determine whether your autonomous system is a candidate for ODDC conformance. This phase is free of charge and non-binding.

What You Do

- Contact Sentinel Authority via conformance@sentinelauthority.org or the portal at app.sentinelauthority.org
- Provide a plain-language description of the autonomous system under consideration
- Identify the operational domain: healthcare AI, autonomous vehicle, industrial automation, robotic systems, financial AI, or other
- Describe the system's decision-making scope, autonomy level, and human oversight model
- Indicate whether the system is in production, pre-production, or development

What You Provide

Deliverable	Format	Notes
System overview (1–2 pages)	PDF or email	Plain-language description: what it does, how it makes decisions, what it controls
Operational domain description	Free-form	Where, when, and under what conditions the system operates
Contact & billing information	Portal or email	Primary technical contact, business contact, billing entity
Current compliance status	Free-form	Any existing certifications, regulatory filings, audits, or industry standards met

What Sentinel Does

- Reviews submission for eligibility against ODDC scope within 5 business days
- Evaluates whether the system's operational domain can be expressed as quantitative, enforceable boundaries
- Provides a fee estimate, projected timeline, and preliminary scope assessment
- Assigns a preliminary Conformance Engineer if eligibility is likely

Sentinel SLA

- Initial response within 2 business days of inquiry receipt
- Eligibility determination within 5 business days
- If additional information is needed, Sentinel will specify exactly what is required

OUTCOME

> Eligibility confirmation and invitation to proceed to formal application, or specific feedback on what must change before the system qualifies.

PHASE 2

Formal Application

Timeline: 1 week | **Owner:** Applicant

The formal application establishes the scope, boundaries, and technical profile of the system under assessment. This is the binding document Sentinel uses to structure the entire certification engagement.

What You Do

- Complete the ODDC Application Form via the Sentinel portal (app.sentinelauthority.org)
- Define the Operational Design Domain (ODD) — the precise conditions under which the system is declared to operate
- Declare operational tolerances for each boundary parameter (these become the pass/fail criteria for CAT-72)
- Identify all subsystems, models, and firmware versions included in scope
- Execute the Conformance Assessment Agreement and submit payment

What You Provide

Deliverable	Format	Notes
ODDC Application Form	Portal submission	System identity, version, architecture overview, production status
ODD Specification	Template (provided)	Quantitative boundaries: geospatial, temporal, environmental, behavioral
Tolerance Declaration	Template (provided)	Acceptable deviation ranges per parameter — locked at submission
System architecture diagram	PDF or image	Model inputs, outputs, decision paths, actuator connections, subsystems
Signed Conformance Agreement	Digital signature	Terms, fees ($12,000 base), timeline acknowledgment, data handling terms

> ⚠️ Tolerance declarations are locked at submission. They define the pass/fail criteria for CAT-72 and cannot be amended during testing. Carefully review all tolerance ranges before submitting.

ODD Parameter Examples by Domain

The following examples illustrate the type and specificity of ODD parameters expected for different industries:

Autonomous Vehicle

Parameter	Unit	Min	Max
Vehicle speed	m/s	0.0	35.0

Ambient temperature	°C	-10.0	45.0
Visibility range	meters	50.0	unlimited
Lane offset	meters	-0.5	0.5
Wind speed	m/s	0.0	20.0
GPS accuracy	meters	0.0	2.0

Healthcare AI (Diagnostic)

Parameter	Unit	Min	Max
Model confidence score	probability	0.85	1.0
Input image resolution	pixels	512	4096
Patient age range	years	18	99
Processing latency	ms	0	500
Concurrent sessions	count	1	50
Model version hash	SHA-256	(declared)	(declared)

Industrial Automation (Robotic Arm)

Parameter	Unit	Min	Max
Joint torque (per axis)	Nm	0	120
End-effector speed	m/s	0	2.0
Proximity to human	meters	0.5	unlimited
Payload weight	kg	0	25.0
Operating temperature	°C	5.0	40.0
Vibration amplitude	mm/s^2	0	15.0

These are examples. Your ODD parameters will be specific to your system. Sentinel provides a blank template and your Conformance Engineer can advise on parameter selection during Phase 1.

OUTCOME

> Accepted application with assigned Case ID (ODDC-YYYY-NNNNN). Sentinel assigns a dedicated Conformance Engineer to your case who will be your primary contact through certification.

PHASE 3

ODD Specification Review

Timeline: 2–3 weeks | **Owner:** Sentinel

Sentinel conducts an independent review of your declared Operational Design Domain to verify it is complete, internally consistent, measurable, and enforceable by ENVELO at runtime.

What You Do

- Respond to clarification requests from your assigned Conformance Engineer within 5 business days
- Revise ODD parameters if gaps, ambiguities, or conflicts are identified
- Confirm the final ODD specification in writing before proceeding

What Sentinel Does

- Reviews each ODD parameter for measurability, precision, and real-time enforceability
- Validates that tolerance declarations are internally consistent (no parameter conflicts)
- Confirms all boundaries can be monitored and enforced by ENVELO at runtime
- Issues ODD Acceptance or requests revision (up to 2 revision cycles included in base fee)

Sentinel SLA

- Initial review findings delivered within 10 business days of application acceptance
- Each revision cycle reviewed within 5 business days of resubmission
- Additional revision cycles beyond 2 are billed at $1,500 per cycle

Common Review Findings

- **Vague boundaries:** Parameters like “normal operating conditions” or “acceptable range” cannot be enforced. Every parameter must have a numeric min/max.
- **Missing constraints:** Environmental factors (temperature, humidity, lighting) or temporal constraints (time-of-day, season) that affect system behavior but were not declared.
- **Conflicting tolerances:** Parameter ranges that overlap or contradict each other, making enforcement ambiguous.
- **Excluded subsystems:** Components that affect boundary behavior but were excluded from the certification scope.
- **Non-measurable parameters:** Parameters that exist conceptually but have no sensor, API, or telemetry source to provide a real-time value.

