Политики - Android

- Сводка
- Управление приложениями
- Режим киоска
- Безопасность
- Мультимедиа
- Сотовая связь
- Сеть
- Система
- Местоположение и геозоны
- Управление пользователями
- Личное использование
- Межпрофильные политики
- Отчёты о состоянии
- Разное
- Правила соответствия требованиям

Сводка

Политики Android — основные сущности системы: они определяют правила, применяемые и исполняемые на управляемых устройствах.

Вы можете просматривать свои политики и создавать новые в разделе **Политики** панели управления. Чтобы открыть политику Android, нажмите строку политики в таблице: система откроет страницу **Редактор политики**.

Политику можно связать с токеном регистрации, и тогда она будет автоматически применяться к устройствам в процессе подготовки. Вы также можете изменить политику, назначенную устройству, после подготовки.

> Каждое устройство может быть связано только с одной политикой одновременно.

> Многие параметры политики применяются только к определённым типам устройств (полностью управляемые, выделенные, рабочий профиль) и версиям Android. Неподдерживаемые параметры могут игнорироваться устройством или приводить к отчёту о несоответствии.

Структура редактора политики

Редактор политики организован в виде набора раскрывающихся разделов. В верхней части страницы всегда можно изменить:

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

Разделы ниже соответствуют панелям редактора политики (например: «Управление приложениями», «Безопасность», «Сеть», «Система», «Личное использование», «Межпрофильные политики» и другим). При открытии сохранённой политики разделы с изменёнными настройками уже открыты, а остальные остаются закрытыми. Используйте страницы глав этого руководства, чтобы подробно изучить каждую панель.

Сохранение, удаление и связанные устройства

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

Если вы открыли существующую политику (у неё есть Id), в нижней части страницы отображаются действие **Удалить политику** и список **Связанные устройства**, чтобы вы могли видеть, сколько устройств сейчас используют политику.

Управление приложениями

В этом разделе можно задать политики, связанные с доступностью приложений, установкой, обновлениями и управлением разрешениями.

> Аккаунты управляемого Google Play создаются автоматически при подготовке устройств.

1. Режим Play Store

Этот режим определяет, какие приложения доступны пользователю в Play Store, и поведение на устройстве при удалении приложений из политики.

Белый список (по умолчанию): доступны только приложения, включённые в политику, а любое приложение, отсутствующее в политике, будет автоматически удалено с устройства. Play Store будет показывать только доступные приложения.

Чёрный список: все приложения доступны, а любое приложение, которого не должно быть на устройстве, следует явно отметить как **заблокированное** в политике приложений. Play Store будет показывать все приложения, кроме заблокированных.

2. Политика недоверенных приложений

Политика недоверенных приложений (приложений из неизвестных источников), применяемая на устройстве. Этот параметр управляет системной настройкой Android, которая определяет, может ли пользователь устанавливать приложения вне Play Store (боковая загрузка).

Запретить (по умолчанию): запретить установку недоверенных приложений на всём устройстве.

Только личный профиль: для устройств с рабочими профилями разрешить установку недоверенных приложений только в личном профиле устройства.

Разрешить: разрешить установку недоверенных приложений на всём устройстве.

3. Google Play Protect

Применяется ли проверка приложений Google Play Protect.

Принудительно (по умолчанию): принудительно включает проверку приложений.

Выбор пользователя: позволяет пользователю выбрать, включать ли проверку приложений.

4. Политика разрешений по умолчанию

Политика предоставления запросов разрешений приложениям во время выполнения.

Запрос (по умолчанию): запрашивать у пользователя разрешение.

Предоставить: автоматически предоставлять разрешение.

Запретить: автоматически отклонять разрешение.

5. Функции приложений

Управляет тем, разрешено ли приложениям на полностью управляемых устройствах или в рабочих профилях предоставлять функции приложений. Требуется Android 16 или новее.

Разрешено (по умолчанию): приложения на полностью управляемых устройствах или в рабочих профилях могут предоставлять функции приложений.

Запрещено: приложения на полностью управляемых устройствах или в рабочих профилях не могут предоставлять функции приложений.

6. Установка приложений отключена

Отключена ли установка приложений пользователем.

7. Удаление приложений отключено

Отключено ли удаление приложений пользователем.

8. Политики разрешений

Явные предоставления или запреты разрешений либо групп для всех приложений. Эти значения переопределяют настройку **Политика разрешений по умолчанию**.

Используйте **Добавить политику разрешений**, чтобы создать записи, и удаляйте их с помощью действия удаления.

Каждая запись включает:

> **Разрешение/группа Android**: разрешение или группа Android (обязательно), например **android.permission.READ_CALENDAR** или **android.permission_group.CALENDAR**.
>
> **Политика**: предоставить / запретить / запросить (используются те же параметры политики, что и в **Политика разрешений по умолчанию**).

9. Приложения

Список приложений, которые необходимо включить в политику. Поведение содержимого списка зависит от значения, заданного в **Режим Play Store**.

Если **Режим Play Store** установлен на **белый список**, доступны только приложения, включённые в политику, а любое приложение, отсутствующее в политике, будет автоматически удалено с устройства.

Если **Режим Play Store** установлен на **чёрный список**, все приложения доступны, а любое приложение, которого не должно быть на устройстве, следует явно отметить как **заблокированное** в политике приложений.

Чтобы добавить новое приложение, нажмите кнопку **Добавить приложения** (или значок **Добавить приложения**), выберите **Из управляемого Google Play**, затем выберите приложение в Play Store и нажмите кнопку **Выбрать** в карточке приложения.

Чтобы добавить приложение, которое не опубликовано в Google Play, но уже присутствует на устройстве (например, системное приложение или приложение производителя), нажмите **Добавить приложения**, выберите **По имени пакета (предустановленные приложения)**, введите имя пакета приложения (например, **com.example.app**) и нажмите **Добавить** .Приложение добавляется с типом установки **Принудительно установлено**. Чтобы показывать приложение в пользовательской программе запуска киоска, его **Тип установки** должен быть **Предустановлено** или **Принудительно установлено**: при значении **Доступно** приложение не отображается.

Приложения, недоступные в управляемом Google Play, отмечены значком Android в списке приложений. Их нельзя установить из Google Play, поэтому они должны уже присутствовать на устройстве: устройства, на которых нет приложения, не могут его установить.

Все приложения, опубликованные в Play Store в вашей стране, по умолчанию доступны для выбора. Чтобы выбрать собственные частные приложения или веб-приложения, сначала необходимо загрузить их в систему. Дополнительные сведения см. на странице **Частные приложения**.

Каждое приложение можно настроить отдельно; настройки отображаются в карточке:

9.1. Тип установки

Тип установки приложения.

Доступно: приложение доступно для установки.

Предустановлено: приложение устанавливается автоматически, пользователь может его удалить.

Принудительно установлено: приложение устанавливается автоматически, пользователь не может его удалить.

Заблокировано: приложение заблокировано, и его нельзя установить. Если приложение было установлено по предыдущей политике, оно будет удалено.

Требуется для настройки: приложение устанавливается автоматически, пользователь не может его удалить, и настройка не завершится, пока не закончится установка.

Киоск: приложение автоматически устанавливается в режиме киоска: оно назначается предпочтительным домашним намерением и добавляется в белый список для режима блокировки задач. Настройка устройства не завершится, пока приложение не будет установлено. После установки пользователи не смогут удалить приложение. Этот **тип установки** можно задать только для одного приложения в политике. Если он присутствует в политике, строка состояния автоматически отключается.

Дополнительные сведения см. на странице **Режим киоска**.

9.2. Ограничения установки

Определяет набор ограничений для установки приложения. При выборе нескольких ограничений для установки приложения должны выполняться все они.

> Этот параметр отображается только когда**Тип установки** имеет значение **Предустановлено** или **Принудительно установлено**.

Неограниченная сеть: устанавливать приложение только когда устройство подключено к сети без ограничений трафика (например, Wi-Fi).

Зарядка: устанавливать приложение только когда устройство заряжается.

Простой: устанавливать приложение только когда устройство не используется.

9.3. Режим автообновления

Управляет режимом автообновления приложения.

По умолчанию: приложение автоматически обновляется с низким приоритетом, чтобы свести к минимуму влияние на пользователя. Приложение обновляется при соблюдении всех следующих условий: (1) устройство активно не используется, (2) устройство подключено к сети без ограничений трафика, (3) устройство заряжается. Устройство получает уведомление о новом обновлении в течение 24 часов после его публикации разработчиком, после чего приложение обновляется при следующем соблюдении перечисленных условий.

Отложено: приложение не обновляется автоматически максимум 90 дней после того, как устаревает. Через 90 дней после того, как приложение устарело, последняя доступная версия устанавливается автоматически с низким приоритетом (см. режим автообновления **По умолчанию** режим автообновления). После обновления приложение снова не обновляется автоматически, пока не пройдёт 90 дней с момента его повторного устаревания. Пользователь по-прежнему может обновить приложение вручную из Play Store в любое время.

Высокий приоритет: приложение обновляется как можно скорее. Ограничения не применяются. Устройство немедленно получает уведомление о новом обновлении, когда оно становится доступным.

9.4. Минимальный код версии

Минимальная версия приложения, которая работает на устройстве. Если задано, устройство пытается обновить приложение как минимум до этого кода версии. Если приложение не обновлено, устройство будет содержать **сведения о несоответствии** с **причиной несоответствия**, равной **APP_NOT_UPDATED**. Приложение должно быть уже опубликовано в Google Play с кодом версии, большим или равным этому значению. В политике не более 20 приложений могут указывать минимальный код версии.

