Политики - Apple

- Политики Apple
- Приложения и профили
- Киоск и экран «Домой»
- Код-пароль
- Ограничения
- Сеть
- Обновления ПО
- macOS
- Местоположение и геозоны
- Аккаунты
- Правила соответствия требованиям

Политики Apple

Политики Apple определяют настройки управления, которые Cerberus Enterprise применяет к устройствам Apple через MDM. Эти настройки задаются в панели управления в редакторе политик Apple.

Перед началом

Для управления устройствами Apple необходимо настроить Apple Management (APNs). При необходимости прочитайте страницу Настройка Apple Management (APNs).

Открытие редактора политик Apple

В панели управления откройте **Политики** и нажмите **Создать новую политику Apple**. Чтобы изменить существующую политику Apple, нажмите на её строку в таблице политик.

Структура редактора

Редактор политик Apple состоит из набора раскрывающихся разделов. В верхней части страницы всегда можно изменить:

- **Имя** (обязательно)
- **Id** (только для чтения)
- **Описание** (необязательно)

Разделы политики

Разделы ниже соответствуют панелям, доступным в редакторе политик Apple в настоящее время. При открытии сохранённой политики разделы с изменёнными настройками уже открыты, а остальные остаются закрытыми:

- **Управление приложениями**: настройка ограничений для приложений, управляемых приложений и настроек приложения Cerberus Enterprise.
- **Киоск и экран «Домой»**: режим одного приложения, разрешённые и заблокированные приложения, расположение на экране «Домой», веб-клипы, настройки уведомлений и сообщение на экране блокировки.
- **Безопасность**: управление такими функциями, как автоматическая разблокировка и биометрическая разблокировка.
- **Настройки кода-пароля**: настройка требований к коду-паролю и связанных правил.
- **Мультимедиа**: разрешение или запрет камеры и связанных функций.
- **Сотовая связь**: управление настройками сотовой связи (сотовые данные приложений, eSIM, смена плана) и APN сотовой сети.
- **Сеть**: сети Wi-Fi (включая корпоративные 802.1X), VPN, сертификаты, глобальный прокси, зашифрованный DNS и фильтр веб-содержимого, а также ограничения подключения, такие как AirDrop и Bluetooth.
- **Система и пользовательский интерфейс**: ограничение системных функций, таких как Handoff, имя устройства и экранная заставка.
- **Обновления ПО**: требовать определённую версию ОС к сроку и управлять загрузкой и установкой обновлений.
- **macOS**: Firewall, Gatekeeper, заставка и блокировка, внешние и сетевые накопители, «Общий экран», разрешения конфиденциальности и объекты входа на Mac.
- **Приложения и сервисы Apple**: ограничение приложений и сервисов Apple, таких как iMessage, Game Center и «Локатор».
- **Siri и Apple Intelligence**: ограничение Siri, диктовки и функций Apple Intelligence.
- **iCloud**: разрешать или запрещать отдельные службы iCloud (резервное копирование, синхронизация связки ключей, частный узел и т. д.).
- **Местоположение и геозоны**: области, о входе в которые и выходе из которых сообщают iPhone и iPad с приложением Cerberus Enterprise, для правил событий.
- **Аккаунты**: ограничение изменения аккаунтов и настройка аккаунтов Mail, Exchange, Google, календаря, контактов и каталога.
- **Правила соответствия требованиям**: требования (код-пароль, минимальная версия ОС, управление устройством, FileVault), при несоблюдении которых устройства считаются несоответствующими, с необязательной блокировкой.

> Многие параметры в редакторе политик Apple содержат подсказку с описанием требований и поддерживаемых версий ОС.

Сохранение, удаление и связанные устройства

Используйте **Сохранить политику**, чтобы применить изменения. Кнопка недоступна, если нет несохранённых изменений или срок действия лицензии истёк.

При изменении существующей политики на странице также отображается действие **Удалить политику**. В нижней части редактора может отображаться список **Связанные устройства**, чтобы вы видели, сколько устройств сейчас используют политику.

Следующие страницы

- Приложения и профили: настройка установленных приложений и профилей конфигурации.
- Киоск и экран «Домой»: режим одного приложения, разрешённые приложения, расположение на экране «Домой» и веб-клипы.
- Код-пароль: настройка требований к коду-паролю и связанных параметров безопасности.
- Ограничения: определение разрешённых функций и ограничений на уровне ОС.
- Сеть: сети Wi-Fi, VPN, сертификаты и ограничения подключения.
- Обновления ПО: обязательные обновления ОС и настройки обновления ПО.
- macOS: Firewall, Gatekeeper, блокировка экрана, накопители, разрешения конфиденциальности и объекты входа на Mac.
- Местоположение и геозоны: области, о входе в которые и выходе из которых сообщают iPhone и iPad, и что нужно для их работы.
- Аккаунты: аккаунты почты, Exchange, Google, календаря, контактов и каталога.
- Правила соответствия требованиям: требования к устройствам и блокировка несоответствующих устройств.

Приложения и профили

В этом разделе описано, как настроить управляемые приложения и полезные нагрузки аккаунтов для устройств Apple.

Управление приложениями

Панель **Управление приложениями** содержит как общие ограничения, связанные с приложениями, так и список управляемых приложений.

Общие ограничения приложений

- **Разрешить App Clips**
- **Разрешить установку приложений**
- **Разрешить удаление приложений**
- **Разрешить автоматическую загрузку приложений**
- **Разрешить скрытие приложений**
- **Разрешить блокировку приложений**
- **Разрешить встроенные покупки**
- **Разрешить изменение браузера по умолчанию**
- **Разрешить доверие корпоративным приложениям**

Управляемые приложения

Используйте **Добавить приложение**, чтобы добавить приложение в политику. Каждое управляемое приложение отображается в виде карточки. Вы можете развернуть карточку, чтобы изменить её настройки, и удалить приложение с помощью действия удаления.

- **ID в App Store**: идентификатор управляемого приложения в App Store.
- **Bundle ID**: идентификатор пакета приложения.
- **Поведение при установке**: определяет, должно ли приложение оставаться установленным или пользователь может устанавливать и удалять его.
- **Назначение**: тип лицензии, выбираемый Cerberus для каждого устройства: лицензия устройства на корпоративных устройствах, пользовательская лицензия управляемого аккаунта Apple на личных iPhone и iPad (регистрация пользователя). Поле изменить нельзя.
- **Лицензия VPP**: тип лицензии VPP, используемый для установки через App Store.

Список выбора приложений показывает доступные и общие лицензии каждого приложения. Бесплатные приложения показывают **Без ограничений**: Apple предоставляет для них неограниченное число лицензий. Приложение можно добавить в политику только один раз: приложение с тем же ID в App Store или Bundle ID, что и приложение, уже присутствующее в политике, отклоняется, как и политика, в которой одно и то же приложение указано дважды при сохранении.

Список выбора приложений показывает приложения из вашей библиотеки Apple Business. Чтобы добавить приложение, в Apple Business откройте **Apps & Services → Apps & Books → App Store**, найдите приложение и нажмите **View**. Для бесплатного приложения нажмите **Add**, выберите **All current and future** (или подразделение вашего токена Apps and Books) в **Organizational Units**, нажмите **Add**, затем **Review** и подтвердите. Для платного приложения нажмите его цену, выберите **Managed Licenses** как **License Type** (коды погашения не могут использоваться Cerberus Enterprise), выберите **Organizational Unit** вашего токена Apps and Books, введите количество **Licenses** (до 1 000 за заказ), затем **Review** и купите. Сначала нужно настроить способ оплаты в **Settings → Payments & Billing → Apps & Services → Payment Methods**. После этого приложения появятся в списке выбора приложений.

