

????????? ?????????????? ????? ?? Android ? iOS ? KSMM

“ **И** **Информация:** приведенная на данной статье информация подготовлена в формате практического руководства команды Presale и не является заменой официальной документации. Перед применением параметров в продуктивной среде проверьте их соответствие архитектуре Microsoft Exchange, используемому способу аутентификации и политике информационной безопасности организации.

?????????

Kaspersky Secure Mobility Management позволяет централизованно передавать на управляемые мобильные устройства параметры корпоративной электронной почты. В зависимости от платформы и используемого клиента настройка выполняется разными способами.

Для Android в политике KSMM предусмотрена отдельная конфигурация **Exchange ActiveSync для Gmail**. Для сторонних клиентов, например Microsoft Outlook, используется механизм **Настройка прочих приложений**, позволяющий передавать приложению Managed Configuration. Оба механизма предназначены для корпоративных Android-устройств и устройств с корпоративным контейнером. support.kaspersky.ru

Для iOS MDM конфигурация Exchange ActiveSync создается средствами политики и передается на устройство через Сервер iOS MDM. Эта настройка применяется к устройствам в режимах **Расширенный контроль** и **Базовый контроль**. support.kaspersky.ru

В данной статье рассмотрим три сценария:

1. настройка Exchange ActiveSync для Gmail на Android;
2. настройка Microsoft Outlook как стороннего почтового клиента на Android;
3. настройка Exchange ActiveSync и S/MIME для iOS MDM.

В примерах используются адреса `example.com` и `mail.example.com`. В рабочей инфраструктуре их необходимо заменить на реальные DNS-имена вашего Exchange ActiveSync.

1. ?????????? Exchange ActiveSync ??? Gmail ?? Android

Параметры Gmail настраиваются внутри политики Kaspersky Mobile Devices Protection and Management.

Перейдите `Управление активами → Политики → <политика KSMM> → Параметры приложения → Android → Конфигурация приложений`

На карточке **Exchange ActiveSync** нажмите **Параметры** и включите переключатель **Exchange ActiveSync**.

1.1. ?????????? ????????????

На вкладке **Общие** укажите адрес Exchange ActiveSync и данные пользователя.

В рассматриваемом примере используются следующие значения:

Параметр	Значение в примере	Назначение
Адрес сервера Exchange ActiveSync	<code>example.com</code>	DNS-имя сервера Exchange ActiveSync
Идентификатор устройства	<code>%device_id%</code>	Идентификатор управляемого устройства
Имя пользователя	<code>%user_name%</code>	Имя пользователя из данных KSC / Active Directory
Адрес электронной почты	<code>%email%</code>	Email пользователя

Параметр	Значение в примере	Назначение
Тип аутентификации	Современная аутентификация на основе токенов	Token-based authentication
Сертификат аутентификации	Почтовый сертификат	Сертификат пользователя, выданный через KSC

В KSMM поля имени пользователя, адреса электронной почты и идентификатора устройства могут заполняться с использованием макросов. Для аутентификации поддерживаются современная аутентификация на основе токенов и базовая аутентификация. В поле **Сертификат аутентификации** можно выбрать почтовый сертификат пользователя или профиль SCEP.

“ **Важно:** значения `%device_id%`, `%user_name%` и `%email%` позволяют использовать одну политику для группы устройств. При применении политики KSMM подставляет данные соответствующего пользователя и устройства.

Exchange ActiveSync

Exchange ActiveSync ВКЛЮЧЕН

ОбщиеДополнительные

Адрес сервера Exchange ActiveSync

example.com

Учетные данные пользователя

Идентификатор устройства

%device_id%+

Имя пользователя

%user_name%+

Адрес электронной почты

%email%+

Аутентификация

Тип аутентификации

Базовая аутентификация

Сертификат аутентификации

Почтовый сертификат

□ Скриншот 1 — основные параметры Exchange ActiveSync для Gmail

В примере выбрана базовая аутентификация и назначен **Почтовый сертификат**. Фактически используемая схема аутентификации должна соответствовать конфигурации Exchange и требованиям вашей инфраструктуры.

