Безопасность

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

Действия при угрозах безопасности

Выберите, что делать, когда устройство сообщает о риске безопасности (SecurityRisk) в отчетах о состоянии.

Поддерживаемые типы угроз безопасности (SecurityRisk):

Неизвестная ОС: Play Integrity API обнаруживает, что на устройстве запущена неизвестная ОС (проверка basicIntegrity пройдена, но ctsProfileMatch не удалась).

Взломанная ОС: Play Integrity API обнаруживает, что на устройстве запущена взломанная ОС (проверка basicIntegrity не удалась).

Ошибка проверки на базе аппаратного обеспечения: Play Integrity API обнаруживает, что устройство не имеет надежных гарантий целостности системы (если в поле целостности устройства отсутствует метка MEETS_STRONG_INTEGRITY).

Доступные действия:

Удаление корпоративных данных (по умолчанию): Отмена регистрации и удаление рабочих данных (всего устройства, если оно полностью управляемое, или только рабочего профиля, если управление осуществляется на уровне профиля).

Без действий: Оставить устройство зарегистрированным и ничего не предпринимать автоматически.

При выборе параметра **Удаление корпоративных данных** вы также можете настроить параметры удаления:

Сохранение защиты от сброса до заводских настроек: Сохранение данных защиты от сброса до заводских настроек (FRP) при удалении данных с устройства.

Удаление внешнего хранилища: Дополнительное удаление данных с внешнего хранилища устройства (например, SD-карт) при выполнении сброса.

Удаление eSIM: Для устройств, принадлежащих компании, это удаляет все eSIM с устройства при его сбросе. На устройствах, принадлежащих частным лицам, это удалит только управляемые eSIM (те, что были добавлены через команду ADD_ESIM), а личные eSIM удалены не будут.

1. Максимальное время до блокировки

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

2. Не выключать экран при зарядке

Режимы работы от сети, в которых устройство остается включенным. При использовании этой настройки рекомендуется очистить параметр **Максимальное время до блокировки**, чтобы устройство не блокировалось само по себе при включенном экране.

Зарядное устройство переменного тока: Источник питания — зарядное устройство переменного тока.

USB-порт: Источник питания — USB-порт.

Беспроводная зарядка: Источник питания — беспроводная зарядка.

3. Блокировка экрана отключена

Если значение установлено в true, это отключает экран блокировки для основного и/или дополнительного дисплеев. Эта политика поддерживается только в режиме управления выделенными устройствами (dedicated device).

4. Требования к паролю

Политики требований к паролю.

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

Требования к паролю могут использовать область действия **Авто** (одно требование) или отдельные области действия **Устройство**/**Рабочий профиль**. Требования, основанные на сложности, должны сочетаться с требованиями, основанными на качестве, для одной и той же области действия.

4.1. Область действия

Область действия, к которой применяется требование к паролю.

> **Авто**: Область действия не указана. Требования к паролю применяются к рабочему профилю для устройств с рабочим профилем и ко всему устройству для полностью управляемых или выделенных устройств.
>
> **Устройство**: Требования к паролю применяются только к устройству.
>
> **Рабочий профиль**: Требования к паролю применяются только к рабочему профилю.

4.2. История паролей

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

4.3. Максимальное количество неудачных попыток ввода пароля для сброса данных

Количество неправильных паролей для разблокировки устройства, которые могут быть введены до того, как произойдет сброс данных. Значение 0 означает отсутствие ограничений.

4.4. Срок действия пароля (в днях)

Эта настройка обязывает пользователя периодически обновлять пароль по истечении указанного количества дней.

4.5. Требовать разблокировку паролем

Промежуток времени после разблокировки устройства или рабочего профиля с помощью надежного метода аутентификации (пароль, PIN-код, графический ключ), в течение которого разрешена разблокировка любыми другими методами (например, отпечатком пальца, доверенными агентами или распознаванием лица). По истечении указанного периода времени для разблокировки устройства или рабочего профиля будут разрешены только надежные методы аутентификации.

> **По умолчанию для устройства**: Период ожидания устанавливается по умолчанию для устройства.

Каждый день: Период ожидания устанавливается на 24 часа.

4.6. Качество пароля

Требуемое качество пароля.

Высокая сложность: Определяет высокий уровень сложности пароля как: в Android 12 и выше — PIN-код без повторяющихся (4444) или последовательных (1234, 4321, 2468) цифр, длина не менее 8 символов; буквенный пароль, длина не менее 6 символов; буквенно-цифровой пароль, длина не менее 6 символов.