Приложения на личных устройствах (регистрация пользователя)

Личные iPhone и iPad, зарегистрированные с помощью регистрации пользователя, не имеют серийного номера, поэтому они получают приложения App Store из политики с **пользовательской лицензией** управляемого аккаунта Apple, в который выполнен вход на устройстве. Cerberus регистрирует аккаунт в Apps and Books и сам назначает лицензии, включая бесплатные приложения. Управляемые аккаунты Apple и токен Apps and Books должны принадлежать одной организации Apple Business. Платное приложение использует одну лицензию на аккаунт, общую для всех личных устройств этого аккаунта.

- **Ожидание пользовательской лицензии**: приложение отправляется на устройство только после того, как Apple подтвердит его лицензию, обычно в течение нескольких минут. Панель **Приложения** устройства показывает причину.
- **Не удалось получить пользовательскую лицензию**: Apple не смогла назначить лицензию, например потому что у платного приложения не осталось лицензий. Добавьте лицензии в Apple Business, затем используйте **Запросить снова**; Cerberus также повторяет попытку самостоятельно каждый день.
- **Запрос на установку**: iOS спрашивает пользователя перед установкой каждого приложения. Если пользователь отменяет, приложение показывает **Ожидание подтверждения установки пользователем**; **Запросить снова** снова показывает запрос.
- **Освобождение**: удаление приложения из политики или отмена регистрации последнего личного устройства аккаунта удаляет приложение и освобождает его

лицензию, если только другое зарегистрированное устройство того же аккаунта всё ещё не нуждается в ней.

Подробнее см. в разделе **Регистрация Apple на основе аккаунта**.

Управляемая конфигурация

Управляемая конфигурация передаёт приложению его настройки (например, адрес сервера или имя аккаунта) так, как их описывает поставщик приложения. Откройте приложение в политике и нажмите **Добавить управляемую конфигурацию**. Она отправляется на iPhone и iPad с **iOS или iPadOS 18.4 или новее** и на Mac с **macOS 27 или новее**; на Apple Vision Pro она пока не отправляется. Приложение должно поддерживать управляемую конфигурацию: приложение, которое её не читает, игнорирует её. Панель приложения показывает количество ключей рядом с названием приложения.

- **Ключи**: каждая строка содержит ключ, тип и значение. Типы: текст, целое число, десятичное число, логическое значение, дата, список текста и список целых чисел. Ключи чувствительны к регистру и должны быть уникальными. **Добавить ключ** добавляет строку; **Удалить конфигурацию** удаляет все ключи.
- **Переменные**: значения типа «текст» и «список текста» могут содержать $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$ и $UDID$, которые заменяются значениями каждого устройства и его пользователя. Переменная без значения (например, $EMAIL$ на устройстве без пользователя) остаётся пустой, и в системных журналах это указывается. Когда данные пользователя меняются, устройства получают новые значения; для пользователей, синхронизированных из Google Directory, значения обновляются при следующем изменении политики или устройства.
- **Импорт конфигурации**: откройте или вставьте файл, который поставщик приложения публикует для MDM, затем нажмите **Читать**. **Спецификация AppConfig** (specfile.xml) перечисляет все ключи, поддерживаемые приложением, с описанием, типом, значением по умолчанию и допустимыми значениями: выберите ключи для импорта (ключи со значением по умолчанию уже выбраны) и заполните остальные после импорта. Появляется предупреждение, если спецификация относится к другому приложению. **Список свойств** (весь список свойств или только его <dict>) импортируется как есть. Затем выберите, заменить текущие ключи или добавить к ним. Вложенные словари, значения данных и списки со смешанными или неизвестными типами не поддерживаются и перечисляются как пропущенные. Apple не публикует ключи конфигурации приложений, поэтому запросите файл у поставщика, если его нет в их документации. **Копировать как plist** копирует конфигурацию в том виде, в каком её получает устройство, до замены переменных.
- **Ограничения**: до 200 ключей на приложение; ключи до 255 символов; текстовые значения до 4 096 символов; списки до 200 элементов по 1 024 символа каждый; даты с 1970 по 9999 год; всего 64 КБ на приложение.
- **Не для паролей**: конфигурация отправляется только на устройство, для которого она создана, а журналы показывают только имена ключей и типы, но

администраторы панели управления могут читать значения, а адрес, с которого устройство загружает конфигурацию, меняется в зависимости от значений, поэтому легко угадываемое значение (логическое или небольшое число) можно из него вывести. Не помещайте пароли и другие секреты в управляемую конфигурацию.
- **Состояние**: когда устройство сообщает, что приложение не приняло свою конфигурацию, панель «Приложения» устройства показывает **Конфигурация не принята** рядом с приложением. Это не делает устройство несоответствующим требованиям. Конфигурация, которую устройство не может загрузить, делает его несоответствующим требованиям.

Параметры приложения

У каждого приложения политики (из App Store и пользовательских приложений) есть эти параметры. **По умолчанию на устройстве** оставляет выбор устройству. Устройства, которые не поддерживают параметр, не получают его; приложение всё равно устанавливается.

- **Автоматические обновления**: параметр App Store, «Всегда» или «Никогда». iOS, iPadOS, macOS и visionOS 26 или новее. Для пользовательских приложений параметр App Store работает как «Никогда».
- **Загрузки через сотовую сеть**: параметр App Store, «Всегда» или «Никогда», для автоматических установок и обновлений. Только на контролируемых iPhone и iPad с iOS или iPadOS 26 или новее.
- **Резервное копирование данных приложения**: включаются ли данные приложения в резервные копии устройства. Не на Mac.
- **Пользователь может скрыть приложение** и **Пользователь может заблокировать приложение**: iOS и iPadOS 18.1 или новее, применяется на контролируемых устройствах. Запрет блокировки также предотвращает скрытие. Ограничения **Разрешить скрытие приложений** и **Разрешить блокировку приложений** применяются ко всем приложениям.
- **Блокировать устройство после транзакций Tap to Pay, требующих PIN клиента**: только iPhone.
- **Связанные домены**: домены, с которыми связано приложение (например, для универсальных ссылок или автозаполнения паролей), до 50. Вводите простые имена хостов, например www.example.com, без applinks:, шаблонов и ?mode=. Не на Mac.
- **Проверять домены напрямую**: устройство проверяет файл связи сайта доменов напрямую, а не через серверы Apple. Включайте это только для внутренних доменов, недоступных из интернета.
- **Удаление**: приложения, установленные как **Обязательные**, не могут быть удалены пользователем.

Приложения Mac App Store

Список выбора приложений показывает платформы каждого приложения (iPhone/iPad, Mac, Apple TV, Vision); приложение, существующее только для Mac, показывает значок Mac. Приложение, существующее только для Mac, применяется к Mac при добавлении. Приложение App Store без версии для Mac не отправляется на Mac: политика показывает «У этого приложения нет версии для Mac: оно не отправляется на Mac» в разделе **Применяется к**. Mac получают приложения App Store по их ID в App Store, поэтому приложения с другим Bundle ID на Mac устанавливаются правильно.