Если была настроена интеграция KSMM с Microsoft CA через PKI, здесь можно выбрать ранее выпущенный почтовый сертификат пользователя. В списке KSMM отображает почтовые сертификаты, настроенные в разделе [Управление активами → Мобильные → Сертификаты](#)

[Статья описывающая процесс интеграции KSMM и с Microsoft CA через PKI](#)

1.2. ?????????????????? ??????????? Gmail

Перейдите на вкладку **Дополнительные**.

В нашем примере настроено:

- **период синхронизации — 1 день;**

“i Этот параметр задает не периодичность проверки почтового ящика, а глубину синхронизации почты. На устройство загружаются сообщения за последний день. Новые письма продолжают поступать в соответствии с механизмом синхронизации Exchange ActiveSync. Установка значения «1 день» не означает, что почта обновляется только один раз в сутки. Просто более старые сообщения не хранятся локально и могут потребовать подключения к серверу для просмотра.

- **Использовать SSL-соединение** — включено;
- **Отключить проверку SSL-сертификатов** — выключено;
- **Разрешить неуправляемые учетные записи** — выключено;
- подпись электронной почты — не задана.

KSMM позволяет выбрать период синхронизации от одного дня до одного месяца. Использование SSL по умолчанию включено. Также администратор может определить, разрешено ли пользователю добавлять в Gmail учетные записи, не управляемые организацией.

Скриншот 2 — дополнительные параметры Exchange ActiveSync для Gmail

⚠ Рекомендация: параметр **Отключить проверку SSL-сертификатов** в продуктивной среде лучше оставлять выключенным. Иначе почтовый клиент перестает полноценно проверять подлинность сертификата сервера Exchange.

Если в организации запрещено использование личных почтовых аккаунтов внутри корпоративного Gmail, снимите флажок **Разрешить неуправляемые учетные записи**, как показано на скриншоте.

После настройки нажмите **ОК**, затем **Сохранить** в свойствах политики. Изменения будут переданы на устройства при применении политики.

2. ?????????? Microsoft Outlook ? ???????? ?????????? ??????????

?? Android

Для Microsoft Outlook и других почтовых клиентов на Android в политике KSMM нет отдельной карточки, аналогичной Gmail. Поэтому они настраиваются как сторонние приложения через механизм **Настройка прочих приложений**.

В данном примере рассмотрен именно Microsoft Outlook.

KSMM позволяет создавать Managed Configuration для приложений, которые поддерживают управляемые параметры Android. Конфигурацию можно загрузить из APK, получить из инсталляционного пакета Kaspersky Security Center или создать вручную.

Перейдите `Управление активами → Политики → <политика KSMM> → Параметры приложения → Android → Конфигурация приложений → Настройка прочих приложений`

Включите **Настройка прочих приложений** и нажмите **Добавить**.

2.1. ????????????????????????????????? Outlook

В примере выбран способ из **Инсталляционного пакета Kaspersky Security Center**

После выбора пакета Outlook KSC автоматически получает сведения о приложении.

В нашем примере:

- **Название приложения:** Outlook
- **Имя пакета:** com.microsoft.office.outlook
- **Версия:** 4.2444.0

“i Версия 4.2444.0 приведена только как пример со стенда. В вашей инфраструктуре здесь будет отображаться версия используемого пакета Outlook.

Имя пакета является ключевым параметром: конфигурация будет передана именно приложению с соответствующим Android Package Name. Для одного имени пакета в KSMM можно создать только одну конфигурацию.

