Регистрация Apple по аккаунту

При регистрации по аккаунту пользователи регистрируют свои iPhone, iPad или Mac, входя со своим рабочим аккаунтом (**управляемым аккаунтом Apple**, например *name@company.com*) в настройках устройства. Не нужно загружать профиль и использовать QR-код: Cerberus Enterprise сам находит пользователя, применяет политику и устанавливает владение.

Два режима

- **Регистрация пользователя** (личные устройства): управляются только рабочие приложения, аккаунты и данные в отдельной области устройства. Cerberus не может видеть личные данные, стирать устройство, определять его местоположение или читать его серийный номер. Устройство помечается как личное. Требуется iOS и iPadOS 15 или macOS 14 и новее.
- **Регистрация устройства** (корпоративные устройства, которых нет в Apple Business): управляется всё устройство, как при ручной регистрации. Зарегистрированный так Mac находится под надзором; iPhone или iPad — нет. Устройство помечается как корпоративное. Требуется iOS и iPadOS 17.1 или macOS 14.1 и новее.

> Вы выбираете режим для iPhone и iPad, а также отдельно для Mac: например, регистрацию пользователя для личных iPhone и регистрацию устройства для Mac. Владение устройством можно изменить позже на странице устройства.

> Регистрация по аккаунту доступна, когда настроено управление Apple (APNs). Если вы ещё не завершили настройку APNs, прочитайте **Настройка управления Apple (APNs)** .

Настройка Apple Business

Пользователи входят с управляемыми аккаунтами Apple, которые создаются в Apple Business. Перед началом:

1. **Подтвердите свой домен** (например, *company.com*) в Apple Business, в разделе доменов вашей организации.
2. **Создайте управляемые аккаунты Apple** для своих пользователей или подключите Apple Business к Google Workspace или Microsoft Entra ID: тогда аккаунтом каждого пользователя будет его рабочий адрес электронной почты, и он будет входить со своим паролем.
3. Для регистрации пользователя проверьте в настройках управления доступом, что управляемые аккаунты Apple могут входить на **личных устройствах**: если они могут входить только на устройствах под надзором, регистрация пользователя не удастся.
4. Только для параметра **Apple Business** ниже: откройте **Устройства → Службы управления → Назначение устройств по умолчанию** (Изменить) и выберите службу управления устройствами Cerberus Enterprise для iPhone, iPad и Mac.

> Сохраняйте службу управления устройствами Cerberus Enterprise и её токен в Apple Business, пока устройства зарегистрированы с управляемыми аккаунтами Apple: их удаление может привести к тому, что аккаунты перестанут работать на устройствах.

Настройка Cerberus Enterprise

Откройте раздел **Регистрация** на панели управления и выберите вкладку **Вход по аккаунту Apple**. Контрольный список в верхней части показывает, чего ещё не хватает. Только администраторы могут изменять настройки.

- **Разрешить регистрацию с помощью входа с рабочим аккаунтом**: включает или отключает регистрацию по аккаунту для всей организации.
- **Домены**: домены аккаунтов ваших пользователей (например, *company.com*), до 20. Регистрироваться могут только аккаунты этих доменов и только после подтверждения домена (см. ниже).
- **iPhone и iPad** и **Mac**: «Выкл.», регистрация пользователя или регистрация устройства для каждого семейства устройств.
- **Политика** для каждого режима: применяется к устройствам сразу после их регистрации. Без политики устройства регистрируются без неё. Изменённая политика применяется к последующим регистрациям.
- **Пользователи**: *Только существующие пользователи* (адрес электронной почты пользователя в Cerberus Enterprise должен совпадать с аккаунтом, введённым на устройстве) или *Создавать пользователя для аккаунтов доменов, у которых его нет*.

> Аккаунт, введённый на устройстве, сопоставляется с полем**Управляемый аккаунт Apple** пользователей, затем с их адресом электронной почты. Код всегда отправляется на адрес электронной почты пользователя. Управляемый аккаунт Apple, заданный для пользователя, может зарегистрироваться, даже если его домен не подтверждён в Cerberus, например аккаунт зарезервированного домена Apple Business *org.appleid.com*. При обнаружении службы Apple Business пользователи всегда вводят свой управляемый аккаунт Apple.

