Система

В этом разделе можно настроить политики, связанные с системой.

1. Минимальный уровень API

Минимально допустимый уровень API Android.

2. Политика шифрования

Включено ли шифрование.

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

3. Автоматические дата и время

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

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

4. Настройки для разработчиков

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

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

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

5. Режим Common Criteria

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

Отключено (по умолчанию): отключает режим Common Criteria.

Включено: включает режим Common Criteria.

6. Memory Tagging Extension (MTE)

Управляет Memory Tagging Extension (MTE) на устройстве.

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

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

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

7. Защита содержимого

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

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

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

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

8. Содержимое ассистента

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

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

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

9. Создание окон отключено

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

10. Аварийное сетевое подключение

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

11. Действия по умолчанию

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

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

11.1. Действие-получатель

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

11.2. Действие

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

11.3. Категория

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

12. Разрешённые способы ввода

Указывает разрешённые способы ввода.

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

12.1. Разрешённые способы ввода

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

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

13. Разрешённые службы доступности

Указывает разрешённые службы доступности.

Все разрешены: можно использовать любую службу доступности.

Только системные: можно использовать только встроенные системные службы доступности.

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

13.1. Разрешённые службы доступности

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

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

14. Политика обновления системы

Конфигурация для управления обновлениями системы.

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

Автоматически: устанавливать автоматически, как только появится обновление.

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

Отложить: отложить автоматическую установку максимум на 30 дней.

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

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

14.2. Периоды заморозки обновлений системы

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

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

15. Провайдеры учётных данных по умолчанию

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

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

Revision #55
Created 2025-12-17 09:34:54 UTC by Admin
Updated 2026-11-12 09:57:51 UTC by Admin