

??????????? KSMM ? Microsoft CA ?????? PKI

????????????? ?????????? ?? ?????????? Microsoft AD CS, ??????????????
Windows-???? ? Kaspersky Security Center Linux.

“ **△ Важно.** Материал подготовлен в формате практической базы команды Presale и не заменяет официальную документацию. Перед изменениями в продуктивной PKI оцените последствия и придерживайтесь принципа минимально необходимых привилегий.

В Kaspersky Secure Mobility Management интеграция с Microsoft Certification Authority позволяет автоматически выпускать доменные пользовательские сертификаты. Запросы к Microsoft CA передаются через **промежуточное Windows-устройство с установленным Агентом администрирования Kaspersky Security Center**. Для работы интеграции сервисной доменной учетной записи требуются права на CA и шаблон Enrollment Agent, а в ее пользовательском хранилище должен быть установлен сертификат Enrollment Agent.

Пример стэнда: домен `sales.lab`, CA `sales-DC-01-CA`, сервисная учетная запись `ksmm@sales.lab`

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

В сценарии используются Kaspersky Security Center Linux, Microsoft Active Directory Certificate Services и отдельное Windows-устройство в том же домене, что и CA. На Windows-устройстве должен быть установлен Агент администрирования для Windows. Именно он выступает посредником между Сервером администрирования и Microsoft CA.

- Доменная сервисная учетная запись для передачи запросов в CA.
- Промежуточное Windows-устройство, доступное из Kaspersky Security Center и состоящее в домене CA.
- Права **Issue and Manage Certificates** на CA.
- Права **Read** и **Enroll** на шаблон Enrollment Agent.

- Сертификат Enrollment Agent в хранилище `Current User → Personal` сервисной учетной записи.
- Сетевое соединение Агента администрирования с Kaspersky Security Center; по официальной схеме должен быть доступен порт `13000`.
- Настроенный опрос домена сервером администрирования KSC (Нужен для обнаружения доменной УЗ сервером KSC).

“i Kaspersky Security Center поддерживает только одну активную интеграцию с Microsoft CA через PKI.

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

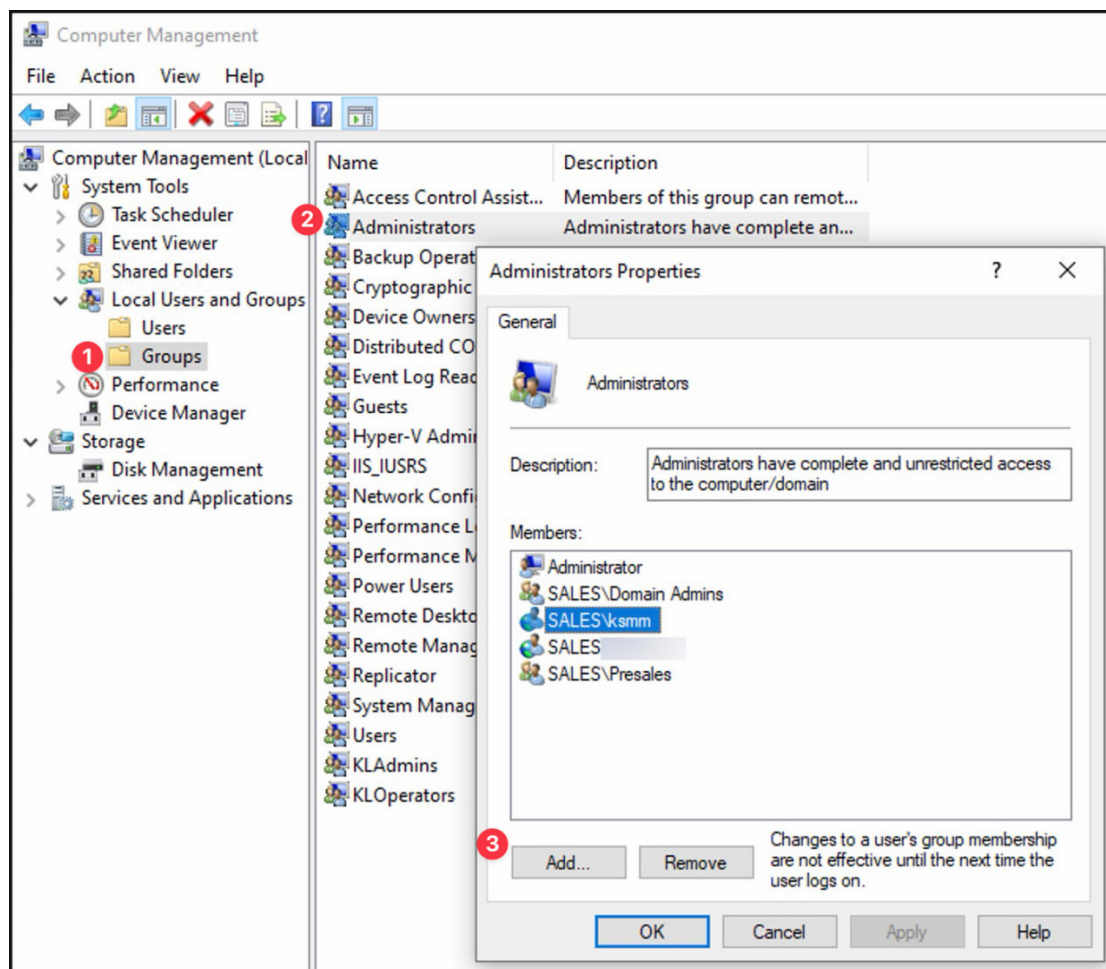
2.1. ?????????? ?????????? ?????????? ?????????? ?????????