OUTCOME

> Accepted ODD specification. This becomes the binding reference document against which CAT-72 conformance is measured. No further changes are permitted after acceptance.

PHASE 4

ENVELO Deployment

Timeline: 1–2 weeks | **Owner:** Applicant

The ENVELO enforcement agent is deployed into your system's runtime environment. ENVELO monitors all declared ODD boundary parameters in real time and enforces fail-closed behavior on any violation. This section is a complete, step-by-step deployment walkthrough. Follow it in order.

Minimum System Requirements

Requirement	Specification
Operating System	Linux (Ubuntu 20.04+, RHEL 8+, Debian 11+), Windows Server 2019+, macOS 12+ (dev/test only)
CPU	2 cores minimum, 4 cores recommended
RAM	512 MB minimum for ENVELO agent (does not include your system's requirements)
Disk	1 GB for agent + logs; 10 GB recommended for 72h CAT-72 telemetry retention
Network	Outbound HTTPS (port 443) to api.sentinelauthority.org; no inbound ports required
Clock	NTP-synchronized; accurate to ±1 second
Docker (if containerized)	Docker Engine 20.10+ or compatible container runtime
Architecture	x86_64 or ARM64

Security Model

Before deployment, understand ENVELO's security posture:

- **Outbound only:** ENVELO opens zero inbound ports. It initiates all connections outbound to Sentinel's API.
- **No remote access:** Sentinel cannot access your system, your network, or your data. ENVELO is entirely customer-controlled.
- **No commands from Sentinel:** The API connection is one-way: ENVELO pushes telemetry out. Sentinel never sends commands in.
- **No PHI/PII:** ENVELO transmits only ODD parameter values (numeric sensor data). It does not access, read, or transmit any business data, patient data, personal information, or application content.
- **Certificate pinning:** All connections use TLS 1.3 with certificate pinning to prevent man-in-the-middle interception.
- **Signed telemetry:** Every telemetry packet is cryptographically signed and hash-chain linked for tamper evidence.

Before You Begin — Pre-Deployment Checklist

Confirm every item before starting:

- ☐ Phase 3 complete — your ODD specification has been formally accepted by Sentinel
- ☐ Portal access — you can log into app.sentinelauthority.org and see your Case ID
- ☐ System access — you have root/administrator access to the target deployment environment
- ☐ Firewall rules — outbound HTTPS to api.sentinelauthority.org:443 is permitted
- ☐ NTP configured — system clock is synchronized (run 'timedatectl' on Linux to verify)
- ☐ Telemetry sources online — every sensor, API, or data source your ODD references is running and accessible
- ☐ Maintenance window — no system updates, deployments, or maintenance planned during deployment + CAT-72

> ⚠️ Do not begin deployment until Phase 3 (ODD Specification Review) is complete and your ODD has been formally accepted.

Step 1: Log Into the Sentinel Portal

Open your browser and navigate to app.sentinelauthority.org. Sign in with the credentials you created during Phase 2.

- From the dashboard, locate your active case (ODDC-YYYY-NNNNN) under "My Cases"
- Click the case to open the case detail view
- Select the "Deployment" tab from the horizontal navigation

The Deployment tab displays:

- Your accepted ODD parameters with tolerance ranges
- Your unique API key (click "Reveal" to show; click "Copy" to copy to clipboard)
- Agent download links for all supported platforms
- The "Download Configuration" button for your pre-populated envelo.yaml file

If you do not see a Deployment tab, your ODD has not yet been accepted. Contact your Conformance Engineer.

Step 2: Download the ENVELO Agent

The ENVELO agent is available in three formats. Choose the one that matches your infrastructure:

Method	Best For	How
Docker container	Cloud, Kubernetes, containerized systems	Pull image from Sentinel's private registry
Standalone binary	Bare-metal servers, VMs, edge devices	Download from portal Deployment tab
Cloud marketplace	AWS, Azure, GCP managed deployments	One-click deploy from your cloud marketplace

Option A: Docker Container

Copy the pull command displayed in the Deployment tab. It includes your unique registry token:

```
docker pull registry.sentinelauthority.org/envelo:latest \
  --username <your-case-id> \
  --password <your-registry-token>
```

Your registry token is displayed in the Deployment tab under "Docker Pull Credentials." It is unique to your case and should not be shared. Tokens expire after 90 days and can be regenerated in the portal.

Verify the image downloaded correctly:

```
docker images | grep envelo
```

✓ Expected: registry.sentinelauthority.org/envelo   latest   <image-id>   <size>

Option B: Standalone Binary

Download the agent package from the Deployment tab. Select your platform:

- Linux x86_64 (.tar.gz)
- Linux ARM64 (.tar.gz)
- Windows Server (.zip)
- macOS Universal (.tar.gz) — development and testing only

```
# Linux example
wget https://app.sentinelauthority.org/agent/<case-id>/envelo-linux-amd64.tar.gz
tar -xzf envelo-linux-amd64.tar.gz
sudo mv envelo /usr/local/bin/
chmod +x /usr/local/bin/envelo
envelo --version
```

✓ Expected output: envelo v1.0.0 (build 2026.01)

✗ If 'command not found': verify the binary is in your PATH and has execute permissions (chmod +x).

