Подготовка устройств - Android

- Поддерживаемые устройства
- Токены регистрации
- Личные устройства
- Корпоративные устройства для работы и личного использования
- Корпоративные устройства только для работы
- Zero-touch
- Аутентификация с помощью регистрации Google

Поддерживаемые устройства

Как правило, любое устройство под управлением Android 6 или новее с Google Play Services совместимо с Cerberus Enterprise.

Для лучшего пользовательского опыта мы рекомендуем использовать устройства, соответствующие требованиям Android Enterprise Recommended.

> Некоторые функции ограничены определёнными версиями Android или могут работать по-разному в разных версиях ОС. Подробнее о конкретной функции см. в разделе Политики документации.

Cerberus Enterprise поддерживает как корпоративные, так и личные устройства, а также два режима управления: владелец устройства и владелец профиля.

Личные устройства можно управлять с помощью **рабочего профиля**. Это обеспечивает решение BYOD, сохраняя рабочие данные и приложения сотрудников отдельно от личных данных и приложений, что повышает как безопасность, так и конфиденциальность. Этот вариант подходит для устройств, уже принадлежащих сотрудникам, которые вы хотите зарегистрировать в своей организации для рабочего использования.

Корпоративные устройства также можно управлять с помощью рабочего профиля, но вы также можете выбрать вариант **полного управления**, который обеспечивает более строгий контроль над устройством. Корпоративные устройства с рабочим профилем подходят, когда вы предоставляете сотрудникам корпоративные устройства для работы, но при этом разрешаете личное использование. Полностью управляемые устройства лучше подходят для устройств, которые должны использоваться только для работы, или для **выделенных устройств** (COSU, корпоративные устройства однократного использования), таких как киоски.

Подробнее о подготовке устройств см. на странице Обзор подготовки устройств.

Токены регистрации

Cerberus Enterprise использует токены регистрации для запуска процесса регистрации (подготовки) устройств Android. Выбранный токен определяет начальную политику, применяемую к зарегистрированным устройствам, и влияет на то, какие режимы подготовки разрешены.

> Вкладка токенов регистрации Android доступна только после выполнения **настройки управления Android**.

Где найти токены регистрации

В панели управления откройте **Токены регистрации**. В зависимости от конфигурации аккаунта страница может показывать несколько вкладок (токены Android, регистрация через вход Google, ручная регистрация Apple и автоматическая регистрация устройств Apple).

> Если ваше предприятие Android поддерживается управляемым доменом Google (Google Workspace), панель управления также может показывать вкладку **Аутентификация с помощью регистрации Google**. Подробнее о включении и использовании см. **Аутентификация с помощью регистрации Google**.

Список токенов регистрации (Android)

На вкладке токенов Android отображается таблица всех токенов. При нажатии на строку открывается страница сведений о токене.

Столбцы

- **Статус**: **Активен** (устройства могут регистрироваться с токеном), **Срок истёк** (дата истечения прошла) или **Использован** (одноразовый токен, который уже использовали).
- **Политика**: политика, назначенная токену (в подсказке показан идентификатор политики). **Удалённая политика** означает, что политика была удалена после создания токена.
- **Пользователь**: необязательный пользователь, заранее назначенный устройствам, зарегистрированным с помощью токена. **Удалённый пользователь** означает, что пользователь был удалён после создания токена.
- **Регистрации**: сколько устройств зарегистрировалось с токеном; для одноразового токена показывается как **n / 1**.
- **Личное использование**: Разрешено / Запрещено / Выделенное устройство.
- **Создан**: когда был создан токен. В таблице сначала показываются самые новые токены.
- **Срок действия**: дата и время истечения срока действия или **Никогда**.
- **Код регистрации**: код токена, который вы вводите на устройстве при регистрации без QR-кода.

Действия

- Каждая строка имеет действие удаления (**Удалить токен регистрации**). Удаление недоступно, если срок действия лицензии истёк.
- Таблица поддерживает выбор нескольких строк: можно включить режим выбора, выбрать несколько токенов и удалить их с помощью **Удалить выбранные токены**.
- Используйте действие обновления, чтобы перезагрузить список. Таблица разбита на страницы (10/25/50 элементов на странице).

Создание нового токена регистрации

На вкладке токенов Android нажмите **Новый токен регистрации**, чтобы открыть страницу создания токена. Если срок действия лицензии истёк, кнопка создания недоступна.

Параметры токена

1. Политика

Обязательно. Политика, автоматически применяемая ко всем устройствам, зарегистрированным с помощью этого токена. Выберите одну из ваших **политик Android**.