Создайте в Active Directory отдельного пользователя, от имени которого Kaspersky Security Center будет передавать запросы на выпуск сертификатов. В примере используется `SALES\ksmm` с UPN `ksmm@sales.lab`.

“□ Не используйте персональную учетную запись администратора. Для интеграции лучше выделить отдельную сервисную учетную запись с контролируемым паролем и минимальным набором прав.

2.2. ?????????? ?????????? ?????????? ?????????? ?? ?????????????????? Windows-???????????????

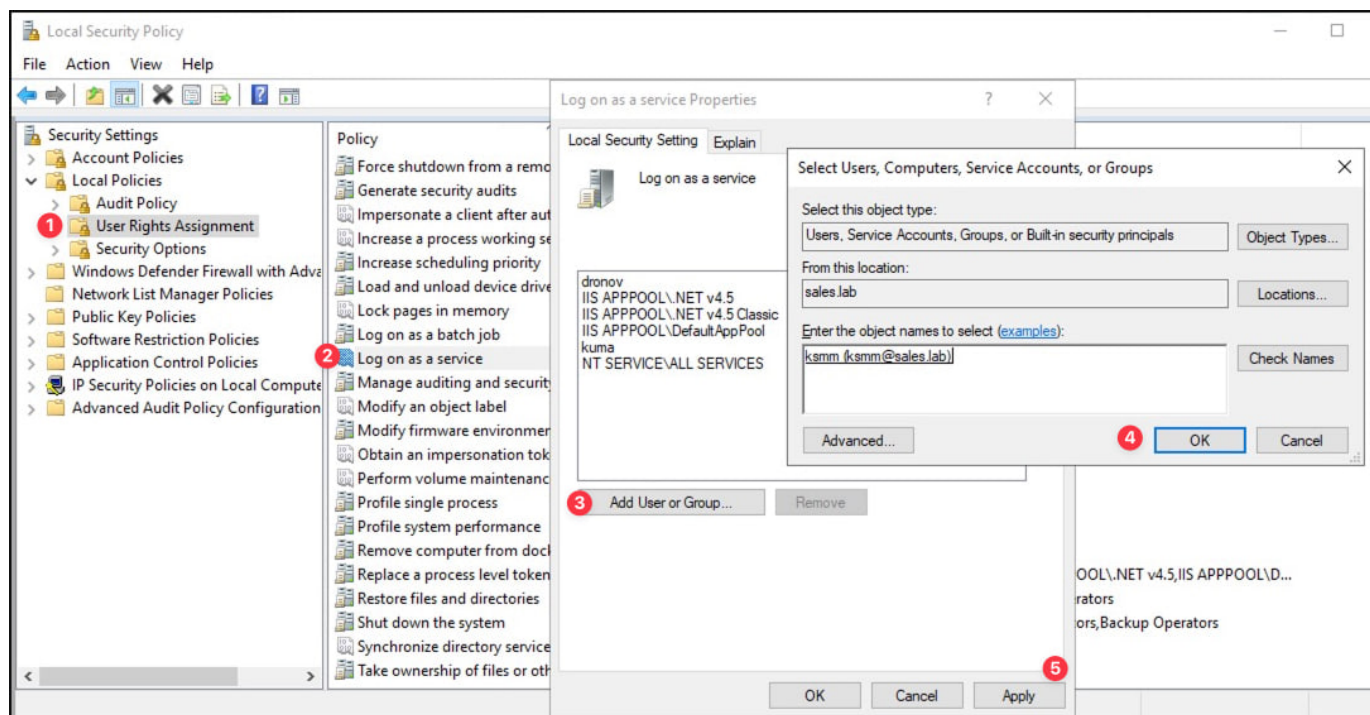
Предоставьте созданной доменной учетной записи доступ к промежуточному Windows-устройству в качестве локального администратора. Добавьте пользователя в локальную группу **Administrators**.



Скриншот 1. Учетная запись добавлена в локальную группу Administrators на тестовом Windows-узле.

2.3. ???????? ?????? Log on as a service ?? Microsoft CA

На CA откройте `secpol.msc` и перейдите `Local Policies → User Rights Assignment → Log on as a service`. Добавьте сервисную доменную учетную запись и примените изменения.

