# ??????????

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.

---

Revision #34
Created 2025-12-17 09:34:55 UTC by Admin
Updated 2026-04-22 15:53:29 UTC by Admin