???????? - Android

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

Политики для Android являются основными элементами системы: они определяют правила, которые применяются и обеспечиваются на управляемых устройствах.

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

Политику можно связать с токеном регистрации, поэтому она будет автоматически применяться к устройствам во время процесса настройки. Вы также можете изменить политику, назначенную устройству, после его настройки.

> К каждому устройству может быть применена только одна политика одновременно.

> Многие параметры политики применяются только к определенным типам устройств (полностью управляемые, выделенные, рабочий профиль) и версиям Android. Неподдерживаемые настройки могут быть проигнорированы устройством или считаться не соответствующими требованиям.

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

Редактор политик организован в виде набора разворачиваемых разделов. В верхней части страницы вы всегда можете редактировать:

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

Ниже приведены разделы, соответствующие панелям Редактора политик (например: управление приложениями, безопасность, сети, система, личное использование, политики для разных профилей и т.д.). Используйте страницы глав этого руководства, чтобы подробно ознакомиться с каждой панелью.

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

Используйте **Сохранить политику**, чтобы применить ваши изменения. Кнопка неактивна, если нет ожидаемых изменений или если срок действия лицензии истек.

Если вы открыли существующую политику (у нее есть идентификатор), на странице отображаются действия "**Удалить политику** и список "**Подключенные устройства** внизу, чтобы вы могли видеть, сколько устройств в настоящее время используют эту политику.

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

В этом разделе вы можете настроить политики, касающиеся доступности приложений, установки, обновлений и управления разрешениями.

> Управляемые учетные записи Google Play автоматически создаются при добавлении устройств в систему.

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

Этот режим определяет, какие приложения доступны пользователю в магазине приложений, а также поведение устройства при удалении приложений из списка разрешенных.

Список разрешенных приложений (по умолчанию): Только приложения, включенные в список разрешенных, будут доступны, а любые приложения, отсутствующие в списке, будут автоматически удалены с устройства. В магазине приложений будут отображаться только разрешенные приложения.

Черный список: Все приложения доступны, и любое приложение, которое не должно быть установлено на устройстве, должно быть явно помечено как **заблокировано** в политике приложений. Play Store будет отображать все приложения, за исключением заблокированных.

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

Политика безопасности для ненадежных приложений (приложений из неизвестных источников), применяемая к устройству. Эта опция управляет настройкой Android, определяющей, может ли пользователь устанавливать приложения, не полученные из Play Store (установка сторонних приложений).

Запретить (по умолчанию): Запретить установку ненадежных приложений на все устройство.

Только для личного профиля: Для устройств с рабочим профилем разрешите установку ненадежных приложений только в личном профиле устройства.

Разрешить: Разрешить установку ненадежных приложений на всем устройстве.

3. Google Play Protect

Включена ли принудительная проверка приложений Google Play Protect.

Включено (по умолчанию): Принудительно включает проверку приложений.

Выбор пользователя: Позволяет пользователю выбирать, включить ли проверку приложений.

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

Политика предоставления разрешений приложениям во время работы.

Запрос (по умолчанию): Запросите у пользователя разрешение на использование определенной функции.

Предоставить: Автоматически предоставить разрешение.

Запретить: Автоматически запретить доступ к разрешению.

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

Разрешает ли приложениям на устройствах с полным управлением или в рабочих профилях предоставлять доступ к своим функциям. Требуется Android 16 или выше.

Разрешено (по умолчанию): Приложениям на устройствах с полным управлением или в рабочих профилях разрешено предоставлять доступ к своим функциям.

Запрещено: Приложениям на устройствах с полным управлением или в рабочих профилях не разрешается предоставлять доступ к своим функциям.

6. ?????????? ???????????????? ??????????

Запрещена ли установка приложений пользователем.

7. ?????? ????????? ?????????? ?????????????

Отключена возможность удаления приложений пользователем.

8. ???????? ??????????

Явные разрешения, групповые разрешения или запреты для всех приложений. Эти значения переопределяют настройку "**Политики разрешений по умолчанию**.

Используйте **политику разрешений для добавления** и удаления записей с помощью действия "удалить".

Каждая запись содержит:

> **Разрешение/группа Android**: Разрешение или группа Android (обязательно), например **android.permission.READ_CALENDAR** или **android.permission_group.CALENDAR**.
>
> **Политика**: Разрешить / Запретить / Запросить (использует те же опции политики, что и **политика разрешения по умолчанию**).

9. ??????????

Список приложений, которые должны быть включены в политику. Поведение содержимого списка зависит от значения, установленного в параметре **Режим Play Store**.

Если **режим Play Store** установлен в режим **белого списка**, доступны только приложения, включенные в политику, а любое приложение, не входящее в политику, будет автоматически удалено с устройства.

Если **режим Play Store** установлен в значение "**черный список**", все приложения доступны, и любое приложение, которое не должно быть установлено на устройстве, должно быть явно помечено как **заблокировано** в политике приложений.

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

> Все приложения, доступные в Play Store в вашей стране, по умолчанию доступны для выбора. Чтобы выбрать собственные, приватные или веб-приложения, вы должны сначала загрузить их в систему. Для получения дополнительной информации ознакомьтесь со страницей **Приватные приложения**.

Каждое приложение можно настроить с помощью собственных параметров, которые удобно отображаются в виде карточки

9.1. ??? ?????????

Тип установки, который будет выполнен для приложения.

Доступно: Приложение доступно для установки.

Установлено автоматически: Приложение установлено автоматически и может быть удалено пользователем.

Принудительная установка: Приложение устанавливается автоматически и не может быть удалено пользователем.

Заблокировано: Приложение заблокировано и не может быть установлено. Если приложение было установлено ранее в рамках другой политики, оно будет удалено.

Требуется для настройки: Приложение автоматически устанавливается и не может быть удалено пользователем, и процесс настройки не будет завершен до завершения установки.

Режим киоска: Приложение автоматически устанавливается в режиме киоска, устанавливается как предпочтительное приложение для запуска и добавляется в список разрешенных для режима блокировки. Настройка устройства не будет завершена до завершения установки приложения. После установки пользователи не смогут удалить приложение. Вы можете указать этот **тип установки** только для одного приложения в рамках политики. При наличии этой настройки в политике, строка состояния будет автоматически отключена. Для получения дополнительной информации, пожалуйста, ознакомьтесь со специальной страницей **Режим киоска**.

9.2. ?????????? ???????????

Определяет набор ограничений для установки приложения. Если выбрано несколько ограничений, все они должны быть выполнены для установки приложения.

> Эта опция отображается только в том случае, если **тип установки** является **установленным по умолчанию** или **установленным принудительно**.

Сеть без ограничения трафика: Установите приложение только при подключении устройства к сети без ограничения трафика (например, Wi-Fi).

Зарядка: Установите приложение только тогда, когда устройство подключено к зарядному устройству.

Режим ожидания: Установите приложение только тогда, когда устройство находится в режиме ожидания.

9.3. ????? ????????????? ??????????

Управляет режимом автоматического обновления приложения.

По умолчанию: Приложение автоматически обновляется с низким приоритетом, чтобы минимизировать влияние на пользователя. Обновление приложения происходит, когда выполняются все следующие условия: (1) устройство не используется активно, (2) устройство подключено к сети без тарификации, (3) устройство подключено к зарядному устройству. Пользователь получает уведомление о новом обновлении в течение 24 часов после его публикации разработчиком, после чего приложение обновляется при следующем выполнении вышеуказанных условий.

Отложено: Автоматическое обновление приложения не производится в течение максимального срока в 90 дней после того, как приложение устарело. Через 90 дней после того, как приложение устарело, последняя доступная версия устанавливается автоматически с низким приоритетом (см. **Режим** Автоматического обновления). После обновления приложения, оно не будет обновляться автоматически снова до истечения 90 дней после того, как оно снова станет устаревшим. Пользователь всегда может вручную обновить приложение из Play Store в любое время.

Высокий приоритет: Приложение обновляется как можно быстрее. Не применяются никакие ограничения. Устройство немедленно уведомляется о новом обновлении после его выхода.

9.4. ??????????? ????? ??????

Минимальная версия приложения, установленного на устройстве. Если указана, устройство попытается обновить приложение до указанной версии. Если приложение не является актуальной версией, на устройстве будет отображено сообщение о **несоответствии** с указанием **причины несоответствия**: **APP_NOT_UPDATED**. Приложение должно быть уже опубликовано в Google Play с номером версии, не меньшим указанного значения. В рамках одного правила политики можно указать минимальную версию для не более чем 20 приложений.

9.5. ?????????????? ??????? ???????

Области доступа, делегированные приложению из политики Android. Вы можете предоставить другим приложениям определенный набор специальных разрешений Android:

Установка сертификатов: Предоставляет доступ к установке и управлению сертификатами.

Управляемые конфигурации: Предоставляет доступ к управлению управляемыми конфигурациями.

Запрет удаления: Предоставляет доступ к функции блокировки удаления.