Если у вас ещё нет политики, сначала создайте её.

2. Пользователь

Необязательно. Если задано, вновь зарегистрированные устройства автоматически связываются с этим пользователем.

3. Личное использование

Управляет тем, разрешено ли личное использование на устройстве, подготовленном с помощью этого токена регистрации:

- **Разрешено**: подходит для личных устройств (рабочий профиль) и корпоративных устройств для работы и личного использования.
- **Запрещено**: подходит для корпоративных устройств только для работы (полностью управляемые).
- **Выделенное устройство**: подходит для киосковых/выделенных устройств (устройство не связано с одним пользователем).

4. Допустимые использования

Выберите, может ли токен использоваться многократно (**Многократно**) или только один раз (**Только один раз**).

5. Срок действия

Выберите единицу срока действия (**Минуты**, **Часы**, **Дни** или **Никогда**). Если выбрано не «Никогда», введите значение срока действия. Допустимый диапазон зависит от выбранной единицы и может достигать 10 000 дней.

6. Аутентификация Google

Управляет тем, должен ли пользователь аутентифицироваться с помощью аккаунта Google во время регистрации устройства:

- **Не указано**: используется настройка аутентификации Google на уровне предприятия, чтобы определить, нужно ли пользователю аутентифицироваться с помощью Google во время регистрации.
- **Необязательно**: пользователь может пропустить аутентификацию Google во время регистрации.
- **Обязательно**: пользователь должен аутентифицироваться с помощью аккаунта Google, чтобы продолжить регистрацию.

Если выбрано **Обязательно**, появляется необязательное поле **Эл. почта обязательного аккаунта**. Если оно задано, пользователь должен аутентифицироваться с помощью этого конкретного аккаунта Google во время регистрации.

Параметры подготовки (только QR-код)

Эти дополнительные параметры встраиваются в QR-код и применяются при подготовке полностью управляемых устройств, зарегистрированных сканированием QR-кода. Они не применяются к рабочим профилям или устройствам, зарегистрированным с помощью URL регистрации или токена.

Настройка Wi-Fi

Используйте это, чтобы устройство автоматически подключалось к Wi-Fi во время подготовки и могло скачать и инициализировать приложение управления. Доступные поля: **SSID**, **Скрытый SSID**, **Безопасность** и (при необходимости) **Парольная фраза**.

Вы также можете настроить HTTP-прокси (**Прокси**) и в зависимости от режима указать **Хост /Порт**, **URI PAC** и **Хост в обход прокси**.

Другие параметры

Дополнительные параметры: **Локаль**, **Часовой пояс** и **Пропустить шифрование**.

Сведения о токене регистрации

Когда вы открываете токен, страница сведений показывает конфигурацию токена и информацию об использовании:

- **Статус**, **Срок действия**, **Использование**, **Личное использование**, **Допустимые использования** и (если задано) **Аутентификация Google** с необязательным **Эл. почта обязательного аккаунта**.
- **Токен**: необработанное значение токена регистрации (можно скопировать).
- **URL регистрации**: URL регистрации Google Android Enterprise (можно скопировать и отправить по электронной почте).
- **QR-код**: отображается в правой части страницы и используется для регистрации полностью управляемых устройств.

> Пошаговые процедуры подготовки см. в руководствах по регистрации Android: **Личные устройства**, **Корпоративные устройства для работы и личного использования**, **Корпоративные устройства только для работы** и **Zero-touch**.

Личные устройства

Устройства, принадлежащие сотрудникам, можно настроить с **рабочим профилем**. Рабочий профиль предоставляет изолированное пространство для рабочих приложений и данных, отдельное от личных приложений и данных. Большинство политик приложений, данных и других политик управления применяются только к рабочему профилю, а личные приложения и данные сотрудников остаются конфиденциальными.
Чтобы настроить рабочий профиль на личном устройстве, используйте один из следующих способов подготовки (убедитесь, что для токена регистрации параметр ***Личное использование*** имеет значение **Разрешено**):

Ссылка на токен регистрации

Версия Android
6.0+

Вы можете предоставить URL регистрации конечным пользователям. Когда конечный пользователь откроет ссылку на своём устройстве, он будет проведён через настройку рабочего профиля.

Добавить рабочий профиль из *«Настроек»*

Версия Android
6.0+

Чтобы настроить рабочий профиль на своём устройстве, пользователь может открыть приложение ***Настройки*** устройства, затем с помощью строки поиска найти и коснуться параметра ***Настройка рабочего профиля***.