Добавить конфигурацию приложения

Способ добавления конфигурации

Инсталляционный пакет Kaspersky Security Center

Инсталляционный пакет

Выбрать другой инсталляционный пакет

Данные конфигурации

Название приложения*

Outlook

Имя пакета*

com.microsoft.office.outlook

Версия

4.2444.0

Комментарий

Параметры конфигурации

Ключ

om.microsoft.outlook.EmailProfile.EmailAddress

Тип

String

Значение

%email%

Ключ

crosoft.outlook.EmailProfile.EmailAccountName

Тип

String

Значение

%user_name%

Ключ

com.microsoft.outlook.EmailProfile.ServerHostN

Тип

String

Значение

mail.example.com

❏ Скриншот 3 — Managed Configuration для Microsoft Outlook

В показанном примере для Outlook задаются основные параметры почтового профиля:

```
com.microsoft.outlook.EmailProfile.EmailAddress
    %email%

com.microsoft.outlook.EmailProfile.EmailAccountName
    %user_name%

com.microsoft.outlook.EmailProfile.ServerHostName
    mail.example.com
```

Значение `%email%` позволяет автоматически передавать Outlook адрес корпоративной почты текущего пользователя, `%user_name%` — имя пользователя, а `ServerHostName` определяет сервер Exchange ActiveSync.

???????????????? Outlook

В зависимости от вашей схемы Exchange профиль может быть дополнен следующими параметрами:

Ключ	Назначение
<code>com.microsoft.outlook.EmailProfile.EmailAccountName</code>	Имя пользователя
<code>com.microsoft.outlook.EmailProfile.EmailAddress</code>	Адрес электронной почты
<code>com.microsoft.outlook.EmailProfile.EmailUPN</code>	UPN пользователя для аутентификации
<code>com.microsoft.outlook.EmailProfile.ServerAuthentication</code>	Способ проверки подлинности
<code>com.microsoft.outlook.EmailProfile.ServerHostName</code>	FQDN Exchange ActiveSync
<code>com.microsoft.outlook.EmailProfile.AccountDomain</code>	Домен учетной записи
<code>com.microsoft.outlook.EmailProfile.AccountType</code>	Тип учетной записи / способ аутентификации

Для `ServerAuthentication` указываются значения `Username and Password` / `Certificates`. Для `AccountType` предусмотрены `ModernAuth` / `BasicAuth`. `ModernAuth` для Exchange Online и `BasicAuth` для локального Exchange. Конкретные параметры должны соответствовать настройкам вашего почтового сервера.

“ **Сертификаты:** KSMM позволяет передавать приложениям сертификаты, установленные через Kaspersky Security Center. Для почтового сертификата используется псевдоним `MailCert`, для VPN — `VpnCert`, для SCEP — имя соответствующего SCEP-профиля. Конкретный Managed Configuration key, в котором приложение ожидает этот

псевдоним, необходимо сверять с документацией самого приложения.

После заполнения параметров нажмите **Добавить**, затем **ОК** и сохраните политику.

“ ⚠ Некоторые сторонние приложения могут не уведомлять Kaspersky Endpoint Security for Android о том, что Managed Configuration была применена.

3. ?????????? Exchange ActiveSync ?? iOS

Для iOS настройка выполняется не через параметры отдельного почтового приложения, а через конфигурацию Exchange ActiveSync, которая доставляется на устройство посредством iOS MDM.

Перейдите `Управление активами → Политики → <политика KSMM> → Параметры приложения → iOS → Конфигурация устройств → Exchange ActiveSync`

Откройте **Параметры**, включите Exchange ActiveSync и нажмите **Добавить**.

3.1. ?????????? ?????????? ?????????? ?????????

На вкладке **Общие** задайте учетные данные пользователя и сервер Exchange.

На стенде используется следующая конфигурация:

Параметр	Значение
Имя учетной записи	<code>%full_name%</code>

Параметр	Значение
Адрес Exchange ActiveSync	example.com
Домен пользователя	не указан
Имя пользователя	%short_name%
Адрес электронной почты	%email%
Пароль	не указан
Сертификат аутентификации	Почтовый сертификат 1

KSMM позволяет вводить данные вручную или использовать макросы. В качестве сертификата аутентификации можно выбрать сертификат пользователя, уже добавленный в систему управления сертификатами KSC.