Разрешения: Предоставляет доступ к настройкам разрешений и статусу предоставления разрешений.

Доступ к пакетам: Предоставляет доступ к информации о состоянии доступа к пакетам.

Системное приложение: Предоставляет доступ для включения системных приложений.

9.6. ?????????????? ????

Предпочтительный сетевой сервис для использования этим приложением. Если он указан, приложение будет использовать указанный корпоративный сетевой сегмент для своих подключений, если это возможно. Он должен соответствовать сетевому сегменту, настроенному в разделе **Настройка сетевых сегментов 5G** панели **Сотовая связь**.

9.7. Политика разрешений по умолчанию

Это политика по умолчанию для всех разрешений, запрашиваемых приложением. Если она указана, она переопределяет политику разрешений на уровне **политики по умолчанию**, которая применяется ко всем приложениям. Она не переопределяет **политики разрешений**, которые применяются ко всем приложениям.

Запрос (по умолчанию): Запросите у пользователя разрешение на использование определенной функции.

Предоставить: Автоматически предоставить разрешение.

Запретить: Автоматически запретить доступ к разрешению.

9.8. ?????????? ?????? ? ?????? ??????????

Определяет, может ли приложение взаимодействовать с самим собой между рабочим и личным профилями устройства, с согласия пользователя (Android 11 и выше).

Запрещено (по умолчанию): Предотвращает взаимодействие приложения между разными профилями.

Разрешено: Позволяет приложению взаимодействовать между разными профилями после получения согласия пользователя.

9.9. ?????????? ??? ?????? ??????????? VPN-??????????

Указывает, разрешено ли приложению сетевое взаимодействие, когда VPN-соединение не установлено и включен режим блокировки. **Эта функция поддерживается только на устройствах с Android 10 и выше.**.

Принудительно (по умолчанию): Приложение уважает настройку блокировки VPN, которая всегда включена.

Исключено: Приложение не подвергается действию настройки постоянной блокировки VPN.

9.10. ??????? ??????? ??????

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. ????????? ?????????? ?????????? ?????????????

Определяет, разрешено ли управление приложением пользователем. Управление приложением включает действия пользователя, такие как принудительная остановка и очистка данных приложения (Android 11 и выше). Если для приложения включена **extensionConfig**, управление приложением пользователем запрещено независимо от этой настройки. Для приложений в режиме киоска можно использовать **Разрешено** для включения управления приложением пользователем.

Не указано: Используется поведение приложения по умолчанию для определения, разрешено ли или запрещено управление пользователем.

Разрешено: Управление приложением пользователем разрешено.

Запрещено: Управление приложением пользователем запрещено.

9.12. ?????????

Приложение отключено. При отключении данные приложения сохраняются.

9.13. ????????? ????????????? ?????????? ??????? ??????

Разрешено ли приложению выступать в качестве провайдера учетных данных в Android 14 и выше.

9.14. ??????????? ???????????

Чтобы настроить параметры приложения через централизованное управление, нажмите кнопку **Включить централизованное управление конфигурацией**. Если для приложения уже настроена централизованная конфигурация, вы можете изменить ее с помощью кнопки **Изменить конфигурацию** или удалить ее с помощью кнопки **Удалить конфигурацию**.

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

9.15. ???????? ??????????

Явные разрешения или запреты для приложения. Эти значения переопределяют **политику разрешений по умолчанию** и **политики разрешений**, которые применяются ко всем приложениям.

Используйте **политику добавления разрешений**, чтобы добавить одно или несколько правил разрешений для карточки приложения, и удалите их с помощью действия "удалить".

9.16. ????????????? ??????????????

Список идентификаторов закрытых тестовых версий приложения, к которым устройство может получить доступ. Если выбрано несколько идентификаторов, устройство получает последнюю версию из всех доступных тестовых версий. Если ни один идентификатор не выбран, устройство имеет доступ только к производственной версии приложения.

> **Параметр "Идентификаторы версий"** доступен только для приложений, у которых для вашей организации есть хотя бы один доступный идентификатор версии. Для получения более подробной информации о том, как добавить вашу организацию в закрытую тестовую версию конкретного приложения, пожалуйста, прочитайте здесь.

10. ????????? ?????????? ?? ?????????

Установите приложения по умолчанию для поддерживаемых типов. Если для хотя бы одного типа установлено приложение по умолчанию, пользователям не разрешается изменять приложения по умолчанию в этом профиле.

> Разрешена установка только одного приложения по умолчанию для каждого **типа приложения по умолчанию**. Список приложений по умолчанию не должен содержать дубликатов.

10.1. ??? ?????????? ?? ?????????

Выберите категорию приложения для настройки (например, Браузер, Телефон, SMS, Кошелек или Помощник). Доступность зависит от версии Android и режима управления.

10.2. ??????? ?????????? ?????????? ?? ?????????

Выберите, к каким устройствам должны применяться настройки по умолчанию (полностью управляемые устройства, рабочий профиль или личный профиль). Можно выбрать только те параметры, которые поддерживаются выбранным типом устройств.

>

> Если ни один из выбранных параметров не применим к режиму управления устройством, устройство сообщит о нарушении соответствия.

10.3. ?????????? ?? ?????????

Список приложений, которые можно установить по умолчанию для выбранного типа. Первое установленное и соответствующее приложению становится приложением по умолчанию.

> Если области охвата включают **полное управление** или **рабочий профиль**, каждое приложение также должно присутствовать в списке **приложений**, где параметр **тип установки** не установлен в значение **заблокировано**.

11. ????? ????????? ?????

Позволяет отображать интерфейс на устройстве, чтобы пользователь мог выбрать псевдоним закрытого ключа, если нет соответствующих правил в **Выберите правила для закрытых ключей**.

> Для устройств с версией Android ниже P установка этой настройки может сделать корпоративные ключи уязвимыми.

12. ???????? ??????? ??? ????????? ??????

Управление доступом приложений к приватным ключам. Правило определяет, какой приватный ключ, если таковой имеется, Android Device Policy предоставляет указанному приложению. Доступ предоставляется либо когда приложение вызывает KeyChain.choosePrivateKeyAlias (или любую его перегрузку) для запроса псевдонима приватного ключа для данного URL, либо для правил, не зависящих от URL (то есть, если urlPattern не установлен или установлен в пустую строку или ".*") на Android 11 и выше, непосредственно, чтобы приложение могло вызвать KeyChain.getPrivateKey, не вызывая предварительно KeyChain.choosePrivateKeyAlias. Если приложение вызывает KeyChain.choosePrivateKeyAlias и несколько правил choosePrivateKeyRules соответствуют условиям, то последнее совпадающее правило определяет, какой псевдоним ключа будет возвращен.

Используйте **правило добавления закрытого ключа** для создания записей и удаления их с помощью действия "удалить".

12.1. ??? ?????????? ????????? ?????

Псевдоним закрытого ключа, который будет использоваться.

12.2. ?????? URL

Шаблон URL, который будет использоваться для сопоставления с URL-адресом запроса. Если не указан или пуст, будет соответствовать всем URL-адресам. Используется синтаксис регулярных выражений, определенный в java.util.regex.Pattern.

12.3. ????? ???????

Имена пакетов, к которым применяется это правило. Хеш сертификата подписи для каждого приложения проверяется на соответствие хешу, предоставленному Play. Если имена пакетов не указаны, то псевдоним предоставляется всем приложениям, вызывающим KeyChain.choosePrivateKeyAlias или любые его перегруженные версии (но только при вызове KeyChain.choosePrivateKeyAlias, даже в Android 11 и выше). Любое приложение с тем же Android UID, что и пакет, указанный здесь, получит доступ при вызове KeyChain.choosePrivateKeyAlias.

Используйте **Укажите имя пакета**, чтобы добавлять записи и удалять их с помощью действия "удалить".

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

????? ??????

В режиме киоска можно ограничить функциональность устройства одним или несколькими приложениями. Выбор между режимом киоска с одним приложением и режимом с несколькими приложениями зависит от ваших бизнес-целей.

В **режиме киоска с одним приложением** устройство настроено для работы только с одним приложением и не позволяет конечным пользователям получать доступ к другим приложениям на устройстве. Они также не могут выйти из приложения, что делает его специализированным устройством для конкретного приложения. Чтобы включить этот режим, укажите приложение в разделе **Управление приложениями** и установите значение **Тип установки** на **Киоск**.

В режиме **киоска с поддержкой нескольких приложений** устройствам разрешен доступ к нескольким приложениям. Конечные пользователи могут переключаться между разными приложениями с помощью настроенного лаунчера. Чтобы включить этот режим, активируйте опцию **настраиваемого лаунчера киоска**.

При включенном режиме киоска вы также можете настроить, какие системные функции, например, системные настройки и строка состояния, доступны конечным пользователям.

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

Определяет, включен ли собственный лаунчер для киоска. Это заменяет главный экран лаунчером, который ограничивает работу устройства только приложениями, установленными через раздел ""**Управление приложениями**". Приложения отображаются на одной странице в алфавитном порядке.

