SYNAPSE-EDGE

ENDPOINT DETECTION & RESPONSE

User & Administrator Guide

Version 1.0

Part of the Synapse suite

Self-hosted | Docker Compose | Windows and Linux endpoints

Contents

SECTION 1

Introduction

Synapse-Edge is a self-hosted endpoint detection and response platform. It has three parts, and understanding the split makes everything else in this guide easier to follow.

COMPONENT	RUNS	RESPONSIBILITY
Endpoint agent	On each protected host	Collects telemetry, matches it against cached intelligence, and executes containment. Works with no connectivity.
Gateway	In Docker on your infrastructure	Ingests telemetry, stores intelligence and alerts, queues response actions, and enforces access control.
Console	In Docker, served by nginx	The web interface. Talks only to the gateway, on the same origin.

The detection loop

The agent polls for process and network activity on a fixed interval and reports only what has changed since the previous cycle. Each event is checked against the intelligence bundle cached on the host, so detection does not depend on the gateway being reachable. Events and any matches are queued and uploaded when the gateway is available.

> Because detection runs on the endpoint, an agent that has been offline for a week still detects against the intelligence it last received. Enforcement deliberately does not stop when the cached bundle goes stale — old intelligence is far better than none — but the age is reported so you can see the drift.

SECTION 2

Installing the management platform

The gateway, console and database run under Docker Compose. Only the console publishes a host port; the gateway and PostgreSQL sit on an internal network with no external route.

Prerequisites

- Docker Engine with the Compose plugin
- `openssl` for secret generation
- A host reachable from your endpoints on the console port

Install

```
cd Synapse-Edge
cp .env.example .env
./scripts/gen-secrets.sh >> .env

# Set SYNAPSE_BOOTSTRAP_ADMIN_PASSWORD in .env (12 characters minimum)

docker compose up -d --build
```

The gateway applies its database migrations at start-up and creates the initial Super Admin. The console is then available on `https://your-host:8443`.

Secrets

VARIABLE	PURPOSE
SYNAPSE_SECRET_KEY	Signs session tokens and derives the encryption key for secrets at rest. Minimum 32 bytes.
SYNAPSE_AGENT_SERVICE_KEY	Shared token presented by agents and by the Synapse-Conectiv health probe.
POSTGRES_PASSWORD	Database credential.
SYNAPSE_BOOTSTRAP_ADMIN_PASSWORD	Initial Super Admin password. Used only on an empty database.

Rotating SYNAPSE_SECRET_KEY invalidates every session and makes existing encrypted TOTP secrets undecryptable. Plan MFA re-enrolment before you rotate it. The gateway refuses to start if the key still contains a placeholder such as "changeme".

SECTION 3

Signing in and multi-factor authentication

Sign in with the bootstrap administrator created at first boot, then change the password. Authentication is a two-step exchange when MFA is in play: the password step returns a short-lived challenge token that carries no access on its own, and only a valid TOTP code exchanges it for a session.

Enrolling an authenticator

- The server issues a secret and a provisioning URI for your authenticator app.
- Enter a code from the app to prove possession. MFA is not active until this succeeds.
- Ten single-use recovery codes are displayed once. Store them securely.

Enrolment is deliberately two-phase. Storing the secret without verifying it would let a mistyped setup lock a user out of their own account, so MFA only becomes active after a code is accepted.

Enforcing MFA for everyone

A Super Admin can require MFA across the platform. Users who have not yet enrolled are not refused at sign-in; they receive an enrolment challenge instead. Refusing them outright would lock out every existing account the moment enforcement was switched on.

SECTION 4

The console

Navigation runs down the left side and is grouped into three areas. The menu is filtered by your permissions and by the active deployment mode, so it shows only what you can actually use.

AREA	ITEMS	PURPOSE
Operations	Dashboard, Alerts, Endpoints	Day-to-day monitoring and response.
Endpoint Admin	Manage Endpoints, Deploy Agent	Fleet lifecycle and rollout.