Приложение Cerberus Enterprise

Cerberus устанавливает своё приложение **Cerberus Enterprise** на каждый iPhone и iPad с **iOS или iPadOS 18.4 или новее**, с политикой или без неё. Приложение передаёт местоположение устройства и получает уведомления и запросы отслеживания в реальном времени. Оно устанавливается как **Обязательное** с лицензией устройства из Apps and Books (на личных устройствах — пользовательской лицензией), поэтому пользователь не может его удалить.

- **One-time setup**: добавьте бесплатное приложение в библиотеку один раз. В Apple Business откройте **Apps & Services → Apps & Books → App Store**, найдите «Cerberus Enterprise», нажмите **View**, затем **Add**, выберите **All current and future** в **Organizational Units**, нажмите **Add**, затем **Review** и подтвердите. Если приложение показывает **Manage**, оно уже есть в вашей библиотеке: откройте его и проверьте, что его подразделения — **All current and future units**. До этого панель управления показывает баннер, а на устройствах приложение отображается как не установленное. См. **Account settings**.
- **Не в политиках**: приложение нельзя добавить в политику. Оно отключено в списке выбора приложений и отклоняется как пользовательское приложение (тот же Bundle ID). Политика, в которой оно уже указано, удаляет эту запись при открытии: сохраните политику для подтверждения.
- **Не устанавливается на**: устройства с iOS или iPadOS старше 18.4. Установка на Shared iPad поддерживается, но функции приложения там не проверены.
- **Личные устройства**: на iPhone и iPad, зарегистрированных с помощью регистрации пользователя, приложение также устанавливается — с запросом на установку и пользовательской лицензией управляемого аккаунта Apple. Оно получает сообщения от вашей организации и не получает доступ к местоположению, если в политике не включён параметр **Местоположение и геозоны на личных устройствах** и пользователь это не разрешит.
- **Остаётся установленным**: если срок действия токена Apps and Books истекает или приложение покидает вашу библиотеку, приложение остаётся на устройствах, а страница устройства сообщает, что Apps and Books требует внимания. Оно удаляется, только если приложение по-прежнему отсутствует в вашей библиотеке через 24 часа.

Пользовательские приложения

Пользовательские приложения — это ваши собственные приложения для iPhone и iPad (файлы .ipa), распространяемые без App Store. В Xcode экспортируйте приложение для распространения **Enterprise** (Apple Developer Enterprise Program: оно устанавливается на каждое устройство) или **Ad Hoc** (оно устанавливается только на устройства, зарегистрированные в его профиле обеспечения). Сборки App Store загрузить нельзя.

Нажмите **Добавить пользовательское приложение**, чтобы открыть пользовательские приложения вашей организации. **Загрузить приложение** добавляет файл .ipa (до 2 ГБ). Выберите приложение и нажмите **Добавить в политику**. Список показывает версию, тип подписи, количество устройств в профиле ad hoc приложений и дату истечения срока действия профиля обеспечения.

- **Новая версия**: загрузите приложение с тем же Bundle ID. Оно заменяет предыдущую версию, и устройства из политик, которые его используют, обновляют приложение.
- **Требования**: iPhone и iPad с iOS 17.2 или новее. Устройства, которые не могут установить приложение, не получают его: приложение только для iPad на iPhone, более старая версия iOS, чем требуется приложению, устройство, которого нет в профиле ad hoc приложения, или истёкший профиль обеспечения.
- **Истечение срока**: когда срок действия профиля обеспечения истекает, приложение больше не открывается. Загрузите версию, подписанную новым профилем, до даты истечения срока.
- **Зарезервированный Bundle ID**: пользовательское приложение с Bundle ID приложения Cerberus Enterprise (com.lsdroid.Cerberus.Enterprise) нельзя добавить в политику, потому что Cerberus устанавливает это приложение сам.
- **Удаление**: сначала удалите приложение из его политик; затем устройства удалят его.

Пакеты Mac

Пользовательские приложения также принимают установочные пакеты Mac (файлы .pkg). Пакет должен быть дистрибутивным пакетом, собранным с помощью **productbuild** (компонентный пакет, созданный только с помощью pkgbuild, отклоняется), и подписан сертификатом **Developer ID Installer**. Рекомендуется нотаризовать его и прикрепить билет (**notarytool** и **stapler**). Неподписанные пакеты, пакеты, изменённые после подписания, и пакеты, подписанные другими сертификатами, отклоняются.

Загрузите файл .pkg с помощью **Загрузить приложение** и добавьте его в политику: он появится в разделе **Пакеты Mac**. iPhone и iPad игнорируют его.

Mac с **macOS 26 или новее** (под надзором, что включает Mac, зарегистрированные вручную, но не User Enrollment) получают пакет как **объявление**: Mac сам скачивает, устанавливает,

повторяет попытки и обновляет его и сообщает своё состояние. Более старые Mac, а также пакеты, установленные как управляемые приложения, получают его с помощью **команды MDM** в любой версии macOS. Mac, обновлённый до macOS 26, сам переходит на объявление; он может установить каждый пакет ещё раз. То же может произойти, когда Mac переходит в другую политику с тем же пакетом.

- **Новая версия**: загрузите пакет с тем же идентификатором пакета. Он заменяет предыдущую версию, и Mac политик, которые его используют, устанавливают новую.
- **Пропущенные Mac**: Mac с более старой версией macOS, чем допускает пакет, и Intel Mac для пакетов, собранных только для Apple silicon. На странице устройства пакет отображается как «Пропущен» с указанием причины; ранее установленная версия остаётся на Mac.
- **Установка**: **Обязательно** (по умолчанию) устанавливает пакет на Mac; **Необязательно** делает пакет доступным на Mac без его установки. macOS 26 не показывает необязательные пакеты пользователю в «Системных настройках» или App Store (проверено на macOS 26.3), поэтому приложение или скрипт на Mac должен их установить; выбирайте «Необязательно», только если он у вас есть. Это применяется к Mac с macOS 26 или новее; более старые Mac всегда устанавливают пакет. Выбор недоступен для пакетов, установленных как управляемые приложения.
- **Удалять файлы пакета при его удалении из политики (macOS 27 или новее)**: когда пакет удаляется из политики, Mac с macOS 27 или новее удаляют установленные им файлы. По умолчанию выключено. На более старых Mac файлы остаются. Недоступно для пакетов, установленных как управляемые приложения.
- **Установить как управляемое приложение**: включите его для пакета политики, чтобы установить его приложение как управляемое (macOS 11 или новее, не при пользовательской регистрации). Тогда macOS сообщает о сбое установки, и MDM может удалить приложение. Приложение должно быть установлено непосредственно в папку Applications, подписано сертификатом **Developer ID Application** и нотаризовано; на macOS с 11 по 13 пакет должен содержать только это приложение (без других файлов или скриптов). Пользовательские приложения показывают, какие пакеты подходят. Если параметр нельзя применить на Mac, пакет устанавливается там как обычно, а на странице устройства указывается причина.
- **Параметры удаления** управляемого приложения: **Удалить приложение, когда пакет удаляется из политики** (включено по умолчанию) и **Удалить приложение, когда Mac выходит из управления**. Удаление приложения также удаляет его данные. Если пользователь уже установил то же приложение, эта копия становится управляемой и тоже удаляется.
- **Удаление**: команда MDM не может удалить пакет. Для пакета, установленного как управляемое приложение, удаление из политики удаляет приложение (если параметр включён); его остальные файлы и квитанция пакета остаются. Пакеты с включённым параметром **Удалять файлы пакета** удаляются с Mac под управлением macOS 27 или новее. Другие пакеты: удаление из политики только

прекращает новые установки, файлы остаются на Mac. Mac, который пропущен (например, после новой версии, требующей более новой macOS), сохраняет приложение, пока пакет в политике; удаление пакета из политики тогда тоже удаляет его. Удалите оставшиеся файлы на Mac (например, с помощью собственного деинсталлятора пакета) и выполните `sudo pkgutil --forget <identifier>`, чтобы удалить квитанцию пакета.

