НАСТРОЙКИ КЛИЕНТА И ГРУПП

Возможности каналов

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.

Для чего нужны возможности

Возможности определяют разрешённый состав функций агента для группы или клиента. Они позволяют ограничить сбор данных и операции до необходимого объёма. Отдельно учитываются поддержка установленным агентом, настройки разрешения, права оператора и текущая готовность устройства.

Каталог функций

Функция	Назначение	Когда использовать и ограничения
Приложения	Процессы и приложения	Выявление запрещённых запусков и контекста событий; данные зависят от агента и ОС.
Установленные программы	Инвентаризация установленного ПО	Оценка состава ПО и изменений; снимок инвентаризации не подтверждает активный запуск.
Сетевые интерфейсы	Инвентаризация и изменения сетевых адаптеров	Поиск неразрешённых подключений; не является полным перехватом сетевого трафика.
USB и накопители	Накопители и события их подключения	Контроль съёмных носителей; сведения о диске не доказывают копирование конкретного файла.

Функция	Назначение	Когда использовать и ограничения
Буфер обмена	Наблюдение и проверка буфера обмена	Обнаружение чувствительного текста в контексте приложений; результат реакции проверяется отдельно.
Мониторинг клавиатуры	Наблюдение клавиатурного ввода	Контекстный контроль ввода; виртуальная клавиатура и защищённые поля могут иметь ограничения.
Активное окно	Сведения об активном окне	Сопоставление действий с приложением; заголовок не заменяет анализ содержимого документа.
Периодические и ручные скриншоты	Ручные и периодические снимки	Визуальное подтверждение; нужен пользовательский сеанс, защищённые окна могут быть недоступны.
Браузер	Наблюдения поддерживаемых браузеров	Контекст веб-активности; не гарантирует чтение HTTPS-содержимого всех сайтов и мессенджеров.
Мониторинг файлов	События файловой системы	Выявление изменений; область и типы событий зависят от мониторинга и настроек.
Поиск файлов	Поиск по заданию на компьютерах	Выявление файлов по выбранным условиям; доступ, формат и размер ограничивают анализ.
Просмотр найденных файлов	Предпросмотр найденного файла	Быстрая оценка результата; зависит от поиска, формата, размера и доступности файла.

Функция	Назначение	Когда использовать и ограничения
Скачивание найденных файлов	Получение найденного файла	Сохранение материала расследования; зависит от поиска и разрешения скачивания.
Передача файлов на клиент	Передача файла на компьютер	Доставка согласованного материала; не означает автоматический запуск переданного файла.
Live Screen	Просмотр рабочего стола в реальном времени	Проверка текущей ситуации; нужны пользовательский сеанс и активная связь. Удалённого ввода нет.
Remote Shell	Интерактивная PowerShell-консоль	Административные операции; контекст и права задаются исполнителем, произвольные команды не гарантируют повышение привилегий.
Управление устройствами	Управление USB-функциями	Ограничение устройств; отличается от контроля накопителей. Итог зависит от Windows и устройства.
Управление процессами	Операции с процессами	Реагирование на запущенные программы; принудительное завершение может потерять несохранённые данные.
Локальные пользователи Windows	Управление локальными пользователями Windows	Администрирование доступных учётных записей; ограничения защищённых и доменных пользователей сохраняются.
Обслуживание агента	Обслуживание агента	Штатные операции обслуживания; ожидание команды не подтверждает завершение операции.

Функция	Назначение	Когда использовать и ограничения
Питание и пользовательская сессия	Питание и сеанс Windows	Согласованные действия с компьютером и сеансом; связь может прекратиться, данные могут быть потеряны.
Сетевая изоляция	Изоляция компьютера от сети	Локализация инцидента с сохранением предусмотренного служебного доступа; отмену и повторную связь проверяют отдельно.
Карантин файлов	Карантин выбранного файла	Изоляция материала для реагирования; занятый или недоступный файл может не быть перемещён.
Telegram: переписка и отправка	Доступный текст и контекст сообщений	Условия чата, отправителя, вложения и действия политики Telegram. Неполученный текст не проверяется.
Сертификаты Windows	Инвентарь и изменения хранилищ	Условия сертификатов и разрешённые действия политики; доверие оценивается в контексте конкретной проверки.
Безопасность Windows	Признаки работающей ОС и загрузки	Контроль тестовой подписи, отладки, целостности и Secure Boot; исправление BCD требует явного действия политики.

Как читать итоговое состояние

«Поддерживается» означает, что агент заявил техническую возможность. «Разрешено» означает результат групповых и индивидуальных настроек. Итоговая доступность требует обоих условий, а также зависимостей функции. «Включить» неподдерживаемую функцию не добавляет её в старый агент.

Группы, приоритеты и наследование

Для каждого параметра выбирается явная настройка группы с наибольшим приоритетом. Если равноприоритетные группы противоречат друг другу, запрет функции имеет преимущество; интерфейс показывает конфликт. Для интервала снимков при таком конфликте выбирается больший интервал. Индивидуальная явная настройка клиента переопределяет групповой результат; «наследовать» возвращает управление группам. При отсутствии переопределений действуют значения по умолчанию, которые следует проверить перед вводом.

Предпросмотр и скачивание найденных файлов требуют включённого поиска файлов. Право оператора на запуск операции и готовность пользовательской сессии проверяются дополнительно. Разрешение канала не выдаёт пользователю административную роль.

Дополнительные настройки

Интервал периодических снимков задаётся в минутах и влияет на нагрузку и объём материалов. Очистка отправленных локальных журналов относится к очереди агента; она не задаёт срок хранения истории на сервере. Изменения доставляются агенту при обмене настройками, поэтому результат не обязан появиться сразу после сохранения.

Практический сценарий

1. Создайте тестовую группу и включите необходимые функции.
2. Откройте итоговые возможности клиента и проверьте источник каждой настройки и конфликты.
3. Для индивидуального случая задайте явное переопределение либо верните наследование.
4. Дождитесь получения настроек; проверьте наблюдение или безопасную тестовую команду.
5. Сопоставьте поддержку, разрешение, права и фактический результат. Документируйте исключения перед распространением настроек.

Наблюдение и реагирование

Функции наблюдения дают данные для расследования, политики принимают решения, а функции реагирования выполняют явные операции. Например, включённый мониторинг сети не равен сетевой изоляции, а включённый поиск файлов не разрешает скачивание. В составе агента есть также технические признаки поддержки версий правил; они не являются отдельными переключателями пользовательского контроля.

Связь с правилами и нагрузкой

Разрешение функции не создаёт правило автоматически. Условия, режимы наблюдения, действий и исключения настраиваются в семи редакторах политик; критичность не заменяет приоритет. Периодические снимки включаются и получают интервал здесь, а не отдельным правилом политики. Уменьшение интервала увеличивает число снимков, сетевой поток и хранение обратно пропорционально интервалу. Расчёт для 1000 агентов и допущения приведены в «Системных требованиях».

Возможности в AI-анализе

AI-чат — серверный аналитический интерфейс, а не дополнительный канал слежения агента. Администратор может прочитать эффективные возможности компьютера или явные настройки группы. Сводка не изменяет наследование, поддержку платформой или доступ пользователя.

Подробнее: AI-чат: анализ безопасности.

Политики новых каналов

Подробные поля, реакции и примеры Telegram, скриншотов, сертификатов и безопасности Windows включены в руководство «Политики и каналы контроля» и его PDF. Разрешение возможности не создаёт правило автоматически. Для материалов инцидента отдельно учитываются разрешения скриншотов и видеозаписи; для видео нужен разрешённый экран или камера, звук зависит от микрофона.