9.5. Делегированные области

Области, делегированные приложению от Android Device Policy. Вы можете предоставить другим приложениям набор специальных разрешений Android:

Установка сертификата: предоставляет доступ к установке и управлению сертификатами.

Управляемые конфигурации: предоставляет доступ к управлению управляемыми конфигурациями.

Блокировка удаления: предоставляет доступ к блокировке удаления.

Разрешения: предоставляет доступ к политике разрешений и состоянию предоставления разрешений.

Доступ к пакетам: предоставляет доступ к состоянию доступа к пакетам.

Системное приложение: предоставляет доступ для включения системных приложений.

9.6. Приоритетная сеть

Приоритетная сетевая служба, используемая для этого приложения. Если задано, приложение будет использовать указанный корпоративный сетевой сегмент для своих подключений, когда он доступен. Это должно соответствовать сетевому сегменту, настроенному в разделе **Конфигурация сетевых сегментов 5G** панели **Сотовая связь**.

9.7. Политика разрешений по умолчанию

Политика по умолчанию для всех разрешений, запрашиваемых приложением. Если указана, она переопределяет заданную на уровне политики настройку **Политика разрешений по умолчанию**, которая применяется ко всем приложениям. Она не переопределяет **Политики разрешений**, которые применяются ко всем приложениям.

Запрос (по умолчанию): запрашивать у пользователя разрешение.

Предоставить: автоматически предоставлять разрешение.

Запретить: автоматически отклонять разрешение.

9.8. Связанное рабочее и личное приложение

Управляет тем, может ли приложение взаимодействовать с самим собой в рабочих и личных профилях устройства при согласии пользователя (Android 11+).

Запрещено (по умолчанию): не позволяет приложению взаимодействовать между профилями.

Разрешено: позволяет приложению взаимодействовать между профилями после получения согласия пользователя.

9.9. Исключение из блокировки Always On VPN

Указывает, разрешено ли приложению сетевое взаимодействие, когда VPN не подключён и включена **блокировка**. Поддерживается только на устройствах под управлением Android 10 и новее.

Принудительно (по умолчанию): приложение соблюдает настройку блокировки Always On VPN.

Исключение: приложение исключено из настройки блокировки Always On VPN.

9.10. Виджеты рабочего профиля

Указывает, разрешено ли приложению, установленному в рабочем профиле, добавлять виджеты на главный экран.

Разрешено: приложение может добавлять виджеты на главный экран.

Запрещено: приложение не может добавлять виджеты на главный экран.

9.11. Настройки управления пользователем

Указывает, разрешено ли управление пользователем для данного приложения. Управление пользователем включает такие действия, как принудительная остановка и очистка данных приложения (Android 11+). Если для приложения включён **extensionConfig**, управление пользователем запрещено независимо от этой настройки. Для приложений киоска можно использовать **Разрешено**, чтобы разрешить управление пользователем.

Не указано: используется поведение приложения по умолчанию, чтобы определить, разрешено или запрещено управление пользователем.

Разрешено: управление пользователем разрешено для приложения.

Запрещено: управление пользователем запрещено для приложения.

9.12. Отключено

Отключено ли приложение. Если приложение отключено, его данные сохраняются.

9.13. Разрешить поставщика учётных данных

Разрешено ли приложению выступать в качестве поставщика учётных данных на Android 14 и новее.

9.14. Управляемая конфигурация

Чтобы настроить управляемые параметры приложения, нажмите кнопку **Включить управляемую конфигурацию**. Если для приложения уже задана управляемая конфигурация, её можно изменить с помощью кнопки **Управляемая конфигурация** или удалить с помощью кнопки **Удалить конфигурацию**.

> **Управляемая конфигурация** доступен только для приложений, поддерживающих эту функцию.

9.15. Политики разрешений

Явные предоставления или запреты разрешений для приложения. Эти значения переопределяют **Политика разрешений по умолчанию** и **Политики разрешений**, которые применяются ко всем приложениям.

Используйте **Добавить политику разрешений**, чтобы добавить одно или несколько правил разрешений для карточки приложения, и удаляйте их с помощью действия удаления.

9.16. Идентификаторы треков

Список идентификаторов закрытых тестовых треков приложения, к которым может получить доступ устройство. Если выбрано несколько идентификаторов треков, устройства получают последнюю версию среди всех доступных треков. Если идентификаторы треков не выбраны, устройства имеют доступ только к производственному треку приложения.

> **Идентификаторы треков** — параметр, доступный только для приложений, у которых есть хотя бы один идентификатор трека, доступный вашей организации. Подробнее о том, как добавить организацию в закрытый тестовый трек для конкретного приложения, читайте здесь.

10. Настройки приложений по умолчанию

Задайте приложения по умолчанию для поддерживаемых типов. Если приложение по умолчанию задано хотя бы для одного типа, пользователи не смогут изменять приложения по умолчанию в этом профиле.

> Допускается только одна настройка приложения по умолчанию для каждого значения **Тип приложения по умолчанию**. Список приложений по умолчанию не должен содержать дубликатов.

10.1. Тип приложения по умолчанию

Выберите категорию приложения для настройки (например, браузер, телефон, SMS, кошелёк или помощник). Доступность зависит от версии Android и режима управления.

10.2. Области применения приложения по умолчанию

Выберите, где должно применяться приложение по умолчанию (полностью управляемое устройство, рабочий профиль или личный профиль). Можно выбрать только области, поддерживаемые выбранным типом.

> Если ни одна из выбранных областей не применима к режиму управления устройства, устройство сообщает сведения о несоответствии.

10.3. Приложения по умолчанию

Список приложений, которые можно назначить по умолчанию для выбранного типа. Первое установленное и подходящее приложение назначается по умолчанию.

> Если области включают **Полностью управляемое устройство** или **Рабочий профиль**, каждое приложение также должно присутствовать в списке **Приложения** с параметром **Тип установки**, не равным **Заблокировано**.

11. Выбор закрытого ключа

Позволяет показывать на устройстве интерфейс, в котором пользователь может выбрать псевдоним закрытого ключа, если в разделе **Правила выбора закрытого ключа** нет подходящих правил.

> Для устройств ниже Android P эта настройка может сделать корпоративные ключи уязвимыми.

12. Правила выбора закрытого ключа

Управляет доступом приложений к закрытым ключам. Правило определяет, какой закрытый ключ, если таковой имеется, Android Device Policy предоставляет указанному приложению. Доступ предоставляется либо когда приложение вызывает KeyChain.choosePrivateKeyAlias (или любые перегрузки) для запроса псевдонима закрытого ключа для заданного URL-адреса, либо для правил, не привязанных к URL-адресу (то есть если urlPattern не задан, или

задан как пустая строка или .*) на Android 11 и новее, напрямую, чтобы приложение могло вызвать KeyChain.getPrivateKey без предварительного вызова KeyChain.choosePrivateKeyAlias. Когда приложение вызывает KeyChain.choosePrivateKeyAlias и совпадает более одного choosePrivateKeyRules, последнее совпавшее правило определяет, какой псевдоним ключа вернуть.

Используйте **Добавить правило закрытого ключа**, чтобы создать записи, и удаляйте их с помощью действия удаления.

12.1. Псевдоним закрытого ключа

Псевдоним закрытого ключа, который нужно использовать.

12.2. Шаблон URL

Шаблон URL, с которым сопоставляется URL-адрес запроса. Если не задан или пуст, соответствует всем URL-адресам. Используется синтаксис регулярных выражений java.util.regex.Pattern.

12.3. Имена пакетов

Имена пакетов, к которым применяется это правило. Хеш сертификата подписи каждого приложения проверяется по хешу, предоставленному Play. Если имена пакетов не указаны, псевдоним предоставляется всем приложениям, которые вызывают KeyChain.choosePrivateKeyAlias или любые перегрузки (но не без вызова KeyChain.choosePrivateKeyAlias, даже на Android 11 и новее). Любое приложение с тем же Android UID, что и указанный здесь пакет, получит доступ при вызове KeyChain.choosePrivateKeyAlias.

Используйте **Добавить имя пакета**, чтобы добавить записи, и удаляйте их с помощью действия удаления.

> Чтобы удалить приложение, нажмите на значок **корзины**, в нижней части карточки приложения.

Режим киоска

С помощью режима киоска вы можете ограничить функциональность устройства одним приложением или несколькими приложениями. Выбор между режимом киоска для одного приложения и для нескольких приложений зависит от ваших бизнес-задач.

В **режиме киоска для одного приложения** устройство настраивается для одного приложения и не позволяет конечным пользователям получать доступ к другим приложениям на устройстве. Они также не могут выйти из приложения, что делает устройство выделенным для этого конкретного приложения. Чтобы включить этот режим, укажите приложение в разделе **Управление приложениями** с параметром **Тип установки**, установленным в **Киоск**.

В **режиме киоска для нескольких приложений** устройствам разрешён доступ к нескольким приложениям. Конечные пользователи могут переключаться между приложениями через настраиваемую программу запуска. Чтобы включить этот режим, включите параметр **Настраиваемая программа запуска киоска**.

Когда режим киоска включён, вы также можете настроить, могут ли конечные пользователи получать доступ к определённым системным функциям, например к системным настройкам и строке состояния.