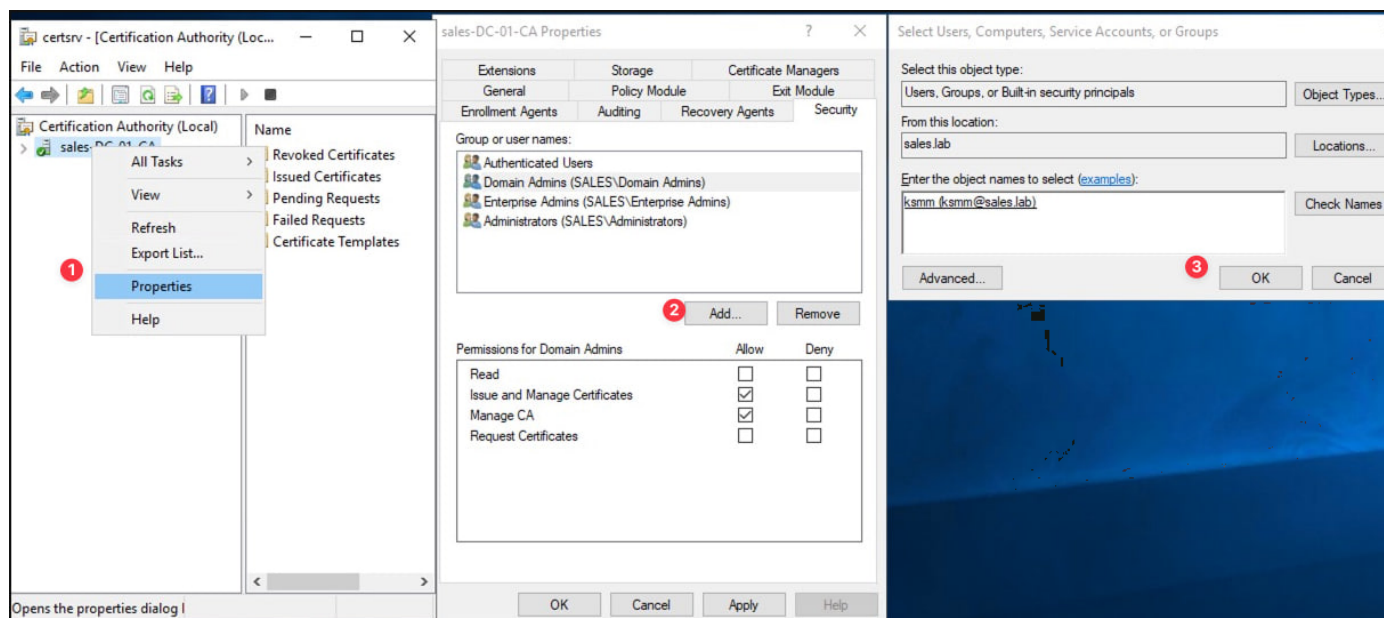


Скриншот 2. Добавление УЗ в политику Log on as a service.

3. ??????? ????? ?????????????? ?????????? ????????? ?? Microsoft CA

3.1. ??????????? ??????????? ?????????? ? ACL ????????? ????????????????????

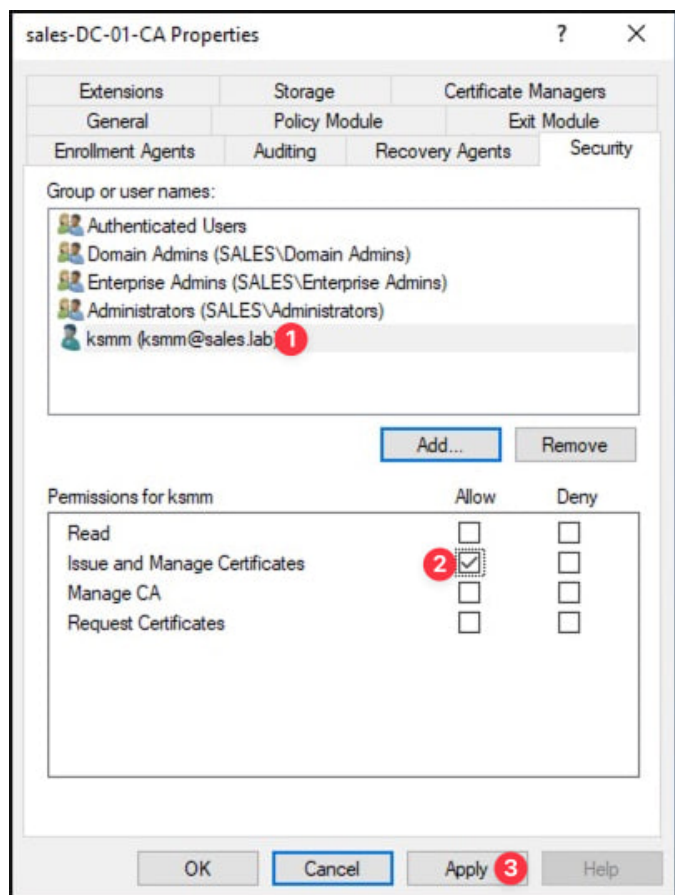
На сервере Microsoft CA запустите `certsrv.msc`. Откройте свойства центра сертификации, перейдите на вкладку **Security** и нажмите **Add**. Укажите ранее созданную доменную учетную запись.



Скриншот 3. Добавление УЗ в список безопасности Microsoft CA.

3.2. ?????????? Issue and Manage Certificates

Выберите сервисную учетную запись и включите **Allow** для разрешения **Issue and Manage Certificates**. Сохраните изменения.



Скриншот 4. Разрешение *Issue and Manage Certificates* для учетной записи *ksmm*.