Подтверждение доменов

После сохранения настроек в разделе **Подтверждение домена** для каждого домена отображается запись TXT. Добавьте её в DNS домена, затем нажмите **Подтвердить**. Изменения DNS могут стать видимыми не сразу. Подтверждённый домен остаётся подтверждённым: запись можно удалить позже. Пользователи неподтверждённого домена не могут зарегистрироваться.

Обнаружение службы: как устройства находят Cerberus Enterprise

Когда пользователь входит, устройство запрашивает у домена аккаунта (например, *https://company.com*), какой сервер им управляет. Настройте хотя бы один из этих трёх вариантов. Раздел **Обнаружение службы** на вкладке показывает URL-адрес обнаружения вашей организации и точный текст для копирования для каждого варианта.

Вариант 1: Apple Business (рекомендуется)

Нажмите **Зарегистрировать в Apple Business**: Cerberus Enterprise сохраняет свой URL-адрес обнаружения в вашей организации Apple Business, и ничего не нужно публиковать в ваших доменах. **Проверить в Apple Business** показывает URL-адрес, который Apple Business использует сейчас, а **Удалить из Apple Business** удаляет его.

- Требуется iOS и iPadOS 18.2 или macOS 15.2 и новее. Более старым устройствам нужен вариант 2 или 3.

- Требуется Apple Business, подключённое в Cerberus Enterprise (токен службы автоматической регистрации устройств), и описанное выше назначение устройств по умолчанию.
- Устройство обращается к Apple Business, только когда ваш домен не отвечает: адрес *https://company.com/.well-known/com.apple.remotemanagement* не должен существовать (допустима ошибка, например "not found"). Если ваш веб-сайт отвечает на него веб-страницей, устройства останавливаются на нём. Используйте **Проверить конфигурацию**, чтобы увидеть, что он отвечает.

> Apple Business хранит один URL-адрес обнаружения на организацию: при его регистрации все управляемые аккаунты Apple организации направляются в эту организацию Cerberus Enterprise. Не регистрируйте его из двух организаций Cerberus Enterprise, использующих одну и ту же организацию Apple Business.

Вариант 2: перенаправление с вашего веб-сайта

На веб-сервере каждого домена перенаправьте */.well-known/com.apple.remotemanagement* на URL-адрес обнаружения вашей организации, **сохраняя строку запроса** (в ней передаётся аккаунт, введённый пользователем). Это работает во всех версиях ОС, поддерживающих регистрацию по аккаунту, а режим может различаться для iPhone и Mac. Скопируйте текст для Apache или nginx со вкладки; он выглядит так, с ключом вашей организации:

Apache (.htaccess или виртуальный хост):

```
RewriteEngine On
RewriteRule ^\.well-known/com\.apple\.remotemanagement$
https://enterprise.cerberusapp.com/account-enroll/YOUR-KEY/discovery [R=302,L,QSA]
```

nginx:

```
location = /.well-known/com.apple.remotemanagement {
    return 302 https://enterprise.cerberusapp.com/account-enroll/YOUR-
KEY/discovery$is_args$args;
}
```

На других веб-серверах или в сервисах (IIS, Cloudflare, панели управления хостингом) создайте правило перенаправления (302) с того же пути на URL-адрес обнаружения с параметром, который сохраняет или передаёт строку запроса.