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

Определяет поведение устройства в режиме киоска при длительном нажатии кнопки питания пользователем.

> **Доступно (по умолчанию)**: Меню питания (например, Выключить, Перезагрузить) отображается, когда пользователь нажимает и удерживает кнопку питания устройства в режиме киоска.
>
> **Заблокировано**: Меню питания (например, Выключить, Перезагрузить) не отображается, когда пользователь удерживает кнопку питания устройства в режиме киоска. Обратите внимание: это может помешать пользователям выключить

устройство.

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

Указывает, заблокированы ли диалоговые окна системных ошибок для приложений, аварийно завершивших работу или не отвечающих, в режиме киоска. Если блокировка включена, система принудительно завершает работу приложения, как если бы пользователь выбрал опцию "закрыть приложение" в пользовательском интерфейсе.

Заблокировано (по умолчанию): Все системные диалоговые окна ошибок, такие как сбои и зависания приложений (ANR), заблокированы. В заблокированном состоянии система принудительно завершает работу приложения, как если бы пользователь закрыл приложение через пользовательский интерфейс.

Включено: Все системные окна ошибок, такие как сбои и зависания приложений (ANR), отображаются.

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

Определяет, какие элементы навигации (например, кнопки "Главная", "Обзор") активны в режиме киоска.

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

Только кнопка "Главная": Активирована только кнопка "Главная".

Включено: Активированы кнопки "Главная" и "Обзор".

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

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

Отключено (по умолчанию): Системная информация и уведомления отключены в режиме киоска.

Только системная информация: На строке состояния отображается только системная информация.

Включено: В режиме киоска на строке состояния отображается системная информация и уведомления. Обратите внимание: для того чтобы эта политика вступила в силу, кнопка "Домой" на устройстве должна быть включена с помощью параметра kioskCustomization.systemNavigation.

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

Указывает, разрешено ли использование приложения "Настройки" в режиме киоска.

Разрешено (по умолчанию): Доступ к приложению "Настройки" разрешен в режиме киоска.

Заблокировано: Доступ к приложению "Настройки" запрещен в режиме киоска.

??????????

В этом разделе можно настроить политики, связанные с безопасностью.

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

Выберите, какие действия выполнять, когда устройство сообщает о проблеме безопасности в отчетах о состоянии.

Поддерживаемые типы проблем безопасности:

Неизвестная операционная система: API Play Integrity обнаружил, что устройство работает под управлением неизвестной операционной системы (проверка basicIntegrity прошла успешно, но ctsProfileMatch не удалась).

Скомпрометированная операционная система: API Play Integrity обнаружил, что устройство работает под управлением скомпрометированной операционной системы (проверка basicIntegrity не пройдена).

Проверка, основанная на аппаратном обеспечении, не удалась: API Play Integrity обнаружил, что устройство не обладает надежной гарантией целостности системы, если в поле целостности устройства не отображается метка MEETS_STRONG_INTEGRITY.

Доступные действия:

Удалить корпоративные данные (по умолчанию): Отменить регистрацию и удалить рабочие данные (весь устройство, если оно полностью управляется, или только рабочий профиль, если устройство принадлежит компании).

Без действий: Не отменять регистрацию и не выполнять никаких автоматических действий.

При выборе **Удалить корпоративные данные**, вы также можете настроить параметры удаления:

Сохранить защиту от сброса к заводским настройкам: Сохраняйте данные Factory Reset Protection (FRP) при очистке устройства.

Очистить внешнюю память: При очистке устройства также очищается его внешняя память (например, карты памяти SD).

Удалить eSIM: Для устройств, принадлежащих компании, эта функция удаляет все eSIM с устройства при его очистке. Для устройств, принадлежащих частным лицам, она удаляет только управляемые eSIM (eSIM, добавленные с помощью команды ADD_ESIM), а личные eSIM не будут удалены.

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

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

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

Режимы зарядки, при которых устройство остается включенным. При использовании этой настройки рекомендуется очистить поле "**Максимальное время блокировки**", чтобы устройство не блокировалось автоматически, пока оно включено.

Источник питания: используется сетевое зарядное устройство.

Разъем USB: Источник питания – разъем USB.

Беспроводное зарядное устройство: Источник питания – беспроводной.

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

Если установлено значение "true", блокировка экрана отключается для основного и/или дополнительных дисплеев. Эта политика поддерживается только в режиме управления устройством.

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

Политики, определяющие требования к паролям.

Используйте **Настройки требований к паролю**, чтобы добавить один или несколько блоков с требованиями к паролю. Используйте **Очистить все**, чтобы удалить все

настроенные требования к паролю.

Требования к паролю могут использовать **автоматический** диапазон (одно требование) или отдельные **устройства**/**профиль рабочей среды** диапазоны. Требования, основанные на сложности, должны быть согласованы с требованиями, основанными на качестве, для одного и того же диапазона.

4.1. ??????? ???????????

Область применения требования к паролю.

> **Автоматически**: Область применения не указана. Требования к паролю применяются к рабочему профилю для устройств с рабочим профилем и ко всему устройству для устройств, управляемых централизованно или выделенных.
>
> **Устройство**: Требования к паролю применяются только к этому устройству.
>
> **Рабочий профиль**: Требования к паролю применяются только к рабочему профилю.

4.2. ???????????? ??????? ???????

Длительность истории паролей. После установки этого значения пользователь не сможет ввести новый пароль, который совпадает с каким-либо из паролей в истории. Значение 0 означает отсутствие ограничений.

4.3. ???????????? ?????????? ????????? ??????? ????? ??????, ????? ??????? ?????????? ????? ?????????????

Количество неправильных попыток разблокировки устройства, после которых устройство будет очищено. Значение 0 означает отсутствие ограничений.

4.4. ????? ???????? ????????? ????? ???????? ?????? (? ????)

Эта настройка заставляет пользователя периодически менять свой пароль, через указанное количество дней.

4.5. ????????? ????????????? ???????

Время, прошедшее после разблокировки устройства или рабочего профиля с использованием надежного метода аутентификации (пароль, PIN-код, шаблон), в течение которого устройство можно разблокировать любым другим методом (например, отпечатком пальца, доверенными агентами, распознаванием лица). После истечения указанного периода можно использовать только надежные методы аутентификации для разблокировки устройства или рабочего профиля.

> **Значение по умолчанию для устройства**: В этом случае период ожидания установлен на значение по умолчанию для устройства.

Каждый день: Период ожидания установлен на 24 часа.

4.6. ???????? ??????

Необходимое качество пароля.

Высокая сложность: Для устройств Android 12 и выше: PIN-код без повторяющихся (4444) или упорядоченных (1234, 4321, 2468) последовательностей, длиной не менее 8 символов; буквенный, длиной не менее 6 символов; буквенно-цифровой, длиной не менее 6 символов.

Средняя сложность: Определите диапазон средней сложности пароля следующим образом: PIN-код без повторяющихся (4444) или упорядоченных (1234, 4321, 2468) последовательностей, длиной не менее 4 символов; буквенный, длиной не менее 4 символов; буквенно-цифровой, длиной не менее 4 символов.

Низкая сложность: Определите диапазон низкой сложности пароля следующим образом: шаблон; PIN-код с повторяющимися (4444) или упорядоченными (1234, 4321, 2468) последовательностями.

Нет: Требования к паролю не установлены.

Слабая: Устройство должно быть защищено с использованием биометрической технологии с низким уровнем безопасности, как минимум. Это включает в себя технологии, которые могут распознавать личность человека и примерно эквивалентны 3-значному PIN-коду (вероятность ложного срабатывания менее 1 из 1000).

Любой: требуется пароль, но на его содержимое не накладываются никаких ограничений.

Числовой: пароль должен содержать цифры.

Сложные числовые: пароль должен содержать числовые символы, без повторяющихся последовательностей (например, 4444) или упорядоченных последовательностей (например, 1234, 4321, 2468).

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

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

Сложный: Пароль должен соответствовать минимальным требованиям, указанным в параметрах passwordMinimumLength, passwordMinimumLetters, passwordMinimumSymbols и т.д. Например, если passwordMinimumSymbols равен 2, пароль должен содержать не менее двух специальных символов.

4.7. ?????????? ?????

Минимальная допустимая длина пароля. Значение 0 означает отсутствие ограничений.

4.8. ??????????? ?????????? ????????

Минимальное количество символов, требуемое для пароля.

4.9. ??????????? ?????????? ???????? ????

Минимальное количество строчных букв, требуемых в пароле.

4.10. ??????????? ?????????? ????????? ????

Минимальное количество заглавных букв, требуемых в пароле.

4.11. ??????????? ?????????? ????????, ???????? ?? ????

Минимальное количество символов, отличных от букв (цифр или символов), требуемое для пароля.

4.12. ??????????? ?????????? ????

Минимальное количество цифр, требуемое в пароле.

4.13. ??????????? ?????????? ????????

Минимальное количество символов, требуемое для пароля.

4.14. ???????????????? ??????????

