macOS

Раздел **macOS** редактора политик Apple управляет настройками безопасности, конфиденциальности и входа на Mac: FileVault, Firewall, Gatekeeper, заставка и блокировка, внешние и сетевые накопители, Screen Sharing, разрешения конфиденциальности, объекты входа и системные расширения и расширения ядра, которым разрешено загружаться. Он также устанавливает файлы конфигурации системных служб и фоновых задач. Остальные устройства политики не получают эти параметры. Включите параметр, чтобы управлять им; пока он выключен, пользователи сохраняют свой выбор.

> Большинство параметров устанавливаются на Mac как профили конфигурации, видимые в разделе «Системные настройки» > «Основные» > «Управление устройством». FileVault, разрешения конфиденциальности, объекты входа и параметры расширений требуют MDM, одобренного пользователем: на Mac, зарегистрированном с помощью URL регистрации или QR-кода, пользователь одобряет профиль регистрации в «Системных настройках». Страница устройства показывает это в поле **MDM, одобренный пользователем**. Когда пользователь одобряет его позже, Mac автоматически получает эти параметры.

FileVault

FileVault шифрует диск Mac. Если этот параметр включён, пользователям предлагается включить FileVault с помощью своего пароля, и Mac отправляет свой личный ключ восстановления в Cerberus Enterprise, зашифрованный ключом, который принадлежит только вашей организации. Ключ отображается и изменяется в поле **FileVault** на странице устройства (см. «Команды устройства»). Параметр требует macOS 13 или новее и MDM, одобренного пользователем; без MDM, одобренного пользователем, Mac не получает запрос на включение FileVault, но если пользователь включает его, его ключ сохраняется.

- **Требовать при входе**: при следующем входе, после нескольких пропусков (пользователю снова предлагается при каждом входе и при выходе) или только когда пользователь выходит из системы.
- **Не спрашивать при выходе**: пользователю предлагается только при входе. Это нельзя сочетать с «Только при выходе».
- **Показывать ключ восстановления пользователю**: по умолчанию выключено, поэтому ключ знают только администраторы — со страницы устройства.
- **Запретить выключение FileVault**: включено по умолчанию.
- **Удалять ключ из памяти в режиме ожидания**: пользователь снова вводит пароль, когда Mac выходит из режима ожидания.

- **Где хранится ключ**: текст, отображаемый пользователю в окне входа, например кому позвонить для восстановления Mac (по умолчанию «Cerberus Enterprise»).

> Mac, который уже был зашифрован при получении параметра, сохраняет свой текущий ключ, который Cerberus Enterprise не получает: ключ сохраняется только после того, как пользователь выключит и снова включит FileVault (при выключенном параметре «Запретить выключение FileVault»). Выключение параметра или удаление Mac из управления не выключает FileVault, и сохранённый ключ продолжает работать. Параметр нельзя сохранить, если сервер не настроен для хранения ключей восстановления.

Firewall

- **Включить Firewall**: когда он выключен, Firewall остаётся выключенным, и пользователи не могут включить его.
- **Блокировать все входящие соединения**: только базовые сетевые службы (DHCP, Bonjour, IPSec) могут принимать соединения.
- **Скрытый режим**: Mac не отвечает на ping-запросы и подключения к закрытым портам.
- **Разрешить встроенное ПО** и **Разрешить загруженные подписанные приложения** принимать соединения, не спрашивая пользователя (macOS 12.3 или новее).
- **Правила для отдельных приложений**: разрешите или заблокируйте входящие соединения приложения по bundle ID.

Gatekeeper

Gatekeeper проверяет приложения перед их открытием. Выберите, открывают ли Mac только приложения App Store или также приложения известных разработчиков. Если Gatekeeper выключен, можно открыть любое приложение, в том числе неподписанное или повреждённое. В macOS 15 или новее вы также можете выбрать, предлагается ли пользователям отправлять заблокированное вредоносное ПО в Apple.

Заставка и блокировка

Запускать заставку после периода бездействия и запрашивать пароль при запуске заставки или переходе дисплея в спящий режим — сразу или с задержкой. Параметр, оставленный

как **Не управляется**, остаётся выбором пользователя.

Внешние и сетевые накопители

Разрешайте, делайте доступным только для чтения или блокируйте внешние накопители (USB-накопители, карты SD, внешние диски) и сетевые накопители (общие файловые ресурсы) на Mac. Требуется macOS 15 или новее.

Screen Sharing

Ограничения для тех, кто подключается к этим Mac с помощью Screen Sharing: копирование файлов с Mac или на Mac, высокопроизводительные соединения и количество виртуальных дисплеев. Включение Screen Sharing остаётся выбором пользователя. Требуется macOS 14 или новее.

Разрешения конфиденциальности

Предоставляйте или запрещайте приложениям доступ, который пользователи иначе разрешали бы в разделе «Системные настройки» > «Конфиденциальность и безопасность», например «Полный доступ к диску» для приложения резервного копирования, или запретите приложению доступ к камере. Для каждого разрешения выберите:

- **Разрешение**: «Полный доступ к диску», «Универсальный доступ», «Автоматизация», папки, контакты, календари, фото, камера, микрофон, запись экрана и другие из раздела «Конфиденциальность и безопасность».
- **Доступ**: разрешить или запретить. Камеру, микрофон, запись экрана и мониторинг ввода нельзя разрешить профилем, только запретить; для записи экрана и мониторинга ввода вы можете позволить пользователям разрешать их и без прав администратора.
- **Приложение**: bundle ID приложения или путь к программе (например, к инструменту командной строки).
- **Требование кода**: идентифицирует приложение по его подписи. Получите его в Terminal с помощью `codesign -dr - /Applications/Example.app` и скопируйте текст после `designated =>`.
- **Автоматизация** также требует управляемое приложение (например, Finder) и его требование кода.