- **Состояние на устройстве**: панель «Приложения» на Mac показывает каждый пакет политики как «В очереди», «Принят» (Mac принял команду), «Загружен», «Установлен» (только для пакетов, содержащих приложения, когда приложения найдены на Mac) или «Сбой» (с ошибкой). macOS не сообщает об установке пакета, отправленного командой, поэтому «Загружен» — последнее состояние для пакетов без приложений. Пакет, установленный как управляемое приложение, также переходит в «Сбой», когда macOS сообщает, что приложение не удалось установить или оно было удалено с Mac. **Установить снова** снова отправляет пакет на Mac.
- **Состояние с объявлением**: пакеты, доставленные как объявление, показывают метку **Объявление** и состояние, которое сообщает Mac: «В очереди», «Доступен» (необязательный пакет, который пользователь не установил), «Ожидание пользователя», «Загрузка», «Установка», «Установлен» или «Сбой» (с причиной, например неудачная загрузка или установка либо объявление, которое Mac отклонил). Метка **Файлы удалены вместе с политикой** отмечает пакеты, файлы которых Mac с macOS 27 удаляет, когда они покидают политику. **Установить снова** появляется только после сбоя и просит Mac повторить попытку; он не предлагается, когда Mac отклонил объявление.

Аккаунты

Панель **Аккаунты** позволяет настроить аккаунты, применяемые к управляемым устройствам. Она также включает переключатель ограничения на изменение аккаунтов.

Ограничение

- **Разрешить изменение аккаунтов**: если выключено, пользователи не могут изменять такие аккаунты, как Apple Account и интернет-аккаунты.

Добавление аккаунтов

Используйте **Добавить аккаунт Google** или **Добавить почтовый аккаунт**, чтобы добавить конфигурации аккаунтов в политику. Каждый аккаунт отображается в виде карточки с полями конфигурации.

Учётные данные аккаунтов от пользователей

Карточки аккаунтов Google и Mail предоставляют переключатель **Учётные данные аккаунтов от пользователей**. Когда он включён, система применяет учётные данные аккаунта отдельно для каждого пользователя. Когда он выключен, вы вводите идентификатор аккаунта в политике.

Поля аккаунта Google

- **Отображаемое имя**: имя, которое отображается пользователю для аккаунта.
- **Адрес электронной почты Google**: адрес электронной почты пользователя.
- **Полное имя**: полное имя пользователя.

Поля почтового аккаунта

Почтовые аккаунты включают поля идентификации, а также конфигурацию серверов входящей и исходящей почты. Имена хостов обязательны.

- **Отображаемое имя**: имя, которое отображается пользователю для почтового аккаунта.
- **Адрес электронной почты**: адрес электронной почты пользователя.
- **Полное имя**: полное имя пользователя.

Сервер входящей почты

- **Тип сервера**: почтовый протокол (например, IMAP или POP).
- **Метод аутентификации**: метод аутентификации для сервера.
- **Префикс пути IMAP**: отображается только когда «Тип сервера» — IMAP.
- **Имя хоста**: обязательно.
- **Порт**: порт сервера (1–65535).

Сервер исходящей почты

- **Метод аутентификации**
- **Имя хоста**: обязательно.
- **Порт**: порт сервера (1–65535).

Параметры S/MIME

Для почтовых аккаунтов вы также можете настроить шифрование и подписывание S/MIME.

Шифрование

- **Шифрование S/MIME**
- **Идентификатор переопределяется пользователем**
- **Переключатель для каждого сообщения включён**
- **Переопределяется пользователем**

Подписывание

- **Подписывание S/MIME**
- **Идентификатор переопределяется пользователем**
- **Переопределяется пользователем**

> Параметры аккаунтов и ограничений включают в панели управления подсказки с описанием предварительных требований и поддерживаемых версий ОС.

Киоск и экран «Домой»

Раздел **Киоск и экран «Домой»** редактора политик Apple блокирует устройства на одном приложении, выбирает, какие приложения можно открывать, упорядочивает экран «Домой» и добавляет значки веб-сайтов. Каждый параметр устанавливается на устройства как профиль конфигурации.

> Apple применяет большинство этих параметров только к iPhone и iPad под наблюдением (устройствам, зарегистрированным с помощью Automated Device Enrollment или подготовленным с помощью Apple Configurator). Другие устройства их не получают. Веб-клипы также работают на iPhone и iPad без наблюдения. На Mac ни один из этих параметров не применяется.

Выбор приложений

Приложения идентифицируются по их bundle ID. Введите название приложения, чтобы выбрать его из встроенных приложений Apple и приложений политики, или введите любой bundle ID, например `com.example.app`.

Режим одного приложения

Устройство запускает только выбранное приложение: пользователи не могут вернуться на экран «Домой» или открыть другие приложения. Сначала установите приложение с помощью политики. Устройство выходит из режима одного приложения, когда вы выключаете параметр или удаляете приложение.

- **Параметры**: отключите сенсорный экран, поворот экрана, кнопки громкости, переключатель «Звонок/Без звука», боковую кнопку или автоблокировку и включите функции доступности, такие как VoiceOver или Zoom.
- **Функции доступности, которые может включить пользователь**: функции, которые пользователь может включить тройным нажатием боковой кнопки.

Разрешённые и заблокированные приложения

- **Заблокированные приложения**: устройства скрывают эти приложения и не открывают их. `com.apple.webapp` блокирует все веб-клипы. Настройки и, на iPhone, «Телефон» заблокировать нельзя.
- **Разрешить только некоторые приложения**: устройства показывают только эти приложения. Оставьте список пустым, чтобы разрешить все приложения. **Приложения политики** добавляет приложения, установленные политикой; `com.apple.webapp` разрешает все веб-клипы.
- **Приложения, которые могут запускать режим одного приложения**: приложения, которые могут блокировать устройство на себе, пока им это нужно, например во время экзамена.

> При использовании параметра **Разрешить только некоторые приложения** каждое приложение, которого нет в списке, исчезает с устройств, включая приложения политики. «Настройки» и, на iPhone, «Телефон» всегда остаются.

Раскладка экрана «Домой»

Упорядочьте Dock и страницы экрана «Домой». Добавляйте приложения, папки приложений и веб-клипы политики, выбирая место с помощью **Добавить в**, и перетаскивайте значки, чтобы перемещать их между Dock и страницами. Нажмите на папку, чтобы изменить её имя и приложения.

Пользователи не могут перемещать значки или удалять приложения с экрана «Домой». Приложения, которых нет в раскладке, попадают на страницы после определённых вами. iPhone показывает четыре значка в Dock. Пользователи по-прежнему могут удалять приложения, не являющиеся обязательными, на экране хранилища в «Настройках». Чтобы этого не было, выключите **Разрешить удаление приложений** в разделе «Управление приложениями».

Веб-клипы

Веб-клип — это значок на экране «Домой», который открывает веб-сайт. Задайте название и URL, а также при необходимости изображение (PNG или JPEG, обрезанное до квадрата).