Средняя сложность: Определяет средний уровень сложности пароля как: PIN-код без повторяющихся (4444) или последовательных (1234, 4321, 2468) цифр, длина не менее 4 символов; буквенный пароль, длина не менее 4 символов; буквенно-цифровой пароль, длина не менее 4 символов.

Низкая сложность: Определяет низкий уровень сложности пароля как: графический ключ; PIN-код с повторяющимися (4444) или последовательными (1234, 4321, 2468) цифрами.

Нет: Требования к паролю отсутствуют.

Слабая: Устройство должно быть защищено как минимум технологией биометрического распознавания с низким уровнем безопасности. Сюда входят технологии, способные идентифицировать личность человека с точностью, примерно эквивалентной 3-значному PIN-коду (вероятность ложного срабатывания менее 1 на 1000).

Любой: Пароль обязателен, но ограничений на его содержимое нет.

Цифровой: Пароль должен содержать цифры.

Сложный цифровой: Пароль должен содержать цифры без повторяющихся (4444) или последовательных (1234, 4321, 2468) комбинаций.

Буквенный: Пароль должен содержать буквы (или символы).

Буквенно-цифровой: Пароль должен содержать как цифры, так и буквы (или символы).

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

4.7. Минимальная длина

Минимально допустимая длина пароля. Значение 0 означает отсутствие ограничений.

4.8. Минимум букв

Минимально необходимое количество букв в пароле.

4.9. Минимум строчных букв

Минимально необходимое количество строчных букв в пароле.

4.10. Минимум прописных букв

Минимально необходимое количество прописных букв в пароле.

4.11. Минимум символов, не являющихся буквами

Минимально необходимое количество символов, не являющихся буквами (цифр или специальных знаков), в пароле.

4.12. Минимум цифр

Минимально необходимое количество цифр в пароле.

4.13. Минимум символов

Минимально необходимое количество символов в пароле.

4.14. Единая блокировка

Определяет, разрешена ли единая блокировка для устройства и рабочего профиля на устройствах с Android 9 и выше, имеющих рабочий профиль. На других устройствах это не влияет.

> **Разрешить единую блокировку**: разрешается использование общей блокировки для устройства и рабочего профиля.
>
> **Требовать отдельную блокировку для рабочего профиля**: требуется отдельная блокировка для рабочего профиля.

5. Сброс к заводским настройкам отключен

Отключен ли сброс к заводским настройкам через настройки. Применяется только к полностью управляемым устройствам.

6. Защита от сброса к заводским настройкам

Адреса электронной почты администраторов устройства для защиты от сброса к заводским настройкам. Если на устройстве произойдет несанкционированный сброс к заводским настройкам, для разблокировки потребуется, чтобы один из этих администраторов вошел в систему, используя адрес электронной почты и пароль от своего аккаунта Google. Если администраторы не указаны, защита от сброса к заводским настройкам на устройстве будет отключена. Применяется только к полностью управляемым устройствам.

Адреса электронной почты администраторов: используйте **Включить защиту от сброса к заводским настройкам**, чтобы начать настройку администраторов. Затем используйте **Добавить адрес электронной почты администратора**, чтобы добавить адреса, и действие удаления, чтобы их убрать.

7. Функции блокировки экрана

Функции блокировки экрана, которые можно отключить.

7.1. Отключить все

Отключить все текущие и будущие настройки блокировки экрана.

7.2. Отключить камеру

Отключить камеру на экранах с защищенной блокировкой (например, при вводе PIN-кода).

7.3. Отключить уведомления

Отключить отображение всех уведомлений на экранах с защищенной блокировкой.

7.4. Отключить отображение содержимого уведомлений

Отключить отображение содержимого уведомлений на экранах с защищенной блокировкой.

7.5. Игнорировать состояние доверенного агента

Игнорировать состояние доверенного агента на экранах с защищенной блокировкой.

7.6. Отключить отпечаток пальца

Отключить датчик отпечатка пальца на экранах с защищенной блокировкой.

7.7. Отключить текстовый ввод в уведомлениях

Отключить текстовый ввод в уведомлениях на экранах с защищенной блокировкой.

7.8. Отключить аутентификацию по лицу

Отключить аутентификацию по лицу на экранах с защищенной блокировкой.

7.9. Отключить аутентификацию по радужной оболочке глаза

Отключить аутентификацию по радужной оболочке глаза на экранах с защищенной блокировкой.

7.10. Отключить всю биометрическую аутентификацию

Отключить всю биометрическую аутентификацию на экранах с защищенной блокировкой.

7.11. Отключить все ярлыки

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

Revision #47
Created 2025-12-17 09:34:55 UTC by Admin
Updated 2026-07-07 10:57:41 UTC by Admin