Команды

Страница устройства предоставляет панель **Команды** для отправки удалённых команд управляемому устройству. Доступные команды зависят от платформы (Android или Apple) и состояния устройства.

Команды можно отправлять только на устройство, которое сейчас зарегистрировано. На незарегистрированном устройстве, на устройстве ADE, которое ещё не зарегистрировано, и в истории прошлой регистрации панель показывает только историю команд.

> Если устройство сейчас не в сети, команда будет доставлена и выполнена, как только устройство подключится к Интернету. Для команд Android можно задать параметр **Срок действия**, чтобы определить, как долго недоставленная команда остаётся действительной.

Команды Android (AMAPI)

Для устройств Android панель «Команды» содержит поле **Срок действия** (значение + единица) и селектор **Команда**. Некоторые команды требуют дополнительных параметров, которые появляются динамически при выборе команды.

Общие параметры

- **Срок действия**: как долго команда остаётся действительной, если её нельзя выполнить немедленно.
- **Команда**: выберите действие, которое нужно отправить на устройство.

Команды без дополнительных полей

- **Заблокировать устройство**: блокирует устройство.
- **Перезагрузить устройство**: перезагружает устройство. Требуется Android 7.0 или новее.
- **Отключить режим пропажи**: выводит устройство из режима пропажи.
- **Передать право собственности**: удаляет рабочий профиль и все политики с корпоративного устройства с Android 8.0 или новее и оставляет его для личного использования. Приложения и данные личного профиля сохраняются. Устройство

удаляется с сервера после того, как подтвердит команду. Это действие нельзя отменить.

Команды с дополнительными полями

- **Сбросить пароль**: требуются **Новый пароль** и **Подтвердите новый пароль**. Дополнительные переключатели: **Заблокировать сейчас**, **Требовать ввод** и **Не запрашивать учётные данные при загрузке**.
- **Очистить данные приложения**: требуется **Имя пакета**.
- **Включить режим пропажи**: требуется **Сообщение режима пропажи**; поддерживаются необязательные контактные поля (почтовый адрес, организация, номер телефона, эл. почта). Когда устройство сообщит об этом, его состояние станет **Потеряно**, страница устройства покажет баннер, а эта команда будет скрыта до отключения режима пропажи.
- **Стереть устройство**: поддерживает **Сообщение о причине стирания** (отображается пользователям на личных устройствах) и необязательные флаги стирания, включая **Стереть eSIM**.

> Команды eSIM (**Добавить eSIM**, **Удалить eSIM**, **Запросить EID**) доступны на отдельной панели **Управление SIM**.

История команд

Ниже элементов управления отправкой панель управления показывает таблицу истории команд. Таблица сортируется и поддерживает разбивку на страницы. Некоторые строки можно развернуть, чтобы просмотреть дополнительные параметры или сведения о выполнении.

Столбцы истории Android

- **Дата создания**
- **Команда**
- **Срок действия**
- **Статус**
- **Ошибка**
- **Дата выполнения**

Команды Apple (MDM)

Для устройств Apple панель «Команды» предоставляет селектор **Команда**. Некоторые команды требуют дополнительных входных данных. Как и для Android, ниже отображается таблица истории команд.

Команды с дополнительными полями

- **Установить приложение**: требуется **Bundle ID** приложения.
- **Отправить уведомление**: требуется **Текст уведомления** (максимальная длина — 200 символов).

На iPhone и iPad команды **Отправить уведомление** и отслеживание в реальном времени доходят до устройства через приложение **Cerberus Enterprise**: они отключены, пока приложение не установлено и не зарегистрировано для получения уведомлений (см. поле **Приложение Cerberus Enterprise**). При запуске отслеживания в реальном времени отображается сообщение «Запрос на отслеживание в реальном времени отправлен на устройство»: отслеживание начинается, когда устройство отправляет первое местоположение. iOS может задержать запрос или не доставить его, например в режиме энергосбережения или без подключения к сети: если местоположение не поступает в течение 2 минут, попросите пользователя один раз открыть приложение. При сбое запроса в сообщении указывается причина, например приложение ещё не зарегистрировано, отсутствует ключ уведомлений сервера или токен уведомлений устройства больше не действителен.