Настраиваемая программа запуска киоска

Включена ли настраиваемая программа запуска киоска. Она заменяет главный экран программой запуска, которая ограничивает устройство приложениями, установленными с помощью параметра **Управление приложениями**. Приложения отображаются на одной странице в алфавитном порядке.

Действия кнопки питания

Задаёт поведение устройства в режиме киоска, когда пользователь нажимает и удерживает кнопку питания.

> **Доступно (по умолчанию)**: Когда пользователь нажимает и удерживает кнопку питания устройства в режиме киоска, отображается меню питания (например, «Выключить», «Перезагрузить»).

Заблокировано: Когда пользователь нажимает и удерживает кнопку питания устройства в режиме киоска, меню питания (например, «Выключить», «Перезагрузить») не отображается. Примечание. Это может помешать пользователям выключить устройство.

Системные предупреждения об ошибках

Указывает, блокируются ли в режиме киоска системные диалоги ошибок для приложений, которые зависли или перестали отвечать. В случае блокировки система принудительно остановит приложение, как если бы пользователь выбрал в интерфейсе вариант «закрыть приложение».

Заблокировано (по умолчанию): Блокируются все системные диалоги ошибок, например при сбое и приложении, не отвечающем на запросы (ANR). В случае блокировки система принудительно останавливает приложение, как если бы пользователь закрыл приложение из интерфейса.

Включено: Отображаются все системные диалоги ошибок, например при сбое и приложении, не отвечающем на запросы (ANR).

Системная навигация

Указывает, какие функции навигации включены (например, кнопки «Главная» и «Обзор») в режиме киоска.

Отключено (по умолчанию): Кнопки «Главная» и «Обзор» недоступны.

Только «Главная»: Включена только кнопка «Главная».

Включено: Кнопки «Главная» и «Обзор» включены.

Строка состояния

Указывает, отключены ли в режиме киоска системная информация и уведомления.

Отключено (по умолчанию): В режиме киоска системная информация и уведомления отключены.

Только системные: В строке состояния отображается только системная информация.

Включено: В режиме киоска в строке состояния отображаются системная информация и уведомления. Примечание. Чтобы эта политика вступила в силу, кнопка «Главная» на

устройстве должна быть включена с помощью kioskCustomization.systemNavigation.

Настройки устройства

Указывает, разрешено ли приложение «Настройки» в режиме киоска.

Разрешено (по умолчанию): В режиме киоска доступ к приложению «Настройки» разрешён.

Заблокировано: В режиме киоска доступ к приложению «Настройки» запрещён.

Безопасность

В этом разделе можно настроить политики безопасности.

Действия при угрозах безопасности

Выберите, что делать, когда устройство сообщает о SecurityRisk в отчётах о состоянии.

Поддерживаемые типы SecurityRisk:

Неизвестная ОС: Play Integrity API определяет, что устройство работает под управлением неизвестной ОС (проверка basicIntegrity проходит, но ctsProfileMatch не проходит).

Скомпрометированная ОС: Play Integrity API определяет, что устройство работает под управлением скомпрометированной ОС (проверка basicIntegrity не проходит).

Ошибка оценки с аппаратной поддержкой: Play Integrity API определяет, что устройство не имеет надёжной гарантии целостности системы, если метка MEETS_STRONG_INTEGRITY не отображается в поле целостности устройства.

Доступные действия:

Стереть корпоративные данные (по умолчанию): отменить регистрацию и стереть рабочие данные (всё устройство, если оно полностью управляемое, или только рабочий профиль для устройств с профилем).

Нет действия: оставить устройство зарегистрированным и ничего не делать автоматически.

При выборе **Стереть корпоративные данные** можно также настроить параметры очистки:

Сохранять защиту от сброса настроек: сохранять данные Factory Reset Protection (FRP) при очистке устройства.

Стереть внешнее хранилище: дополнительно стереть внешнее хранилище устройства (например, SD-карты) при выполнении очистки.

Стереть eSIM: для корпоративных устройств при очистке устройства удаляются все eSIM. На личных устройствах при этом удаляются управляемые eSIM (eSIM, добавленные командой ADD_ESIM), а личные eSIM не удаляются.

1. Макс. время до блокировки

Максимальное время (в секундах) активности пользователя до блокировки устройства. Значение 0 означает отсутствие ограничений.

2. Не выключать при зарядке

Режимы подключения к источнику питания, при которых устройство остаётся включённым. При использовании этого параметра рекомендуется очистить **Максимальное время до блокировки**, чтобы устройство не блокировалось само, пока остаётся включённым.

Зарядное устройство от сети: источник питания — зарядное устройство от сети переменного тока.

Порт USB: источник питания — порт USB.

Беспроводное зарядное устройство: источник питания — беспроводной.

3. Экран блокировки отключён

Если включено, отключает экран блокировки для основного и/или дополнительного дисплея. Эта политика поддерживается только в режиме управления выделенными устройствами.

4. Требования к паролю

Политики требований к паролю.

Используйте **Настроить требования к паролю**, чтобы добавить один или несколько блоков требований к паролю. Используйте **Очистить всё**, чтобы удалить все настроенные требования к паролю.

Требования к паролю могут использовать область **Авто** (одно требование) или отдельные области **Устройство**/**Рабочий профиль**. Требования на основе сложности должны сочетаться с требованиями на основе качества для той же области.

4.1. Область

Область, к которой применяется требование к паролю.

> **Авто**: область не указана. Требования к паролю применяются к рабочему профилю на устройствах с рабочим профилем и ко всему устройству на полностью управляемых или выделенных устройствах.
>
> **Устройство**: требования к паролю применяются только к устройству.
>
> **Рабочий профиль**: требования к паролю применяются только к рабочему профилю.

4.2. Длина истории паролей

Длина истории паролей. После установки этого поля пользователь не сможет ввести новый пароль, совпадающий с каким-либо паролем из истории. Значение 0 означает отсутствие ограничений.

4.3. Макс. неудачных паролей до очистки

Число неверных паролей разблокировки устройства, которые можно ввести до очистки устройства. Значение 0 означает отсутствие ограничений.

4.4. Срок действия пароля (дней)

Этот параметр заставляет пользователя периодически обновлять пароль по истечении указанного числа дней.

4.5. Требовать разблокировку паролем

Промежуток времени после разблокировки устройства или рабочего профиля с помощью надёжного способа аутентификации (пароль, PIN, графический ключ), в течение которого можно разблокировать их любым другим способом аутентификации (например, отпечаток пальца, доверенные агенты, лицо). По истечении указанного периода для разблокировки устройства или рабочего профиля можно использовать только надёжные способы аутентификации.

> **По умолчанию устройства**: период ожидания устанавливается по умолчанию устройства.
>
> **Каждый день**: период ожидания устанавливается равным 24 часам.

4.6. Качество пароля

Требуемое качество пароля.

Высокая сложность: определить высокую полосу сложности пароля как: на Android 12 и выше — PIN без повторяющихся (4444) или упорядоченных (1234, 4321, 2468) последовательностей, длина не менее 8; буквенный — длина не менее 6; буквенно-цифровой — длина не менее 6.

Средняя сложность: определить среднюю полосу сложности пароля как: PIN без повторяющихся (4444) или упорядоченных (1234, 4321, 2468) последовательностей, длина не менее 4; буквенный — длина не менее 4; буквенно-цифровой — длина не менее 4.

Низкая сложность: определить низкую полосу сложности пароля как: графический ключ; PIN с повторяющимися (4444) или упорядоченными (1234, 4321, 2468) последовательностями.

Нет: требования к паролю отсутствуют.

Слабый: устройство должно быть защищено как минимум биометрической технологией распознавания с низким уровнем безопасности. Сюда входят технологии, способные распознавать личность человека и примерно эквивалентные 3-значному PIN (вероятность ложного распознавания менее 1 из 1000).

Любой: пароль обязателен, но к его содержимому нет требований.

Цифровой: пароль должен содержать цифровые символы.

Цифровой сложный: пароль должен содержать цифровые символы без повторяющихся (4444) или упорядоченных (1234, 4321, 2468) последовательностей.

Буквенный: пароль должен содержать буквенные (или символьные) символы.

Буквенно-цифровой: пароль должен содержать как цифровые, так и буквенные (или символьные) символы.

Сложный: пароль должен соответствовать минимальным требованиям, указанным в passwordMinimumLength, passwordMinimumLetters, passwordMinimumSymbols и т. д. Например, если passwordMinimumSymbols равно 2, пароль должен содержать как минимум два символа.

4.7. Минимальная длина

Минимальная допустимая длина пароля. Значение 0 означает отсутствие ограничений.

4.8. Минимум букв

Минимальное число букв, требуемое в пароле.

4.9. Минимум строчных букв

Минимальное число строчных букв, требуемое в пароле.

4.10. Минимум прописных букв

Минимальное число прописных букв, требуемое в пароле.

4.11. Минимум небуквенных символов

Минимальное число небуквенных символов (цифр или символов), требуемое в пароле.

4.12. Минимум цифр

Минимальное число цифр, требуемое в пароле.

4.13. Минимум символов

Минимальное число символов, требуемое в пароле.

4.14. Единая блокировка

Определяет, разрешена ли единая блокировка для устройства и рабочего профиля на устройствах с Android 9 и выше с рабочим профилем. На другие устройства это не влияет.

> **Разрешить единую блокировку**: общая блокировка для устройства и рабочего профиля разрешена.
>
> **Требовать отдельную рабочую блокировку**: требуется отдельная блокировка для рабочего профиля.