Разрешить ли унифицированную блокировку для устройства и рабочего профиля на устройствах с Android 9 и выше, имеющих рабочий профиль. Это не оказывает влияния на другие устройства.

> **Разрешить унифицированную блокировку**: Допускается использование единого механизма блокировки для устройства и рабочего профиля.
>
> **Требуется отдельная блокировка рабочего профиля**: Для рабочего профиля требуется отдельный механизм блокировки.

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

Возможность сброса к заводским настройкам из настроек отключена. Это применимо только к устройствам, управляемым централизованно.

6. ?????? ?? ?????? ? ????????? ??????????

Адреса электронной почты администраторов устройств для защиты от сброса к заводским настройкам. При несанкционированном сбросе устройства к заводским настройкам, для разблокировки устройства потребуется, чтобы один из этих администраторов вошел в систему, используя адрес электронной почты и пароль учетной записи Google. Если администраторы не указаны, функция защиты от сброса к заводским настройкам не будет работать. Применимо только к устройствам, управляемым централизованно.

Адреса электронной почты администраторов: используйте **Включить защиту от сброса к заводским настройкам** для начала настройки администраторов. Затем используйте **Добавить адрес электронной почты администратора** для добавления адресов и удалите их с помощью действия "удалить".

7. ???????? ??????? ?????????? ??????

Основные функции блокировки экрана, которые можно отключить.

7.1. ????????? ???

Отключить все текущие и будущие настройки блокировки экрана.

7.2. ????????? ??????

Отключить камеру на защищенных экранах блокировки (например, при использовании PIN-кода).

7.3. ????????? ???????????

Отключить отображение всех уведомлений на защищенных экранах блокировки.

7.4. ????????? ???????????? ???????????? ??? ???????

Отключить отображение уведомлений без цензуры на защищенных экранах блокировки.

7.5. ???????????? ????????? ???????????? ??????

Игнорировать состояние доверенного агента на защищенных экранах блокировки.

7.6. ????????? ????????? ??????

Отключить сканер отпечатков пальцев на защищенных экранах блокировки.

7.7. ????????? ???? ?????? ? ????????????

Запретить ввод текста в уведомлениях на защищенных экранах блокировки.

7.8. ????????? ????????????? ???

Отключить распознавание лиц на заблокированных экранах.

7.9. ????????? ????????????? ?? ???????? ???????? ?????

Отключить аутентификацию по радужной оболочке глаза на защищенных экранах блокировки.

7.10. ????????? ??? ????????????? ?????? ?????????????

Отключить все биометрические методы аутентификации на защищенных экранах блокировки.

7.11. ????????? ??? ??????

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

??????????

В этом разделе вы можете настроить параметры работы камеры/микрофона, доступа к данным через USB, печати и ограничения, связанные с дисплеем.

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

Управляет использованием камеры и возможностью включения/отключения доступа к камере пользователем (Android 12+). В общем, отключение камеры применяется ко всему устройству на полностью управляемых устройствах и только внутри рабочего профиля на устройствах с рабочим профилем.

> **Выбор пользователя (по умолчанию)**: Стандартное поведение устройства. Камеры доступны, и (в Android 12+) пользователь может включать/отключать доступ к камере.
>
> **Отключено**: Все камеры отключены (в режиме полного управления: для всей системы; в рабочем профиле: только для приложений рабочего профиля). Переключатель доступа к камере не имеет эффекта в управляемой среде.
>
> **Принудительно включено**: Камеры доступны. На устройствах с полным управлением, работающих под управлением Android 12 и выше, пользователь не может включать или отключать доступ к камере. На других устройствах/версиях поведение соответствует выбору пользователя.

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

На устройствах с полным управлением, контролирует использование микрофона и позволяет пользователю включать/отключать доступ к микрофону (Android 12+). Эта настройка не влияет на устройства, которые не находятся под полным управлением.

> **Выбор пользователя (по умолчанию)**: Стандартное поведение. Микрофон доступен, и (в Android 12 и выше) пользователь может включать/отключать доступ к микрофону.
>
> **Отключено**: Микрофон отключен (для всего устройства). Переключатель доступа к микрофону не оказывает никакого эффекта.
>
> **Включен**: Микрофон доступен. В Android 12 и выше пользователю запрещено изменять настройки доступа к микрофону. В Android 11 и ниже эта функция работает так же, как и при выборе пользователем.

3. ?????? ? ?????? ????? USB

Определяет, 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-соединения (например, мышь/клавиатура) разрешены.

Запретить передачу данных: Запрещена любая передача данных через USB (Android 12+ с USB HAL 1.3+). Если функция не поддерживается, устройство переключается в режим "Запретить передачу файлов".

Разрешить передачу данных: Разрешена любая передача данных через USB.

4. ??????

Разрешить печать или нет (Android 9 и выше).

Разрешено (по умолчанию): Печать разрешена.

Запрещено: Печать запрещена (Android 9 и выше).

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

Управляет режимом яркости экрана и (опционально) значением яркости.

Режим яркости экрана:

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

Автоматический: Яркость экрана устанавливается автоматически, и пользователь не может изменить ее. Вы все равно можете указать значение яркости, которое будет использоваться при автоматической регулировке (для полностью управляемых устройств Android 9+; для рабочих профилей на устройствах Android 15+ в корпоративной собственности).

Фиксированное значение: Яркость экрана устанавливается в заданное значение, и пользователь не может ее изменить. Значение яркости обязательно (для полностью управляемых устройств Android 9+; для рабочих профилей на корпоративных устройствах Android 15+).

Яркость экрана:

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

6. ????????? ??????? ??????????????? ?????????? ??????

Определяет, может ли пользователь изменять настройки времени автоматического отключения экрана, и, если это ограничено, устанавливает значение этого времени.

В поле **Режим автоматического отключения экрана** выбирается между режимом, в котором настройки определяются пользователем, и режимом с принудительными настройками.

> **Выбор пользователя (по умолчанию)**: Пользователю разрешено настраивать время автоматического отключения экрана.
>
> **Принудительно**: Время автоматического отключения экрана установлено в заданное значение, и пользователь не может его изменить (полностью управляемые устройства Android 9 и выше; рабочие профили на корпоративных устройствах Android 15 и выше).

Время автоматического отключения экрана:

> Продолжительность таймера в секундах. Значение должно быть больше 0. Если оно превышает **максимальное время блокировки**, система может ограничить его и сообщить о несоответствии.

7. ????????? ?????????

Отключена ли функция создания скриншотов.

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

Регулировка основного уровня громкости отключена.

9. ??????????? ?????????? ????????? ?????????

Включена ли опция отключения подключения внешних физических носителей.

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

В этом разделе вы можете настроить параметры, связанные с мобильной связью.

1. ????? "? ????????"

Разрешает ли пользователю включать/выключать режим "В самолете".

> **Выбор пользователя (по умолчанию)**: Пользователю разрешено включать или выключать режим "В самолете".
>
> **Отключено**: Режим "В самолете" отключен. Пользователю не разрешено включать или выключать режим "В самолете". Поддерживается в Android 9 и выше.

2. ??????? ????? 2G

Разрешает или запрещает пользователю включать/выключать сотовую связь 2G.

> **Выбор пользователя (по умолчанию)**: Пользователю разрешено включать или выключать сотовую связь 2G.
>
> **Отключено**: Сотовая связь 2G отключена. Пользователю не разрешено включать сотовую связь 2G через настройки. Поддерживается в Android 14 и выше.

3. ?????????????? APN

Включает или отключает использование настроенных APN. Если включено, используются только указанные APN, и все остальные APN на устройстве игнорируются.

> **Отключено (по умолчанию)**: Все настроенные параметры APN сохраняются на устройстве, но они отключены и не оказывают никакого эффекта. Все остальные APN на устройстве продолжают использоваться.
>
> **Включено**: Используются только переопределенные APN, все остальные APN игнорируются. Эту настройку можно изменить только на устройствах с полным управлением, работающих под управлением Android 10 или более поздней версии.

4. ????????? APN

Настройте одну или несколько записей APN. Используйте **Добавить APN** для создания записи и **Удалить APN** для ее удаления.

В каждом APN есть обязательные поля:

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

Имя APN: Идентификатор APN, предоставляемый вашим оператором связи.

Отображаемое имя: Удобное имя, отображаемое в пользовательском интерфейсе.

Необязательные поля APN:

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

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

Типы сетей: Ограничьте типы сотовых технологий, которые может использовать APN (например, LTE/5G NR).

Адрес прокси-сервера и **порт прокси-сервера**: HTTP-прокси для передачи данных (при необходимости).

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

Идентификатор числового оператора (MCC+MNC) и **Идентификатор оператора**: поля для идентификации оператора связи.

Режим постоянного подключения: Определяет, должен ли сеанс PDU, активируемый этим APN, быть постоянно активным. Поддерживается в Android 15 и выше.

Тип MVNO: Тип идентификатора виртуального мобильного оператора.

