

??????????

?????????? - Android

- [Поддерживаемые устройства](#)
- [Токены регистрации](#)
- [Устройства, принадлежащие пользователям](#)
- [Устройства, принадлежащие компании и используемые для работы и личных нужд](#)
- [Устройства, принадлежащие компании и предназначенные только для рабочих целей](#)
- [Автоматическая настройка](#)
- [Аутентификация с использованием регистрации Google](#)

??

В целом, любое устройство, работающее под управлением Android 6 и выше и поддерживающее Google Play Services, совместимо с Cerberus Enterprise.

Для обеспечения наилучшего пользовательского опыта мы рекомендуем использовать устройства, соответствующие требованиям [Android Enterprise Recommended](#).

Некоторые функции ограничены определенными версиями Android или могут работать по-разному в разных версиях операционной системы. Для получения дополнительной информации об определенной функции обратитесь к разделу "[Политики](#)" в документации.

Cerberus Enterprise поддерживает устройства как корпоративной, так и личной собственности, а также два режима управления: управление устройством и управление профилем.

Устройства, принадлежащие личному пользователю, могут управляться с помощью **рабочего профиля**. Это позволяет реализовать решение BYOD (Bring Your Own Device), разделяя рабочие данные и приложения сотрудников от личных данных и приложений, что повышает безопасность и конфиденциальность. Этот вариант подходит для устройств, которые уже принадлежат сотрудникам и которые вы хотите подключить к вашей организации для использования в рабочих целях.

Устройства, принадлежащие компании, также могут управляться с помощью рабочего профиля, но вы также можете выбрать вариант **полного управления**, который обеспечивает более строгий контроль над устройством. Устройства, принадлежащие компании и использующие рабочий профиль, подходят, когда вы предоставляете сотрудникам корпоративные устройства для работы, но при этом позволяете использовать их для личных целей. Устройства с полным управлением лучше подходят для устройств, которые должны использоваться только для работы, или для **специализированных устройств** (COSU, корпоративные устройства для однократного использования), таких как киоски.

Для получения дополнительной информации о настройке устройств, обратитесь к странице [Обзор настройки устройств](#).

??????? ????????????????

Cerberus Enterprise использует токены регистрации для запуска процесса регистрации (настройки) устройств Android. Токен, который вы выбираете, определяет начальные политики, применяемые к зарегистрированным устройствам, и влияет на то, какие режимы настройки разрешены.

Вкладка "Токены регистрации Android" доступна только после завершения [Настройки управления Android](#).

??? ?????? ?????????? ??????????????????

На панели управления откройте **Токены регистрации**. В зависимости от конфигурации вашей учетной записи, на странице могут отображаться несколько вкладок (токены для Android, регистрация через Google, ручная регистрация для Apple и автоматическая регистрация устройств для Apple).

Если ваша корпоративная среда Android управляется через домен Google (Google Workspace), на панели управления также может отображаться вкладка **Авторизация с использованием регистрации Google**. Для получения подробной информации о том, как включить и использовать эту функцию, обратитесь к разделу [Авторизация с использованием регистрации Google](#).

??????? ?????????? ?????????????????? (Android)

Вкладка "Токены для Android" отображает таблицу со списком всех токенов. Нажатие на строку открывает страницу с подробной информацией о токене.

?????????

- **Идентификатор:** внутренний идентификатор токена.
- **Статус:** **Доступно**, **Использовано** (одноразовый токен уже использован) или **Истекло**.

- **Срок действия:** дата и время истечения срока, или **Никогда**.
- **Политика:** политика, назначенная токenu (информация об идентификаторе политики также отображается во всплывающей подсказке).
- **Личное использование:** Разрешено / Запрещено / Выделенное устройство.
- **Допустимые варианты использования:** Однократное или многократное использование.
- **Пользователь:** необязательный пользователь, который может быть предварительно назначен устройствам, зарегистрированным с помощью токена.

????????

- Каждая строка содержит действие удаления (**Удалить токен регистрации**). Удаление отключено, если лицензия истекла.
- Таблица поддерживает множественный выбор: вы можете включить режим выбора, выбрать несколько токенов и удалить их с помощью **Удалить выбранные токены**.
- Используйте действие "Обновить", чтобы перезагрузить список. Таблица разбита на страницы (10/25/50 элементов на странице).