5. Сброс до заводских настроек отключён

Отключён ли сброс до заводских настроек из настроек. Применимо только к полностью управляемым устройствам.

6. Защита от сброса до заводских настроек

Адреса электронной почты администраторов устройства для защиты от сброса до заводских настроек. Если устройство подвергнется несанкционированному сбросу до заводских настроек, для разблокировки устройства потребуется, чтобы один из этих администраторов вошёл с адресом и паролем аккаунта Google. Если администраторы не указаны, устройство не будет обеспечивать защиту от сброса до заводских настроек. Применимо только к

полностью управляемым устройствам.

Эл. почта администраторов: используйте **Включить защиту от сброса до заводских настроек**, чтобы начать настройку администраторов. Затем используйте **Добавить эл. почту администратора**, чтобы добавить адреса, и удаляйте их действием удаления.

7. Функции экрана блокировки

Функции экрана блокировки, которые можно отключить.

7.1. Отключить всё

Отключить все текущие и будущие настройки экрана блокировки.

7.2. Отключить камеру

Отключить камеру на защищённых экранах блокировки (например, с PIN).

7.3. Отключить уведомления

Отключить показ всех уведомлений на защищённых экранах блокировки.

7.4. Отключить неотредактированные уведомления

Отключить неотредактированные уведомления на защищённых экранах блокировки.

7.5. Игнорировать состояние доверенного агента

Игнорировать состояние доверенного агента на защищённых экранах блокировки.

7.6. Отключить отпечаток пальца

Отключить датчик отпечатка пальца на защищённых экранах блокировки.

7.7. Отключить ввод текста в уведомления

Отключить ввод текста в уведомления на защищённых экранах блокировки.

7.8. Отключить аутентификацию по лицу

Отключить аутентификацию по лицу на защищённых экранах блокировки.

7.9. Отключить аутентификацию по радужной оболочке

Отключить аутентификацию по радужной оболочке на защищённых экранах блокировки.

7.10. Отключить всю биометрическую аутентификацию

Отключить всю биометрическую аутентификацию на защищённых экранах блокировки.

7.11. Отключить все ярлыки

Отключить все ярлыки на защищённом экране блокировки на Android 14 и выше.

Мультимедиа

В этом разделе вы можете настроить поведение камеры и микрофона, доступ к данным через USB, печать и ограничения, связанные с дисплеем.

1. Доступ к камере

Управляет использованием камеры и тем, может ли пользователь получить доступ к переключателю доступа к камере (Android 12+). Как правило, отключение камеры действует на всё устройство на полностью управляемых устройствах и только внутри рабочего профиля на устройствах с рабочим профилем.

Выбор пользователя (по умолчанию): Поведение устройства по умолчанию. Камеры доступны, и (Android 12+) пользователь может переключать доступ к камере.

Отключено: Все камеры отключены (полностью управляемые: на всё устройство; рабочий профиль: только для приложений рабочего профиля). Переключатель доступа к камере не действует в управляемой области.

Принудительно: Камеры доступны. На полностью управляемых устройствах под управлением Android 12+ пользователь не может переключать доступ к камере. На других устройствах и версиях это работает как «Выбор пользователя».

2. Доступ к микрофону

На полностью управляемых устройствах управляет использованием микрофона и тем, может ли пользователь получить доступ к переключателю доступа к микрофону (Android 12+). Этот параметр не действует на устройствах, которые не являются полностью управляемыми.

Выбор пользователя (по умолчанию): Поведение по умолчанию. Микрофон доступен, и (Android 12+) пользователь может переключать доступ к микрофону.

Отключено: Микрофон отключён (на всё устройство). Переключатель доступа к микрофону не действует.

Принудительно: Микрофон доступен. На Android 12+ пользователь не может переключать доступ к микрофону. На Android 11 или ниже это работает как «Выбор пользователя».

3. Доступ к данным через USB

Управляет тем, какие файлы и/или данные можно передавать через USB. Поддерживается только на устройствах, принадлежащих компании.

Запретить передачу файлов (по умолчанию): Передача файлов запрещена, но другие USB-подключения для передачи данных (например, мышь/клавиатура) разрешены.

Запретить передачу данных: Все типы передачи данных через USB запрещены (Android 12+ с USB HAL 1.3+). Если это не поддерживается, устройство переключается на режим «Запретить передачу файлов».

Разрешить передачу данных: Все типы передачи данных через USB разрешены.

4. Печать

Управляет тем, разрешена ли печать (Android 9+).

Разрешено (по умолчанию): Печать разрешена.

Запрещено: Печать запрещена (Android 9+).

5. Настройки яркости экрана

Управляет режимом яркости экрана и (необязательно) значением яркости.

Режим яркости экрана:

Выбор пользователя (по умолчанию): Пользователю разрешено настраивать яркость экрана.

Автоматически: Яркость устанавливается автоматически, и пользователь не может её изменить. Вы всё равно можете задать значение яркости, которое используется при автоматической регулировке (полностью управляемые Android 9+; рабочие профили на устройствах компании Android 15+).

Фиксированная: Яркость устанавливается в заданное значение, и пользователь не может её изменить. Значение яркости обязательно (полностью управляемые Android 9+; рабочие профили на устройствах компании Android 15+).

Яркость экрана:

> Значение от 1 до 255 (1 — минимальное, 255 — максимальное). Значение 0 означает, что значение яркости не задано.

6. Настройки тайм-аута экрана

Управляет тем, может ли пользователь настраивать тайм-аут экрана и, при принудительном режиме, значение тайм-аута.

Поле **Режим тайм-аута экрана** выбирает между поведением, управляемым пользователем, и принудительным поведением.

> **Выбор пользователя (по умолчанию)**: Пользователю разрешено настраивать тайм-аут экрана.
>
> **Принудительно**: Тайм-аут экрана устанавливается в заданное значение, и пользователь не может его изменить (полностью управляемые Android 9+; рабочие профили на устройствах компании Android 15+).

Тайм-аут экрана:

> Длительность тайм-аута в секундах. Значение должно быть больше 0. Если оно больше **Максимальное время до блокировки**, система может ограничить его и сообщить о несоответствии.

7. Захват экрана отключён

Отключён ли захват экрана.

8. Регулировка громкости отключена

Отключена ли регулировка общей громкости.

9. Монтирование физических носителей отключено

Отключено ли монтирование физических внешних носителей.

Сотовая связь

В этом разделе можно настроить политики, связанные с сотовой связью.

1. Режим полёта

Управляет тем, может ли пользователь переключать режим полёта.

> **Выбор пользователя (по умолчанию)**: пользователь может включать или отключать режим полёта.
>
> **Отключено**: режим полёта отключён. Пользователь не может включить режим полёта. Поддерживается на Android 9 и новее.

2. Сотовая связь 2G

Управляет тем, может ли пользователь переключать настройку сотовой связи 2G.

> **Выбор пользователя (по умолчанию)**: пользователь может включать или отключать сотовую связь 2G.
>
> **Отключено**: сотовая связь 2G отключена. Пользователь не может включить сотовую связь 2G через настройки. Поддерживается на Android 14 и новее.

3. Переопределение APNs

Управляет тем, включено или отключено переопределение APNs. Если включено, используются только настроенные переопределённые APNs, а все остальные APNs на устройстве игнорируются.

> **Отключено (по умолчанию)**: Все настроенные параметры APN сохраняются на устройстве, но они отключены и не действуют. Все остальные APN на устройстве продолжают использоваться.
>
> **Включено**: Используются только переопределённые APN, все остальные APN игнорируются. Этот параметр можно настроить только на полностью управляемых устройствах с Android 10 и выше.

4. Параметры APN

Настройте одну или несколько записей APN. Используйте **Добавить APN**, чтобы создать запись, и **Удалить APN**, чтобы удалить её.

У каждой APN есть обязательные поля:

Типы APN: Выберите один или несколько типов трафика для этой APN (доступность зависит от режима управления и версии Android).

Имя APN: Идентификатор APN, предоставленный вашим оператором.

Отображаемое имя: Понятное имя, отображаемое в интерфейсе.

Необязательные поля APN:

Тип аутентификации, **Имя пользователя**, **Пароль**: Настройте аутентификацию у оператора (если требуется).

Протокол и **Протокол роуминга**: Настройка IP-протокола.

Типы сетей: Ограничьте сотовые технологии, которые может использовать APN (например, LTE/5G NR).

Адрес прокси и **Порт прокси**: HTTP-прокси для передачи данных (если применимо).

Адрес MMS-прокси, **Порт MMS-прокси**, **MMSC (URI центра MMS)**: Параметры, связанные с MMS.

Числовой идентификатор оператора (MCC+MNC) и **Идентификатор оператора**: Поля идентификации оператора.

Настройка постоянного подключения: Должен ли сеанс PDU, активированный этой APN, оставаться постоянно активным. Поддерживается на Android 15 и выше.

Тип MVNO: Тип идентификатора виртуального мобильного оператора.

MTU IPv4 и **MTU IPv6**: Максимальная единица передачи для маршрутов IPv4/IPv6. Поддерживается на Android 13 и выше.

5. Настройка сотового вещания отключена

Отключена ли настройка сотового вещания.

6. Конфигурация мобильных сетей отключена

Отключена ли настройка мобильных сетей.

7. Роуминг данных отключён

Отключены ли услуги роуминга данных.

8. Исходящие вызовы отключены

Отключены ли исходящие вызовы.

9. SMS отключены

Отключены ли отправка и получение SMS-сообщений.