MTU IPv4 и **MTU IPv6**: Максимальный размер передаваемого блока для маршрутов IPv4/IPv6. Поддерживается в Android 13 и более поздних версиях.

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

Является ли конфигурация широковещательной рассылки отключенной.

6. ???????????? ????????? ????? ?????????

Включена ли опция отключения конфигурации мобильных сетей.

7. ????????? ??????? ????????

Включена ли опция отключения мобильного роуминга.

8. ???????? ????????? ??????? ?????????

Запрещены ли исходящие вызовы.

9. ???????? SMS ?????????

Включена/отключена отправка и получение SMS-сообщений.

10. ???????????? ??????? ????????? 5G

Настройте параметры приоритетной сетевой службы для включения разделения сети 5G для предприятий. Вы можете создать до 5 корпоративных сегментов и назначать приложения определенным сетям для оптимизации маршрутизации трафика.

10.1. ???? ? ????????????? ??????????? ?? ?????????

Идентификатор сети с приоритетными настройками по умолчанию для приложений, отсутствующих в списке приложений, или если для приложения не установлен **параметр «Предпочтительная сеть»**. Должна быть настроена конфигурация для указанного идентификатора сети (если не установлено значение «**Нет предпочтительной сети»**»).

Обратите внимание: критически важные приложения, такие как **com.google.android.apps.work.clouddpc** и **com.google.android.gms**, исключены из этой настройки по умолчанию.

10.2. ????????? ??????? ?????

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

Идентификатор предпочтительной сети (назначается автоматически): Идентификатор сети назначается автоматически и не может быть изменен.

Переключение на стандартное подключение: Определяет, разрешено ли автоматическое переключение на стандартную сеть устройства. Если это отключено, приложения не смогут получить доступ к интернету, если сеть 5G недоступна.

Несовместимые сети: Определяет, могут ли приложения, подпадающие под действие этой настройки, использовать сети, отличные от предпочтительной. Если установлено значение **Запрещено**, то опция **Переключение на стандартное подключение** также должна быть установлена в значение **Запрещено**. Требуется Android 14 и выше.

????

В этом разделе можно настроить политики, связанные с сетевыми подключениями.

> Настройки Wi-Fi могут быть настроены и управляться системой через **раздел настроек Wi-Fi**. В зависимости от значения, установленного в **разделе "Настройка Wi-Fi"** , у пользователей может быть ограниченный или отсутствующий контроль над добавлением/изменением сетей.

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

1. ????????? Wi-Fi

Управляет текущим состоянием Wi-Fi и позволяет пользователю изменять его.

Выбор пользователя (по умолчанию): Пользователю разрешено включать/выключать Wi-Fi.

Включено: Wi-Fi включен, и пользователю не разрешено его отключать (Android 13 и выше).

Отключено: Wi-Fi выключен, и пользователю не разрешено его включать (Android 13 и выше).

2. ??????????? ??????? ???????????? Wi-Fi

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

Открытая сеть (по умолчанию): Устройство может подключаться ко всем типам Wi-Fi сетей.

Личная сеть: Запрещает использование открытых Wi-Fi сетей; требуется как минимум персональный уровень безопасности (например, WPA2-PSK).

Корпоративная сеть: Требует использование корпоративных сетей EAP; запрещает использование Wi-Fi сетей с уровнем безопасности ниже указанного.

Корпоративная сеть с шифрованием 192 бит: Требуется использование корпоративных сетей с шифрованием 192 бит; самый строгий вариант.

3. ????????? ?????? ?????????? Ultra Wideband (UWB)

Управляет состоянием функции Ultra Wideband и позволяет пользователю включать или отключать ее.

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

Отключено: Функция UWB отключена, и пользователь не может включить ее через настройки (Android 14 и выше).

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

4. ????? ?????? ????? Bluetooth

Разрешает или запрещает общий доступ через Bluetooth.

Разрешено: Общий доступ через Bluetooth разрешен (по умолчанию для устройств с полным контролем, Android 8 и выше).

Запрещено: Обмен данными по Bluetooth запрещен (по умолчанию для рабочих профилей, Android 8 и выше).

5. ????????? Wi?Fi

Управление привилегиями настройки Wi-Fi. В зависимости от выбранного варианта, пользователь имеет полный, ограниченный или отсутствующий контроль над настройкой сетей Wi-Fi.

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

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

Запретить настройку Wi-Fi: Запрещает настройку сетей Wi-Fi. Для полностью управляемых устройств это удаляет сети, настроенные пользователем, и сохраняет только сети, настроенные через **настройки Wi-Fi**. Для рабочих профилей, принадлежащих компании, существующие сети не изменяются, но пользователям не разрешается добавлять, удалять или изменять сети Wi-Fi.

> Если настройка Wi-Fi отключена, и устройство не может подключиться при загрузке, система может отобразить **специальный режим для подключения к сети**, позволяющий пользователю временно подключиться и обновить параметры.

6. ????????? Wi-Fi Direct

Настройки управления и использования Wi-Fi Direct. Поддерживается на корпоративных устройствах с Android 13 и выше.

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

Запрещено: Пользователю запрещено использование Wi-Fi Direct.

7. ????????? ??????????? ? ????????? ????? ????????? ??????????

Управляет настройками подключения к интернету через мобильное устройство. В зависимости от установленного значения, пользователю может быть частично или полностью запрещено использование различных способов подключения.

Разрешить все способы подключения к интернету (по умолчанию): Позволяет настроить и использовать все доступные способы подключения.

Запретить использование Wi-Fi для подключения к сети: Запрещает пользователю использовать Wi-Fi для подключения к сети (только для Android 13+ на корпоративных устройствах).

Запретить все виды подключения через модем: Запрещает все типы подключения через модем (для полностью управляемых устройств и рабочих профилей, установленных на корпоративных устройствах).

8. ???????? ??? Wi-Fi ???? (SSID)

Ограничения для подключения устройства к Wi-Fi сетям (SSID) (не влияет на то, какие сети могут быть настроены на устройстве). Поддерживается на корпоративных устройствах с Android 13 и выше.

> **Список запрещенных SSID (по умолчанию)**: Устройство не может подключиться к Wi-Fi сетям, SSID которых указаны в списке, но может подключаться к другим сетям.
>
> **Список разрешенных SSID**: Устройство может подключаться только к Wi-Fi сетям, чьи имена (SSID) указаны в списке. Список SSID не должен быть пустым.

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

В интерфейсе редактора политик список SSID имеет метку **Разрешенные сети Wi-Fi (SSID)** для разрешенных списков и **Запрещенные сети Wi-Fi (SSID)** для запрещенных списков.

9. ????????? ???????? Wi?Fi

Настройте режим роуминга Wi-Fi для каждой сети SSID. Используйте **Добавить настройку роуминга Wi-Fi** для создания записей.

Каждая запись содержит:

> **SSID**: Имя сети, к которой применяется настройка роуминга (обязательно).
>
> **Режим роуминга Wi-Fi**: По умолчанию / Отключено / Агрессивный. Режимы «Отключено» и «Агрессивный» требуют Android 15 или более поздней версии и поддерживаются только на устройствах с полным управлением и в рабочих профилях на корпоративных устройствах.

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

10. Bluetooth ????????

Bluetooth отключен.

????????? ??????? ?????? ?????????? ????? Bluetooth

Функция обмена контактами через Bluetooth отключена.

12. ???????????? Bluetooth ?????????

Включена ли опция отключения Bluetooth.

13. ????? ??????? ???????? ????????

Сброс сетевых настроек отключен.

14. ????????? ???????? ?????????

Использовать NFC для передачи данных из приложений отключено.

VPN

?????????? "?????? ??????????" ??? VPN

Укажите имя пакета Always On VPN, чтобы обеспечить, чтобы данные из указанных управляемых приложений всегда передавались через настроенное VPN-соединение.

> Обратите внимание: для использования этой функции необходимо установить VPN-клиент, поддерживающий как Always On, так и VPN для отдельных приложений.

16. VPN-??????????

Запрещает сетевые подключения, когда VPN не подключен.

17. ????????? ???????????? VPN

Включена ли настройка VPN.

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

18. ????????????????? ??????? ??????

Определяет, включен ли привилегированный сетевой сервис для рабочего профиля. Например, организация может заключить соглашение с оператором связи, по которому данные, используемые для работы, передаются через выделенный сетевой сервис, предназначенный для корпоративного использования (например, выделенный сегмент сети 5G). Это не влияет на устройства с полным управлением.

Отключено: Привилегированный сетевой сервис отключен для рабочего профиля.

Включено: Привилегированный сетевой сервис включен для рабочего профиля.

> Если вы используете сетевое разделение для корпоративных сетей, также настройте **Конфигурацию сетевого разделения 5G** в разделе **Сотовая связь** и назначайте приложениям разделы, используя их **Настройку приоритетной сети**.

19. ????????????? ?????????? ??????-??????