????????? ?????? ?????? ????????????????

На вкладке «Токены Android» нажмите **Новый токен регистрации**, чтобы открыть страницу создания токена. Если срок действия вашей лицензии истек, кнопка создания будет неактивна.

????????? ?????????????????????? ??????????

1. ??????????

Обязательно. Политика автоматически применяется ко всем устройствам, зарегистрированным с использованием этого токена. Выберите одну из ваших [политик для Android](#). Если у вас еще нет политики, создайте ее сначала.

2. ????????????????

Необязательно. Если установлено, новые устройства, добавляемые в систему, автоматически связываются с этим пользователем.

3. ?????????????????? ??? ??????? ??????

Разрешить ли использование устройства для личных нужд при подключении с помощью этого токена регистрации:

- **Доступно:** подходит для устройств, принадлежащих сотрудникам (рабочий профиль), и для корпоративных устройств, используемых для работы и личных нужд.
- **Запрещено:** подходит для корпоративных устройств, используемых только для рабочих задач (полное управление).
- **Выделенное устройство:** подходит для киосков или выделенных устройств (устройство не привязано к конкретному пользователю).

4. ?????????????? ?????????? ??????????????????

Выберите, может ли токен использоваться несколько раз (**Несколько раз**) или только один раз (**Только один раз**).

5. ????? ????????????

Выберите единицу измерения срока действия (**минуты, часы, дни** или **никогда**). Если выбрано значение, отличное от "никогда", введите значение срока действия. Допустимый диапазон зависит от выбранной единицы измерения и может достигать 10 000 дней.

????????????? ?????????????? (????????? QR-?????)

Эти дополнительные параметры встроены в QR-код и применяются при настройке полностью управляемых устройств, зарегистрированных путем сканирования QR-кода. Они не применяются к рабочим профилям или устройствам, зарегистрированным с использованием URL-адреса регистрации или токена.

????????????? Wi-Fi

Используйте это, чтобы устройство автоматически подключалось к сети Wi-Fi во время настройки, чтобы оно могло загрузить и инициализировать приложение управления. Доступные поля включают **SSID, Скрытый SSID, Тип безопасности**, и (при необходимости) **Пароль**.

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

????????? ??????????????

Дополнительные параметры включают **Регион, Часовой пояс** и **Пропустить шифрование**.

????????????????? ? ?????????????? ??????????????????????

При открытии токена страница с деталями отображает информацию о конфигурации и использовании токена:

- **Статус, Срок действия, Использование, Личное использование и Разрешенные способы использования.**
- **Токен:** необработанное значение токена регистрации (можно скопировать).
- **URL регистрации:** URL регистрации для Google Android Enterprise (можно скопировать и отправить по электронной почте).
- **QR-код:** отображается справа на странице и используется для регистрации устройств с полным управлением.

Для получения подробных инструкций по настройке, следуйте руководствам по регистрации для Android: [Устройства, принадлежащие лично пользователю](#), [Устройства, принадлежащие компании и используемые для работы и личных целей](#), [Устройства, принадлежащие компании и используемые только для работы](#), и [Автоматическая регистрация](#).

????????????, ??????????????
????????????

Устройства, принадлежащие сотрудникам, могут быть настроены с использованием **рабочего профиля**. Рабочий профиль предоставляет изолированное пространство для рабочих приложений и данных, отдельно от личных приложений и данных. Большинство политик управления приложениями, данными и другими параметрами применяются только к рабочему профилю, в то время как личные приложения и данные сотрудников остаются конфиденциальными.

Чтобы настроить рабочий профиль на устройстве, принадлежащем личным данным пользователя, используйте один из следующих методов настройки (убедитесь, что [токен регистрации](#) имеет установленный параметр **Личное использование** равным **Разрешено**):

?????? ?? ????? ?????????????

Версия Android
6.0+

Вы можете предоставить URL-адрес регистрации конечным пользователям. Когда конечный пользователь откроет ссылку на своем устройстве, ему будет предложено выполнить настройку рабочего профиля.

????????? ?????????? ?????????? ?? ?????????? "????????????"

Версия Android
6.0+

Чтобы настроить рабочий профиль на своем устройстве, пользователь может открыть приложение **Настройки** устройства, а затем воспользоваться строкой поиска, чтобы найти и нажать на пункт **Настройте рабочий профиль**.

