ОБЩЕЕ ТЕХНИЧЕСКОЕ ОПИСАНИЕ

Протокол Рой: принципы обмена

Продукт: СОПКА.Рой · Версия: 1.0.0 · Агент: 1.0.1 · Протокол: 1 · Редакция: 15.10.2026

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

Назначение и границы описания

Протокол Рой обеспечивает взаимодействие Windows-агента, сервера и веб-консоли. Документ описывает общий принцип работы и требования эксплуатации. Он не является инструкцией по воспроизведению запросов, подключению сторонних клиентов или диагностике внутренних интерфейсов. Маршруты, заголовки, форматы подписи, ключи и служебные примеры в публичную документацию не входят.

Участники и рабочие области

Сервер связывает пользователя и устройство с рабочей областью. Веб-консоль работает с полномочиями пользователя, агент - с собственной проверенной идентичностью. Идентификатор компьютера сам по себе не даёт доступа к его данным. Один и тот же принцип действует в SaaS и локальной инсталляции.

Регистрация

Администратор получает ограниченный регистрационный ключ для своей рабочей области. При установке агент проходит регистрацию и получает данные для дальнейшей аутентификации. Регистрационный ключ и рабочие данные устройства имеют разное назначение. Отзыв доступа прекращает разрешённый обмен; повторная регистрация выполняется штатным способом.

Регулярный обмен

Агент периодически сообщает состояние и получает актуальные настройки, политики и ожидающие команды. Сервер различает доступность устройства, версию программы, применённую конфигурацию и возможности функций. Отсутствие новых настроек в очередном обмене не означает их сброс. Потеря связи отражается в статусе и не подтверждает остановку всех локальных модулей.

Политики и возможности

Агент проверяет подлинность и совместимость полученных политик до применения. Возможности разрешают функции, правила задают условия, а действия исполняются отдельно. Администратор сверяет полученную версию и фактическое поведение. Обновление серверной настройки не гарантирует немедленное применение на отключённом устройстве.

События и доставка

Наблюдения формируются локально и передаются на сервер с контекстом и результатами обработки. При временной недоступности используется локальная очередь в пределах её лимитов и правил хранения. После восстановления связи возможна доставка событий, возникших раньше. Время события, время приёма и время отображения могут различаться; бесконечное хранение и отсутствие потерь при любых сбоях не гарантируются.

Команды

Пользователь инициирует разрешённую операцию, сервер проверяет права и адресата, агент принимает команду и сообщает её состояние. Очередь, доставка, начало и завершение - отдельные этапы. Для оперативных операций может использоваться временный канал связи; регулярный обмен остаётся основой контроля доступности. Система должна сохранять проверку полномочий независимо от используемого транспорта.

Интерактивные сеансы

Прямой экран и удалённая консоль создаются по явной операции пользователя. Для них применяются временные сессионные ключи и защищённый обмен. Сеанс зависит от связи и готовности пользовательского процесса. При невозможности согласовать защиту функция завершается ошибкой, а не переключается на открытый обмен.

Защита и границы доверия

Соединения защищаются HTTPS; запросы устройства аутентифицируются, а механизмы проверки целостности и повторов снижают риск подмены и повторной доставки. Сервер контролирует рабочую область и разрешения. Шифрование интерактивного потока не означает, что сервер не обрабатывает телеметрию и файловые материалы других функций.

Обновления и совместимость

Версия продукта, версия протокола и возможности агента относятся к разным уровням совместимости. Агент проверяет предлагаемый пакет и использует штатную процедуру обновления. При несовместимости требуется поддерживаемая версия, а не обход проверок. Результат подтверждается повторной связью и работой нужных функций.

Эксплуатация

Поддерживайте рабочие DNS, TLS, системное время и согласованный прокси. Для диагностики пользователь передаёт время, версию, статус и обезличенный результат операции; служебные журналы и детали обмена доступны только уполномоченному сопровождению. Сокращение публичных технических деталей дополняет проверку доступа и не заменяет её.

Внутренний MCP AI-чата

POST /internal/api/ai/mcp — сессионный Streamable HTTP JSON-RPC интерфейс: чтение данных, создание PDF и подготовка карточек команд. Отправка команд выполняется отдельным подтверждением браузера. Поддерживаются initialize, ping, tools/list и tools/call; требуется действующая сессия, CSRF, выбранная область и соответствующее право. Протокол 2025-11-25, также согласуется 2025-06-18. Это внутренний интерфейс консоли, а не анонимный API агентов. Внешние запросы не расширяют права пользователя.

Подробнее: AI-чат: анализ безопасности.