Объекты входа и фоновые объекты

Объекты входа и фоновые объекты, соответствующие правилам, управляются: они запускаются без запроса, и пользователи не могут выключить их в разделе «Системные настройки» > «Основные» > «Объекты входа». Правило соответствует идентификатору команды разработчика приложения, его bundle ID или метке демона или агента launchd (также по их первой части). Требуется macOS 13 или новее.

Системные расширения

Системные расширения — современный способ для приложений расширять macOS: сетевые фильтры и VPN, агенты и драйверы безопасности конечных точек. Если этот параметр включён, системные расширения перечисленных команд разработчиков загружаются, не спрашивая пользователя. Требуется macOS 10.15 или новее и MDM, одобренный пользователем.

- **Team ID**: 10-символьный идентификатор команды разработчика (например, в сведениях «Подписано» приложения или с помощью `codesign -dv`). Каждая команда может встречаться только один раз.
- **Разрешить**: все расширения команды или только расширения с перечисленными bundle ID.
- **Типы**: ограничивает команду драйверами, сетевыми расширениями или расширениями безопасности конечных точек. Если ничего не выбрано, разрешены все типы.
- **Удаление** (только для перечисленных расширений): приложение может удалить своё расширение без администратора (macOS 12 и новее), расширение нельзя выключить или удалить, пока включена System Integrity Protection, либо его нельзя удалить в «Системных настройках» и Finder (macOS 15 и новее). Mac с более старой версией macOS по-прежнему разрешают расширение, но без параметра удаления.
- **Пользователи могут одобрять другие системные расширения**: включено по умолчанию. Когда выключено, могут загружаться только расширения, разрешённые профилем; если какой-либо профиль на Mac выключает его, оно выключено.

> В macOS 11.3 и новее удаление этого параметра выключает системные расширения, которые он разрешал, например агент безопасности или сетевой фильтр. Это происходит при выключении параметра, при удалении политики и когда Mac переходит в политику без него. Редактор запрашивает подтверждение перед

выключением параметра.

Расширения ядра (устаревшие)

Расширения ядра — более старый, устаревший способ расширять macOS: предпочитайте системные расширения, когда поставщик их предлагает. Расширения ядра перечисленных команд (все расширения команды или только перечисленные bundle ID) загружаются, не спрашивая пользователя, после перезагрузки. Требуется macOS 10.13.2 или новее и MDM, одобренный пользователем.

- **Пользователи могут одобрять другие расширения ядра**: по умолчанию выключено, поэтому только перечисленные команды могут загружать расширения ядра.
- **Обычные пользователи также могут одобрять их**: при включённых пользовательских одобрениях пользователи без прав администратора также могут одобрять их (macOS 11 и новее).

На Mac с Apple silicon одного профиля недостаточно: кто-то должен запустить Mac в recoveryOS, выбрать «Сниженная безопасность» в Startup Security Utility и разрешить управление расширениями ядра пользователем от известных разработчиков. Mac также может нуждаться в Bootstrap Token, депонированном в Cerberus Enterprise, чтобы одобрить их (см. поле «Bootstrap Token» на странице устройства).

Файлы Mac

Файлы конфигурации служб и фоновые задачи используют файлы, которые вы загружаете в **Файлы Mac** вашей организации: zip-архивы и списки свойств (.plist) размером до 20 МБ. Загружайте, проверяйте, где они используются, или удаляйте их с помощью кнопки **Файлы Mac** в разделе macOS либо с помощью **Выбрать файл** в параметре. Файл, используемый политикой, нельзя удалить. Чтобы изменить файл, загрузите новую версию и выберите её в политике: Mac скачают его снова.

Файлы конфигурации служб

Устанавливает файлы конфигурации системной службы из zip-архива. Встроенные службы: SSH-сервер (sshd), sudo, PAM, печать (CUPS), веб-сервер Apache, bash, zsh, вход по смарт-карте и авторизация. Вы также можете использовать собственную службу с идентификатором обратного DNS, например `com.example.service`: она находит файлы с

помощью библиотеки управляемых файлов конфигурации macOS. Каждая служба может иметь один параметр. Требуется macOS 14 или новее.

> Встроенная служба использует только файлы архива и игнорирует собственные файлы, например /etc/ssh для sshd: поместите всю конфигурацию в архив, в папки, начинающиеся от корня диска (например, `etc/ssh/sshd_config`). Файлы доступны на Mac только для чтения и удаляются вместе с параметром. Сначала протестируйте архив на одном Mac: неверная конфигурация sudo или PAM может лишить пользователей возможности входить в систему или использовать права администратора.

Фоновые задачи

Программы и скрипты, которые выполняются в фоновом режиме и запускаются launchd. Пользователи не могут выключить их, и они удаляются вместе с параметром. Требуется macOS 15 или новее. Для каждой задачи выберите:

- **Идентификатор задачи**: идентификатор обратного DNS, например `com.example.task`, разный для каждой задачи.
- **Программы и скрипты** (необязательно): zip-архив, который Mac распаковывает в `/var/db/ManagedConfigurationFiles/BackgroundTaskServices/Services/`, после чего указывается идентификатор задачи. Сохраняйте право на выполнение файлов и не помещайте в него списки свойств.
- **Списки свойств launchd**: задания, которые запускают программы, загружаемые как демон (для всей системы, от имени root) или как агент (в каждом сеансе пользователя). Ссылайтесь на программы по их пути в папке выше.

Задаче нужны программы или хотя бы один список свойств. Когда файлы изменяются, Mac перезапускают задачу.

Revision #6
Created 2026-11-10 15:18:04 UTC by Admin
Updated 2026-11-12 09:57:47 UTC by Admin