10. Конфигурация слайсинга сети 5G

Настройте параметры приоритетного сетевого обслуживания, чтобы включить корпоративный слайсинг сети 5G. Вы можете настроить до 5 корпоративных слайсов и назначить приложения определённым сетям для оптимизированной маршрутизации трафика.

10.1. Приоритетная сеть по умолчанию

Идентификатор приоритетной сети по умолчанию для приложений, которых нет в списке приложений, или если у приложения не задана **Приоритетная сеть**. Для указанного идентификатора сети должна быть конфигурация (если не выбрано **Без приоритетной сети**).

Примечание. Критические приложения, такие как **com.google.android.apps.work.clouddpc** и **com.google.android.gms**, исключены из этого параметра по умолчанию.

10.2. Конфигурации сетевых служб

Используйте **Добавить конфигурацию сети**, чтобы создать конфигурацию слайса. Вы можете добавить до 5 конфигураций. Каждая конфигурация содержит:

Идентификатор приоритетной сети (назначается автоматически): Идентификатор сети назначается автоматически, и его нельзя изменить.

Возврат к подключению по умолчанию: Разрешён ли возврат к сети по умолчанию для всего устройства. Если это запрещено, приложения не смогут получить доступ в интернет, когда слайс 5G недоступен.

Несоответствующие сети: Могут ли приложения, к которым применяется эта конфигурация, использовать сети, отличные от приоритетного сервиса. Если выбрано **Запрещено**, параметр **Возврат к подключению по умолчанию** также должен быть **Запрещено**. Требуется Android 14 и выше.

Сеть

В этом разделе вы можете настроить политики, связанные с сетью.

> Конфигурации Wi-Fi могут предоставляться и управляться системой через **Конфигурации Wi-Fi**. В зависимости от значения параметра **Настройка Wi-Fi** пользователи могут иметь ограниченный контроль над добавлением и изменением сетей или не иметь его вовсе.

Состояние радиомодулей устройства

1. Состояние Wi-Fi

Управляет текущим состоянием Wi-Fi и тем, может ли пользователь изменить его состояние.

> **Выбор пользователя (по умолчанию)**: Пользователю разрешено включать и выключать Wi-Fi.
>
> **Включено**: Wi-Fi включён, и пользователь не может его отключить (Android 13+).
>
> **Отключено**: Wi-Fi отключён, и пользователь не может его включить (Android 13+).

2. Минимальный уровень безопасности Wi-Fi

Минимально требуемый уровень безопасности сетей Wi-Fi, к которым может подключаться устройство. Поддерживается на Android 13 и выше для полностью управляемых устройств и рабочих профилей на устройствах компании.

> **Открытая сеть (по умолчанию)**: Устройство может подключаться ко всем типам сетей Wi-Fi.
>
> **Личная сеть**: Запрещает открытые сети Wi-Fi; требуется как минимум личная безопасность (например, WPA2-PSK).

Корпоративная сеть: Требуются корпоративные сети EAP; сети Wi-Fi ниже этого уровня безопасности запрещены.

Корпоративная сеть 192-бит: Требуются корпоративные сети 192-бит; самый строгий вариант.

3. Состояние сверхширокополосной связи (UWB)

Управляет состоянием настройки сверхширокополосной связи и тем, может ли пользователь включать или отключать её.

Выбор пользователя (по умолчанию): Пользователю разрешено включать или отключать UWB.

Отключено: UWB отключена, и пользователь не может включать или отключать её через настройки (Android 14+).

Управление подключениями устройства

4. Общий доступ через Bluetooth

Управляет тем, разрешён ли общий доступ через Bluetooth.

Разрешено: Общий доступ через Bluetooth разрешён (по умолчанию на полностью управляемых устройствах, Android 8+).

Запрещено: Общий доступ через Bluetooth запрещён (по умолчанию в рабочих профилях, Android 8+).

5. Настройка Wi-Fi

Управляет правами настройки Wi-Fi. В зависимости от выбранного варианта пользователь имеет полный, ограниченный контроль или не имеет контроля над настройкой сетей Wi-Fi.

Разрешить настройку Wi-Fi (по умолчанию): Пользователю разрешено настраивать Wi-Fi.

Запретить добавление конфигурации Wi-Fi: Добавление новых конфигураций Wi-Fi запрещено. Пользователь может переключаться между уже настроенными сетями (Android 13+; полностью управляемые устройства и рабочие профили на устройствах компании).

Запретить настройку Wi-Fi: Запрещает настройку сетей Wi-Fi. На полностью управляемых устройствах это удаляет сети, настроенные пользователем, и оставляет только сети, настроенные через **Конфигурации Wi-Fi**. В рабочих профилях на устройствах компании существующие сети не затрагиваются, но пользователи не могут добавлять, удалять или изменять сети Wi-Fi.

> Если настройка Wi-Fi отключена и устройство не может подключиться во время загрузки, система может показать **аварийный выход для сети**, чтобы пользователь мог временно подключиться и обновить политику.

6. Настройки Wi-Fi Direct

Управляет настройкой и использованием Wi-Fi Direct. Поддерживается на устройствах компании под управлением Android 13 и выше.

Разрешить (по умолчанию): Пользователю разрешено использовать Wi-Fi Direct.

Запретить: Пользователю не разрешено использовать Wi-Fi Direct.

7. Настройки раздачи интернета

Управляет настройками раздачи интернета. В зависимости от заданного значения пользователю частично или полностью запрещается использовать различные способы раздачи интернета.

Разрешить любую раздачу интернета (по умолчанию): Разрешает настройку и использование всех способов раздачи интернета.

Запретить раздачу интернета по Wi-Fi: Запрещает пользователю использовать раздачу интернета по Wi-Fi (устройства компании, Android 13+).

Запретить любую раздачу интернета: Запрещает все способы раздачи интернета (полностью управляемые устройства и рабочие профили на устройствах компании).

8. Политика SSID Wi-Fi

Ограничения на то, к каким SSID Wi-Fi может подключаться устройство (это не влияет на то, какие сети можно настроить на устройстве). Поддерживается на устройствах компании под управлением Android 13 и выше.

> **Список запрещённых SSID (по умолчанию)**: Устройство не может подключаться к сетям Wi-Fi, SSID которых указаны в списке, но может подключаться к другим сетям.
>
> **Список разрешённых SSID**: Устройство может подключаться только к указанным SSID. Список SSID не должен быть пустым.

Используйте **Добавить SSID**, чтобы добавить записи. В зависимости от выбранного типа политики список интерпретируется как разрешённые или запрещённые SSID.

В интерфейсе редактора политик список SSID обозначен как **Разрешённые SSID Wi-Fi** для списков разрешений и **Запрещённые SSID Wi-Fi** для списков запретов.

9. Настройки роуминга Wi-Fi

Настройте режим роуминга Wi-Fi для каждого SSID. Используйте **Добавить настройку роуминга Wi-Fi**, чтобы создать записи.

Каждая запись включает:

> **SSID**: SSID, к которому применяется настройка роуминга (обязательно).
>
> **Режим роуминга Wi-Fi**: По умолчанию / Отключено / Агрессивный. Для «Отключено» и «Агрессивный» требуется Android 15+, и они поддерживаются только на полностью управляемых устройствах и в рабочих профилях на устройствах компании.

Сетевые ограничения

10. Bluetooth отключён

Отключён ли Bluetooth. Предпочитайте этот параметр параметру «Конфигурация Bluetooth отключена», поскольку пользователь может обойти отключение конфигурации Bluetooth.

11. Общий доступ к контактам через Bluetooth отключён

Отключён ли общий доступ к контактам через Bluetooth.

12. Конфигурация Bluetooth отключена

Отключена ли настройка Bluetooth.

13. Сброс сетевых настроек отключён

Отключён ли сброс сетевых настроек.

14. Исходящая передача через Beam отключена

Отключена ли передача данных из приложений через NFC Beam.

VPN

15. Приложение Always On VPN

Укажите имя пакета Always On VPN, чтобы данные из указанных управляемых приложений всегда проходили через настроенный VPN.

> Примечание. Для этой функции требуется развернуть VPN-клиент, поддерживающий как Always On, так и VPN для отдельных приложений.

16. Блокировка VPN

Запрещает работу сети, когда VPN не подключён.

17. Конфигурация VPN отключена

Отключена ли настройка VPN.

Прокси и сетевые службы

18. Приоритетная сетевая служба

Управляет тем, включена ли приоритетная сетевая служба в рабочем профиле. Например, у организации может быть соглашение с оператором о том, что рабочие данные передаются через сетевую службу оператора, предназначенную для корпоративного использования (например, корпоративный слайс в сетях 5G). Это не влияет на полностью управляемые устройства.

Отключено: Приоритетная сетевая служба отключена в рабочем профиле.

Включено: Приоритетная сетевая служба включена в рабочем профиле.

> Если вы используете корпоративный слайсинг сети, также настройте **Конфигурация слайсинга сети 5G** на панели политики **Сотовая связь** и назначьте приложения слайсу с помощью их параметра **Приоритетная сеть**.

19. Рекомендуемый глобальный прокси

Глобальный HTTP-прокси, не зависящий от сети. Обычно прокси следует настраивать для каждой сети в конфигурациях Wi-Fi. Глобальный прокси может быть полезен для необычных конфигураций, например для общей внутренней фильтрации. Глобальный прокси является лишь рекомендацией, и некоторые приложения могут его игнорировать.