Option C: Cloud Marketplace

For AWS, Azure, or GCP, search for "ENVELO Agent — Sentinel Authority" in your cloud marketplace. The marketplace listing handles installation and base networking configuration automatically. You will still need to complete Steps 3–7 below for configuration, validation, and activation.

Step 3: Download and Configure envelo.yaml

The ENVELO agent requires a YAML configuration file that maps your declared ODD parameters to the actual telemetry sources in your system. Sentinel generates a starter configuration from your accepted ODD.

3a. Download the Starter Configuration

In the Deployment tab, click "Download Configuration." Save the envelo.yaml file. This file is pre-populated with:

- Your Case ID and API key
- Every ODD parameter from your accepted specification, including name, unit, min, and max
- The Sentinel API endpoint (api.sentinelauthority.org)

- Default polling intervals and telemetry batch sizes

3b. Map Your Telemetry Sources

Open envelo.yaml in any text editor. For each ODD parameter, you need to tell ENVELO how to read the current value from your system. Each parameter block looks like this:

```
parameters:
  - name: vehicle_speed          # Locked — from your ODD
    unit: m/s                     # Locked — from your ODD
    tolerance_min: 0.0            # Locked — from your ODD
    tolerance_max: 35.0           # Locked — from your ODD
    source_type: mqtt             # YOU CONFIGURE THIS
    source_address: /sensors/speed  # YOU CONFIGURE THIS
    poll_interval_ms: 100         # YOU CONFIGURE THIS
```

ENVELO supports the following telemetry source types:

Source Type	Use Case	Example Address
mqtt	IoT sensors, robotics, vehicle CAN bus bridges	mqtt://localhost:1883/sensors/speed
http	REST APIs, model inference endpoints, health checks	http://localhost:8080/api/v1/state
grpc	High-performance model serving (TensorFlow Serving, etc.)	localhost:50051/ModelService/GetState
file	Log files, CSV state outputs, rotating logs	/var/log/system/state.csv
prometheus	Systems already exporting Prometheus metrics	http://localhost:9090/metrics#vehicle_speed
websocket	Real-time streaming data feeds	ws://localhost:9001/telemetry
custom	Anything else — use the adapter SDK to write a thin bridge	See Adapter SDK documentation in portal

3c. Full Configuration Example: Autonomous Vehicle

```
# envelo.yaml — Autonomous Vehicle Example
case_id: ODDC-2026-00142
api_key: sk-envelo-xxxxxxxxxxxxxxxxxxxx
api_endpoint: https://api.sentinelauthority.org
```

```
telemetry:
  batch_size: 50
  flush_interval_ms: 1000
  retry_attempts: 3

parameters:
  - name: vehicle_speed
    unit: m/s
    tolerance_min: 0.0
    tolerance_max: 35.0
    source_type: mqtt
    source_address: mqtt://localhost:1883/vehicle/speed
    poll_interval_ms: 100

  - name: ambient_temperature
    unit: celsius
    tolerance_min: -10.0
    tolerance_max: 45.0
    source_type: mqtt
    source_address: mqtt://localhost:1883/environment/temp
    poll_interval_ms: 5000

  - name: gps_accuracy
    unit: meters
    tolerance_min: 0.0
    tolerance_max: 2.0
    source_type: http
    source_address: http://localhost:8080/gps/accuracy
    poll_interval_ms: 1000

  - name: lane_offset
    unit: meters
    tolerance_min: -0.5
    tolerance_max: 0.5
    source_type: mqtt
    source_address: mqtt://localhost:1883/perception/lane_offset
    poll_interval_ms: 100
```

3d. Full Configuration Example: Healthcare AI

```
# envelo.yaml — Healthcare Diagnostic AI Example
case_id: ODDC-2026-00287
api_key: sk-envelo-yyyyyyyyyyyyyyyyyyyy
api_endpoint: https://api.sentinelauthority.org

telemetry:
  batch_size: 20
  flush_interval_ms: 5000
  retry_attempts: 3

parameters:
  - name: model_confidence
    unit: probability
    tolerance_min: 0.85
    tolerance_max: 1.0
    source_type: http
    source_address: http://localhost:5000/api/v1/inference/confidence
    poll_interval_ms: 500

  - name: processing_latency
    unit: ms
    tolerance_min: 0
    tolerance_max: 500
    source_type: prometheus
    source_address: http://localhost:9090/metrics#inference_latency_ms
    poll_interval_ms: 1000

  - name: concurrent_sessions
    unit: count
    tolerance_min: 1
    tolerance_max: 50
    source_type: http
    source_address: http://localhost:5000/api/v1/sessions/active
    poll_interval_ms: 2000
```

> ⚠️ Do not modify the name, unit, tolerance_min, or tolerance_max fields. These are locked to your accepted ODD. Changing them will cause pre-flight validation to fail.