Глобальный HTTP-прокси, не зависящий от сети. Обычно прокси-серверы должны настраиваться для каждой сети в настройках Wi-Fi. Глобальный прокси-сервер может быть полезен для нестандартных конфигураций, таких как общая фильтрация трафика. Глобальный прокси-сервер – это всего лишь рекомендация, и некоторые приложения могут ее игнорировать.

Отключено

Прямой прокси

Автоматическая настройка прокси (PAC)

19.1. ????

Хост прямого прокси.

19.2. ????

Порт прямого прокси.

19.3. URI ????? PAC

URI скрипта PAC, используемого для настройки прокси.

19.4. ??????????? ?????

Для прямого прокси-сервера указываются хосты, для которых прокси-сервер не используется. Имена хостов могут содержать подстановочные символы, такие как ***.example.com**.

Используйте **Добавить исключенный хост** для добавления записей (доступно только для прямого прокси).

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

Настройте параметры беспроводных сетей Wi-Fi, которые система будет применять на устройствах. Используйте **Добавить конфигурацию Wi-Fi** для создания записи и удалите ее с помощью действия удаления.

20. ???? ???????????? Wi-Fi

Каждая настройка включает в себя:

Название конфигурации: обязательно.

SSID: Обязательно.

Автоматическое подключение: Определяет, будет ли сеть подключаться автоматически, когда она находится в зоне досягаемости.

Быстрый переход: Определяет, следует ли клиенту использовать функцию быстрого перехода (IEEE 802.11r-2008) для подключения к сети.

Скрытый SSID: Определяет, будет ли идентификатор сети (SSID) транслироваться.

Режим случайной генерации MAC-адреса: Аппаратный или автоматический (Android 13 и выше).

20.1. ???????????

Варианты безопасности Wi-Fi:

WEP-PSK: WEP (ключ, заданный пользователем).

WPA-PSK: WPA/WPA2/WPA3-Personal (ключ, заданный пользователем).

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

Режим WPA3 с длиной ключа 192 бита: Сеть WPA-EAP, поддерживающая только режим WPA3 с длиной ключа 192 бита.

20.2. ????????? ????? (?????????????? ????? ????)

Показывается, когда используется тип безопасности **WEP-PSK** или **WPA-PSK**. Требуется ввод парольной фразы.

20.3. ????? EAP (??? ????????????? ?????)

Показывается, когда используется защита **WPA-EAP** или **режим WPA3 с 192-битной шифровкой**. Выберите один внешний метод EAP:

EAP-TLS

EAP-TTLS

PEAP

EAP-SIM

EAP-AKA

20.4. ??????????????, ???? 2

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

MSCHAPv2

PAP

20.5. ?????? ?????????????? EAP, ?????????????? ??????????????

При включенной опции система автоматически применяет данные аутентификации EAP к устройствам для каждого пользователя отдельно. Настройки учетных данных пользователей можно изменить в разделе "**Пользователи**".

20.6. ?????????? ???????

Для **EAP-TLS** можно назначить клиентский сертификат, используемый для аутентификации Wi-Fi. Для получения дополнительной информации ознакомьтесь со страницей **Управление сертификатами**.

Если сертификат уже назначен, вы можете использовать **"Открыть сертификат"** для его просмотра или **"Изменить сертификат"** для выбора другого.

В качестве альтернативы, вы можете указать **псевдоним пары ключей клиентского сертификата**, который ссылается на клиентский сертификат, хранящийся в хранилище ключей Android, и разрешает аутентификацию по Wi-Fi.

> Если установлены оба параметра: **Сертификат клиента** и **Псевдоним пары ключей сертификата клиента**, то псевдоним пары ключей игнорируется.

20.7. ?????????????

Идентификация пользователя. Для туннелирования внешних протоколов (PEAP, EAP-TTLS) это используется для аутентификации внутри туннеля, а **анонимная идентификация** используется для EAP-идентификации вне туннеля. Для внешних протоколов, не использующих туннелирование, это используется для EAP-идентификации.

20.8. ????????? ?????????????

Только для протоколов туннелирования: это указывает на идентификацию пользователя, представленную внешнему протоколу.

20.9. ??????

Пароль пользователя. Если не указан, пользователю предлагается ввести его.

20.10. ??????????? ?????? ???????????? ???????

Список сертификатов центра сертификации (CA), которые будут использоваться для проверки цепочки сертификатов устройства. Должен быть хотя бы один сертификат CA, который соответствует. Для получения дополнительной информации ознакомьтесь со страницей **Управление сертификатами**.

Используйте **функцию "Добавить сертификат CA сервера"** для добавления записей и удаления их с помощью действия "удалить".

20.11. ??????? ?????? ?????????????

Список ограничений для доменного имени сервера. Записи используются как требования для сопоставления суффиксов с DNS-именами альтернативного имени субъекта сертификата сервера аутентификации.

???????

В этом разделе вы можете настроить системные политики.

1. ??????????? ??????? API

Минимально допустимый уровень Android API.

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

Включено ли шифрование.

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

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

Включена ли автоматическая установка даты, времени и часового пояса на корпоративных устройствах.

> **Выбор пользователя (по умолчанию)**: Автоматическая установка даты, времени и часового пояса определяется выбором пользователя.
>
> **Принудительно:** Автоматически устанавливайте дату, время и часовой пояс на устройстве.

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

Управление доступом к настройкам разработчика: опции разработчика и безопасная загрузка.

> **Отключено (по умолчанию)**: Отключает все настройки для разработчиков и предотвращает доступ пользователя к ним.

Доступно: Разрешает использование всех настроек для разработчиков. Пользователь может получить доступ к этим настройкам и, при необходимости, изменить их.

5. ????? ???????????? ????????? Common Criteria

Режим "Общие критерии" — это стандарты безопасности, определенные в "Общих критериях оценки безопасности информационных технологий" (CC). Включение режима "Общие критерии" повышает уровень безопасности устройства (например, шифрование Bluetooth Long Term Keys с использованием AES-GCM, дополнительная проверка сетевых сертификатов и проверка целостности криптографических политик). Режим "Общие критерии" поддерживается только на корпоративных устройствах с Android 11 и выше. Предупреждение: режим "Общие критерии" применяет строгую модель безопасности, которая обычно требуется только для организаций, работающих с конфиденциальной информацией. Использование устройства в обычном режиме может быть ограничено; включайте его только при необходимости.

Отключено (по умолчанию): Отключает режим "Общие критерии".

Включено: Включает режим "Общие критерии".

6. ?????????? ??? ???????????? ?????? (Memory Tagging Extension)

Управляет расширением для отслеживания памяти (Memory Tagging Extension) на устройстве.

Выбор пользователя (по умолчанию): Пользователь может выбрать, включить или отключить расширение для отслеживания памяти (MTE) на устройстве (если устройство поддерживает эту функцию).

Принудительно включено: MTE включен, и пользователь не может изменить эту настройку (Android 14 и выше; поддерживается на устройствах с полным управлением и в рабочих профилях на корпоративных устройствах).

Отключено: MTE отключен, и пользователь не может изменить эту настройку (Android 14 и выше; поддерживается только на устройствах с полным управлением).

7. ?????? ????????

Включает ли защиту от нежелательного контента (проверяет наличие подозрительных приложений). Поддерживается на Android 15 и выше.

Отключено (по умолчанию): Защита от нежелательного контента отключена, и пользователь не может изменить это.

Принудительно включено: Защита от нежелательного контента включена, и пользователь не может изменить это (Android 15 и выше).

Выбор пользователя: Защита от нежелательного контента не управляется политикой; пользователь может самостоятельно выбирать (Android 15 и выше).

8. ?????? ? ?????????

Разрешает ли отправку контента (включая скриншоты и информацию об приложении, такую как имя пакета) в привилегированные приложения, например, в приложение-помощник (например, Circle to Search). Поддерживается в Android 15 и более поздних версиях.

Разрешено (по умолчанию): Отправка контента (включая скриншоты и информацию о приложении, например, имя пакета) разрешена для привилегированных приложений (Android 15 и выше).

Запрещено: Отправка вспомогательного контента заблокирована для привилегированных приложений (Android 15 и выше).

9. ??????? ???? ? ??????????? ???????????????

Включено ли создание дополнительных окон помимо окон приложения. Эта опция предотвращает отображение следующих системных элементов: всплывающих уведомлений и панелей, действий телефона (например, входящих вызовов) и приоритетных действий телефона (например, текущих вызовов), системных оповещений, системных ошибок и системных наложений.

10. ??????? "?????????? ??????" ?? ????

Включен ли "аварийный выход" из сети. Если во время загрузки устройства не удается подключиться к сети, функция "аварийного выхода" предложит пользователю временно подключиться к сети для обновления политики устройства. После применения политики временное сетевое подключение будет отключено, и устройство продолжит загрузку. Это предотвращает ситуацию, когда устройство не может подключиться к сети, если в последней примененной политике нет подходящей сети, и устройство загружается в режим блокировки приложения или пользователь не может получить доступ к настройкам устройства.

11. ???????? ????????