Отключено

Прямой прокси

Автонастройка прокси (PAC)

19.1. Хост

Хост прямого прокси.

19.2. Порт

Порт прямого прокси.

19.3. URI PAC

URI скрипта PAC, используемого для настройки прокси.

19.4. Исключённые хосты

Для прямого прокси — хосты, для которых прокси обходится. Имена хостов могут содержать подстановочные знаки, например ***.example.com**.

Используйте **Добавить исключённый хост**, чтобы добавить записи (доступно только для прямого прокси).

Конфигурации Wi-Fi

Определите конфигурации сети Wi-Fi, которые система будет применять на устройствах. Используйте **Добавить конфигурацию Wi-Fi**, чтобы создать запись, и удалите её действием удаления.

20. Поля конфигурации Wi-Fi

Каждая конфигурация включает:

Имя конфигурации: обязательно.

SSID: обязательно.

Автоподключение: подключаться ли к сети автоматически, когда она в зоне действия.

Быстрый переход: должен ли клиент пытаться использовать быстрый переход (IEEE 802.11r-2008) при работе с сетью.

Скрытый SSID: будет ли SSID транслироваться.

Режим рандомизации MAC: аппаратный или автоматический (Android 13+).

20.1. Безопасность

Параметры безопасности Wi-Fi:

WEP-PSK: WEP (общий ключ).

WPA-PSK: WPA/WPA2/WPA3-Personal (общий ключ).

WPA-EAP: WPA/WPA2/WPA3-Enterprise (расширяемый протокол аутентификации).

Режим WPA3 192-бит: сеть WPA-EAP, разрешающая только режим WPA3 192-бит.

20.2. Парольная фраза (общий ключ)

Отображается, если для безопасности выбран **WEP-PSK** или **WPA-PSK**. Парольная фраза обязательна.

20.3. Метод EAP (Enterprise)

Отображается, если для безопасности выбран **WPA-EAP** или **Режим WPA3 192-бит**. Выберите один внешний метод EAP:

EAP-TLS

EAP-TTLS

PEAP

EAP-SIM

EAP-AKA

20.4. Аутентификация на этапе 2

Отображается для туннелирующих внешних методов (**EAP-TTLS** и **PEAP**).

MSCHAPv2

PAP

20.5. Учётные данные EAP от пользователей

Если включено, система автоматически применяет учётные данные EAP на устройствах для каждого пользователя. Учётные данные пользователей можно настроить в разделе **Пользователи**.

20.6. Клиентский сертификат

Для **EAP-TLS** можно назначить клиентский сертификат, используемый для аутентификации Wi-Fi. Дополнительные сведения см. на странице **Управление сертификатами**.

Если сертификат уже назначен, используйте **Открыть сертификат**, чтобы просмотреть его, или **Изменить сертификат**, чтобы выбрать другой.

Кроме того, можно указать **Псевдоним пары ключей клиентского сертификата**, который ссылается на клиентский сертификат, хранящийся в хранилище ключей Android и разрешённый для аутентификации Wi-Fi.

> Если заданы и **Клиентский сертификат**, и **Псевдоним пары ключей клиентского сертификата**, псевдоним пары ключей игнорируется.

20.7. Идентификатор

Идентификатор пользователя. Для туннелирующих внешних протоколов (PEAP, EAP-TTLS) он используется для аутентификации внутри туннеля, а **Анонимный идентификатор** используется как идентификатор EAP вне туннеля. Для нетуннелирующих внешних протоколов он используется как идентификатор EAP.

20.8. Анонимный идентификатор

Только для туннелирующих протоколов: указывает идентификатор пользователя, предъявляемый внешнему протоколу.

20.9. Пароль

Пароль пользователя. Если не указан, по умолчанию запрашивается у пользователя.

20.10. Сертификаты CA сервера

Список сертификатов CA, используемых для проверки цепочки сертификатов хоста. Должен совпадать хотя бы один сертификат CA. Дополнительные сведения см. на странице **Управление сертификатами**.

Используйте **Добавить сертификат CA сервера**, чтобы добавить записи, и удаляйте их действием удаления.

20.11. Совпадения суффиксов домена

Список ограничений для доменного имени сервера. Записи используются как требования совпадения суффикса с DNS-именем (именами) альтернативного имени субъекта сертификата сервера аутентификации.

Система

В этом разделе можно настроить политики, связанные с системой.

1. Минимальный уровень API

Минимально допустимый уровень API Android.

2. Политика шифрования

Включено ли шифрование.

> **По умолчанию**: это значение игнорируется, то есть шифрование не требуется.
>
> **Включено без пароля**: шифрование требуется, но пароль для загрузки не требуется.
>
> **Включено с паролем**: шифрование требуется, и для загрузки требуется пароль.

3. Автоматические дата и время

Включены ли автоматические дата, время и часовой пояс на корпоративном устройстве.

> **Выбор пользователя (по умолчанию)**: автоматические дата, время и часовой пояс оставляются на усмотрение пользователя.
>
> **Принудительно**: принудительно применять автоматические дату, время и часовой пояс на устройстве.

4. Настройки для разработчиков

Управляет доступом к настройкам для разработчиков: параметрам разработчика и безопасной загрузке.

> **Отключено (по умолчанию)**: отключает все настройки для разработчиков и запрещает пользователю доступ к ним.

Разрешено: разрешает все настройки для разработчиков. Пользователь может открывать и при необходимости настраивать их.

5. Режим Common Criteria

Управляет режимом Common Criteria — стандартами безопасности, определёнными в Common Criteria for Information Technology Security Evaluation (CC). Включение режима Common Criteria усиливает некоторые компоненты безопасности на устройстве (например: шифрование AES-GCM долговременных ключей Bluetooth, дополнительная проверка некоторых сетевых сертификатов и криптографические проверки целостности политики). Режим Common Criteria поддерживается только на устройствах, принадлежащих компании, под управлением Android 11 или выше. Внимание: режим Common Criteria применяет строгую модель безопасности, обычно требуемую только для особо чувствительных организаций. Обычное использование устройства может быть затронуто; включайте его только при необходимости.

Отключено (по умолчанию): отключает режим Common Criteria.

Включено: включает режим Common Criteria.

6. Memory Tagging Extension (MTE)

Управляет Memory Tagging Extension (MTE) на устройстве.

По выбору пользователя (по умолчанию): пользователь может включить или отключить MTE на устройстве (если устройство это поддерживает).

Принудительно: MTE включено, и пользователь не может это изменить (Android 14+; поддерживается на полностью управляемых устройствах и в рабочих профилях на устройствах, принадлежащих компании).

Отключено: MTE отключено, и пользователь не может это изменить (Android 14+; поддерживается только на полностью управляемых устройствах).

7. Защита содержимого

Управляет тем, включена ли защита содержимого (которая сканирует приложения на предмет обмана). Поддерживается на Android 15 и выше.

Отключено (по умолчанию): защита содержимого отключена, и пользователь не может это изменить.

Принудительно: защита содержимого включена, и пользователь не может это изменить (Android 15+).

По выбору пользователя: защита содержимого не контролируется политикой; пользователь может выбирать (Android 15+).

8. Содержимое ассистента

Управляет тем, разрешено ли отправлять AssistContent привилегированному приложению, такому как приложение-ассистент (например, Circle to Search). AssistContent включает снимки экрана и информацию о приложении, например имя пакета. Поддерживается на Android 15 и выше.

Разрешено (по умолчанию): содержимое ассистента разрешено отправлять привилегированному приложению (Android 15+).

Запрещено: отправка содержимого ассистента привилегированному приложению заблокирована (Android 15+).

9. Создание окон отключено

Отключено ли создание окон помимо окон приложений. Этот параметр запрещает отображение следующих системных интерфейсов: всплывающих уведомлений и снекбаров, телефонных действий (например, входящих вызовов) и приоритетных телефонных действий (например, текущих вызовов), системных предупреждений, системных ошибок и системных наложений.

10. Аварийное сетевое подключение

Включено ли аварийное сетевое подключение. Если при загрузке не удаётся установить сетевое соединение, аварийное подключение предлагает пользователю временно подключиться к сети, чтобы обновить политику устройства. После применения политики временная сеть будет забыта, и устройство продолжит загрузку. Это предотвращает ситуацию, когда подключиться к сети невозможно, если в последней политике нет подходящей сети, а устройство загружается в приложение в режиме блокировки задач, или пользователь иным образом не может открыть настройки устройства.

11. Действия по умолчанию

Список действий по умолчанию для обработки интентов, соответствующих определённому фильтру интентов. Например, эта функция позволит ИТ-администраторам выбирать, какое приложение браузера автоматически открывает веб-ссылки или какое приложение-лаунчер используется при нажатии кнопки «Домой».

Используйте **Добавить действие по умолчанию**, чтобы создать записи. Внутри записи используйте **Добавить действие** и **Добавить категорию**, чтобы построить фильтр интентов.

11.1. Действие-получатель

Действие, которое должно быть обработчиком интентов по умолчанию. Это должно быть имя компонента Android, например com.android.enterprise.app/.MainActivity. Кроме того, значением может быть имя пакета приложения, что заставит Android Device Policy выбрать подходящее действие из приложения для обработки интента.

11.2. Действие

Действия интентов для сопоставления в фильтре. Если в фильтр включены какие-либо действия, то действие интента должно быть одним из этих значений для совпадения. Если действия не включены, действие интента игнорируется.