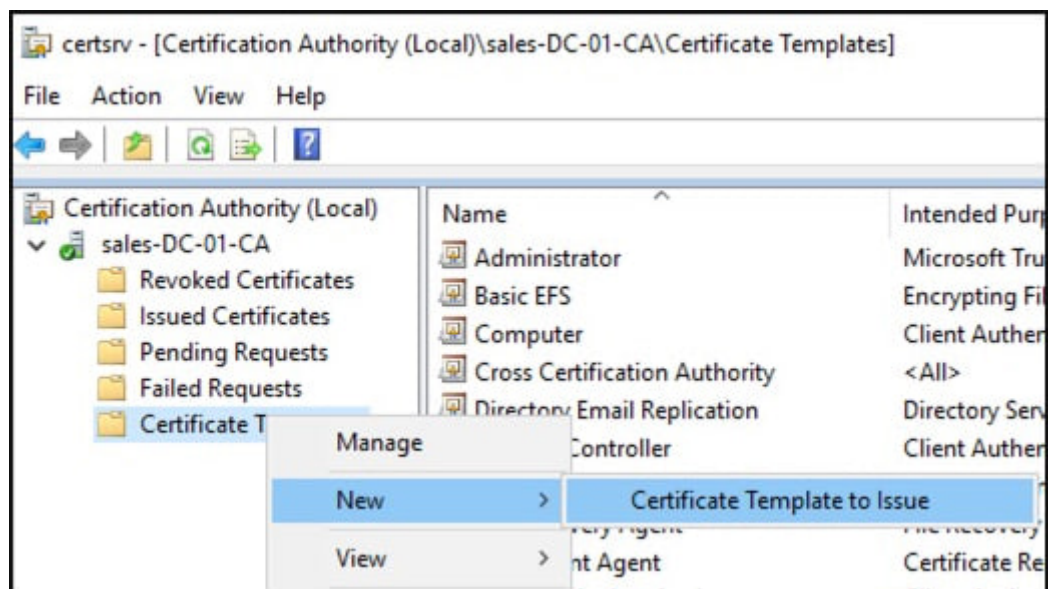
“ ⚠ Не выдавайте `Manage CA` или `Full Control`, если это не требуется вашей административной моделью.

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

Enrollment Agent

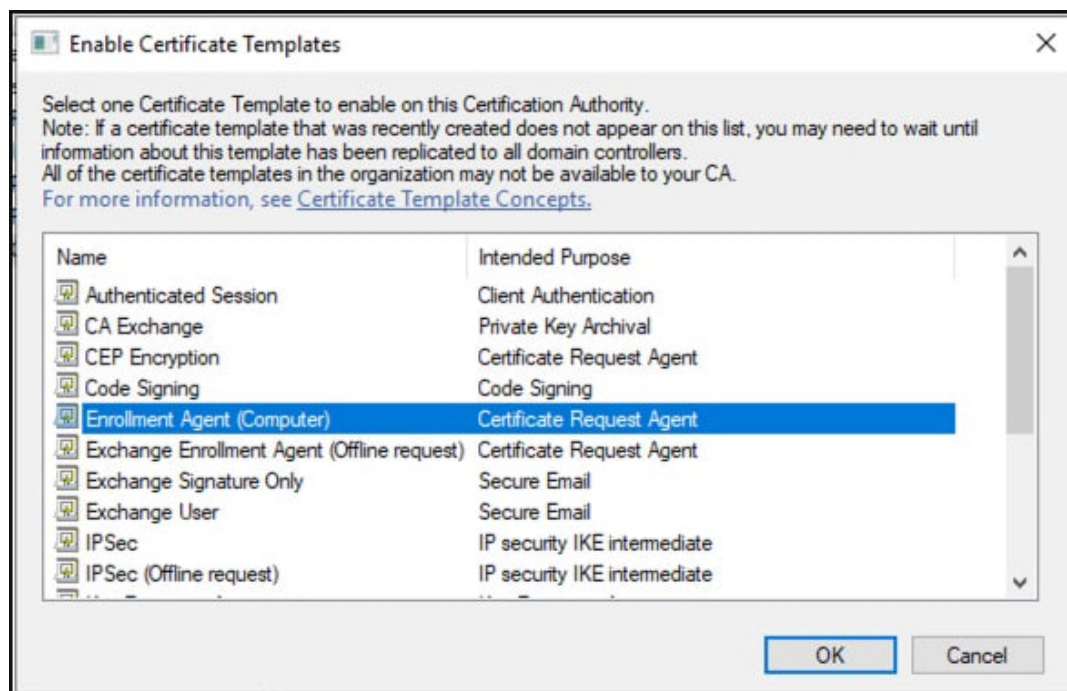
4.1. ????????????????? ????????? ?? CA

В `certsrv.msc` нажмите правой кнопкой мыши `Certificate Templates → New → Certificate Template to Issue`.



Скриншот 5. Публикация нового шаблона сертификата на СА.

В списке доступных шаблонов выберите **Enrollment Agent**. Нажмите **OK**.