Вариант 3: статический файл на вашем веб-сайте

Если вы не можете добавить перенаправление, опубликуйте файл по адресу *https://company.com/.well-known/com.apple.remotemanagement* (без расширения файла), отдаваемый с *Content-Type: application/json*. Скопируйте его содержимое со вкладки. Статический файл не может выбирать режим для каждого устройства: он использует один и тот же режим для iPhone, iPad и Mac. Для регистрации пользователя он выглядит так:

```
{"Servers":[{"Version":"mdm-byod","BaseURL":"https://enterprise.cerberusapp.com/account-enroll/YOUR-KEY/byod"}]}
```

а для регистрации устройства:

```
{"Servers":[{"Version":"mdm-adde","BaseURL":"https://enterprise.cerberusapp.com/account-enroll/YOUR-KEY/adde"}]}
```

> Режим в файле также должен совпадать с режимом, заданным на вкладке для семейства устройств, иначе в регистрации будет отказано.

Проверить конфигурацию

В разделе **Проверить конфигурацию** выберите домен и устройство (iPhone или Mac) и нажмите **Проверить**: Cerberus Enterprise запрашивает у домена то же, что запросило бы устройство, и показывает ответ, каждое перенаправление и результат. Домен, указывающий на Cerberus Enterprise, означает, что варианты 2 или 3 работают; ответ с ошибкой (например, "not found") подходит для варианта 1; веб-страница или файл, указывающие в другое место, останавливают устройства. Проверка также предупреждает, если перенаправление теряет строку запроса или файл отдаётся не как *application/json*.

Ключ регистрации

URL-адреса обнаружения и регистрации содержат ключ вашей организации. Если URL-адреса были опубликованы по ошибке, нажмите **Создать новый ключ**: старые URL-адреса сразу перестанут работать, поэтому обновите перенаправления и статические файлы на ваших веб-сайтах. Cerberus Enterprise сам регистрирует новый URL-адрес в Apple Business, если используется вариант 1.

Как регистрируются пользователи

1. iPhone и iPad: откройте *Настройки → Основные → VPN и управление устройством → Вход в рабочий или учебный аккаунт*. Mac: *Системные настройки → Основные → Управление устройством → Войти* (в macOS 14: *Конфиденциальность и безопасность → Профили → Войти*).
2. Введите управляемый аккаунт Apple или рабочий адрес электронной почты пользователя в Cerberus (например, *name@company.com*). Если управляемый аккаунт Apple пользователя отличается от введённого, устройство затем попросит войти с этим аккаунтом.
3. Откроется страница Cerberus Enterprise: коснитесь *Отправить код*, затем введите 6-значный код, полученный по электронной почте. Код действует 10 минут; после 5 неверных кодов пользователь должен закрыть страницу и войти снова.
4. Войдите с паролем управляемого аккаунта Apple (или на странице входа компании, если Apple Business подключено к Google Workspace или Microsoft Entra ID), затем разрешите управление устройством.

> Аккаунты, которые не могут зарегистрироваться (домен не подтверждён, нет подходящего пользователя, когда пользователи не создаются автоматически, несколько пользователей с одинаковым адресом электронной почты), видят сообщение "Этот аккаунт не настроен для регистрации. Обратитесь к администратору ИТ." События записываются в системные журналы панели управления.

После регистрации

- На странице устройства показан **управляемый аккаунт Apple**, использованный для регистрации, и тип регистрации (регистрация пользователя или регистрация устройства по аккаунту). В списке устройств устройства с регистрацией пользователя отображаются как "Регистрация пользователя".
- На устройствах с регистрацией пользователя команды и параметры политики, которые не разрешает Apple (стирание, местоположение, режим пропажи, обновления ОС, многие ограничения), не предлагаются и не отправляются. Приложения App Store из политики используют лицензию пользователя вместо лицензии устройства (см. **Приложения на личных устройствах** ниже).
- На устройствах с регистрацией пользователя веб-клипы появляются на экране «Домой», но не отображаются в разделе *Настройки → Основные → VPN и управление устройством*.

- Сертификат MDM этих устройств не продлевается автоматически, а **Возврат в эксплуатацию** недоступен: до истечения срока действия сертификата MDM (через год после регистрации, см. страницу устройства) попросите пользователя зарегистрировать устройство заново.
- Чтобы выйти из-под управления, пользователь выходит из рабочего аккаунта в том же месте настроек, или вы отменяете регистрацию устройства в Cerberus Enterprise. При регистрации пользователя удаляются только рабочие приложения, аккаунты и данные; личные данные остаются. Устройство, зарегистрированное заново, отображается как новое устройство.