Действия с устройством

Перечислены только команды, поддерживаемые устройством: некоторые требуют iPhone или iPad под наблюдением, другие недоступны на Mac. Для прерывающих действий требуется подтверждение.

- **Заблокировать устройство**: блокирует экран, можно указать сообщение и номер телефона. Mac перезагружается и блокируется шестизначным PIN-кодом, который показывается один раз после отправки команды и в сведениях о команде. iPhone показывает заголовок «Потерянный iPhone» над вашим сообщением, хотя эта команда не включает режим пропажи.
- **Включить режим потерянного устройства** (iPhone и iPad под наблюдением): блокирует устройство и показывает ваше сообщение, номер телефона и примечание на экране блокировки. Пока режим потерянного устройства включён, страница показывает баннер и команды **Определить устройство** (местоположение отображается на карте местоположений), **Воспроизвести звук** и **Отключить режим потерянного устройства**.
- Устройство сообщает тому, кто его держит, что оно найдено: после **Найти устройство** на экране блокировки отображается **iPhone найден** со временем и именем сервера, получившего местоположение, и кнопкой **Продолжить**. iOS

показывает это уведомление, и его нельзя отключить.
- **Сбросить код-пароль**: удаляет код-пароль iPhone или iPad, например если пользователь его забыл. Если политика требует код-пароль, пользователю предлагается задать новый.
- **Обновить сведения об устройстве**: запрашивает у устройства его сведения (наблюдение, версия ОС, состояние безопасности, сертификат MDM) и его инвентаризацию.
- **Настройки устройства**: открывает окно для изменения имени устройства, имени хоста Mac, Bluetooth, роуминга данных, точки доступа, часового пояса, обоев, разрешён ли Activation Lock, а на Shared iPad — его настроек (см. ниже). Отправляются только изменённые настройки; неподдерживаемые устройством отключаются с указанием причины. Устройство может подтвердить роуминг данных или точку доступа, не применив их (например, если тарифный план SIM не поддерживает точку доступа), поэтому Cerberus Enterprise считывает их повторно примерно через 30 секунд и записывает предупреждение в системные журналы, если они не изменились.
- **Перезагрузить устройство** и **Выключить устройство**: перезагружают или выключают устройство сразу, после подтверждения.
- **Стереть устройство**: стирает всё содержимое и настройки и удаляет устройство из управления. На iPhone и iPad можно сохранить план данных eSIM и пропустить настройку по близости; Mac получает шестизначный PIN-код.
- **Return to Service** (параметр команды **Стереть устройство**, iPhone и iPad с iOS 17 или новее): после стирания устройство снова настраивается само, без участия человека, и повторно регистрируется с текущей политикой, пользователем и владельцем. Для настройки выберите сеть Wi-Fi из политики устройства, если только устройство не использует Ethernet или сотовые данные: можно использовать только личные сети (с паролем, без сертификатов), поскольку у устройства ещё нет пользователя и сертификата. Activation Lock должен быть отключён.
- **Обновить сотовые планы** (iPhone и iPad с сотовой связью, iOS 13 или новее, не User Enrollment): введите **URL сервера eSIM оператора**, предоставленный оператором (адрес https://, имя хоста или код активации LPA, из которого используется только сервер), и устройство загрузит планы eSIM, которые оператор привязал к его EID. EID устройства показан под полем, чтобы отправить его оператору. См. страницу **Управление SIM**.
- **Сохранить план данных eSIM** в выключенном состоянии удаляет все eSIM при стирании. Ограничение политики **Сохранять eSIM при стирании устройства** (устройства под наблюдением, iOS 17.2 или новее) применяется к стираниям, запущенным на самом устройстве (слишком много неудачных попыток ввода код-пароля, «Стереть всё содержимое и настройки»): Apple не документирует его влияние на эту команду.
- **Выйти из аккаунта пользователя** (Shared iPad): выполняет выход текущего пользователя и возвращает на экран входа. Данные, ещё не синхронизированные с iCloud, остаются на iPad.