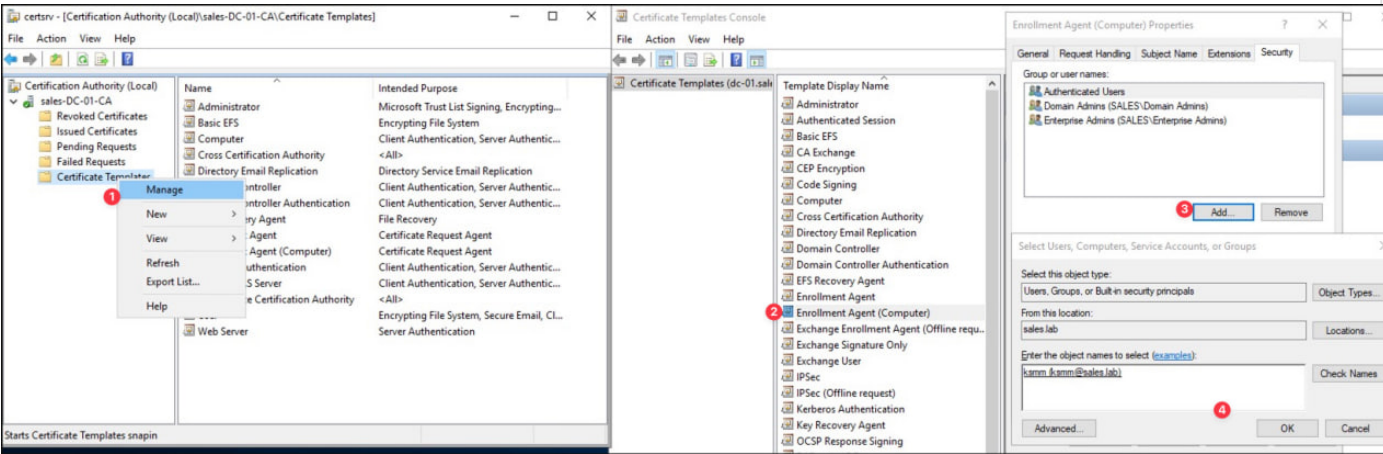


Скриншот 6. Выбор шаблона Enrollment Agent для выпуска.

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

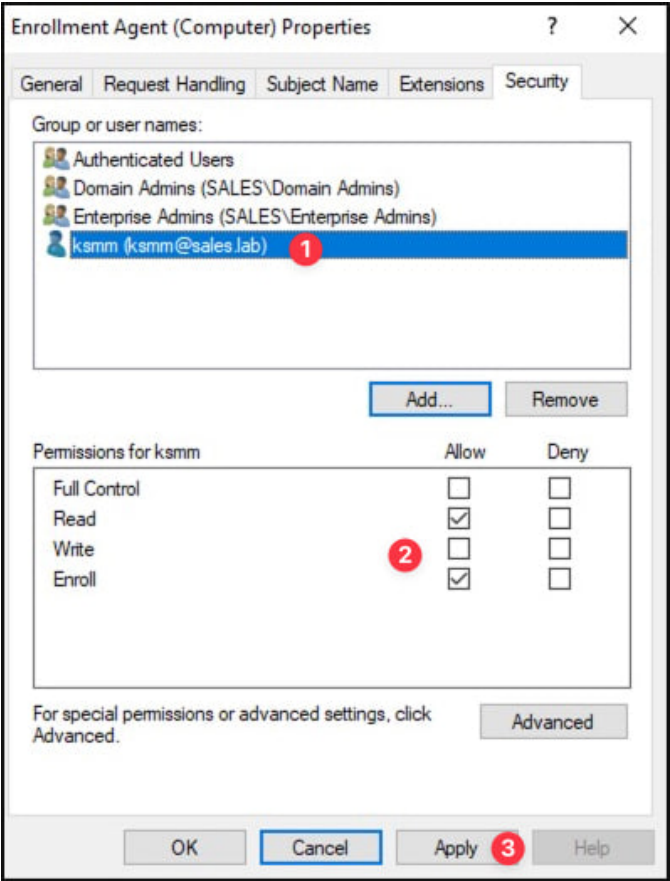
Откройте `Certificate Templates → Manage`. В консоли Certificate Templates откройте свойства шаблона Enrollment Agent и перейдите на вкладку **Security**. Добавьте

сервисную учетную запись.



Скриншот 7. Добавление УЗ в ACL шаблона Enrollment Agent.

Для учетной записи разрешите как минимум **Read** и **Enroll**, затем нажмите **Apply**.

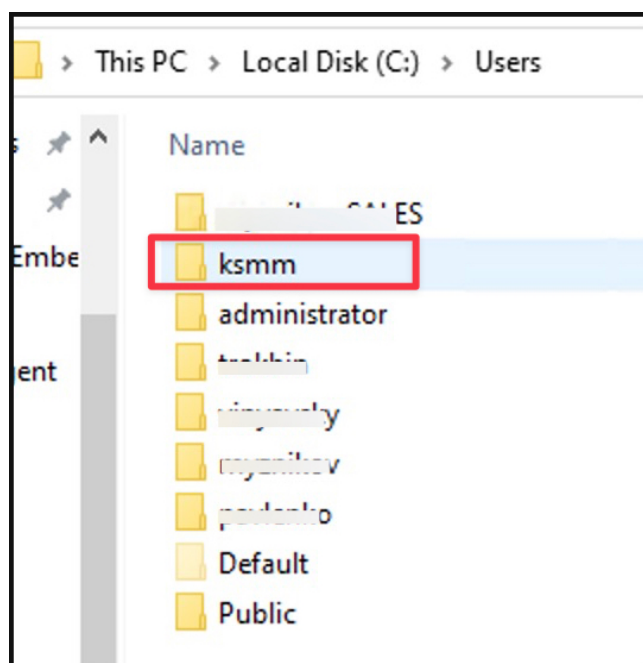


Скриншот 8. Права Read и Enroll для учетной записи ksmm на шаблоне Enrollment Agent.