- **Пользователи могут удалить его**: выключите, чтобы значок оставался на устройствах.
- **Полный экран**: веб-сайт открывается как веб-приложение, без адресной строки Safari. **Оставаться в полноэкранном режиме на других веб-сайтах** также открывает ссылки на другие веб-сайты в веб-приложении.
- **Открывать в этом приложении**: приложение, которое открывает URL вместо Safari.

Настройки уведомлений

Выберите, как устройства показывают уведомления некоторых приложений: разрешены ли они, где они появляются (экран блокировки, Центр уведомлений, CarPlay), значки, звуки, критически важные оповещения, стиль баннеров, группировку и предварительный просмотр. Пользователи не могут изменять эти настройки.

Сообщение на экране блокировки

Сообщение, отображаемое в нижней части экрана блокировки, например кому позвонить, если устройство найдено, и инвентарная метка. Оба могут содержать переменные $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$ и $UDID$: переменная без значения для устройства остаётся пустой.

Код-пароль

Раздел **Настройки код-пароля** управляет требованиями к код-паролю устройства и связанными правилами безопасности (например, минимальной длиной и сложностью). На Mac (macOS 13 или новее, не с User Enrollment) правила применяются к паролю для входа пользователей.

Параметры

В редакторе политик Apple параметры кода доступа настраиваются с помощью переключателей и числовых полей. Многие поля содержат подсказки с указанием поддерживаемых версий ОС и требований к надзору.

Переключатели кода доступа

- **Изменить при следующей аутентификации**: принудительно сбросить код доступа при следующей аутентификации пользователя.
- **Требовать буквенно-цифровой код доступа**: требовать хотя бы один буквенный символ и одну цифру.
- **Требовать сложный код доступа**: требовать «сложный» код доступа (без повторяющихся/последовательных шаблонов и хотя бы с одним небуквенно-цифровым символом).
- **Требовать код доступа**: требовать код доступа без дополнительных требований к длине и качеству. Примечание: установка других ключей кода доступа неявно требует код доступа.

Числовые поля

- **Сброс неудачных попыток (минуты)**: минуты до сброса счётчика неудачных попыток (требуется параметр «Максимум неудачных попыток»).
- **Максимальное число неудачных попыток**: количество неудачных попыток, разрешённых до стирания iPhone или iPad либо до блокировки Mac (диапазон: 2–11).
- **Максимальный льготный период (минуты)**: сколько времени устройство может оставаться разблокированным без запроса кода доступа (0 = нет).
- **Максимальное время бездействия (минуты)**: время бездействия до блокировки устройства (диапазон: 0–15).
- **Максимальный срок действия кода доступа (дни)**: максимальный срок действия кода доступа до принудительной смены (диапазон: 0–730).

- **Минимум сложных символов**: минимальное количество «сложных» символов (диапазон: 0–4).
- **Минимальная длина**: минимальная длина кода доступа (диапазон: 0–16).
- **Лимит повторного использования кода доступа**: длина истории кодов доступа для предотвращения повторного использования старых кодов (диапазон: 1–50).

Ограничения

Разделы «Ограничения» управляют тем, какие функции ОС разрешены на управляемых устройствах Apple. В редакторе политик Apple эти параметры представлены в виде сгруппированных панелей с несколькими переключателями.

Переключатели панелей **Управление приложениями** и **Сеть** описаны на страницах Приложения и профили и Сеть политик Apple.

> Многие ограничения поддерживаются только в определённых версиях ОС и могут требовать устройства под надзором. Используйте подсказки в панели управления для получения точных требований.

> На устройствах User Enrollment (личных устройствах, зарегистрированных входом с рабочей учётной записью) не отправляются ограничения, которые Apple там не разрешает. Если ни одно из ограничений политики не применяется, эти устройства не получают профиль ограничений. Редактор политик показывает, сколько ограничений не применяется к устройствам User Enrollment.

Безопасность

- **Разрешить автоматическую разблокировку**
- **Разрешить разблокировку по отпечатку пальца**
- **Разрешить изменение отпечатка пальца**
- **Разрешить стирание содержимого и настроек**
- **Разрешить включение ограничений**
- **Разрешить установку профилей пользователями**
- **Разрешить сопряжение с хостом**
- **Разрешить отправку диагностических данных**
- **Разрешить изменение отправки диагностических данных**
- **Разрешить персонализированную рекламу Apple**
- **Разрешить изменение Remote Management**

Мультимедиа

- **Разрешить камеру**
- **Разрешить изменение общего доступа к файлам**
- **Разрешить доступ приложения «Файлы» к USB-накопителям**
- **Разрешить запись звонков**
- **Разрешить AirPrint**
- **Разрешить сохранение учётных данных AirPrint**
- **Разрешить обнаружение iBeacon для AirPrint**

Сотовая связь

- **Разрешить изменение сотовых данных приложений**
- **Разрешить изменение сотового плана**
- **Разрешить изменение eSIM**
- **Разрешить исходящую передачу eSIM**
- **Сохранять eSIM при стирании устройства**
- **Разрешить фоновое обновление в роуминге**

APN сотовой сети

APN сотовой сети задаёт имя точки доступа (APN), которое предоставил ваш оператор, например для частной или корпоративной мобильной сети. Задайте **имя точки доступа** и, если оператор требует, аутентификацию (PAP или CHAP), имя пользователя (переменные, такие как $EMAIL$, разрешены), пароль, версии IP (также при роуминге), прокси-сервер с его портом и XLAT464. Включайте **Attach APN** только если оператор предоставляет отдельный APN для подключения к сети.

- Его получают только iPhone и iPad с сотовой связью, в том числе без надзора. Устройства, зарегистрированные с User Enrollment (личные устройства), его не получают.
- Это применяется только к SIM-карте, используемой для сотовых данных. Устройство, на котором уже установлен профиль APN другим способом, не устанавливает его.
- Пароль защищён так же, как другие сетевые пароли: профиль отправляется только на устройство, для которого он создан, а пароль не записывается в журналы.

> Неверный APN может оставить устройства без сотовых данных: сначала опробуйте настройки на тестовом устройстве с SIM-картой оператора.

Система и пользовательский интерфейс

- **Разрешить Handoff**
- **Разрешить автокоррекцию**
- **Разрешить автоматическое затемнение**
- **Разрешить автоматическую экранную заставку**
- **Разрешить клавиатуру QuickPath**
- **Разрешить поиск определений**
- **Разрешить изменение имени устройства**
- **Разрешить сон устройства**
- **Разрешить iPhone Mirroring**
- **Разрешить виджеты iPhone на Mac**
- **Разрешить сочетания клавиш**

Приложения и сервисы Apple

- **Разрешить iMessage**
- **Разрешить Game Center**
- **Разрешить добавление друзей Game Center**
- **Разрешить функцию «Локатор» для устройства**
- **Разрешить «Локатор» для друзей**
- **Разрешить изменение «Локатор» для друзей**
- **Разрешить Book Store**
- **Разрешить эротику в Book Store**
- **Разрешить резервное копирование корпоративных книг**
- **Разрешить синхронизацию метаданных корпоративных книг**
- **Разрешить iTunes Store**
- **Разрешить контент для взрослых**

Siri и Apple Intelligence

- **Разрешить Siri**
- **Разрешить контент, созданный пользователями Siri**
- **Разрешить Siri на заблокированном устройстве**
- **Разрешить диктовку**
- **Разрешить интеграции внешнего интеллекта**

- **Разрешить вход во внешний интеллект**
- **Разрешить Genmoji**
- **Разрешить Image Playground**
- **Разрешить Image Wand**

iCloud

- **Разрешить адресную книгу iCloud**
- **Разрешить резервное копирование iCloud**
- **Разрешить закладки iCloud**
- **Разрешить календарь iCloud**
- **Разрешить рабочий стол и документы iCloud**
- **Разрешить синхронизацию документов iCloud**
- **Разрешить iCloud Freeform**
- **Разрешить синхронизацию связки ключей iCloud**
- **Разрешить iCloud Mail**
- **Разрешить заметки iCloud**
- **Разрешить медиатеку iCloud**
- **Разрешить частный узел iCloud**
- **Разрешить напоминания iCloud**

Аккаунты (ограничение)

Панель «Аккаунты» содержит ограничение и (необязательно) конфигурацию аккаунтов. Переключатель ограничения определяет, может ли пользователь изменять системные аккаунты.