Если поиск не даст результатов, расположение этого параметра может меняться. Вот несколько вариантов:

- *Настройки -> Сервисы и предпочтения Google -> Все услуги -> Настройте свой рабочий профиль.*
- *Настройки -> Google -> Настройка и восстановление -> Настройте свой рабочий профиль.*

Эти шаги запускают мастер настройки, который загружает *политику безопасности для устройств Android* на устройство. Далее пользователю будет предложено отсканировать QR-

код или ввести вручную токен регистрации для завершения настройки рабочего профиля.

???????? ?????????? ?????????????????? ??? ?????????????? Android

Версия Android
6.0+

Чтобы настроить рабочий профиль на своем устройстве, пользователь может скачать приложение "Политика безопасности для устройств Android" из Google Play Store. После установки приложения пользователю будет предложено отсканировать QR-код или вручную ввести токен регистрации, чтобы завершить настройку рабочего профиля.

????????????, ??????????????
????????? ? ?????????????????? ????
????????? ? ?????????? ??????

Настройка устройства, принадлежащего компании, с **рабочим профилем** позволяет использовать устройство как для работы, так и для личных нужд. На устройствах, принадлежащих компании, с рабочими профилями:

- Большинство политик управления приложениями, данными и другими аспектами применяются только к рабочему профилю.
- Личные профили сотрудников остаются приватными. Однако, организации могут применять определенные политики, действующие на всем устройстве, а также политики использования личных функций.
- Организации могут использовать *область действия блокировки* для применения мер обеспечения соответствия ко всему устройству или только к его рабочему профилю.
- Отмена регистрации устройства и выполнение команд для устройства применяются ко всему устройству.

Для настройки корпоративного устройства с рабочим профилем используйте один из следующих методов настройки (убедитесь, что у [токена регистрации](#) установлен параметр **Личное использование** в значении **Разрешено**):

????? ?????????????????? QR-????

Версия Android
8.0+

На новом или сброшенном к заводским настройкам устройстве пользователь (обычно администратор IT-отдела) шесть раз нажимает в одном и том же месте. Это заставляет устройство предложить пользователю отсканировать QR-код.

????????????, ??????????????
???????????? ? ??????????????????
???????????? ???? ????????????? ?????

Полное управление устройством подходит для корпоративных устройств, предназначенных исключительно для рабочих целей. Организации могут управлять всеми приложениями на устройстве и применять весь спектр политик и команд Android Management API.

Также возможно заблокировать устройство (с помощью политики) и разрешить использование только одного приложения или небольшого набора приложений для выполнения определенной задачи или сценария использования. Эта группа полностью управляемых устройств называется **выделенными устройствами**.

Для настройки полного управления на принадлежащем компании устройстве используйте один из следующих методов настройки (убедитесь, что [токен регистрации](#) имеет параметр **Личное использование** установлен в значение **Запрещено**):

????? ?????????????????? QR-?????

Версия Android
7.0+

На новом или сброшенном к заводским настройкам устройстве пользователь (обычно администратор IT-отдела) шесть раз нажимает в одном и том же месте. Это заставляет устройство предложить пользователю отсканировать QR-код.

????? ?????????????????? DPC

Версия Android
5.1+

Если невозможно добавить политику Android через QR-код, пользователь или администратор IT может выполнить следующие действия для настройки устройства с полным управлением или выделенного устройства:

1. Следуйте инструкциям мастера настройки на новом или сброшенном к заводским настройкам устройстве.
2. Введите данные для подключения к Wi-Fi, чтобы устройство подключилось к интернету.
3. Когда появится запрос на ввод данных для входа, введите **afw#setup**, чтобы загрузить политику для Android-устройств.

4. Отсканируйте QR-код или введите вручную код активации для настройки устройства.

????????????????????????????????????

Администраторы могут настроить корпоративные устройства с помощью метода быстрой настройки, описанного в [Раздел о быстрой настройке для администраторов](#). При первом включении устройства оно автоматически переходит в настройки, определенные администратором.

Администраторы могут предварительно настроить устройства, приобретенные у [авторизованных дистрибьюторов](#), и управлять ими с помощью панели управления Cerberus Enterprise. Чтобы подключить ваш аккаунт Zero-touch, перейдите в раздел **Zero-touch** в панели управления и следуйте инструкциям.