3e. Place the Configuration File

```
# Docker: mount as a read-only volume
docker run -v /path/to/envelo.yaml:/etc/envelo/envelo.yaml:ro \
  registry.sentinelauthority.org/envelo:latest

# Standalone binary: pass as argument
envelo --config /path/to/envelo.yaml

# Recommended location (Linux)
sudo mkdir -p /etc/envelo
sudo cp envelo.yaml /etc/envelo/envelo.yaml
sudo chmod 600 /etc/envelo/envelo.yaml
```

Step 4: Verify Network Connectivity

ENVELO requires outbound HTTPS access to exactly two endpoints:

Direction	Destination	Port	Protocol	When
Outbound	api.sentinelauthority.org	443	HTTPS / TLS 1.3	Always (telemetry)
Outbound	registry.sentinelauthority.org	443	HTTPS / TLS 1.3	Docker pull only

Run the built-in connectivity test:

```
envelo test-connectivity --config /path/to/envelo.yaml
```

> ✓ Expected: ✓ API reachable | ✓ TLS 1.3 negotiated | ✓ Certificate pinned | ✓ API key valid

> ✗ If this fails: Check firewall rules, proxy settings, and VPN configuration. See troubleshooting table below.

> ⚠️ SSL inspection proxies (Zscaler, Palo Alto, Fortinet, etc.) will break ENVELO’s certificate pinning. You must add api.sentinelauthority.org to your proxy bypass/allowlist. This is the most common deployment blocker in enterprise environments.

Step 5: Run Pre-Flight Validation

Pre-flight validation confirms that every component is correctly configured before you go live. This is mandatory — the CAT-72 test cannot begin until pre-flight passes.

```
envelo preflight --config /path/to/envelo.yaml
```

Pre-flight runs the following checks in order:

#	Check	What It Validates	Common Fix If Failed
1	Configuration integrity	envelo.yaml matches accepted ODD exactly	Re-download config from portal
2	API authentication	API key is valid and matches Case ID	Re-copy API key from Deployment tab
3	Clock synchronization	System clock within ±1 second of UTC	Configure NTP: ntpd or chronyd
4	TLS verification	TLS 1.3 with certificate pinning	Bypass SSL inspection proxy
5	Parameter connectivity	Every telemetry source is reachable and returning data	Check source_address and source_type
6	Value range check	Current values fall within declared tolerances	System may be in abnormal state — investigate
7	Hash-chain initialization	Cryptographic chain can be established	Ensure sufficient entropy (Linux: check /dev/urandom)

> ✓ All checks pass: ✓ Config ✓ Auth ✓ Clock ✓ TLS ✓ Params (12/12) ✓ Values ✓ Chain

If any check fails, the output identifies the exact failure and suggested fix:

> ✗ ✗ Check 5 FAILED: Parameter ‘ambient_temp’ — source unreachable at mqtt://localhost:1883/sensors/temp. Verify MQTT broker is running and topic exists.

You can run pre-flight as many times as needed. It is non-destructive, does not transmit telemetry, and does not start the CAT-72 clock.

Step 6: Activate the Agent

Once all pre-flight checks pass, activate the agent to begin live enforcement:

```
envelo activate --config /path/to/envelo.yaml
```

Upon activation, the following happens immediately:

- ENVELO begins monitoring all declared ODD parameters at the configured polling intervals
- Telemetry is transmitted to Sentinel via encrypted, outbound-only HTTPS in signed batches
- The portal dashboard updates to show “Agent Active” with a green status indicator
- If any parameter exceeds its declared tolerance, ENVELO triggers its fail-closed interlock and the system halts
- The cryptographic hash-chain begins — every telemetry record links to the previous one

Verify Activation in the Portal

- Log into app.sentinelauthority.org → My Cases → your case → Deployment tab
- Status indicator: green circle with “Agent Active”
- Last telemetry timestamp: should show “< 1 minute ago”
- Parameter list: each parameter shows its current live value and green/amber/red status

- Hash-chain: “Chain Active — 0 gaps”

> ✓ If the portal shows “Agent Active” with all parameters green, deployment is complete. You are ready for CAT-72.

> ⚠️ Do not modify your system, update models, change configuration, or perform infrastructure maintenance after activation. Any changes invalidate the deployment state and require re-running pre-flight.

Step 7: Configure as a Persistent Service (Required for CAT-72)

ENVELO must run continuously through the 72-hour CAT-72 window. Configure it to start automatically on boot and restart on failure. This is not optional — an agent restart during CAT-72 will break the hash-chain and fail the test.

Linux (systemd)

```
# Create service file
sudo cat > /etc/systemd/system/envelo.service << EOF
[Unit]
Description=ENVELO Enforcement Agent
After=network-online.target
Wants=network-online.target

[Service]
Type=simple
ExecStart=/usr/local/bin/envelo --config /etc/envelo/envelo.yaml
Restart=always
RestartSec=5
User=envelo
Group=envelo
LimitNOFILE=65535

[Install]
WantedBy=multi-user.target
EOF

# Create dedicated user
sudo useradd -r -s /usr/sbin/nologin envelo
sudo chown envelo:envelo /etc/envelo/envelo.yaml

# Enable and start
sudo systemctl daemon-reload
sudo systemctl enable envelo
sudo systemctl start envelo
sudo systemctl status envelo
```

Docker Compose

```
# docker-compose.yml
version: '3.8'
services:
  envelo:
    image: registry.sentinelauthority.org/envelo:latest
    restart: always
    volumes:
      - ./envelo.yaml:/etc/envelo/envelo.yaml:ro
    network_mode: host
    logging:
      driver: json-file
      options:
        max-size: '100m'
        max-file: '5'

docker compose up -d
docker compose logs -f envelo
```