- **Разрешить изменение аккаунтов**

Сеть

Раздел **Сеть** редактора политик Apple настраивает сети Wi-Fi и VPN на устройствах, устанавливает сертификаты и ограничивает функции подключения, такие как AirDrop и Bluetooth. Каждая сеть Wi-Fi, VPN и сертификат устанавливаются как отдельный профиль конфигурации, который можно увидеть на устройстве в разделе **Настройки > Основные > VPN и управление устройством** (Mac: **Системные настройки > Основные > Управление устройством**, или **Конфиденциальность и безопасность > Профили** в macOS 13 и 14) и на панели **Профили, сертификаты и безопасность** страницы устройства.

> Сертификаты берутся со страницы **Сертификаты**: сначала импортируйте их там. Политика только ссылается на них, поэтому сертификат никогда не копируется в политику.

Ограничения

- **Разрешить AirDrop**
- **Разрешить входящие запросы AirPlay**
- **Разрешить изменение Bluetooth**
- **Разрешить изменение общего доступа по Bluetooth**
- **Разрешить доступ приложения «Файлы» к сетевым дискам**
- **Разрешить изменение общего доступа к интернету**
- **Разрешить кэширование содержимого**
- **Разрешить общий доступ к файлам iTunes**

Сети Wi-Fi

Нажмите **Добавить сеть Wi-Fi** и заполните:

- **Имя сети (SSID)**: имя сети, до 32 символов.
- **Безопасность**: нет (открытая сеть), WEP, WPA или WPA2, WPA2 или WPA3, только WPA3 или любая.
- **Пароль**: пароль личной сети.
- **Подключаться автоматически** и **Скрытая сеть** (для сетей, которые не транслируют своё имя).

- **Прокси**: нет, вручную (сервер и порт) или автоматически (URL файла PAC; пусто — чтобы найти настройки в сети с помощью WPAD).
- **Имя профиля** (необязательно) и **Применяется к**, чтобы ограничить сеть определёнными типами устройств.

Корпоративные сети (802.1X)

Включите **Корпоративная сеть (802.1X)**, когда пользователи аутентифицируются по своим учётным данным или сертификату вместо общего пароля.

- **Аутентификация**: PEAP, TTLS (с внутренней аутентификацией, например MSCHAPv2) или TLS (только сертификат).
- **Учётные данные пользователя устройства**: каждое устройство использует EAP-идентификатор, анонимный идентификатор и пароль своего пользователя, заданные на странице «Пользователи». Устройства без пользователя не получают сеть.
- **Идентификатор**, **Анонимный идентификатор** и **Пароль**: одинаковые для каждого устройства. Идентификатор может содержать переменные $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$ и $UDID$. Оставьте пароль пустым, чтобы пользователь ввёл его на устройстве.
- **Сертификат идентификации**: клиентский сертификат, который представляет устройство (обязателен для TLS). См. параметры сертификатов ниже.
- **Доверенные сертификаты**: сертификаты CA, которые выпустили сертификат вашего сервера RADIUS. Они устанавливаются вместе с сетью.
- **Доверенные имена серверов**: имена сертификатов сервера RADIUS, которые принимают устройства, например radius.example.com или *.example.com.

VPN

Нажмите **Добавить VPN**, чтобы настроить VPN IKEv2 или Cisco IPSec, встроенный в iOS, iPadOS и macOS (приложение VPN не требуется).

- **Тип** и **Сервер**. Для IKEv2 также **Удалённый идентификатор** (идентификатор сервера; пусто означает адрес сервера) и **Локальный идентификатор**, который может содержать переменные $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$ и $UDID$.
- **Аутентификация** устройства: сертификат (со страницы «Сертификаты», сертификат пользователя устройства или запрошенный у сервера SCEP), общий секрет (с необязательным именем группы для IPSec) или ничего для серверов IKEv2, которые проверяют только имя пользователя и пароль.
- **Доверенные сертификаты**: сертификаты CA вашего VPN-сервера, устанавливаемые вместе с VPN. Для IKEv2 вы также можете задать ожидаемые

издателя и имя сертификата сервера.
- **Имя пользователя и пароль**: пользователь также аутентифицируется по имени пользователя (переменные разрешены) и паролю (EAP для IKEv2, XAuth для IPSec). Оставьте пароль пустым, чтобы пользователь ввёл его на устройстве.
- **Имя VPN** (отображается в «Настройках») и **Применяется к**.

Подключение

- **Пользователь подключается в «Настройках»**: VPN установлен, и пользователь включает его при необходимости.
- **По требованию**: устройство подключает VPN автоматически. С параметром **кроме доверенных сетей Wi-Fi** VPN не используется в перечисленных вами сетях Wi-Fi, например в офисной сети.
- **Всегда включён** (IKEv2, только iPhone и iPad под надзором): весь трафик проходит через VPN в сотовой сети и Wi-Fi, и пользователь не может выключить его. Другие устройства не получают этот VPN. Если в VPN используется имя пользователя, пароль должен быть задан в политике.
- **VPN для отдельных приложений**: только некоторые приложения используют VPN. Выберите VPN для каждого приложения в разделе **Управление приложениями** (поле **VPN** приложения, недоступно на Mac) и при необходимости перечислите домены Safari, которые его используют.

> Сначала протестируйте VPN «Всегда включён» или «По требованию» на тестовом устройстве: если сервер недоступен, у устройства может не быть подключения.

Глобальный прокси, шифрованный DNS и фильтр веб-содержимого

Эти параметры применяются ко всему трафику устройства. Включайте их соответствующим переключателем.

- **Глобальный HTTP-прокси** (iPhone и iPad под надзором, Mac): весь HTTP-трафик проходит через прокси в любой сети. Задайте сервер и порт (с необязательными именем пользователя и паролем) или автоматическую конфигурацию (URL файла PAC; пусто — чтобы найти её в сети). **Разрешить страницы входа Wi-Fi** позволяет пользователю входить в общедоступные сети Wi-Fi без прокси.

- **Шифрованный DNS**: устройство разрешает имена с помощью вашего DNS-сервера через DNS over HTTPS (URL сервера) или DNS over TLS (имя сервера), при необходимости только для некоторых доменов. На устройствах под надзором вы можете запретить пользователю выключать его.
- **Фильтр веб-содержимого** (iPhone и iPad под надзором): встроенный в iOS фильтр ограничивает сайты для взрослых, используя списки всегда разрешённых или всегда заблокированных веб-сайтов, либо разрешает только список веб-сайтов, отображаемых как закладки в Safari.