Shared iPad

Shared iPad используется несколькими людьми, у каждого свой управляемый аккаунт Apple (Managed Apple Account), или гостями с временными сеансами. Он настраивается с помощью профиля ADE, который включает Shared iPad (см. страницу **Apple Automated Device Enrollment**), а его поле **Тип регистрации** показывает **Shared iPad**.

- **Пользователи Shared iPad**: пользователи iPad, вошедший пользователь, используемое ими хранилище и признак того, что некоторые данные ещё не синхронизированы с iCloud. Нажмите **Обновить**, чтобы снова запросить у iPad список. Пользователя можно удалить вместе с его данными, кроме вошедшего пользователя (сначала выполните его выход); для **Удалить всех пользователей** требуется iPadOS 14 или новее. Если данные ещё не синхронизированы, подтверждение предупреждает, что они будут потеряны.
- **Настройки устройства**: хранилище для каждого пользователя, ожидаемое число пользователей, время бездействия, после которого пользователи и гостевые сеансы выходят из системы, только гостевые сеансы, домены управляемых аккаунтов Apple (Managed Apple Account), предлагаемые на экране входа, сколько дней пользователь может входить без проверки пароля онлайн и пропуск настройки языка и региона для новых пользователей. Пустые поля сохраняют текущее значение; настройки, требующие более новой iPadOS, отключаются.

Пользователи Mac

На Mac панель **Пользователи Mac** перечисляет пользователей, зарегистрированных в управлении, обычно это пользователь, зарегистрировавший Mac. Аккаунты из политики устанавливаются в их сеансах. Для каждого пользователя показывается, когда он был зарегистрирован, последний отчёт его сеанса и состояние аккаунтов: **Актуально**, **Ожидание пользователя** (Mac устанавливает их, когда пользователь входит в систему), **Не применено** с причинами, сообщёнными Mac, или **Нет аккаунтов**, если в политике их нет. Нажмите **Перезагрузить**, чтобы снова прочитать список.

Activation Lock

Поле **Activation Lock** показывает, включён ли Activation Lock. Когда он включён, стёртое устройство можно снова настроить только с аккаунтом Apple пользователя или с кодом обхода устройства. Устройства под наблюдением включают Activation Lock, только если это разрешено в **Настройках устройства**. Cerberus Enterprise запрашивает у устройств под наблюдением их код обхода и сохраняет его: используйте **Показать код обхода** в меню поля, чтобы увидеть его (это могут только администраторы, и каждый просмотр записывается в системный журнал), затем введите его как пароль на экране Activation Lock

устройства, оставив аккаунт Apple пустым.

Recovery Lock и пароль прошивки (Mac)

Mac с Apple silicon показывает поле **Recovery Lock**, Mac на базе Intel — поле **Пароль прошивки**. Оба защищают Mac при запуске: с Recovery Lock recoveryOS запрашивает пароль; с паролем прошивки Mac запрашивает его для запуска с другого диска или из режима восстановления. Поле показывает, сообщает ли Mac о наличии пароля, а в подсказке — когда Cerberus Enterprise его сохранил и когда он последний раз проверялся.

- **Задать или изменить пароль**: Cerberus Enterprise создаёт пароль из 20 букв, расположенных на одних и тех же клавишах при любой раскладке клавиатуры, либо администратор вводит свой (от 8 до 64 символов без диакритики; другие роли могут только создать пароль, так как не видят сохранённые пароли). Пароль сохраняется в зашифрованном виде перед отправкой и заменяет сохранённый, только когда Mac подтвердит его. Если на Mac уже задан пароль вне Cerberus Enterprise, введите его как текущий пароль: он используется один раз и не сохраняется.
- **Проверить пароль**: спрашивает у Mac, верен ли сохранённый пароль. Результат отображается в подсказке и в системном журнале.
- **Показать пароль**: только администраторы могут видеть сохранённый пароль, и каждый просмотр записывается в системный журнал. Созданные пароли показываются группами по четыре буквы: вводите их без пробелов.
- **Очистить пароль**: удаляет пароль с Mac.

Mac на базе Intel перезагружается, чтобы применить изменение пароля прошивки: до этого по-прежнему нужен прежний пароль (он указан в разделе «Показать пароль»), и отправить ещё одно изменение нельзя. Apple также принимает только одну команду пароля прошивки каждые 30 секунд. Пароли скрыты в истории команд.