Версия Android	Профиль работы	Полностью управляемое устройство	Выделенное устройство
8.0+ (Pixel 7.1+)	✓	✓	✓

???????????????? ?

??

Google

Используйте аутентификацию через Google (также известную как **Google Authentication for Enrollment**), чтобы пользователи могли аутентифицироваться с помощью своей учетной записи Google Workspace при регистрации Android-устройства.

Эта функция доступна только для корпоративных Android-устройств, подключенных к управляемой учетной записи Google Workspace.

??? ??? ?????

На панели управления откройте **токены регистрации** и выберите вкладку **Аутентификация с использованием регистрации Google**. Эта вкладка отображается только при настроенном Android Management и доступной интеграции с Google Workspace для вашей организации.

????????? (??? ??????????????)

???????????????????? ? ?????????????????????

????????? ?????????? Google

Аутентификация с использованием учетной записи Google включена через **консоль администратора Google**. После изменения настройки вернитесь в Cerberus Enterprise и используйте **Обновить статус** для перезагрузки текущей конфигурации.

1. Войдите в [консоль администратора Google](#) с использованием учетной записи администратора.
2. Откройте **Устройства**.
3. Перейдите в раздел **Мобильные устройства и конечные точки** → **Настройки** → **Интеграции с сторонними сервисами**.
4. Найдите **интеграцию Android EMM** для Cerberus Enterprise и откройте ее.

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

????? ?????????????? ?????? Google Authentication

При включенной аутентификации через Google на панели управления отображается специальный токен регистрации, используемый для этого режима регистрации. На странице может отображаться **QR-код**, значение **токена регистрации** и **URL-адрес регистрации** (который можно скопировать и отправить по электронной почте).

????????? ??????????????

- **Разрешить использование в личных целях:** определяет, может ли устройство быть зарегистрировано для использования как в рабочих, так и в личных целях (сценарии с рабочим профилем) или только для рабочих целей (полностью управляемые/выделенные сценарии).
- **Основная политика по умолчанию:** политика, применяемая, когда у пользователя, подключающего устройство, не назначена конкретная политика Google Authentication по умолчанию.

????????????????????? ? ??????????????????

Настройка политики **аутентификации при настройке рабочей учетной записи** (workAccountSetupConfig.authenticationType) определяет, как пользователи проходят аутентификацию при настройке рабочей учетной записи, но настройки консоли управления Google, такие как **Аутентификация с использованием Google**, и тип токена регистрации все равно могут требовать аутентификации.

Для устройств, которые уже зарегистрированы, данная политика применяется только в том случае, если устройство управляется с использованием учетной записи Google Play для предприятий (т.е. зарегистрировано без **Аутентификации с использованием Google**).

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

???????????????????? ???? ?????????

Во время регистрации пользователю предлагается пройти аутентификацию с использованием своей учетной записи Google Workspace. После успешной регистрации устройство связывается с аутентифицированным пользователем.

???????? ???? (???? ???? ??????)

- Поделитесь **ссылкой для регистрации** с пользователем. Когда пользователь откроет ее на своем Android-устройстве, ему будет предложено настроить рабочий профиль и пройти аутентификацию через Google.
- В качестве альтернативы, пользователь может начать настройку из настроек Android и выбрать процесс создания рабочего профиля, а затем отсканировать QR-код или ввести токен регистрации, когда будет предложено.

????????, ????????????????????? ???? ??????

- **Метод QR-кода:** на новом устройстве или устройстве, сброшенном к заводским настройкам, несколько раз нажмите в одном и том же месте на экране, пока не появится запрос на использование QR-кода, затем отсканируйте QR-код, отображаемый на панели управления.
- **Метод идентификации устройства через DPC** (если сканирование QR-кода недоступно): следуйте инструкциям мастера настройки, подключитесь к сети Wi-Fi, затем, когда появится запрос на вход, введите **afw#setup** и продолжите процесс, отсканировав QR-код или введя код регистрации. Когда будет предложено, пройдите аутентификацию с использованием учетной записи Google Workspace.

Для получения информации о стандартных процедурах настройки Android (профиль работы против полностью управляемого устройства), обратитесь к соответствующим разделам руководства.