> Неверный прокси или DNS-сервер может оставить устройства без подключения: сначала опробуйте настройки на тестовом устройстве.

Сертификаты

Нажмите **Добавить сертификат**, чтобы установить сертификат отдельно: центр сертификации, которому должны доверять Safari и приложения, или идентификатор, используемый приложениями. Сертификаты сети Wi-Fi или VPN не нужно добавлять здесь.

Параметры сертификатов

- **Сертификат со страницы «Сертификаты»**: один и тот же сертификат на каждом устройстве. Нажмите **Выбрать сертификат**, чтобы выбрать его.
- **Сертификат пользователя устройства**: каждое устройство получает клиентский сертификат, привязанный к его пользователю. Устройства, пользователь которых не имеет сертификата, его не получают. Когда вы привязываете к пользователю другой сертификат, устройства обновляются.
- **Запрошен у сервера SCEP**: каждое устройство запрашивает собственный сертификат у вашего сервера SCEP (например, Microsoft NDES), поэтому закрытый ключ никогда не покидает устройство. Задайте URL сервера, запрос, если сервер его требует, субъект (например, CN=$EMAIL$), альтернативные имена, размер ключа и назначение ключа.

> Клиентские сертификаты (.p12), защищённые старым шифрованием RC2, нельзя установить на устройства Apple. Перед импортом экспортируйте их снова с шифрованием 3DES или AES.

Безопасность

Профили, содержащие пароли или закрытые ключи, отправляются только на устройство, для которого они созданы: устройство должно подписать свой запрос сертификатом управления. Пароли и сертификаты не записываются в журналы.

Обновления ПО

Раздел **Обновления ПО** редактора политик Apple поддерживает устройства в актуальном состоянии: он позволяет требовать определённую версию ОС к определённому сроку и управлять загрузкой и установкой обновлений на устройствах.

Обязательные обновления ОС

Нажмите **Добавить обязательное обновление**, чтобы задать обязательную версию ОС. Устройство загружает обновление, сообщает пользователю о сроке и устанавливает его к сроку, если пользователь не сделал этого раньше. Устройства, на которых уже установлена эта или более новая версия, игнорируют его. Требуется iOS и iPadOS 17 или macOS 14.

- **Применяется к** (обязательно): iPhone и iPad или Mac. У каждой ОС свои номера версий, поэтому добавьте отдельное обязательное обновление для каждой.
- **Версия ОС**: версия для установки, например 18.5 или 15.4.1.
- **Сборка** (необязательно): конкретная сборка, например бета-версия или улучшение безопасности в фоновом режиме.
- **Установить до**: крайний срок по местному времени каждого устройства. Если дата в прошлом, устройства установят обновление как можно скорее.
- **URL с подробностями** (необязательно): веб-страница об обновлении, отображаемая пользователю.

> Устройство сообщает о ходе обновления (загрузка, установка, сбои) на панели **Состояние устройства** страницы устройства.

Настройки обновления ПО

Включите **Настройки обновления ПО для iPhone и iPad** или **Настройки обновления ПО для Mac**, чтобы управлять обновлениями на этих устройствах. Если переключатель выключен, устройства сохраняют собственные настройки. Требуется iOS и iPadOS 18 или macOS 15: более старые устройства игнорируют эти настройки.

- **Отложить обновления**: новые обновления показываются пользователю только через указанное число дней (от 1 до 90). На Mac можно задать разные периоды для основных и промежуточных обновлений, а также для других системных

обновлений.

- **Обновления, показываемые пользователю** (iPhone и iPad): если доступно несколько обновлений, показывать все, только самое старое промежуточное или только самое новое.
- **Стандартные пользователи могут устанавливать обновления** (Mac): пользователи без прав администратора могут устанавливать обновления macOS.
- **Уведомлять пользователя об обязательных обновлениях**: показывать уведомления об обязательных обновлениях и их сроке.
- **Автоматическая загрузка**, **автоматическая установка** и **автоматические обновления безопасности**: позволить пользователю решать (по умолчанию в Apple) или всегда включать либо всегда отключать.
- **Улучшения безопасности в фоновом режиме**: предлагать пользователю быстрые исправления безопасности Apple и выбирать, может ли пользователь их удалять.
- **Бета-программы**: разрешить пользователю участвовать в бета-программах Apple или исключить устройство из них и запретить их (на iPhone и iPad — только для устройств под управлением).

Установка обновления со страницы устройства

Панель **Состояние устройства** устройства содержит список доступных для него обновлений. Используйте **Проверить обновления**, чтобы запросить у устройства список, и **Установить**, чтобы установить обновление сейчас или загрузить его и позволить пользователю установить. Это работает на iPhone и iPad под управлением и на Mac. Apple удаляет эти команды в iOS, iPadOS и macOS 27: в этих версиях используйте обязательные обновления политики.

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.

Местоположение и геозоны

Раздел **Местоположение и геозоны** редактора политик Apple определяет области, например площадку или склад. iPhone и iPad с приложением Cerberus Enterprise сообщают о входе в одну из этих областей или выходе из неё, и правила событий могут на это реагировать: отправить письмо, заблокировать или отключить устройство либо снова включить его. На Mac геозоны не используются.

Поля геозоны

Используйте **Добавить геозону**, чтобы создать новую запись. Политика может содержать до **10 геозон**, и их имена должны быть уникальными в пределах политики. Каждая геозона содержит следующие поля:

- **Имя**: обязательно и уникально.
- **Широта** и **Долгота**: центр области. Вы также можете нажать на карту, чтобы задать его.
- **Радиус (м)**: обязательно, от **200** до **10000** метров.
- **Описание**: необязательные заметки для администраторов.
- **Сообщать о входе** и **Сообщать о выходе**: выберите, какие события генерируются. Хотя бы одно должно оставаться включённым.
- **Активна**: включает или выключает геозону без её удаления.

У каждой геозоны есть предварительный просмотр карты. Центр и радиус сохранённой геозоны заблокированы: используйте кнопку блокировки на карте, чтобы изменить их. Остальные кнопки центрируют карту на области или на вашем текущем местоположении.

При сохранении политики Cerberus Enterprise запрашивает у iPhone и iPad политики получение новых геозон. Обычно это занимает несколько минут, но iOS может отложить это, например в режиме энергосбережения или без подключения к сети. Страница устройства показывает, когда приложение ещё не применило последние геозоны.

Требования

Геозоны работают на iPhone и iPad с приложением Cerberus Enterprise. Mac их игнорируют. На устройстве:

- приложение Cerberus Enterprise установлено (Cerberus устанавливает его), и пользователь открывал его хотя бы раз;
- доступ к геопозиции для приложения установлен как **Всегда**;
- **Точная геопозиция** включена для приложения;
- **Обновление контента** включено.

> **Геопозиция и геозоны на личных устройствах** в верхней части раздела по умолчанию выключены. Пока этот параметр выключен, Cerberus не собирает геопозицию личных устройств (User Enrollment), их события геозон не генерируются, а на их странице устройства не предлагаются «Найти» или отслеживание в реальном времени. Когда вы включаете его, личные устройства политики передают свою геопозицию и события геозон, как корпоративные устройства, но только если пользователь разрешает геопозицию для приложения Cerberus Enterprise; приложение объясняет это пользователю до запроса iOS. Ваша организация отвечает за информирование пользователей и за соблюдение местных правил о геопозиции сотрудников. Режим пропажи и запрос геопозиции MDM никогда не доступны на личных устройствах (Apple этого не разрешает).