5. ?????????? ?????????????????? Windows-????????????

5.1. ?????????? ?????????????? ?????????? ????????????? ?????????? ??????????

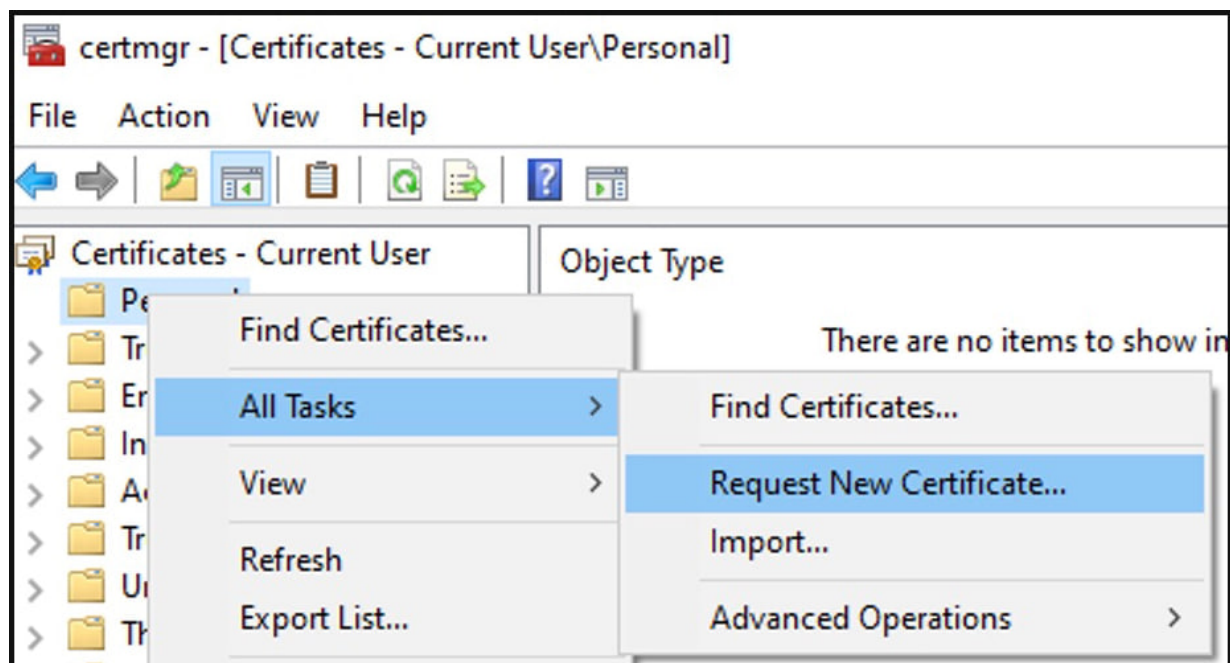
Войдите на промежуточное Windows-устройство под сервисной доменной учетной записью. Это создаст постоянный профиль пользователя, в котором затем будет храниться сертификат Enrollment Agent. После входа можно убедиться, что появился каталог, например `C:\Users\<имя УЗ>`.



Скриншот 9. Профиль пользователя создан на промежуточном Windows-устройстве.

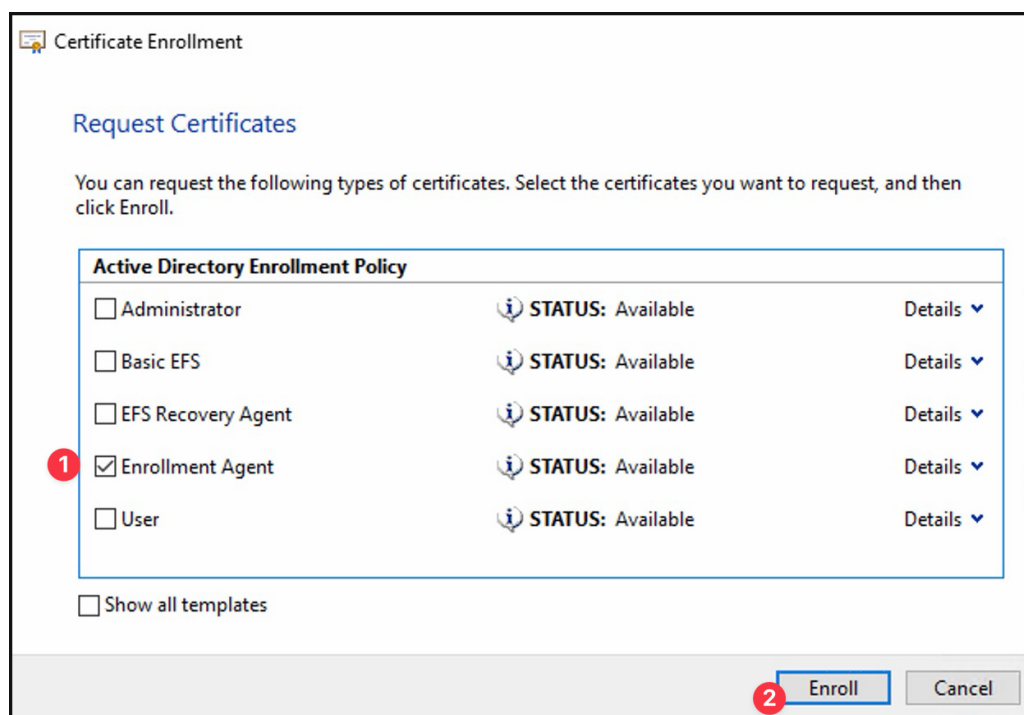
5.2. ?????????????? ?????????????? Enrollment Agent

Оставаясь в сеансе сервисной учетной записи, запустите `certmgr.msc`. В разделе **Personal** выберите `All Tasks → Request New Certificate...` и пройдите шаги мастера с настройками по умолчанию до шага **Request Certificates**.