Изменить аккаунт Exchange ActiveSync

Общие

Дополнительные

Имя учетной записи*

%full_name%

+

Адрес сервера Exchange ActiveSync*

example.com

Учетные данные пользователя

Домен пользователя

+

Имя пользователя*

%short_name%

+

Адрес электронной почты

%email%

+

Аутентификация

Пароль

Сертификат аутентификации

Почтовый сертификат 1

Скриншот 4 — параметры Exchange ActiveSync для iOS

В данном примере пароль не задается в политике, а для аутентификации выбран **Почтовый сертификат 1**.

“□ Если используется настроенная ранее интеграция с Microsoft CA, этим сертификатом может быть почтовый сертификат пользователя, автоматически выпущенный через PKI и доставленный на iOS MDM-устройство.

[Статья описывающая процесс интеграции KSMM и с Microsoft CA через PKI](#)

Поле **Домен пользователя** можно оставить пустым, если используемая схема аутентификации и формат имени пользователя этого не требуют. Для параметров, зависящих от конкретного пользователя, удобнее применять макросы вместо фиксированных значений.

3.2. ????????????, SSL ? S/MIME ?? iOS

Перейдите на вкладку **Дополнительные**.

В рассматриваемом примере:

- период синхронизации — **1 неделя**;

“i Этот параметр задает не периодичность проверки почтового ящика, а глубину синхронизации почты. На устройство загружаются сообщения за последний день. Новые письма продолжают поступать в соответствии с механизмом синхронизации Exchange ActiveSync. Установка значения «1 день» не означает, что почта обновляется только один раз в сутки. Просто более старые сообщения не хранятся локально и могут потребовать подключения к серверу для просмотра.

- перемещение сообщений между рабочими и личными учетными записями запрещено;
- синхронизация последних использованных адресов разрешена;
- ограничение «использовать только приложение Почта» выключено;

- SSL включен;
- подпись S/MIME включена;
- шифрование S/MIME по умолчанию включено;
- пользователю разрешено включать и выключать шифрование отдельных сообщений.

Изменить аккаунт Exchange ActiveSync

Общие Дополнительные

Синхронизация электронной почты

Период синхронизации

1 неделя

Ограничения

☐ Разрешить перемещать сообщения между учетными записями (в том числе между рабочими и личными)

☒ Разрешить синхронизировать последние используемые адреса

☐ Разрешить использовать только приложение Почта

☒ Использовать SSL-соединение

Подпись и шифрование

☒ Подписывать сообщения

Сертификат для подписи исходящих сообщений*

Почтовый сертификат 2

☒ Шифровать сообщения по умолчанию

Сертификат для шифрования*

Почтовый сертификат 3

☒ Показывать переключатель для шифрования отдельных сообщений

Per App VPN

☐ Включить Per App VPN iOS 14+



В разделе "VPN" политики должна быть создана конфигурация VPN с типом подключения, поддерживающим Per App VPN.

❏ Скриншот 5 — дополнительные параметры Exchange ActiveSync и S/MIME

3.3. Настройка параметров безопасности

Если снять флажок **Разрешить перемещать сообщения между учетными записями (в том числе между рабочими и личными)**, то пользователь не сможет свободно переносить почтовые сообщения между корпоративным и личными аккаунтами.

Рекомендуется сочетать это ограничение с запретом передачи документов между управляемыми и неуправляемыми приложениями, если требуется предотвратить сохранение и отправку корпоративных вложений через личные приложения. Это особенно актуально для сценариев BYOD.

3.4. Настройка параметров SSL

Установите **Использовать SSL-соединение** для защиты данных при передаче между мобильным устройством и Exchange ActiveSync. Для продуктивного Exchange рекомендуется использовать сертификат сервера, которому доверяет мобильное устройство, с корректным DNS-именем в SAN.