11.3. Категория

Категории интентов для сопоставления в фильтре. Интент включает категории, которые ему требуются, и все они должны быть включены в фильтр для совпадения. Иными словами, добавление категории в фильтр не влияет на сопоставление, если эта категория не указана в интенте.

12. Разрешённые способы ввода

Указывает разрешённые способы ввода.

> **Все разрешены**: ограничения не применяются. Разрешены все способы ввода.
>
> **Только системные**: разрешены только встроенные системные способы ввода.
>
> **Только системные и указанные**: разрешены только указанные и встроенные системные способы ввода.

12.1. Разрешённые способы ввода

Имена пакетов способов ввода, которые разрешены. Применяется только если для параметра **Разрешённые способы ввода** задано значение **Только системные и указанные**.

Используйте **Добавить способ ввода**, чтобы добавить записи, и удаляйте их с помощью действия удаления.

13. Разрешённые службы доступности

Указывает разрешённые службы доступности.

Все разрешены: можно использовать любую службу доступности.

Только системные: можно использовать только встроенные системные службы доступности.

Только системные и указанные: можно использовать только указанные и встроенные системные службы доступности.

13.1. Разрешённые службы доступности

Разрешённые службы доступности. Применяется только если для параметра **Разрешённые службы доступности** задано значение **Только системные и указанные**.

Используйте **Добавить службу доступности**, чтобы добавить записи, и удаляйте их с помощью действия удаления.

14. Политика обновления системы

Конфигурация для управления обновлениями системы.

По умолчанию: следовать стандартному поведению обновления устройства, которое обычно требует, чтобы пользователь принял обновления системы.

Автоматически: устанавливать автоматически, как только появится обновление.

В окне обслуживания: устанавливать автоматически в течение ежедневного окна обслуживания. Это также настраивает обновление приложений Play в пределах окна. Настоятельно рекомендуется для киоск-устройств, поскольку это единственный способ обновления через Play приложений, постоянно закреплённых на переднем плане.

Отложить: отложить автоматическую установку максимум на 30 дней.

14.1. Окно обслуживания (только для режима «В окне обслуживания»)

Если для параметра **Политика обновления системы** задано значение **В окне обслуживания**, вы можете определить ежедневное окно обслуживания с помощью полей **с** и **по**.

14.2. Периоды заморозки обновлений системы

Ежегодно повторяющийся период, в течение которого обновления системы по воздуху (OTA) откладываются, чтобы зафиксировать версию ОС, работающую на устройстве. Чтобы не замораживать устройство бессрочно, каждый период заморозки должен быть отделён не менее чем 60 днями. Каждый период заморозки не должен превышать 90 дней.

Используйте **Добавить период заморозки обновлений системы**, чтобы создать записи.

15. Провайдеры учётных данных по умолчанию

Управляет тем, каким приложениям разрешено выступать в роли провайдеров учётных данных на Android 14 и выше.

> **Запрещено (по умолчанию)**: приложениям с неуказанным credentialProviderPolicy не разрешено выступать в роли провайдера учётных данных.
>
> **Запрещено, кроме системных**: приложениям с неуказанным credentialProviderPolicy не разрешено выступать в роли провайдера учётных данных, за исключением провайдеров учётных данных OEM по умолчанию.

Местоположение и геозоны

Эта панель объединяет настройки политики Android, которые управляют передачей данных о местоположении устройства, принудительным применением местоположения и определениями геозон. Используйте её, если хотите, чтобы Cerberus Enterprise собирал данные о местоположении устройств или определял, когда устройства входят в настроенные зоны или покидают их.

Передача данных о местоположении

Передавать местоположение

Включает передачу геоданных устройства. Данные о местоположении, собранные с помощью этого параметра, используются на **карте местоположения на панели управления**, в истории местоположений обзора устройства и при обработке геозон.

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

> На устройствах, которые не находятся под полным управлением, данные о местоположении всё равно могут зависеть от наличия у приложения Cerberus Enterprise необходимых разрешений на местоположение и от включения служб геолокации на устройстве.

> На личных устройствах Apple (регистрация пользователя) местоположение и геозоны по умолчанию отключены: они доступны, только если в политике Apple включён

параметр **Местоположение и геозоны на личных устройствах** и только если пользователь разрешает определение местоположения для приложения Cerberus Enterprise.

Режим определения местоположения

Управляет настройкой местоположения на устройствах, принадлежащих компании.

- **Выбор пользователя**: службы определения местоположения не ограничиваются политикой.
- **Принудительно**: службы определения местоположения включены на устройстве.
- **Отключено**: службы определения местоположения отключены на устройстве.

Общий доступ к местоположению отключён

Отключает общий доступ к местоположению для рабочих приложений. На устройствах с владельцем профиля это затрагивает рабочий профиль. На полностью управляемых устройствах это отключает определение местоположения для всего устройства и переопределяет режим определения местоположения устройства.

Автоматическое поведение при активных геозонах

Активные геозоны требуют работающей передачи данных о местоположении. Когда активна хотя бы одна геозона, Cerberus Enterprise автоматически поддерживает согласованность соответствующих настроек местоположения.

- **Передавать местоположение** принудительно включается, пока существуют активные геозоны.
- **Режим определения местоположения** принудительно устанавливается в **Принудительно**.
- **Общий доступ к местоположению отключён** принудительно отключается.

Если вы попытаетесь отключить **Передавать местоположение**, пока активна одна или несколько геозон, Cerberus Enterprise покажет диалог подтверждения. Если вы продолжите, все активные геозоны в политике будут деактивированы.

Список геозон

Политика может содержать до **10 геозон**. Имена геозон должны быть уникальными в пределах политики.

Используйте **Добавить геозону**, чтобы создать новую запись. Каждая геозона содержит следующие основные поля:

- **Имя**: обязательное и уникальное.
- **Широта** и **Долгота**: центр области.
- **Радиус (м)**: обязательный, от **200** до **10000** метров.
- **Описание**: необязательные заметки для администраторов.
- **Сообщать о входе** и **Сообщать о выходе**: выберите, какие события перехода должны создаваться.
- **Активна**: включает или отключает геозону без её удаления.

> Хотя бы один из параметров **Сообщать о входе** или **Сообщать о выходе** должен оставаться включённым для каждой геозоны.

> Раньше минимальный радиус составлял 100 метров. Существующие геозоны меньше 200 метров продолжают работать и сохраняются как есть при сохранении политики, даже если вы перемещаете или переименовываете их. Если вы измените их радиус, он должен быть не менее 200 метров.

Инструменты редактирования карты

Каждая карточка геозоны содержит предварительный просмотр области на карте. Вы можете редактировать геометрию с помощью карты или числовых полей.

- Нажмите на карту, чтобы переместить центр геозоны, когда редактирование области разблокировано.
- Используйте кнопку **Текущее местоположение**, чтобы центрировать карту на текущем местоположении браузера.
- Используйте кнопку **Центрировать карту**, чтобы восстановить предпочтительную область просмотра для этой геозоны.
- Используйте кнопку блокировки, чтобы предотвратить случайные изменения геометрии геозоны.

Где отображаются данные о геозонах

Переходы геозон можно просмотреть на странице Android **Обзор устройства** на вкладке **Геозона** панели местоположения. На этой вкладке переходы отображаются на отдельной карте вместе с инструментами фильтрации и списком переходов.

Управление пользователями

Добавление пользователя отключено

Отключено ли добавление новых пользователей и профилей. Для устройств, где managementMode имеет значение **DEVICE_OWNER**, это поле игнорируется, и пользователю никогда не разрешается добавлять или удалять пользователей.

Изменение аккаунтов отключено

Отключено ли добавление или удаление аккаунтов.

Настройка учётных данных пользователя отключена

Отключена ли настройка учётных данных пользователя.

Удаление пользователя отключено

Отключено ли удаление других пользователей.

Установка значка пользователя отключена

Отключено ли изменение значка пользователя.

Установка обоев отключена

Отключено ли изменение обоев.

Аутентификация при настройке рабочего аккаунта

Управляет тем, как пользователи проходят аутентификацию при настройке рабочего аккаунта. Этот параметр доступен только для организаций Android, поддерживаемых управляемым доменом Google (Google Workspace).

Во время настройки/регистрации устройства эта политика влияет на то, требуется ли вход в рабочий аккаунт, но параметр Google Admin Console **Authenticate Using 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 **Authenticate Using Google Enrollment**).

Для получения дополнительных сведений и устранения неполадок см. **Authenticate Using Google enrollment**.

Заблокированные типы аккаунтов

Типы аккаунтов, которыми пользователь не может управлять. Этот параметр не позволяет пользователям устройства добавлять неутверждённые аккаунты.

Используйте **Добавить заблокированный тип аккаунта**, чтобы добавить один или несколько типов аккаунтов.

Каждая запись содержит поле **Тип аккаунта** (обязательно). Введите строку, например **com.google**. Удалите запись с помощью действия удаления.

Личное использование

При подготовке корпоративного устройства для работы и личного использования можно задать правила, ограничивающие использование устройства пользователем в личных целях вне рабочего профиля.

> Этот раздел применяется только к корпоративным устройствам с рабочим профилем. Он не действует на полностью управляемых или личных устройствах.

1. Камера отключена

Отключена ли камера.

2. Захват экрана отключён

Отключён ли захват экрана.

3. Макс. дней с отключённой работой

Определяет, как долго рабочий профиль может оставаться отключённым.

4. Обмен по Bluetooth

Определяет, разрешён ли обмен по Bluetooth в личном профиле корпоративного устройства с рабочим профилем.