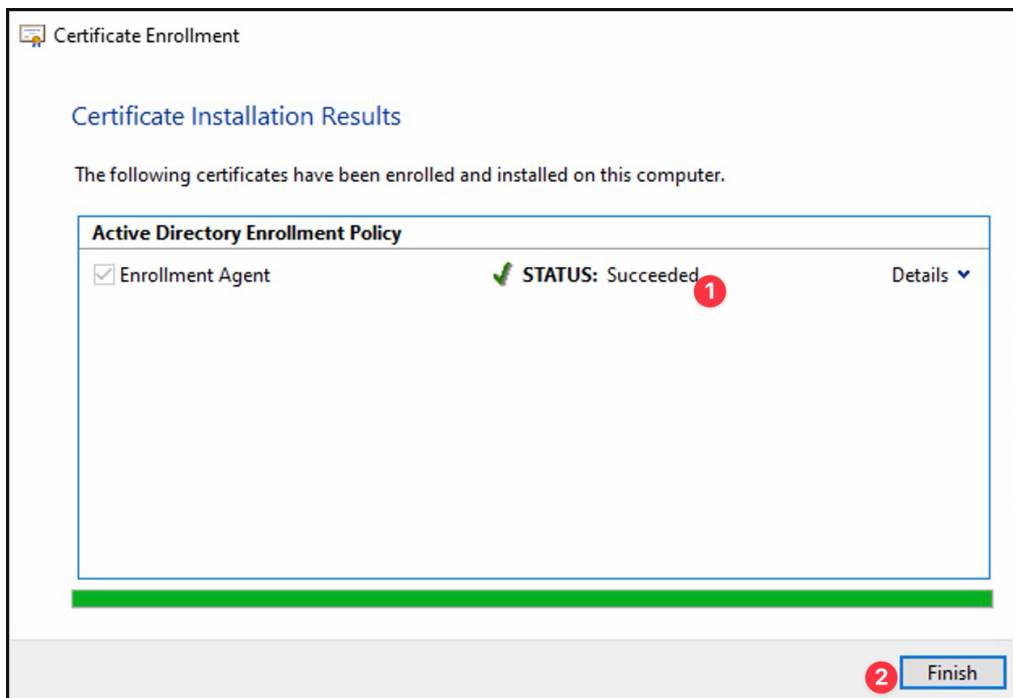
Скриншот 10. Запуск мастера Request New Certificate из хранилища Current User → Personal.

На шаге **Request Certificates** выберите **Enrollment Agent** и нажмите **Enroll**.



Скриншот 11. Выбор сертификата Enrollment Agent и запуск регистрации.

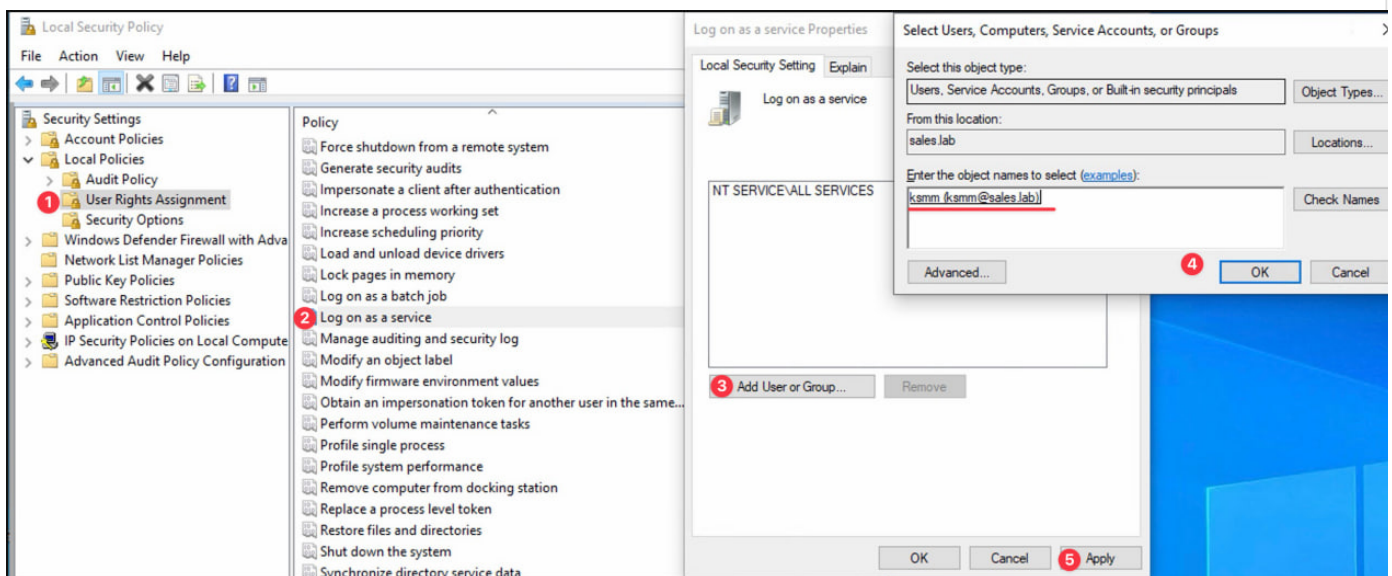
Убедитесь, что мастер завершился со статусом **Succeeded**, затем нажмите **Finish**.