AREA	ITEMS	PURPOSE
Admin	User Admin, API Configuration, AI Configuration	Platform configuration.

A strip across the top of every page shows the live status of each connected Synapse application, and the footer of the sidebar shows who is signed in and which roles they hold.

SECTION 5

Dashboard

Connected applications

Each integration reports one of three states. The distinction matters: an integration you never configured is not failing, and colouring it red would train you to ignore red.

STATE	COLOUR	MEANING
Connected	Green	Reachable and responding. Latency is shown.
Disconnected	Red	Configured but unreachable. The error is shown.
Not configured	Grey	No endpoint has been set for this integration.

Telemetry ingestion

One tile per stream — process, network and system — showing the event count for the last 24 hours, how many endpoints contributed, average ingest latency and the age of the most recent event. Selecting a tile opens the most recent events for that stream.

> A stream sitting at zero is the most important thing on this page. Streams with no data are always listed rather than omitted, because an absent tile is far easier to overlook than a zero.

SECTION 6

Alerts

Alerts are raised when telemetry matches an enabled indicator whose confidence meets the threshold. Repeated matches of the same indicator, on the same host, for the same binary collapse into a single alert with a hit counter rather than filling the queue with duplicates.

SEVERITY	TYPICAL RESPONSE
Critical	Isolate the host, then investigate.
High	Investigate promptly; isolate if the process is still running.
Medium	Review in normal working hours.
Low	Contextual. Useful during an investigation, not on its own.

> In INTEGRATED deployments this page is replaced by a notice pointing to Synapse-Cortex, which owns alerting for the ecosystem.

SECTION 7

Endpoints and response

The Endpoints view lists every enrolled host with its asset ID, MAC address, IP address, hostname and online status.

> Online status is derived from how recently the agent checked in, not from the state column. The state records what you intend; online records what is true right now. A host can read HEALTHY and be unplugged.

Isolating a host

Isolation blocks all network traffic except the gateway allow-list. The allow-rules are installed before the blocking rule and a partial ruleset is rolled back on failure, so an isolated host always retains the path needed to receive its own release command. Isolation survives an agent restart because the state is read back from the operating system firewall, not from agent memory.

> The agent refuses to start unless SYNAPSE_GATEWAY_ALLOWLIST names the gateway addresses. Isolating with an empty allow-list would sever the host from the console with no way to release it remotely.

Terminating a process

A termination request carries both the process ID and the SHA-256 of its image. The agent re-hashes the running image and refuses if it does not match. Process IDs are recycled on a busy host, and acting on a PID alone risks terminating an unrelated — possibly critical — process.

SECTION 8

Deploying agents

Deployment is a single command. The host enrols itself on first run, derives its asset ID from its primary MAC address and appears in the console automatically. There is no separate registration step.

Open **Deploy Agent**, choose the platform, select an active enrolment key and copy the command:

```
curl -fsSL https://edge.example.local/install/synapse-edge-agent.sh \
  | sudo sh -s -- \
      --server-url "https://edge.example.local" \
      --enrolment-key "sek_..."
```

Asset identity

SOURCE	FORM	WHEN USED
Local	SE-XXXX-XXXX-XXXX	Derived from the primary MAC. Used whenever Cortex is not connected.
Cortex	As issued by Cortex	Takes precedence automatically when Cortex is connected.

Because the local identifier is derived from the MAC, a rebuilt or renamed machine resolves to its existing asset rather than enrolling twice. The console tags each row Local or Cortex so you can see whether an identifier is provisional or authoritative.

> Enrolment is refused for randomised or locally administered MAC addresses — the kind produced by Docker bridges, VPN adapters and Windows privacy randomisation. Anchoring an asset to one produces a duplicate on every reboot, and a duplicate-ridden inventory is worse than a failed enrolment.