5. Личное пространство

Определяет, разрешено ли личное пространство на устройстве.

6. Режим Play Store

Этот режим определяет, какие приложения разрешены или заблокированы для пользователя в Play Store личного профиля.

> **Список заблокированных (по умолчанию)**: доступны все приложения, а любое приложение, которого не должно быть на устройстве, следует явно отметить как **Заблокировано** в разделе **Приложения**.
>
> **Список разрешённых**: в личном профиле разрешено устанавливать только приложения, явно указанные в разделе **Приложения** с параметром **Тип установки**, равным **Доступно**.

7. Приложения

Список приложений, которые должны быть разрешены или заблокированы в личном профиле. Поведение содержимого списка зависит от значения параметра **Режим Play Store** .

Чтобы добавить новое приложение из Play Store, нажмите значок **+**.

7.1. Тип установки

Типы поведения при установке, доступные для приложения личного профиля.

> **Заблокировано**: приложение заблокировано и не может быть установлено в личном профиле.
>
> **Доступно**: приложение доступно для установки в личном профиле.

8. Заблокированные типы аккаунтов

Типы аккаунтов, которыми не может управлять пользователь. Этот параметр не позволяет пользователям устройства добавлять неутверждённые аккаунты в свой личный профиль.

Межпрофильные политики

Применяется только к устройствам с личным и рабочим профилями.

Копирование и вставка между профилями

Можно ли вставлять текст, скопированный в одном профиле (личном или рабочем), в другой профиль.

> **Запрещено (по умолчанию)**: Запрещает пользователям вставлять в личный профиль текст, скопированный в рабочем профиле. Текст, скопированный в личном профиле, можно вставлять в рабочий профиль.
>
> **Разрешено**: Текст, скопированный в любом профиле, можно вставлять в другой профиль.

Обмен данными между профилями

Можно ли делиться данными из одного профиля (личного или рабочего) с приложениями в другом профиле. В частности, управляет простым обменом данными через intents. Управление другими каналами связи между профилями, такими как поиск контактов, копирование и вставка,
или связанные рабочие и личные приложения, настраивается отдельно.

> **Запрещено**: Запрещает обмен данными как из личного профиля в рабочий, так и из рабочего профиля в личный.
>
> **Из рабочего в личный запрещено (по умолчанию)**: Запрещает пользователям передавать данные из рабочего профиля приложениям в личном профиле. Личными данными можно делиться с рабочими приложениями.
>
> **Разрешено**: Данными из любого профиля можно делиться с другим профилем.

Виджеты рабочего профиля по умолчанию

Поведение виджетов рабочего профиля по умолчанию. Если для конкретного приложения не задана политика виджетов, применяется значение по умолчанию, указанное здесь.

Функции приложений между профилями

Определяет, могут ли приложения личного профиля вызывать функции приложений рабочего профиля. Требуется Android 16 или выше.

> Этот параметр зависит от параметра **Функции приложений** на уровне политики (в разделе «Управление приложениями»). Если для параметра «Функции приложений» выбрано **Запрещено**, API отклонит настройку «Функции приложений между профилями», установленную в **Разрешено**.

Рабочие контакты в личном профиле

Могут ли контакты, хранящиеся в рабочем профиле, отображаться в поиске контактов и при входящих вызовах в личном профиле.

Разрешено (по умолчанию): Позволяет отображать контакты рабочего профиля в личном профиле.

Запрещено: Запрещает личным приложениям получать доступ к контактам рабочего профиля и искать рабочие контакты.

Запрещено, кроме системных: Запрещает большинству личных приложений доступ к контактам рабочего профиля, кроме стандартных приложений OEM «Телефон», «Сообщения» и «Контакты» (Android 14+).

Если настроен параметр «Рабочие контакты в личном профиле», вы можете дополнительно определить список записей **Исключённое имя пакета**. В зависимости от выбранного режима эти исключения действуют как список разрешённых или запрещённых для личных приложений.

Отчёты о состоянии

В этом разделе можно настроить, какие данные следует получать с устройства. Данные о состоянии можно просмотреть на странице панели управления **Состояние устройства**.

Отчёты о приложениях

Включены ли отчёты о приложениях. (Сведения, передаваемые об установленном приложении.)

> Этот параметр требуется системой (для интеграции с сопутствующим приложением) и всегда включён; его нельзя отключить.

Включать удалённые приложения

Включаются ли удалённые приложения в отчёты о приложениях.

Настройки устройства

Включены ли отчёты о настройках устройства. (Сведения о связанных с безопасностью настройках устройства.)

Сведения о ПО

Включены ли отчёты со сведениями о ПО. (Сведения о программном обеспечении устройства.)

Сведения о памяти

Включены ли отчёты о памяти. (Событие, связанное с измерениями памяти и хранилища.)

Сведения о сети

Включены ли отчёты со сведениями о сети. (Сведения о сети устройства.)

Сведения о дисплее

Включены ли отчёты о дисплеях. Данные отчётов недоступны для личных устройств с рабочими профилями. (Сведения о дисплее устройства.)

События управления питанием

Включены ли отчёты о событиях управления питанием. Данные отчётов недоступны для личных устройств с рабочими профилями.

Состояние оборудования

Включены ли отчёты о состоянии оборудования. Данные отчётов недоступны для личных устройств с рабочими профилями.

Свойства системы

Включены ли отчёты о свойствах системы.

Режим Common Criteria

Включены ли отчёты о режиме Common Criteria.

Разное

1. Игра-пасхалка отключена

Отключена ли игра-пасхалка в приложении «Настройки».

2. Пропускать подсказки при первом использовании

Флаг для пропуска подсказок при первом использовании. Администратор предприятия может включить системную рекомендацию, чтобы приложения пропускали обучающую программу и другие вводные подсказки при первом запуске.

3. Короткое сообщение поддержки

Сообщение, отображаемое пользователю на экране настроек везде, где администратор отключил функциональность. Если сообщение длиннее 200 символов, оно может быть усечено.

4. Длинное сообщение поддержки

Сообщение, отображаемое пользователю на экране настроек администраторов устройства.

5. Информация владельца на экране блокировки

Информация о владельце устройства, отображаемая на экране блокировки.

6. Действия при настройке

Действия, выполняемые в процессе настройки. Во время регистрации вы можете потребовать от пользователя открыть одно или несколько приложений, необходимых для настройки устройства.

Используйте **Добавить действие настройки**, чтобы создать записи, и удаляйте их с помощью действия удаления.

6.1. Запустить приложение

Имя пакета приложения, которое нужно запустить

6.2. Заголовок

Предоставляет сообщение для пользователя, объясняющее, почему приложение необходимо запустить.

6.3. Описание

Предоставляет сообщение для пользователя, объясняющее, почему приложение необходимо запустить.

7. Видимость отображаемого имени предприятия

Управляет тем, видно ли отображаемое имя предприятия на устройстве (например, как сообщение на экране блокировки на устройствах, принадлежащих компании).

Видимо (по умолчанию): Отображаемое имя предприятия видно на устройстве (поддерживается в рабочих профилях на Android 7+ и на полностью управляемых устройствах на Android 8+).

Скрыто: Отображаемое имя предприятия скрыто на устройстве.

Правила соответствия требованиям

Если устройство или рабочий профиль не соответствует каким-либо из перечисленных ниже параметров политики, Android Device Policy по умолчанию немедленно блокирует использование устройства или рабочего профиля:

- **Требования к паролю**
- **Политика шифрования**
- **Экран блокировки отключён**
- **Разрешённые способы ввода**
- **Разрешённые службы специальных возможностей**

Если устройство или рабочий профиль остаётся несоответствующим в течение 10 дней, Android Device Policy выполнит сброс устройства до заводских настроек или удалит рабочий профиль.

В этом разделе можно переопределить правила применения соответствия по умолчанию или добавить новые.

Правила

Список правил, определяющих поведение, когда конкретная политика не может быть применена к устройству.

Используйте **Добавить правило**, чтобы создать новое правило. Каждую карточку правила можно удалить действием удаления.

Имя параметра

Политика верхнего уровня, которую нужно применять. Например, **Приложения** или **Требования к паролю**.

Обязательно. Значение должно совпадать с поддерживаемым именем политики верхнего уровня; в противном случае поле помечается как недопустимое.

Блокировка через дней

Число дней несоответствия политике до блокировки устройства или рабочего профиля. Чтобы заблокировать доступ немедленно, укажите 0. Значение **Блокировка через дней**

должно быть меньше значения **Очистка через дней**. Применимо только к корпоративным устройствам.

Допустимый диапазон: 0–300.

Область блокировки

Задаёт область действия блокировки. Применимо только к корпоративным устройствам.

По умолчанию (новое правило): **Рабочий профиль**.

> **Рабочий профиль**: блокировка применяется только к приложениям в рабочем профиле. Приложения в личном профиле не затрагиваются.
>
> **Всё устройство**: блокировка применяется ко всему устройству, включая приложения в личном профиле.

Очистка через дней

Число дней несоответствия политике до очистки устройства или рабочего профиля. **Очистка через дней** должна быть больше значения **Блокировка через дней**. Применимо только к корпоративным устройствам.

Обязательно. По умолчанию (новое правило): **1**.

Допустимый диапазон: 1–300.

Сохранять защиту от сброса настроек

Сохраняются ли данные защиты от сброса до заводских настроек на устройстве. Этот параметр не применяется к рабочим профилям.

По умолчанию (новое правило): включено.