Когда Mac выходит из управления (отмена регистрации, удаление пользователем или стирание), macOS сам удаляет Recovery Lock, а Cerberus Enterprise удаляет сохранённый пароль Recovery Lock; то же происходит, когда Mac сообщает, что у него нет Recovery Lock, например после повторной регистрации. При отмене регистрации Mac (или удалении его политики) сначала очищается сохранённый пароль прошивки, Mac перезагружается и затем выходит из управления. Если очистка не удалась, Mac всё равно выходит из управления, а пароль остаётся сохранённым, чтобы вы могли его увидеть. Mac, удалённый из управления пользователем или стёртый, сохраняет пароль прошивки: Cerberus Enterprise тоже его сохраняет. Удаление записи устройства удаляет сохранённый пароль, поэтому сначала запрашивается подтверждение: запишите пароль, поскольку без него удалить его может только Apple.

FileVault (Mac)

В поле **FileVault** отображается, зашифрован ли диск Mac, а во всплывающей подсказке — хранит ли Cerberus Enterprise его личный ключ восстановления. Mac отправляет ключ, когда FileVault включается после получения параметра FileVault своей политики (см. страницу **macOS** политик Apple).

- **Показать ключ восстановления**: только администраторы могут видеть ключ, и каждый просмотр записывается в системный журнал. Используйте его на экране входа Mac, чтобы сбросить пароль пользователя, или в режиме восстановления, чтобы разблокировать диск. Он остаётся доступным после выхода Mac из управления; удаление записи устройства удаляет его.
- **Изменить ключ восстановления**: Mac заменяет свой личный ключ восстановления и отправляет новый в зашифрованном виде; старый ключ перестаёт работать. Это возможно, только когда сохранённый ключ можно прочитать: Mac разблокирован с его помощью и пароль пользователя не требуется. Сохранённый ключ скрыт в истории команд и удаляется с сервера, как только Mac ответит (или через 7 дней без ответа).

Bootstrap Token (Mac)

Mac с macOS 10.15 или новее отправляет свой **Bootstrap Token** на сервер управления, когда входит пользователь с безопасным токеном. Сервер хранит его и возвращает только этому Mac, который использует его, чтобы предоставлять новым пользователям безопасный токен и, на Mac с Apple silicon, устанавливать обновления программного обеспечения и одобрять расширения ядра без запроса пароля администратора. Никто не может увидеть токен — ни в панели управления, ни где-либо ещё. Поле **Bootstrap Token** показывает его состояние:

- **Сохранён на сервере**: сервер имеет токен; в подсказке указано, когда Mac его отправил.
- **Сохранён ранее**: сохранённый токен был отправлен до последней регистрации этого Mac или продления его сертификата MDM. После продления это ожидаемо: токен сохраняется, и Mac не отправляет его снова. После новой регистрации он может быть уже недействителен: выполните `sudo profiles install -type bootstraptoken` в Терминале на Mac.
- **Не сохранён**: Mac ещё не отправил токен. Чтобы отправить его сейчас, администратор Mac выполняет `sudo profiles install -type bootstraptoken` в Терминале (`sudo profiles status -type bootstraptoken` показывает, сохранён ли он).

Подсказка также сообщает, разрешает ли Mac использовать токен для аутентификации. Mac, настроенные с помощью Automated Device Enrollment, разрешают это автоматически; на других Mac с Apple silicon пользователь может разрешить это в Startup Security Utility в recoveryOS. Mac на Intel не могут использовать токен для аутентификации (**Не поддерживается**), но сохранённый токен всё равно даёт новым пользователям безопасный токен. Каждый раз, когда Mac отправляет, удаляет или запрашивает свой токен, это

записывается в системный журнал.

Состояние устройства и обновления ОС

Панель **Состояние устройства** показывает, что устройство сообщает о себе: версию и сборку ОС, ход обновления программного обеспечения (ожидаемая версия, крайний срок, что его запустило, сбои), установлен ли код-пароль и соответствует ли он политике, FileVault на Mac, состояние аккумулятора и аккаунты, настроенные на устройстве.