SECTION 9

Endpoint administration

ACTION	EFFECT	REVERSIBLE
Pause	Host stays enrolled but its telemetry is refused. For planned maintenance where an endpoint would otherwise generate noise.	Yes
Revoke	The agent's credential is rejected from now on. History is retained.	By re-enrolling
Delete	Removes the endpoint and cascades to its telemetry, alerts and queued actions.	No

Delete requires you to type the hostname exactly. That confirmation is enforced by the server, not only by the dialog. Pause and revoke have no confirmation step by design — gating every action equally simply trains people to click past the warnings that matter.

> A re-enrolling host cannot escape containment. If an endpoint was ISOLATED or REVOKED, re-enrolment preserves that state until an operator clears it.

SECTION 10

API configuration

Enrolment keys authenticate new agents. Creating a key never affects any existing key — that separation is the whole point of the design. Rotation is a three-step operation you control:

- Create a new key. Every deployed agent keeps working.
- Redeploy or re-enrol hosts onto the new key at your own pace.
- Revoke the old key once you are satisfied nothing depends on it.

> A key's value is displayed once, at creation. Only a hash and a short prefix are stored, so it genuinely cannot be recovered afterwards. If you lose it, create another — existing keys are unaffected.

Revoking the last active key is permitted, but no new agent will be able to enrol until another is created. The console warns you when this happens rather than letting you discover it during a rollout.

SECTION 11

AI configuration

AI assistance is optional and off by default. Each capability is a separate switch, because summarising an alert and advising on containment carry very different risk.

CAPABILITY	WHAT IT DOES
Alert triage	Ranks and clusters incoming detections.
Alert summarisation	Produces a plain-language incident narrative.

CAPABILITY	WHAT IT DOES
Response advisory	Suggests containment. A human still executes it.
Autonomous response	Permanently disabled in version 1.x.

> Autonomous response is blocked by a constraint in the database schema, not merely by the interface control. A model must never isolate a production host or terminate a process without a human decision.

The provider API key is encrypted at rest. Saving the form with the key field left blank preserves the stored key, so you do not have to retype a secret to change an unrelated setting.

SECTION 12

User administration and roles

Access control is built into the database schema. Roles hold permission scopes in the form `resource:action`, and every protected route checks them. Access is denied unless a scope explicitly grants it.

ROLE	INTENDED FOR	NOTABLE LIMITS
Super Admin	Platform owners	Unrestricted, including identity and Sync-Config.
Security Analyst	Incident responders	Full investigation and response. Cannot delete endpoints, issue enrolment keys or change AI settings.
Service Delivery Manager	Service quality reporting	Read-only. Holds no response rights at all.
iRespond Service	Machine identity	Used by Synapse-iRespond for API-driven response.

The analyst role deliberately excludes endpoint deletion. Deleting an endpoint destroys the investigation trail, which is not a decision to put in front of someone working an incident under time pressure.

SECTION 13

Modular Control

Synapse-Edge reshapes itself according to a configuration manifest pushed from your local Synapse-Gateway. A single deployment mode flag resolves deterministically into the feature set below.

MODULE	STANDALONE	INTEGRATED	DELEGATED TO
In-app audit logging	On	Off	Synapse-Cortex
Local alert console	On	Off	Synapse-Cortex
Console response buttons	On	Off	Synapse-iRespond
Telemetry forwarding	Off	On	Synapse-Cortex
API-driven response	Off	On	Synapse-iRespond
Service-quality endpoint	Off	On	Synapse-Conectiv

The mode is enforced by the gateway, not merely reflected in the console. A disabled surface returns a status naming the system that now owns it, so the interface can explain the absence rather than appearing broken.

Safeguards

- A manifest that would leave no response path at all is rejected.
- INTEGRATED mode without a Cortex endpoint is rejected, because local alerting would be off with nowhere to forward — silently discarding every detection.
- A manifest whose revision is not newer than the current one is ignored, so an out-of-order retry cannot roll the deployment backwards.
- The manifest is persisted before it is applied, and reloaded at start-up, so a restart cannot quietly revert the mode.