Список действий по умолчанию для обработки намерений, соответствующих определенному фильтру намерений. Например, эта функция позволяет администраторам ИТ выбирать, какое приложение-браузер автоматически открывает веб-ссылки, или какое приложение-лаунчер используется при нажатии кнопки "Домой".

Используйте **"Добавить действие по умолчанию"** для создания записей. Внутри записи используйте **"Добавить действие"** и **"Добавить категорию"** для создания фильтра намерений.

11.1. ?????????? ??????????

Компонент, который должен быть обработчиком действий по умолчанию. Это должно быть имя компонента Android, например, com.android.enterprise.app/.MainActivity. В качестве альтернативы, значением может быть имя пакета приложения, что позволит Android Device Policy выбрать подходящий компонент из этого приложения для обработки действия.

11.2. ????????

Действия, которые необходимо сопоставить в фильтре. Если в фильтре указаны какие-либо действия, то действие в намерении должно быть одним из этих значений, чтобы соответствовать фильтру. Если действия не указаны, действие в намерении игнорируется.

11.3. ?????????

Категории намерений, используемые для фильтрации. Намерение включает в себя категории, которые оно требует, и все они должны быть включены в фильтр для соответствия. Другими словами, добавление категории в фильтр не влияет на соответствие, если эта категория не указана в намерении.

12. ??????????? ?????? ?????

Указывает разрешенные способы ввода данных.

> **Все разрешено:** Ограничений не установлено. Разрешены все способы ввода данных.
>
> **Только системные**: Разрешены только встроенные системные методы ввода.
>
> **Только системные и предоставленные**: Разрешены только встроенные системные методы ввода и предоставленные методы ввода.

12.1. ??????????? ?????? ?????

Имена пакетов методов ввода, которые разрешены. Это применимо только в том случае, если **Разрешенные методы ввода** установлено в значение **Только системные и предоставленные**.

Используйте **метод ввода "Добавить"** для добавления записей и удалите их с помощью действия "Удалить".

13. ??????????? ?????? ??????????? ????????????

Указывает разрешенные службы специальных возможностей.

> **Доступно всем:** Любая служба специальных возможностей может быть использована.
>
> **Только системные**: Можно использовать только встроенные службы специальных возможностей системы.
>
> **Только системные и предоставленные**: Можно использовать только предоставленные и встроенные системные службы специальных возможностей.

13.1. ??????????? ?????? ??????????? ????????????

Разрешенные службы специальных возможностей. Это правило применяется только в том случае, если **Разрешенные службы специальных возможностей** установлено в значение **Только системные и предоставленные**.

Используйте **службу специальных возможностей "Добавить"** для добавления записей и удаляйте их с помощью действия "Удалить".

14. ???????? ?????????? ???????

Настройки для управления обновлениями системы.

> **По умолчанию:** Устройство следует стандартной процедуре обновления, которая обычно требует от пользователя принятия обновлений системы.
>
> **Автоматически:** Устанавливать автоматически, как только станет доступно обновление.
>
> **В окне обслуживания:** Автоматическая установка в течение ежедневного периода обслуживания. Это также настраивает автоматическое обновление приложений Play в течение этого периода. Это настоятельно рекомендуется для устройств, используемых в режиме киоска, поскольку это единственный способ обновления приложений, закрепленных в фоновом режиме, с помощью Play.

Отложить: Отложить автоматическую установку на срок до 30 дней.

14.1. ????? ???????????? (?????? ??? ????)

Когда **политика обновления системы** установлена в значение **"с графическим интерфейсом"**, вы можете указать ежедневное время обслуживания, используя поля **"с"** и **"до"**.

14.2. ??????? ????????? ????????? ??????????

Период, который повторяется каждый год, в течение которого обновления системы, распространяемые по беспроводной сети (OTA), приостанавливаются для фиксации версии операционной системы на устройстве. Чтобы избежать бесконечной блокировки устройства, между каждым периодом блокировки должно быть не менее 60 дней. Продолжительность каждого периода блокировки не должна превышать 90 дней.

Используйте **функцию "Заморозить период системных обновлений"** для создания записей.

15. ?????????? ??????? ?????? ?? ?????????

Определяет, каким приложениям разрешено выступать в качестве поставщиков учетных данных в Android 14 и более поздних версиях.

Запрещено (по умолчанию): Приложениям, для которых политика credentialProviderPolicy не указана, не разрешено выступать в качестве поставщика учетных данных.

Запрещено (за исключением системных): Приложениям, для которых политика credentialProviderPolicy не указана, запрещено выступать в качестве поставщика учетных данных, за исключением системных поставщиков учетных данных.

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

Этот раздел объединяет настройки политик Android, которые управляют отчетом о местоположении устройства, принудительным использованием местоположения и определениями геозон. Используйте его, когда вам нужно, чтобы Cerberus Enterprise собирал местоположения устройств или определял, когда устройства входят или покидают настроенные области.

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

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

Включает отчетность о геолокации устройства. Данные о местоположении, собираемые с помощью этой настройки, используются в **карте местоположения панели управления**, истории местоположений в обзоре устройства и обработке геозон.

> На устройствах, которые не управляются полностью, данные о местоположении по-прежнему могут зависеть от наличия необходимых разрешений на определение местоположения у приложения Cerberus Enterprise и от включенных служб определения местоположения на устройстве.

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

Управляет настройкой местоположения на корпоративных устройствах.

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

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

Отключает общий доступ к местоположению для рабочих приложений. На устройствах с владельцем профиля это влияет на рабочий профиль. На полностью управляемых

устройствах это отключает определение местоположения для всего устройства и переопределяет режим определения местоположения устройства.

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

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

- **Передача местоположения** принудительно включается при наличии активных геозон.
- **Режим определения местоположения** переходит в **Режим принудительного включения**.
- **Отключение обмена местоположением** включено принудительно.

Если вы попытаетесь отключить **Отчет о местоположении** при активных геограницах, Cerberus Enterprise отобразит диалоговое окно подтверждения. Если вы продолжите, все активные геограницы в политике будут деактивированы.

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

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

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

- **Имя**: обязательно и уникально.
- **Широта** и **долгота**: центр области.
- **Радиус (м)**: обязателен, от **100** до **10000** метров.
- **Описание**: необязательные заметки для администраторов.
- **Определить вход** и **Определить выход**: выберите, какие события переходов следует генерировать.
- **Активен**: включает или отключает геозону без удаления.

> По крайней мере, одно из **Сообщить о входе** или **Сообщить о выходе** должно оставаться включенным для каждой геозоны.

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

Каждая карточка геозоны включает в себя предварительный просмотр карты территории. Вы можете редактировать геометрию с карты или из числовых полей.

- Нажмите на карту, чтобы переместить центр геозоны при разблокировке редактирования области.
- Используйте кнопку **Текущее местоположение**, чтобы расположить карту на вашем текущем местоположении в браузере.
- Используйте кнопку **Расположить карту**, чтобы восстановить предпочитаемый масштаб для этой геозоны.
- Используйте кнопку блокировки, чтобы предотвратить случайное изменение геометрии геозоны.

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

Переходы геозон можно просмотреть на странице Android **Обзор устройства**, во вкладке **Геозоны** панели местоположения. Данная вкладка отображает переходы на специальной карте, а также инструменты фильтрации и список переходов.

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

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

Возможность добавления новых пользователей и профилей отключена. Для устройств, где managementMode имеет значение **DEVICE_OWNER**, это поле игнорируется, и пользователю никогда не будет разрешено добавлять или удалять пользователей.

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

Возможность добавления или удаления учетных записей отключена.

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

Отключена ли настройка учетных данных пользователя.

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

Запрещено ли удаление других пользователей.

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

Возможность изменения значка пользователя отключена.

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

Изменение обоев отключено.

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

Определяет способ аутентификации пользователей при настройке рабочей учетной записи. Эта опция доступна только для Android-устройств в корпоративных средах, использующих управляемую область Google (Google Workspace).

Во время настройки/регистрации устройства данная политика определяет, требуется ли вход в рабочую учетную запись, но настройки консоли администратора Google, такие как **"Аутентификация с использованием Google"**, и тип токена регистрации все равно могут потребовать аутентификацию.

Для устройств, которые уже зарегистрированы, данная политика применяется только в том случае, если устройство управляется учетной записью Google Play для управляемых устройств (то есть, зарегистрировано без **аутентификации с использованием Google**).

Для получения более подробной информации и решения проблем обратитесь к **Аутентификация с использованием Google (регистрация)**.

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

Типы учетных записей, которые пользователь не может управлять. Эта опция предотвращает добавление несанкционированных учетных записей пользователями устройств.

Используйте **Добавить запрещенный тип учетной записи**, чтобы добавить один или несколько типов учетных записей.

Каждый элемент содержит поле **Тип учетной записи** (обязательно). Введите строку, например, **com.google**. Удалите элемент, используя действие "удалить".

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

При настройке устройства, принадлежащего компании и используемого для работы и личных целей, вы можете указать определенные правила, чтобы ограничить способы использования устройства пользователем в личных целях, вне рабочего профиля.