Список **Доступные обновления** показывает обновления ОС, которые устройство может установить; они собираются при регистрации и еженедельно. Используйте **Проверить обновления**, чтобы запросить их сейчас, и **Установить**, чтобы сразу установить обновление (после подтверждения устройство перезагрузится) или только загрузить его и позволить пользователю установить самостоятельно. Это работает на iPhone и iPad под наблюдением и на Mac до iOS, iPadOS и macOS 26: на более поздних версиях и для обновления многих устройств используйте обязательные обновления политики (см. страницу **Обновления ПО** политик Apple).

Mac с Apple silicon устанавливает обновление без запроса пароля администратора, только если он разрешает использование своего Bootstrap Token для аутентификации и токен сохранён (см. Bootstrap Token выше). В противном случае в подтверждении указывается, что пользователю, возможно, придётся ввести пароль администратора перед установкой обновления.

Приложения и инвентаризация

Панель **Приложения** перечисляет все приложения устройства в одной таблице. Состояние установки приложений, установленных политикой или командой, передаётся устройством в реальном времени; версии, размеры и приложения, установленные пользователем, берутся из последнего списка приложений, собранного при регистрации и еженедельно. Используйте **Запросить у устройства**, чтобы запросить его сейчас.

- **Управление**: **Политика** для приложений, установленных политикой устройства, **Управляемое** для приложений, установленных командой, например **Установить приложение**, **Не управляется** для установленных пользователем. У приложения Cerberus Enterprise есть метка **Установлено Cerberus**.
- **Требует внимания**: приложения, которые не удалось установить, были отклонены или удалены пользователем либо ожидают пользователя. Откройте строку, чтобы увидеть ошибку; приложения политики, установка которых не удалась, можно установить снова с помощью кнопки повтора. Встроенные приложения и приложения App Store, которые устройство сообщает как непроверенные, не учитываются.

- **Удалить приложение**: управляемые приложения можно удалить вместе с их данными. Чтобы удалить приложение, установленное политикой, удалите его из политики. Политика также сама отправляет эту команду, когда пакет Mac, установленный как управляемое приложение, удаляется из политики.

Панель **Профили, сертификаты и безопасность** показывает профили конфигурации, сертификаты и состояние безопасности (код-пароль, шифрование, FileVault и брандмауэр на Mac), о которых сообщает устройство.

> На личных устройствах приложения, установленные пользователем, не собираются, и перечисляются только профили и сертификаты, управляемые Cerberus Enterprise.

Панель **Изменения инвентаризации** показывает, что изменилось между двумя списками, отправленными устройством: приложения установлены, удалены или обновлены (со старой и новой версией), профили установлены, удалены или обновлены, сертификаты добавлены или удалены. Изменение обнаруживается, когда устройство отправляет новый список — еженедельно для приложений и профилей, ежедневно для сертификатов, — или когда вы используете **Запросить у устройства**: показанная дата — это дата обнаружения, а изменение произошло между предыдущим списком и этим. Первый список устройства и первый после новой регистрации или смены владельца только фиксируется как отправная точка. Поиск по имени или идентификатору, фильтрация по типу и изменению. Изменения хранятся 365 дней.

> Когда обновление ОС заменяет сразу много приложений Apple, они отображаются одной строкой (например, «Обновлено приложений Apple: 23»), которую можно развернуть. Продление сертификата MDM отображается как **Сертификат MDM продлён**. На личных устройствах показываются только изменения элементов, управляемых Cerberus Enterprise.

Столбцы истории Apple

- **Дата создания**
- **Команда**
- **Статус**: **Отправлено** (ожидает устройство, доставляется, как только оно подключится), **Успешно**, **Есть ответ** (откройте строку, чтобы увидеть результат), **Ожидание устройства** (устройство не может выполнить команду прямо сейчас), **Не выполнено** (откройте строку, чтобы увидеть причину) или **Отменено** (очередь команд устройства была очищена, например при повторной регистрации).
- **Дата выполнения**

Обновить

Используйте действие обновления на панели «Команды», чтобы перезагрузить историю команд.

Revision #53
Created 2025-12-18 17:35:25 UTC by Admin
Updated 2026-11-12 09:57:45 UTC by Admin