Kubernetes

```
# envelo-deployment.yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: envelo-agent
spec:
  replicas: 1      # Must be exactly 1
  selector:
    matchLabels:
      app: envelo
  template:
    metadata:
      labels:
        app: envelo
    spec:
      containers:
      - name: envelo
        image: registry.sentinelauthority.org/envelo:latest
        volumeMounts:
        - name: config
          mountPath: /etc/envelo
          readOnly: true
      volumes:
      - name: config
        secret:
          secretName: envelo-config
```

Windows Service

```
# PowerShell (Run as Administrator)
New-Service -Name 'ENVELO' `
  -BinaryPathName 'C:\Program Files\Sentinel\envelo.exe --config C:\Sentinel\
envelo.yaml' `
  -StartupType Automatic `
  -Description 'ENVELO Enforcement Agent - Sentinel Authority'

Start-Service ENVELO
Get-Service ENVELO
```

Step 8: Deployment Timeline Expectations

Scenario	Estimated Time	Notes
Simple system, 3–5 ODD parameters, Docker	2–4 hours	Download, configure, preflight, activate
Mid-complexity, 10–20 parameters, mixed sources	1–2 days	Telemetry mapping requires testing per source
Enterprise, 20+ parameters, custom adapters	3–5 days	Custom adapter development, security review, proxy config
Fleet deployment (multiple identical systems)	1 day + 1–2 hours per system	First system takes longest; subsequent are config clones

Rollback: Removing ENVELO

If you need to remove ENVELO at any point (before or after CAT-72), the process is straightforward. ENVELO does not modify your system, install kernel modules, or leave persistent artifacts.

Linux (systemd)

```
sudo systemctl stop envelo
sudo systemctl disable envelo
sudo rm /etc/systemd/system/envelo.service
sudo systemctl daemon-reload
sudo rm /usr/local/bin/envelo
sudo rm -rf /etc/envelo/
sudo userdel envelo
```

Docker

```
docker compose down          # or: docker stop <container-id>
docker rmi registry.sentinelauthority.org/envelo:latest
```

Windows

```
Stop-Service ENVELO
Remove-Service ENVELO       # PowerShell 6+; otherwise: sc.exe delete ENVELO
Remove-Item 'C:\Program Files\Sentinel' -Recurse
```

> ⚠️ Removing ENVELO after certification immediately suspends your ODDC conformance status in the public registry. Reinstatement requires a new CAT-72 test.

Deployment Troubleshooting Reference

Symptom	Likely Cause	Fix
Cannot pull Docker image	Registry token expired or incorrect	Regenerate token in portal Deployment tab; tokens expire after 90 days
envelo --version fails	Binary not in PATH or wrong architecture	Verify binary matches your OS/arch; check chmod +x permissions
Pre-flight: config mismatch	envelo.yaml was manually edited in locked fields	Re-download fresh config from portal; only edit source_type and source_address
Pre-flight: parameter unreachable	Telemetry source not running or wrong address	Test source manually (curl, mosquitto_sub, etc.) before retrying
Pre-flight: clock sync failed	System not using NTP	Install ntpd/chronyd; run ‘timedatectl set-ntp true’ on systemd systems
Pre-flight: TLS failure	SSL inspection proxy intercepting traffic	Add api.sentinelauthority.org to proxy bypass list
Portal shows “Agent Offline”	Agent process not running or outbound blocked	Check process status; test outbound: curl https://api.sentinelauthority.org/health

Agent starts then crashes	Insufficient RAM or file descriptor limits	Check dmesg/journalctl for OOM; increase LimitNOFILE in service file
Parameter shows red in portal	Current value outside declared tolerance	This is correct behavior — your system is currently out of bounds; investigate the parameter
Hash-chain gap reported	Agent was restarted or lost connectivity momentarily	If during CAT-72, the test will fail; if pre-CAT-72, restart and re-activate

Getting Help During Deployment

- Your assigned Conformance Engineer is available for deployment support during business hours (9am–6pm ET, Monday–Friday)
- Email conformance@sentinelauthority.org with your Case ID and the output of ‘envelo diagnostics’
- For urgent deployment issues, use the portal’s “Request Support” button on your case detail page
- Sentinel does not access your system remotely — all troubleshooting is based on diagnostics output you provide

```
# Generate a full diagnostics bundle
envelo diagnostics --config /path/to/envelo.yaml > diagnostics.txt

# This outputs: agent version, config checksums, connectivity results,
# parameter status, system resources, clock info. No telemetry data,
# no business data, no PHI/PII.
```

Sentinel SLA for Deployment Support

- Deployment support requests acknowledged within 4 business hours
- Critical deployment blockers (agent won’t start, pre-flight won’t pass) triaged within 1 business day
- Non-critical questions (configuration advice, best practices) responded within 2 business days

OUTCOME

> ENVELO active, pre-flight passed, portal showing green status for all parameters, hash-chain initialized. System is ready for CAT-72 execution.

PHASE 5

CAT-72 Execution

Timeline: 72 hours minimum | **Owner:** Automated (ENVELO)

The Conformance Assessment Test requires 72 hours of continuous, uninterrupted operation within declared ODD boundaries. This is the evidentiary core of the ODDC certification.