> Этот раздел применим только к устройствам, принадлежащим компании и имеющим рабочий профиль. Он не оказывает влияния на устройства, находящиеся под полным управлением или принадлежащие частным лицам.

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

Активна ли функция отключения камеры.

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

Отключена ли функция создания скриншотов.

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

Определяет, как долго можно оставить рабочий профиль отключенным.

4. ????? ??????? ?? Bluetooth

Определяет, разрешен ли обмен данными по Bluetooth в личном профиле устройства, принадлежащего компании, с установленным рабочим профилем.

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

Разрешает ли использование личного пространства на устройстве.

6. ????? ???????? ??????????

Этот режим определяет, какие приложения разрешены или заблокированы для пользователя в магазине приложений (Play Store) в его личном профиле.

> **Черный список (по умолчанию)**: Все приложения доступны, и любое приложение, которое не должно быть на устройстве, должно быть явно помечено как **заблокировано** в разделе **Приложения**.
>
> **Список разрешенных приложений**: Разрешено устанавливать только приложения, явно указанные в разделе **Приложения**, где для параметра **Тип установки** установлено значение **Доступно**.

7. ??????????

Список приложений, которые должны быть разрешены или заблокированы для личного профиля. Поведение содержимого списка зависит от значения, установленного в **режиме Play Store**.

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

7.1. ??? ?????????

Типы поведения при установке, которые может иметь приложение персонального профиля.

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

8. ?????????????? ???? ??????? ???????

Типы учетных записей, которыми пользователь не может управлять. Эта опция предотвращает добавление пользователями устройства несанкционированных учетных записей в их личный профиль.

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

Применяется только к устройствам с личным и рабочим профилями.

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

Можно ли копировать текст из одного профиля (личного или рабочего) и вставлять в другой профиль?

> **Запрещено (по умолчанию)**: Предотвращает вставку пользователями текста из рабочего профиля в личный профиль. Текст, скопированный из личного профиля, можно вставлять в рабочий профиль.
>
> **Разрешено**: Текст, скопированный в любом из профилей, можно вставлять в другой профиль.

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

Определяет, может ли информация из одного профиля (личного или рабочего) использоваться приложениями в другом профиле. Управляет простым обменом данными через интенты. Настройки для других каналов взаимодействия между профилями, таких как поиск контактов, копирование/вставка,
или подключенных рабочих и личных приложений, настраиваются отдельно.

> **Запрещено**: Предотвращает обмен данными как от личного профиля к рабочему, так и от рабочего профиля к личному.
>
> **Запрещено** (по умолчанию): Предотвращает передачу данных из рабочего профиля в приложения, установленные в личном профиле. Личные данные могут быть доступны приложениям, установленным в рабочем профиле.
>
> **Разрешено**: Данные из любого профиля могут быть переданы в другой профиль.

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

Поведение виджетов рабочего профиля по умолчанию. Если конкретное приложение не определяет политику для виджетов, используется политика, установленная здесь.

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

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

> Эта настройка зависит от опции на уровне политики "**Функции приложений**" (в разделе управления приложениями). Если "Функции приложений" установлены в значение "**Запрещено**", API отклонит запросы на использование функций приложений между профилями, если они установлены в значение "**Разрешено**".

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

Можно ли отображать контакты, хранящиеся в рабочем профиле, при поиске контактов в личном профиле и при входящих звонках.

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

Запрещено: Предотвращает доступ личных приложений к контактам рабочего профиля и поиск рабочих контактов.

Запрещено, за исключением системных приложений: Предотвращает доступ большинства личных приложений к контактам рабочего профиля, за исключением стандартных приложений Dialer, Messages и Contacts от производителя устройства (только для Android 14 и выше).

Если контакты рабочей среды настроены в личном профиле, вы можете опционально указать список **исключений по имени пакета**. В зависимости от выбранного режима, эти исключения могут действовать как разрешенный или запрещенный список для личных приложений.

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

В этом разделе можно настроить, какие данные должны извлекаться с устройства. Данные о статусе можно просмотреть на странице панели управления **статуса устройства**.

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

Включены ли отчеты об установленных приложениях. (Предоставляется информация об установленных приложениях)

> Этот параметр обязателен для работы системы (для интеграции с приложениями-компаньонами) и всегда включен; его нельзя отключить.

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

Включает ли удаленные приложения в отчеты об установленных приложениях.

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

Включена ли отправка отчетов о настройках устройства. (Информация о настройках безопасности устройства отправляется на сервер.)

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

Включено ли отображение информации об установленном программном обеспечении. (Информация об установленном программном обеспечении на устройстве.)

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

Включено ли отображение информации об объеме памяти. (Событие, связанное с измерениями памяти и хранилища)

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

Включено ли отображение информации о сети. (Информация о сети устройства.)

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

Включено ли отображение отчетов. Данные отчетов недоступны для устройств, принадлежащих пользователю, с рабочим профилем. (Информация об устройстве, отображаемая на экране)

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

Включено ли отображение событий управления питанием. Данные не доступны для личных устройств с рабочими профилями.

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

Включена ли отправка данных о состоянии оборудования. Данные о состоянии недоступны для устройств, принадлежащих лично, но используемых с рабочим профилем.

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

Включена ли отправка отчетов о системных свойствах.

????? ???????????? ????????? Common Criteria

Включена ли отчетность в режиме соответствия стандарту Common Criteria.

??????

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

Включена/отключена игра с секретом в настройках.

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

Флаг, определяющий, нужно ли пропускать подсказки при первом запуске. Администратор корпоративной сети может включить функцию, которая позволит приложениям пропускать обучающие подсказки и другую вводную информацию при первом запуске.

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

Сообщение, отображаемое пользователю на экране настроек, когда администратор отключил определенную функцию. Если сообщение содержит более 200 символов, оно может быть усечено.

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

Сообщение, которое отображается пользователю на экране настроек администратора устройства.

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

Информация о владельце устройства, которая будет отображаться на экране блокировки.

6. ???????? ?? ?????????

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

Используйте **действие добавления** для создания записей и удалите их с помощью действия удаления.

6.1. ????????? ??????????

Имя пакета приложения для запуска

6.2. ?????????

Предоставляет пользователю информационное сообщение, объясняющее, почему необходимо запустить приложение.

6.3. ????????

Предоставляет пользователю информационное сообщение, объясняющее, почему необходимо запустить приложение.

7. ??????????? ???????? ??????????? ? ????????????? ?????

Определяет, отображается ли название организации на устройстве (например, в виде сообщения на экране блокировки на корпоративных устройствах).

Отображать (по умолчанию): Название организации отображается на устройстве (поддерживается для рабочих профилей в Android 7+ и для полностью управляемых устройств в Android 8+).

Скрытое: Отображение названия организации на устройстве отключено.

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

Если устройство или рабочий профиль не соответствуют каким-либо из политик, указанных ниже, Android Device Policy автоматически блокирует использование устройства или рабочего профиля:

- **Требования к паролю**
- **Политика шифрования**
- **Блокировка экрана отключена**
- **Разрешенные методы ввода**
- **Разрешенные службы специальных возможностей**

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

В этом разделе вы можете изменить правила принудительного соответствия требованиям по умолчанию или добавить новые.

???????

Список правил, определяющих поведение в случае невозможности применения определенной политики к устройству.

Используйте **Добавить правило**, чтобы создать новое правило. Каждую карточку правила можно удалить с помощью действия удаления.

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

Основная политика, которую необходимо применить. Например, **Приложения** или **Требования к паролю**.

Обязательно. Значение должно соответствовать допустимому имени политики верхнего уровня; в противном случае поле будет помечено как недействительное.

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

Количество дней, в течение которых устройство или рабочий профиль не соответствуют требованиям политики, прежде чем они будут заблокированы. Чтобы немедленно заблокировать доступ, установите значение 0. **Блокировка после указанного количества дней** должно быть меньше, чем **Сброс после указанного количества дней**. Применимо только к устройствам, принадлежащим компании.

Допустимый диапазон: 0–300.

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

Определяет область действия операции для устройства. Применимо только к устройствам, принадлежащим компании.

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

> **Рабочий профиль**: Действие блокировки применяется только к приложениям, установленным в рабочем профиле. Приложения, установленные в личном профиле, не затронуты.
>
> **Все устройство**: Действие блокировки применяется ко всему устройству, включая приложения, установленные в личном профиле.

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

Количество дней, в течение которых устройство или рабочий профиль не соответствуют политике, прежде чем данные будут удалены.
Стереть данные через указанное количество дней должно быть больше, чем **Блокировать через указанное количество дней**. Применимо только к устройствам, принадлежащим компании.

Обязательно. Значение по умолчанию (для новых правил): **1**.

Допустимый диапазон: от 1 до 300.

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

Сохраняется ли заводская защита на устройстве? Эта настройка не применяется к рабочим профилям.

По умолчанию (для нового правила): включено.