Если поиск не дал результатов, расположение этого параметра может отличаться. Вот несколько вариантов:

- *Настройки -> Сервисы и настройки Google -> Все сервисы -> Настройка рабочего профиля*.
- *Настройки -> Google -> Настройка и восстановление -> Настройка рабочего профиля*.

Эти шаги запускают мастер настройки, который скачивает *Android Device Policy* на устройство. Затем пользователю будет предложено отсканировать QR-код или вручную ввести токен регистрации, чтобы завершить настройку рабочего профиля.

Скачать Android Device Policy

Версия Android
6.0+

Чтобы настроить рабочий профиль на своём устройстве, пользователь может скачать Android Device Policy из Google Play Store. После установки приложения пользователю будет предложено отсканировать QR-код или вручную ввести токен регистрации, чтобы завершить настройку рабочего профиля.

Личные iPhone и iPad

Личные iPhone и iPad (а также Mac) регистрируются с помощью Apple **Регистрация пользователя**: пользователь входит со своим управляемым аккаунтом Apple в настройках устройства, и управляются только рабочие приложения, аккаунты и данные. На iPhone и iPad приложения App Store из политики и приложение **Cerberus Enterprise** устанавливаются с пользовательской лицензией этого аккаунта. Местоположение личных устройств собирается, только если в их политике включён параметр **Местоположение и геозоны на личных устройствах** и пользователь это разрешает. См. **Регистрация Apple по аккаунту**.

Корпоративные устройства для работы и личного использования

Настройка корпоративного устройства с **рабочим профилем** делает устройство пригодным как для работы, так и для личного использования. На корпоративных устройствах с рабочим профилем:

- Большинство политик приложений, данных и других политик управления применяются только к рабочему профилю.
- Личные профили сотрудников остаются конфиденциальными. Однако предприятия могут применять определённые политики для всего устройства и политики личного использования.
- Предприятия могут использовать *Область блокировки*, чтобы применять действия по обеспечению соответствия ко всему устройству или только к его рабочему профилю.
- Отмена регистрации устройства и команды устройства применяются ко всему устройству.

Чтобы настроить корпоративное устройство с рабочим профилем, используйте один из следующих способов подготовки (убедитесь, что для токена регистрации параметр **Личное использование** имеет значение **Разрешено**):

Способ QR-кода

Версия Android
8.0+

На новом или сброшенном к заводским настройкам устройстве пользователь (обычно ИТ-администратор) шесть раз касается одного и того же места на экране. Это вызывает на устройстве запрос на сканирование QR-кода.

Корпоративные устройства только для работы

Полное управление устройством подходит для корпоративных устройств, предназначенных исключительно для рабочих целей. Предприятия могут управлять всеми приложениями на устройстве и применять весь спектр политик и команд Android Management API.
Также можно заблокировать устройство (с помощью политики) на одном приложении или небольшом наборе приложений для определённой цели или сценария использования. Это подмножество полностью управляемых устройств называется **выделенными устройствами**.
Чтобы настроить полное управление на корпоративном устройстве, используйте один из следующих способов подготовки (убедитесь, что для токена регистрации параметр **Личное использование** имеет значение **Запрещено**):

Способ QR-кода

Версия Android
7.0+

На новом или сброшенном к заводским настройкам устройстве пользователь (обычно ИТ-администратор) шесть раз касается одного и того же места на экране. Это вызывает на устройстве запрос на сканирование QR-кода.

Способ идентификатора DPC

Версия Android
5.1+

Если Android Device Policy невозможно добавить с помощью QR-кода, пользователь или ИТ-администратор может выполнить следующие шаги, чтобы подготовить полностью управляемое или выделенное устройство:

1. Пройдите мастер настройки на новом устройстве или устройстве, сброшенном к заводским настройкам.
2. Введите данные для входа в Wi-Fi, чтобы подключить устройство к интернету.
3. Когда появится запрос на вход, введите **afw#setup**, после чего скачается Android Device Policy.

4. Отсканируйте QR-код или вручную введите токен регистрации, чтобы подготовить устройство.

Zero-touch

ИТ-администраторы могут подготавливать корпоративные устройства методом регистрации Zero-touch, описанным в разделе Регистрация Zero-touch для ИТ-администраторов. При первом включении устройство автоматически принудительно применяет настройки, заданные ИТ-администратором.