What You Do

- Navigate to your case in the portal → CAT-72 tab → click “Begin Test”
- Ensure the system operates normally throughout the entire 72-hour window
- Do not reset, restart, patch, update, or perform maintenance on the system during the test
- Do not modify ENVELO configuration, telemetry sources, or infrastructure
- Optionally monitor the real-time dashboard (monitoring does not affect results)

> ⚠️ The 72-hour clock starts the moment you click “Begin Test.” There is no pause function. If the test fails, you must wait for the full window to expire before re-testing.

What Is Measured

Requirement	Criteria	Failure Condition
Continuous demonstration	72h within declared ODD bounds	Any boundary exceedance at any point
Stress handling	Multi-regime edge conditions	Failure to maintain bounds under load or state transitions
Fail-closed proof	ENVELO halts on deviation	System continues operating after a boundary violation
Telemetry integrity	Signed, hash-chain linked records	Broken chain, unsigned record, or telemetry gap
Tolerance compliance	All parameters within declared range	Any parameter outside declared tolerance range
Clock continuity	Timestamps monotonically increasing	Clock jump, reset, or NTP drift > 1 second

What Happens If CAT-72 Fails

If the test fails for any reason:

- ENVELO captures the exact failure condition, timestamp, and parameter values at the moment of failure
- The portal displays a detailed failure report identifying what failed and why

- You must wait for the 72-hour window to expire before re-testing (you cannot restart mid-test)
- One re-test is included in the base $12,000 assessment fee
- Additional re-tests beyond the first are billed at $3,000 per attempt
- Remediate the root cause, re-run pre-flight, and then initiate a new CAT-72 window

Evidence Generated

- Cryptographically signed telemetry log covering the full 72-hour window
- Hash-chain linked state recordings (each record references the previous)
- Interlock activation events with timestamps and triggering parameter values
- Convergence metrics and boundary proximity data (how close to limits the system operated)
- ENVELO enforcement verification records (proof the agent was active and non-bypassed)

All evidence is generated and signed automatically by ENVELO. Neither the applicant nor Sentinel can modify the evidentiary record after the fact.

OUTCOME

> Complete evidentiary record submitted to Sentinel for independent determination. Applicant receives preliminary status notification within 24 hours of test completion.

PHASE 6

Determination & Attestation

Timeline: 1–2 weeks | **Owner:** Sentinel

Sentinel reviews all CAT-72 evidence, conducts independent verification, and issues a conformance determination.

What Sentinel Does

- Validates the complete telemetry hash-chain — no gaps, no unsigned records, no tampering
- Verifies all Five Gates are satisfied:
  - Gate 1: ODD formally specified with quantitative, enforceable boundaries
  - Gate 2: 72 continuous hours of proven in-bounds behavior
  - Gate 3: ENVELO enforcement active, non-bypassable, fail-closed throughout
  - Gate 4: Tamper-evident cryptographic audit records with unbroken hash-chain
  - Gate 5: Drift protocol established with clear suspension and re-certification path

Issues conformance determination: **CONFORMANT** or **NON-CONFORMANT**

Sentinel SLA

- Preliminary determination communicated within 5 business days of CAT-72 completion
- Final certificate and report issued within 10 business days
- If Non-Conformant, detailed findings report explains every failure and remediation path

What You Receive

Deliverable	Description
ODDC Certificate	Digitally signed PDF certificate with unique ID (ODDC-YYYY-NNNNN), valid 12 months
Conformance Report	Detailed findings, metrics, gate-by-gate verification, boundary proximity analysis
Public Registry Entry	Live listing on registry.sentinelauthority.org with real-time conformance status
Verification QR Code	Embeddable image linking to your registry entry — for customer presentations, regulatory filings, and marketing
Certificate Hash	SHA-256 hash for independent verification against the public registry

OUTCOME

> ODDC certificate issued. System listed on the public registry with active conformance status. Certificate valid for 12 months from issuance, subject to continued monitoring requirements.

PHASE 7

Continued Monitoring

Timeline: Ongoing (annual cycle) | **Owner:** Both parties

ODDC conformance is not a point-in-time event. It is a continuous status that requires ongoing enforcement, monitoring, and annual renewal.

Your Ongoing Obligations

- Maintain ENVELO agent in active, continuous deployment — any gap triggers suspension
- Report material changes to your Conformance Engineer within 48 hours
- Notify Sentinel of any ENVELO interlock activation within 48 hours, with context
- Cooperate with the annual surveillance review
- Pay annual maintenance fee ($6,000 per system per year)

What Triggers Re-Certification ($8,000)

- **Model update:** Any retraining, fine-tuning, or version change that affects the model's decision-making behavior
- **ODD change:** Any modification to declared boundaries, tolerance ranges, or parameter definitions
- **Infrastructure migration:** Moving the system to a new server, cloud provider, or runtime environment
- **Architecture change:** Adding, removing, or replacing subsystems that affect boundary behavior
- **Interlock activation:** Any ENVELO interlock activation that was not determined to be a false positive

Suspension vs. Revocation

	Suspension	Revocation
Trigger	Operational — agent offline, telemetry gap, unreported change, non-payment	Integrity — evidence of tampering, fraud, or deliberate circumvention
Registry status	SUSPENDED (yellow)	REVOKED (red)
Timing	Immediate upon detection	After investigation and due process
Path to reinstatement	Fix the trigger condition + new CAT-72 ($8,000)	No reinstatement — full new application required
Public visibility	Visible on registry with suspension date	Visible on registry permanently