SECTION 14

Service quality reporting

In INTEGRATED deployments the gateway exposes a service-quality endpoint for Synapse-Conectiv, reporting availability, telemetry latency percentiles, engine version and packet error rates, together with a pass or fail verdict against the targets carried in the manifest.

METRIC	MEANING
Availability	Proportion of agent check-ins that succeeded.
Telemetry latency	Time from event observation on the host to gateway receipt, at the 50th, 95th and 99th percentiles.
Packet error rate	Malformed and dropped events as a share of the total.
Fleet rollup	Endpoint counts by state.

> These metrics are computed from a bounded in-memory window, never by querying the telemetry tables. A service-quality probe must not be capable of degrading the service it measures.

SECTION 15

Troubleshooting

SYMPTOM	LIKELY CAUSE AND RESOLUTION
Gateway will not start	A required environment variable is missing, or SYNAPSE_SECRET_KEY still contains a placeholder. The container log names the variable.
An agent does not appear after deployment	The enrolment key may be revoked, or the host's primary MAC may be randomised or locally administered. Both are refused with an explicit reason in the gateway log.
An endpoint shows HEALTHY but Offline	Expected. The state is your intent; online is derived from check-in recency. The host has stopped reporting.
Alerts page shows a delegation notice	The deployment is in INTEGRATED mode and alerting belongs to Synapse-Cortex. Not a fault.
Response buttons are missing	Same cause: response is delegated to Synapse-iRespond in INTEGRATED mode. Raise the action there.
An integration shows Not configured	No endpoint URL has been set for it in the Sync-Config manifest.
A telemetry stream reads zero	No agent is reporting that stream. Confirm agents are online and not paused.

SYMPTOM	LIKELY CAUSE AND RESOLUTION
Isolation failed	The agent needs privileges to modify the host firewall, and SYNAPSE_GATEWAY_ALLOWLIST must be set. The failure reason is recorded against the action.

APPENDIX A

Environment variables

Gateway

VARIABLE	REQUIRED	PURPOSE
SYNAPSE_DATABASE_URL	Yes	PostgreSQL connection string.
SYNAPSE_SECRET_KEY	Yes	Token signing and encryption at rest.
SYNAPSE_AGENT_SERVICE_KEY	Yes	Agent and health-probe token.
SYNAPSE_LISTEN_ADDR	No	Listen address. Defaults to :8080.
SYNAPSE_BOOTSTRAP_ADMIN_EMAIL	No	Initial admin, empty database only.
SYNAPSE_BOOTSTRAP_ADMIN_PASSWORD	No	Initial admin password.

Agent

VARIABLE	REQUIRED	PURPOSE
SYNAPSE_GATEWAY_URL	Yes	Base URL of the gateway.
SYNAPSE_AGENT_ID	Yes	Stable machine identifier.
SYNAPSE_AGENT_SERVICE_KEY	Yes	Shared service token.
SYNAPSE_GATEWAY_ALLOWLIST	Yes	Gateway addresses permitted during isolation. The agent refuses to start without this.
SYNAPSE_POLICY_PATH	No	Cached policy bundle location.

APPENDIX B

Permission scopes

Scopes take the form `resource:action`. A held scope may use an asterisk in either position, so `*:*` grants everything.

SCOPE	GRANTS
endpoint:read	View the endpoint fleet.
endpoint:admin	Pause, resume and revoke endpoints.
endpoint:delete	Permanently delete an endpoint and its history.
telemetry:read	View ingestion data and drill into events.
alert:read / alert:update	View and work alerts.
ioc:read / ioc:write	View and manage threat intelligence.

SCOPE	GRANTS
response:isolate / release / kill	Execute containment actions.
apiconfig:read / write	View and manage enrolment keys.
aiconfig:read / write	View and change AI settings.
user:write	User administration.
settings:write	Global security settings, including MFA enforcement.
syncconfig:push	Accept a Sync-Config manifest.
health:read / sla:read	Service quality reporting.
audit:read	Read the audit log.