ИТ-администраторы могут предварительно настроить устройства, приобретённые у авторизованных реселлеров, и управлять ими с помощью панели управления Cerberus Enterprise. Чтобы связать аккаунт Zero-touch, перейдите в раздел **Zero-touch** в панели управления и следуйте инструкциям.

Версия Android	Рабочий профиль	Полностью управляемое устройство	Выделенное устройство
8.0+ (Pixel 7.1+)	✓	✓	✓

Аутентификация с помощью регистрации Google

Аутентификация с помощью регистрации Google (также называется **Аутентификация Google при регистрации**) позволяет пользователям аутентифицироваться со своим аккаунтом Google Workspace во время регистрации устройства Android.

> Эта функция доступна только для предприятий Android, поддерживаемых управляемым доменом Google (Google Workspace).

Где это найти

В панели управления откройте **Токены регистрации** и выберите вкладку **Аутентификация с помощью регистрации Google**. Вкладка отображается только когда настроено Android Management и для вашего предприятия доступна интеграция с Google Workspace.

Включение (или отключение) аутентификации Google

Аутентификация Google включается в **консоли администратора Google**. После изменения настройки вернитесь в Cerberus Enterprise и используйте **Обновить статус**, чтобы перезагрузить текущую конфигурацию.

1. Войдите в **консоль администратора Google** с учётной записью администратора.
2. Откройте **Устройства**.
3. Перейдите в **Мобильные устройства и конечные точки** → **Настройки** → **Интеграции сторонних производителей**.
4. Найдите интеграцию **Android EMM** для Cerberus Enterprise и откройте её.

5. Нажмите **Управление поставщиками EMM**.
6. Переключите **Аутентификация с помощью Google**, чтобы включить или отключить аутентификацию Google для регистрации.
7. Нажмите **Сохранить**.
8. Вернитесь в панель управления Cerberus Enterprise и нажмите **Обновить статус** на вкладке **Аутентификация с помощью регистрации Google**.

Токен регистрации с аутентификацией Google

Когда аутентификация Google включена, панель управления показывает выделенный токен регистрации, используемый для этого режима регистрации. Страница может показывать **QR-код**, значение **Токен регистрации** и **URL регистрации** (можно скопировать и отправить по электронной почте).

Ключевые параметры

- **Разрешить личное использование**: управляет тем, может ли токен регистрировать устройства для работы и личного использования (сценарии рабочего профиля) или только для работы (полностью управляемые / выделенные сценарии).
- **Резервная политика по умолчанию**: политика, применяемая, когда у регистрирующегося пользователя нет назначенной конкретной политики по умолчанию для аутентификации Google.

Взаимодействие с политикой

Настройка политики **Аутентификация при настройке рабочего аккаунта** (workAccountSetupConfig.authenticationType) управляет тем, как пользователи аутентифицируются во время настройки рабочего аккаунта, но настройка **Аутентификация с помощью Google** в консоли администратора Google и тип токена регистрации всё равно могут требовать аутентификации.

Для уже зарегистрированных устройств эта политика применяется, только если устройство управляется аккаунтом управляемого Google Play (т. е. зарегистрировано без **Аутентификации с помощью регистрации Google**).

>

> Некоторые действия (например, изменение параметров токена) могут быть недоступны, если срок действия лицензии истёк.

Зарегистрировать устройство

Во время регистрации пользователю предлагается аутентифицироваться со своим аккаунтом Google Workspace. После успешной регистрации устройство связывается с аутентифицированным пользователем.

Рабочий профиль (личные устройства)

- Поделитесь **URL регистрации** с пользователем. Когда пользователь откроет его на своём устройстве Android, он будет проведён через настройку рабочего профиля и аутентификацию Google.
- Кроме того, пользователь может начать с приложения «Настройки» Android, выбрать сценарий настройки рабочего профиля, а затем отсканировать QR-код или ввести токен регистрации, когда появится запрос.

Корпоративные устройства

- **Способ QR-кода**: на новом или сброшенном к заводским настройкам устройстве несколько раз коснитесь одного и того же места на экране, пока не появится запрос QR-кода, затем отсканируйте QR-код, показанный в панели управления.
- **Способ идентификатора DPC** (если сканирование QR-кода недоступно): пройдите мастер настройки, подключитесь к Wi-Fi, затем, когда появится запрос на вход, введите **afw#setup** и продолжите, отсканировав QR-код или введя токен регистрации. Когда появится запрос, аутентифицируйтесь с помощью аккаунта Google Workspace.

Общие процедуры подготовки Android (рабочий профиль или полное управление) описаны на стандартных страницах регистрации Android в этом руководстве.