> Сразу после регистрации некоторые профили политики (сертификаты, сети Wi-Fi, веб-клипы) могут отображаться как не выполненные с неизвестной ошибкой, а устройство некоторое время может показываться как **Не соответствует требованиям**. Устройство повторяет попытки само, и через некоторое время они устанавливаются без каких-либо действий. Не сохраняйте политику повторно и не регистрируйте устройство заново из-за этого.

Приложения на личных устройствах

У iPhone и iPad, зарегистрированных с регистрацией пользователя, нет серийного номера, поэтому Apps and Books не может выдать им лицензию устройства. Вместо этого Cerberus Enterprise выдаёт приложениям App Store из их политики **лицензию пользователя**: лицензия привязывается к управляемому аккаунту Apple, в который выполнен вход на устройстве. В политике ничего не меняется: одна и та же политика используется для корпоративных и личных устройств, а Cerberus выбирает тип лицензии для каждого устройства.

- **Автоматически**: при первой регистрации Cerberus регистрирует управляемый аккаунт Apple в Apps and Books, затем запрашивает у Apple лицензию для каждого приложения App Store из политики. Бесплатным приложениям тоже нужна лицензия; Apple предоставляет их в неограниченном количестве. Платное приложение использует одну лицензию на управляемый аккаунт Apple, общую для всех личных устройств этого аккаунта.
- **Одна организация**: управляемые аккаунты Apple и токен Apps and Books для Cerberus Enterprise должны принадлежать одной организации Apple Business, а приложения должны быть в библиотеке местоположения токена.
- **Сначала лицензия**: приложение отправляется на устройство только после того, как Apple подтвердит его лицензию, обычно в течение нескольких минут. До этого панель **Приложения** устройства показывает его как **Ожидание лицензии пользователя** с указанием причины.

- **Запрос на установку**: личные устройства никогда не находятся под надзором, поэтому iOS спрашивает пользователя перед установкой каждого приложения, включая приложение **Cerberus Enterprise**, которое Cerberus также устанавливает на эти устройства (**Установить** или **Отмена**); вход в аккаунт Apple не требуется. Если пользователь отменяет, приложение показывает **Ожидание одобрения установки пользователем**: используйте **Запросить повторно** на странице устройства, чтобы снова показать запрос. Приложения, установленные как **Обязательные**, пользователь не может удалить.
- **Приложения, установленные до регистрации**: Apple не позволяет организации перехватить приложение, которое пользователь установил лично на устройство с регистрацией пользователя. Попросите пользователя удалить свою копию перед регистрацией или удалите её и затем используйте **Запросить повторно** на странице устройства: тогда организация установит управляемую копию.
- **Выход из-под управления**: когда регистрация устройства отменяется, iOS удаляет управляемые приложения и их данные. Лицензия освобождается, когда она больше не нужна ни одному другому зарегистрированному устройству того же управляемого аккаунта Apple, например когда приложение покидает политику или регистрация последнего устройства отменяется; лицензии, которые больше никому не нужны, освобождаются ежедневной проверкой в течение суток.

> Когда Apple не может назначить лицензию, например потому что у платного приложения не осталось лицензий, приложение показывает **Ошибка лицензии пользователя** с сообщением Apple. Добавьте лицензии в Apple Business, затем используйте **Запросить повторно** на странице устройства; Cerberus также повторяет попытку самостоятельно при ежедневной проверке. Строка над списком приложений показывает управляемый аккаунт Apple и статус его пользователя Apps and Books; тот же статус есть на странице пользователя.

> Лицензии пользователей используются только на iPhone и iPad: на Mac, зарегистрированных с User Enrollment, приложения App Store из политики не устанавливаются. Книги и личные аккаунты Apple не поддерживаются.

Revision #6
Created 2026-11-10 15:18:20 UTC by Admin
Updated 2026-11-12 09:58:00 UTC by Admin