В **режиме энергосбережения** геозоны продолжают работать, но iOS сообщает о выходе из области позже и с менее точной геопозицией, а также может задержать получение новых геозон после изменения политики на несколько часов, пока приложение не запустится снова (например, при следующем пересечении или когда пользователь откроет его).

Как поступают события

iOS отслеживает области для приложения и пробуждает его, когда устройство пересекает границу, в том числе когда приложение не открыто. События могут поступать через несколько минут после пересечения, а небольшая область или короткое посещение могут быть пропущены: iOS требуется, чтобы устройство переместилось на некоторое расстояние за границу и оставалось там какое-то время.

Если приложение не может работать, например после перезагрузки до разблокировки устройства, сервер также позже определяет пересечение по геопозициям, которые отправляет приложение. Каждое пересечение запускает правила событий один раз, независимо от того, обнаружило его приложение или сервер.

Когда приложение не связывалось с сервером несколько часов, сервер просит iOS разбудить его, чтобы оно могло снова проверить свои геозоны. iOS не гарантирует выполнение этих запросов.

Страница устройства

На странице устройства вкладка **Геозона** панели **Карта местоположения** показывает переходы устройства. Когда в политике есть активные геозоны, строка состояния сообщает, работает ли геозонирование на устройстве или почему оно не работает: приложение не связывалось с сервером или должно быть обновлено, доступ к геопозиции не **Всегда**, **Точная геопозиция** или **Обновление контента** выключены, **режим энергосбережения** был включён, когда приложение в последний раз сообщало свои настройки, или приложение ещё не применило последние геозоны.

> Переходы геозон и местоположения хранятся **90 дней**, а более старые данные автоматически удаляются каждую ночь. Последнее местоположение каждого зарегистрированного устройства всегда сохраняется, поэтому устройство остаётся на картах.

Ограничения

- Копирование политики не копирует её геозоны: добавьте их снова в копии.
- События геозон на iPhone и iPad выполняются по возможности: iOS решает, когда приложение может работать.

> Чтобы реагировать на события геозон, создайте правило событий для **Устройство входит в геозону** или **Устройство выходит из геозоны**. См. **Правила событий**.

Аккаунты

Раздел **Аккаунты** редактора политик Apple добавляет аккаунты почты, Exchange, Google, календаря, контактов и каталога на iPhone, iPad и Mac. Нажмите **Добавить аккаунт** и выберите тип. Раздел также содержит ограничение **Разрешить изменение аккаунта** (контролируемые устройства).

> На Mac (macOS 13 или новее) аккаунты устанавливаются в сеансе пользователей, зарегистрированных в управлении, обычно пользователя, который зарегистрировал Mac, когда они входят в систему. Страница устройства перечисляет этих пользователей в разделе **Пользователи Mac** с состоянием их аккаунтов. Аккаунты, которые берут адрес электронной почты у пользователя устройства, используют пользователя, назначенного Mac в Cerberus Enterprise.

Общие настройки

- **Имя и электронная почта пользователя устройства** (Mail, Exchange, Google): каждое устройство использует имя и адрес электронной почты своего пользователя, заданные на странице «Пользователи» (для Google — аккаунт Google пользователя). Устройства без пользователя или с пользователем без адреса электронной почты не получают аккаунт. В противном случае задайте фиксированный адрес электронной почты и полное имя.
- **Название аккаунта** (необязательно): название аккаунта в «Настройках» и в приложениях.
- **Имя пользователя** и **Пароль** (необязательно): имя пользователя может содержать переменные $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$ и $UDID$. Оставьте пароль пустым, чтобы пользователь ввёл его на устройстве, или оставьте оба поля пустыми, чтобы пользователь ввёл их.
- **Применяется к**: ограничить аккаунт определёнными типами устройств.

Типы аккаунтов

- **Аккаунт почты**: входящий сервер IMAP или POP и исходящий сервер с их портами и аутентификацией. Исходящий сервер может использовать те же имя пользователя и пароль, что и входящий.

- **Аккаунт Exchange** (Exchange ActiveSync): сервер или пустое значение, чтобы найти его по адресу электронной почты. Выберите службы (почта, контакты, календари, напоминания, заметки) и может ли пользователь их менять. При **современной аутентификации (OAuth)** пользователь входит через страницу вашего поставщика удостоверений, например Microsoft 365. **Сертификат аутентификации** (iOS 17 или новее) аутентифицирует устройство с помощью сертификата.
- **Аккаунт Google**: пользователь входит в аккаунт Google с указанным адресом электронной почты.
- **Аккаунт календаря (CalDAV)** и **Аккаунт контактов (CardDAV)**: сервер, порт и путь.
- **Каталог (LDAP)**: сервер и порт, а также поиски (база поиска, область и описание), используемые для поиска контактов.
- **Подписанный календарь**: URL календаря (https, http или webcal).

S/MIME

Аккаунты Mail и Exchange могут подписывать и шифровать сообщения с помощью S/MIME (iOS 17 или новее). Для каждого из них выберите сертификат: один со страницы сертификатов, сертификат пользователя устройства или запрошенный у сервера SCEP. Вы можете разрешить пользователю отключать это, выбирать другой сертификат и, для шифрования, показывать переключатель для каждого сообщения.

Безопасность

Пароли и сертификаты не входят в настройки, отправляемые на устройства: каждое устройство загружает свои учётные данные из Cerberus Enterprise, подписывая запрос своим сертификатом управления. Они не записываются в журналы.

Правила соответствия требованиям

Раздел **Правила соответствия требованиям** редактора политик Apple задаёт требования к устройствам политики. Устройство, нарушившее правило, сразу становится несоответствующим: страница устройства показывает причину в разделе **Почему устройство не соответствует требованиям**, а список устройств отображает его как несоответствующее. Устройство также считается несоответствующим, когда какой-либо параметр политики нельзя применить на нём.

Правила

- **Код доступа**: на устройстве установлен код доступа, и он соответствует параметрам кода доступа политики.
- **Минимальная версия ОС**: для iPhone и iPad или для Mac. Чтобы обновить устройства, добавьте обязательное обновление в разделе «Обновления ПО».
- **Устройство под надзором**: устройства, зарегистрированные с профилем регистрации или с User Enrollment, не находятся под надзором.
- **FileVault включён (Mac)**: диск Mac зашифрован с помощью FileVault. Другие устройства не затрагиваются.

Правило проверяется, когда устройство отправляет свой статус, при сохранении политики и каждый час. Устройство, статус которого неизвестен (например, Mac, который ещё не сообщил о FileVault), не нарушает правило.

Блокировка устройства

Включите **Блокировать устройство, если оно всё ещё не соответствует требованиям** и укажите, через сколько дней (0 — блокировка сразу). iPhone и iPad под надзором переходят в режим пропажи с заданным вами сообщением. Остальные устройства блокируются один раз; Mac перезагружается и запрашивает PIN-код, который показан в сведениях о команде в истории команд.

- **Разблокировать**: когда устройство снова соответствует требованиям, режим пропажи автоматически выключается.

- **Самостоятельное выключение режима пропажи**: устройство не блокируется снова, пока оно не станет соответствующим требованиям и снова не нарушит правило. Используйте это, чтобы дать пользователю исправить устройство.

> Чтобы получать уведомления или реагировать иначе, создайте правило событий для **Устройство становится несоответствующим**: оно также получает причины.