3.5. Настройка параметров S/MIME

Для включения цифровой подписи установите **Подписывать сообщения**

Затем выберите **Сертификат для подписи исходящих сообщений** → **<Почтовый сертификат>**

KSMM использует S/MIME для цифровой подписи исходящей почты в стандартном приложении **Почта**. Подпись позволяет получателю проверить отправителя и целостность сообщения.

“i Сертификат для подписи должен содержать соответствующее назначение и закрытый ключ пользователя. Если сертификаты выпускаются Microsoft CA, это необходимо учитывать при настройке шаблона сертификата.

[Статья описывающая процесс интеграции KSMM и с Microsoft CA](#)

3.6. ?????????? ?????????? S/MIME

Установите **Шифровать сообщения по умолчанию**

и выберите **Сертификат для шифрования** → <Почтовый сертификат>

При необходимости также включите **Показывать переключатель для шифрования отдельных сообщений**. В этом случае пользователь сможет изменять режим шифрования непосредственно при создании письма.

“ ⚠ Для S/MIME-шифрования одного сертификата отправителя недостаточно. Для отправки зашифрованного сообщения iOS должен иметь доступ к открытому ключу сертификата получателя. Если сертификат получателя неизвестен, зашифровать сообщение невозможно.

На практике сертификат для аутентификации Exchange, сертификат для подписи и сертификат для шифрования **могут быть как одним сертификатом, так и разными сертификатами** — это определяется шаблонами Microsoft CA и принятой PKI-архитектурой.

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

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

После применения политики рекомендуется проверить конфигурацию непосредственно на тестовом устройстве.

Android / Gmail

Убедитесь, что:

1. корпоративная учетная запись появилась в Gmail;
2. адрес пользователя и сервер подставились автоматически;
3. выполняется синхронизация входящей почты;
4. отправка сообщений работает;
5. при использовании сертификатной аутентификации сервер принимает выданный пользователю сертификат;
6. пользователь не может добавить неуправляемый аккаунт, если соответствующая настройка запрещена.

Android / Outlook ??? ?????? ?????????? ???????

Проверьте:

1. наличие Outlook на устройстве;
2. применение конфигурации приложения;
 1. автоматическое заполнение адреса электронной почты;
 2. автоматическое заполнение имени пользователя;
 3. адрес Exchange ActiveSync;
 4. успешную аутентификацию выбранным способом.

iOS

После синхронизации с iOS MDM проверьте:

1. появление корпоративной Exchange-учетной записи;
2. получение входящих сообщений;
3. отправку почты;
4. использование SSL;
5. наличие выбранного сертификата аутентификации;
6. цифровую подпись S/MIME;
7. возможность отправки зашифрованного письма тестовому пользователю.

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

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

Проверьте:

- DNS-имя Exchange ActiveSync;
- формат имени пользователя;
- необходимость указания домена;
- используемый тип аутентификации;
- доверие устройства к сертификату Exchange;
- наличие и срок действия пользовательского сертификата;
- соответствие сертификата требованиям Exchange.

????????

После применения политики Kaspersky Secure Mobility Management централизованно формирует конфигурацию корпоративной почты для управляемых мобильных устройств.

Для Android можно использовать встроенную настройку **Exchange ActiveSync для Gmail** либо передавать параметры стороннему клиенту — например, **Microsoft Outlook** — через Managed Configuration.

Для iOS KSC создает системную конфигурацию Exchange ActiveSync и при необходимости дополнительно назначает сертификаты для аутентификации, подписи и шифрования S/MIME.

При этом администратору не требуется вручную создавать почтовый профиль на каждом устройстве: адрес сервера, идентификаторы пользователя, email, сертификаты и ограничения доставляются политикой.

Материал построен по официальной справке KSMM

- [Управление Exchange ActiveSync для Gmail](#)
- [Настройка прочих приложений](#)
- [Настройка почтового ящика Exchange на iOS MDM-устройствах](#)

Revision #1

Created 2 October 2026 08:47:56 by Сергей

Updated 2 October 2026 10:43:31 by Сергей