Specific Suspension Triggers

- ENVELO agent removed, disabled, or unreachable for more than 1 hour
- Telemetry gap exceeding 24 hours without prior written notification to Sentinel
- Unreported material system change discovered during surveillance
- Failed annual surveillance review (unresolved findings after 30-day remediation window)

- Non-payment of maintenance fees after 30-day grace period

Annual Surveillance Review

Each year, Sentinel reviews the full 12 months of ENVELO telemetry for your certified system:

- Conformance trending: how close to declared boundaries the system has operated over time
- Violation mapping: conditions, timestamps, and patterns of any interlock activations
- Drift analysis: whether the system's behavioral profile is shifting toward boundary edges
- Parameter utilization: which tolerances are consistently near limits (potential ODD refinement opportunities)
- Actionable findings report delivered to the applicant with recommendations
- Certificate renewal upon successful review — new 12-month validity period

Data Retention Policy

Data Type	Retention Period	Notes
Real-time telemetry	90 days	Rolling window; oldest data purged automatically
CAT-72 evidentiary record	7 years	Regulatory-grade retention; tamper-evident archive
Conformance reports	7 years	Accessible via portal for certificate lifetime + 7 years
Annual surveillance findings	7 years	Archived with associated telemetry snapshots
Application and ODD documents	Life of certificate + 3 years	Retained for re-certification reference
Diagnostics bundles	90 days	Auto-deleted; not included in long-term archive

Sentinel stores only ODD parameter values (numeric telemetry). No business data, application content, PHI, or PII is ever stored.

OPERATIONS

Emergency Procedures

ENVELO Interlock Activation (Boundary Violation)

If ENVELO detects a parameter exceeding its declared tolerance, the interlock activates immediately:

- The system enters fail-closed state (safe shutdown)
- ENVELO logs the exact parameter, value, timestamp, and system state at the moment of violation
- The portal displays an alert on your case dashboard
- If this occurs during CAT-72, the test fails automatically

Immediate Actions

- Do not attempt to restart the system or override ENVELO
- Document what was happening when the interlock activated (operator observations, environmental conditions)
- Review the interlock event details in the portal (case → Events tab)
- Notify your Conformance Engineer within 48 hours via email or portal

False Positive Assessment

If you believe the interlock activation was a false positive (sensor malfunction, transient spike, etc.):

- Submit a False Positive Report via the portal (case → Events tab → “Report False Positive”)
- Include sensor calibration data, environmental context, and any supporting evidence
- Sentinel reviews within 5 business days and issues a determination
- If confirmed false positive: no impact on conformance status
- If not confirmed: the event stands and re-certification may be required

Agent Offline / Connectivity Loss

- ENVELO buffers telemetry locally during brief connectivity interruptions (up to 1 hour)
- If connectivity is not restored within 1 hour, the agent enters “Degraded” mode and the portal shows amber status
- If the gap exceeds 24 hours, automatic suspension is triggered
- To prevent suspension during planned maintenance: submit a Maintenance Notification via the portal at least 48 hours in advance

Emergency Contact

- Business hours (9am–6pm ET, Mon–Fri): conformance@sentinelauthority.org or portal support button
- After hours for active CAT-72 tests: emergency@sentinelauthority.org (monitored 24/7 during active test windows)

- Always include your Case ID in all communications

SCALE

Multi-System & Fleet Certification

If you are certifying multiple systems — whether identical units in a fleet or distinct systems across your organization — the following guidance applies.

Identical Systems (Fleet)

For fleets of identical systems (same software, same model, same ODD):

- One ODD Specification Review covers all units (Phase 3 is done once)
- Each unit requires its own ENVELO deployment and CAT-72 test (Phases 4–5 per unit)
- Each unit receives its own certificate and registry entry
- Configuration cloning: after the first unit passes, you can clone envelo.yaml (updating only system-specific source addresses) for subsequent units
- Fleet pricing available — contact conformance@sentinelauthority.org

Distinct Systems

For different systems (different software, different ODDs):

- Each system requires a separate full engagement (Phases 1–7)
- Each system has its own Case ID, ODD, certificate, and annual maintenance
- A dedicated Conformance Engineer can be assigned across multiple cases for organizational consistency

Enterprise Program

Organizations certifying 5 or more systems are eligible for the Enterprise program:

- Volume pricing on assessments and annual maintenance
- Dedicated Conformance Engineer for your organization
- Custom integration support (CI/CD pipeline integration, automated pre-flight in build process)
- Priority SLAs on all review and support timelines
- Quarterly conformance health review across your portfolio
- Contact conformance@sentinelauthority.org to discuss Enterprise terms

REFERENCE

Frequently Asked Questions

How long does the entire certification process take?

Approximately 6–10 weeks from first contact to certificate issuance, depending on system complexity, ODD revision cycles, and how quickly your team completes deployment. The fastest certifications (simple system, clean ODD, no revisions) have completed in 5 weeks.

Can we start deployment before the ODD review is complete?

No. The ENVELO configuration is generated from the accepted ODD specification. If the ODD changes during review, the configuration would be invalid. You must wait until Phase 3 is complete.

What happens if our system legitimately needs to operate outside its declared ODD?

Then the ODD was declared too narrowly. This is caught during Phase 3 review. If discovered post-certification, you must update the ODD and re-certify ($8,000). ENVELO will enforce the boundaries as declared — it does not make exceptions.

Does ENVELO affect system performance?

ENVELO's resource footprint is minimal (512 MB RAM, <5% CPU). It reads telemetry from existing sources and does not intercept, modify, or add latency to your system's primary operations. The fail-closed interlock activates only when a boundary is violated.

