

ИНТЕГРАЦИОННЫЕ ИНТЕРФЕЙСЫ

API v1 и протокол ROY

Продукт: СОПКА.Рой · Версия: 1.0.0 · Агент: 1.0.0 · Протокол: 1 · Редакция: 14.08.2026

Правообладатель ПО: Общество с ограниченной ответственностью «Каннам». ИНН 2543020645, ОГРН 1132543001502. Реквизиты приведены в отдельном разделе документации.

Общие положения

Внешний базовый путь сервера - /roy. В API v1 интерфейсы разделены по границе доверия: Agent API используется DLP-агентами, Owner API предназначен владельцу всей платформы, а Workspace API зарезервирован для будущего пользовательского API рабочих областей. Веб-интерфейс продолжает использовать cookie-сессию, CSRF-защиту и ролевую модель workspace.

Версии текущего контракта

Компонент	Текущая версия
Windows-агент	1.0.0
ROY protocol	1; клиент и сервер в текущей сборке поддерживают только protocol v1.
Agent HTTP API	v1, канонический префикс /roy/api/v1/.
Policy schema	1
Capabilities schema	1

Версия программы агента не обязана совпадать с версией протокола. При несовместимой версии protocol/API сервер отклоняет агентский запрос. Совместимые добавления полей не требуют создания v2; новая версия создаётся только при несовместимом изменении контракта.

Контуры API v1

Контур	Префикс	Аутентификация и назначение
Agent API	/roy/api/v1/...	Регистрационный ключ при первичной регистрации, затем device token клиента. Только обмен агент-сервер.
Owner API	/roy/api/v1/owner/...	Отдельный Bearer token владельца платформы. Доступ ко всем users, workspaces и clients.
Workspace API	/roy/api/v1/workspace	Namespace зарезервирован, но пользовательские методы пока не реализованы.

Agent API v1

Текущий Windows-агент использует только API v1. Основные маршруты:

Метод	Маршрут	Назначение
POST	/roy/api/v1/client_register	Первичная регистрация клиента.
POST	/roy/api/v1/client_heartbeat	Heartbeat, runtime-состояние и fallback доставки команд.
GET	/roy/api/v1/client_commands	Получение ожидающих команд.
POST	/roy/api/v1/client_commands/<id>/ack	Статус выполнения команды.
GET	/roy/api/v1/get_policies/<client_id>	Подписанный policy bundle.
POST	/roy/api/v1/upload_logs	Пакет событий агента.
POST	/roy/api/v1/upload_screenshot	Загрузка снимка экрана.
POST	/roy/api/v1/browser_event	События браузерного канала.
GET/POST	/roy/api/v1/agent/...	Версия, скачивание и статусы обновления агента.

Owner API v1

Owner API - административный интерфейс владельца всей СОПКА ROY. Он не использует пользовательскую веб-сессию. Каждый разрешённый запрос обязан содержать `Authorization: Bearer <token>`. Сетевой режим и токен задаются только через переменные окружения.

```
СОПКА_ROY_OWNER_API_ACCESS=localhost
СОПКА_ROY_OWNER_API_TOKEN=CHANGE_ME_TO_LONG_RANDOM_OWNER_API_TOKEN
RATE_LIMIT_OWNER_API=120/minute
```

СОПКА_ROY_OWNER_API_ACCESS: disabled скрывает API с 404; localhost разрешает loopback; private разрешает loopback и приватные IP; public разрешает внешние IP. Bearer token обязателен во всех режимах, кроме того что при disabled API вообще недоступен.

Метод	Маршрут	Назначение
GET	/roy/api/v1/owner	Метаданные Owner API.
GET	/roy/api/v1/owner/system	Состояние сервера и общие счётчики.
GET/POST	/roy/api/v1/owner/users	Список и создание пользователей.
GET	/roy/api/v1/owner/users/<id>	Карточка пользователя и memberships.
GET/PATCH/PUT	/roy/api/v1/owner/users/<id-or-login>/billing	Оплата, plan_status и paid_until.
GET	/roy/api/v1/owner/workspaces	Все рабочие области.
GET/PATCH	/roy/api/v1/owner/workspaces/<id>	Карточка workspace; переключение active/disabled.
GET	/roy/api/v1/owner/clients	Все DLP-клиенты; поддерживается фильтр workspace_id.
GET	/roy/api/v1/owner/clients/<client_id>	Карточка конкретного клиента.

Старые маршруты /local-admin и /local/users сохранены только как временные compatibility aliases. Для нового кода следует использовать только /api/v1/owner.

Workspace API v1

```
COPKA_ROY_WORKSPACE_API_ENABLED=false
RATE_LIMIT_WORKSPACE_API=120/minute
```

Маршруты /roy/api/v1/workspace и /roy/api/v1/workspace/status пока зарезервированы. При выключенном API сервер возвращает 503 workspace_api_disabled; если включить флаг - 501 workspace_api_not_implemented. Доступ к данным workspace через этот API пока не публикуется.

Лимиты API

Owner и Workspace API имеют независимые лимиты: `RATE_LIMIT_OWNER_API` и `RATE_LIMIT_WORKSPACE_API`. Формат: `120/minute`, `10/second`, `1000/hour` или `5000/day`. Owner API ограничивается по IP и endpoint ещё до проверки Bearer token, чтобы смена неверных токенов не позволяла обходить ограничение.

Socket.IO и команды

Socket.IO работает по ресурсу `/roy/socket.io`. Для агента realtime-канал является основным способом быстрой доставки команд, а HTTP heartbeat остаётся fallback. Команда имеет идентификатор и состояние `queued`, `delivered`, `running`, затем `completed` либо конечную ошибку. Комнаты изолированы по `workspace/client`, а идентификатор клиента определяется серверной `socket identity`.

Форматы и безопасность

- JSON передаётся в UTF-8; крупные пакеты могут использовать gzip;
- секреты, device token и Owner token нельзя помещать в URL;
- данные `workspace/client` из payload повторно проверяются на сервере;
- health endpoints предназначены для локального reverse проху и мониторинга и не являются публичным Owner API;
- для новой несовместимой версии API или protocol создаётся новый контракт, а v1 не меняет семантику молча.