Can we run ENVELO in a staging environment first?

Yes, and we recommend it. Deploy ENVELO in staging, map your telemetry sources, and run pre-flight there before deploying to production. Staging telemetry is not submitted to Sentinel and does not count toward CAT-72.

What if our system uses a proprietary telemetry protocol?

Use the 'custom' source type and write a thin adapter using the ENVELO Adapter SDK (available in the portal). The adapter translates your proprietary protocol into a standard interface ENVELO can poll. Your Conformance Engineer can advise.

Is ODDC recognized by regulators?

ODDC is an independent certification standard. It is designed to satisfy evidentiary requirements for autonomous systems oversight. Regulatory recognition varies by jurisdiction and industry. Sentinel provides documentation formatted for regulatory submission.

Can we pause CAT-72 for planned maintenance?

No. The 72-hour test must be continuous and uninterrupted. Plan all maintenance before initiating the test. If the system requires maintenance during the window, the test fails and must be restarted from zero.

What data does Sentinel store about our system?

Only numeric ODD parameter values (e.g., speed, temperature, confidence scores). Sentinel never stores business data, application content, model weights, source code, PHI, or PII. See the Data Retention Policy section for details.

Can our competitors see our certification details?

The public registry shows your system name, conformance status, certificate date, and ODD parameter names. It does not show tolerance values, telemetry data, or the conformance report. The detailed report is shared only with the certificate holder.

What if ENVELO has a bug or false positive during CAT-72?

Submit a support request immediately. If Sentinel confirms an ENVELO defect caused the failure (not a legitimate boundary violation), the re-test is provided at no charge and the defect is patched before retesting.

Do we need to certify every model version?

Only if the model update affects decision-making behavior. Cosmetic changes, performance optimizations, or infrastructure updates that do not change boundary behavior do not require re-certification. When in doubt, consult your Conformance Engineer.

COMMERCIAL

Fee Schedule

Service	Fee	Includes
Conformance Assessment	$12,000 / system	Application, ODD review (2 revision cycles), ENVELO deployment support, CAT-72, certificate issuance, one re-test
Annual Maintenance	$6,000 / system / year	12-month surveillance review, public registry listing, certificate renewal, annual findings report
Re-Certification	$8,000 / system	Required after material changes; includes ODD re-review, new CAT-72, updated certificate
Additional CAT-72 Re-Test	$3,000 / attempt	Beyond the one re-test included in base assessment fee
Additional ODD Revision Cycle	$1,500 / cycle	Beyond the two revision cycles included in base assessment fee
Enterprise Program	Custom	Volume pricing, dedicated engineer, priority SLAs, portfolio health reviews

All fees USD. Rates are base pricing — final pricing may vary based on system complexity, parameter count, and custom integration requirements. Contact conformance@sentinelauthority.org for a formal quote.

APPENDIX

Quick-Start Checklist

Print this page. Work through it in order. Check each item as you complete it.

Phase 1: Inquiry

- ☐ Contacted Sentinel at conformance@sentinelauthority.org or via portal
- ☐ Provided system overview (1–2 pages, plain language)
- ☐ Received eligibility confirmation

Phase 2: Application

- ☐ Completed application form in portal
- ☐ Defined all ODD parameters with numeric min/max ranges
- ☐ Declared tolerance ranges for every parameter
- ☐ Submitted architecture diagram
- ☐ Signed Conformance Agreement and submitted payment ($12,000)
- ☐ Received Case ID (ODDC-YYYY-NNNNN)

Phase 3: ODD Review

- ☐ Responded to all Conformance Engineer clarification requests
- ☐ Completed all required ODD revisions
- ☐ Received ODD Acceptance confirmation

Phase 4: Deployment

- ☐ Confirmed minimum system requirements met
- ☐ Verified firewall allows outbound to api.sentinelauthority.org:443
- ☐ Downloaded ENVELO agent (Docker, binary, or marketplace)
- ☐ Downloaded envelo.yaml from portal Deployment tab
- ☐ Mapped all telemetry sources (source_type + source_address for every parameter)
- ☐ Passed connectivity test (envelo test-connectivity)
- ☐ Passed pre-flight validation (envelo preflight) — all checks green
- ☐ Activated agent (envelo activate)
- ☐ Verified “Agent Active” green status in portal
- ☐ Configured as persistent service (systemd, Docker Compose, or Windows service)

Phase 5: CAT-72

- ☐ Confirmed no maintenance or updates planned for next 72+ hours
- ☐ Clicked “Begin Test” in portal
- ☐ System operated normally for 72 continuous hours

- □ Received preliminary status notification

Phase 6: Determination

- □ Received conformance determination (CONFORMANT)
- □ Downloaded certificate, report, and QR code
- □ Verified listing on registry.sentinelauthority.org

Phase 7: Ongoing

- □ ENVELO agent running continuously
- □ Material changes reported to Conformance Engineer within 48 hours
- □ Annual maintenance fee paid
- □ Annual surveillance review completed
- □ Certificate renewed

CONTACT

General Inquiries — info@sentinelauthority.org

Conformance & Assessment — conformance@sentinelauthority.org

Emergency (Active CAT-72) — emergency@sentinelauthority.org

Applicant Portal — app.sentinelauthority.org

Public Registry — registry.sentinelauthority.org

Website — www.sentinelauthority.org

— End of Document —