Скриншот 12. Сертификат Enrollment Agent успешно выпущен и установлен.

5.3. ?????????? ?????????? ?????? Log on as a service

На промежуточном Windows-устройстве откройте `secpol.msc` → Local Policies → User Rights Assignment → Log on as a service и укажите соответствующую сервисную УЗ.



Скриншот 13. Настройка права Log on as a service на промежуточном Windows-узле.

5.4. ?????????? ? ?????????? ?????? ???????????????????????????? Windows

Установите на промежуточное устройство Агент администрирования Kaspersky Security Center для Windows и укажите адрес Kaspersky Security Center Linux. Убедитесь, что доступен порт 13000, устройство появилось в Web Console и прошло первую синхронизацию.

“i Рекомендуем включить для данного хоста опцию "Не разрывать соединение" в KSC

6. ???????????? PKI ? Kaspersky Security Center Web Console

Запустите опрос домена в KSC в разделе Обнаружение устройств и развертывание → Обнаружение устройств → Контроллеры доменов. Созданная сервисная доменная УЗ должна повиться в разделе Пользователи и роли → Пользователи и группы

Kaspersky Security Center

KSC FOC Linux

Навигация консоли

Мониторинг

Управление активами

Управление уязвимостями

Задачи

Приложения и службы

Пользователи и роли

Пользователи и группы

Роли

Пользователи и группы

Показать иерархию

KSC FOC Linux

Пользователи

Группы

+ Добавить

× Удалить

Назначить роль

Назначить группу

☐ Полное имя ↑↓

Тип учетной записи ↑↓

☐ ksmm

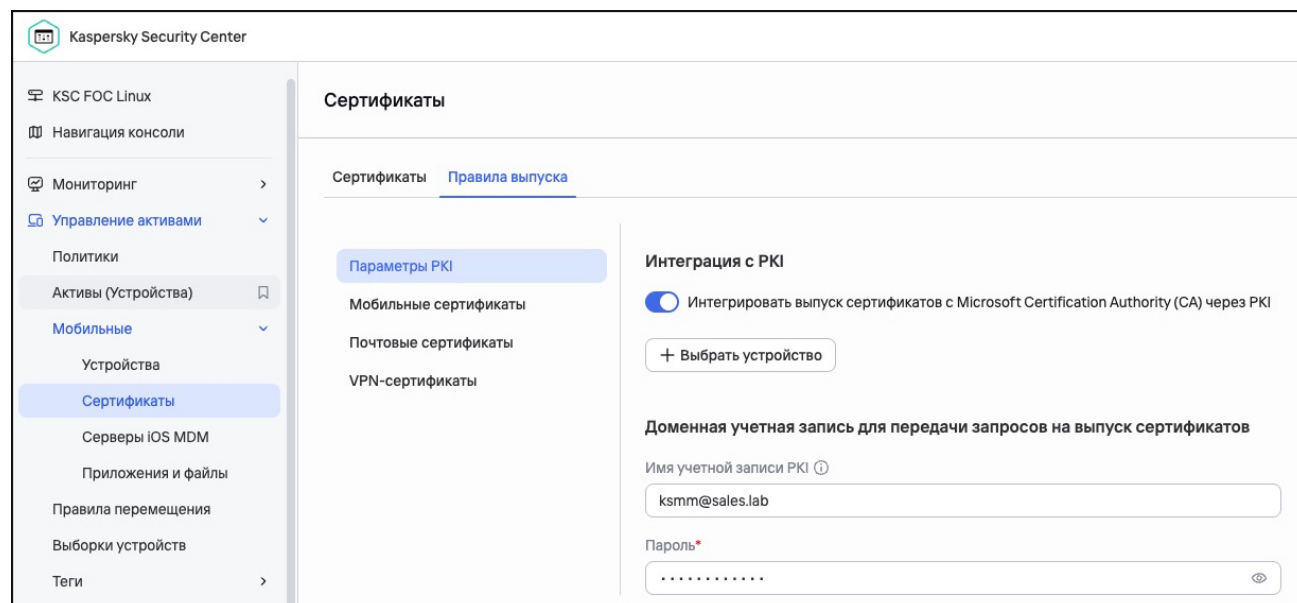
Доменный

Всего 1 / Выбрано 0

Скриншот 14. Наличие доменной УЗ на KSC.

Перейдите [Управление активами](#) → [Мобильные](#) → [Сертификаты](#) → [Правила выпуска](#) → [Параметры PKI](#).

1. Включите **Интегрировать выпуск сертификатов с Microsoft Certification Authority (CA) через PKI**.
2. Нажмите **Выбрать устройство** и укажите подготовленный Windows-узел с Агентом администрирования.
3. В поле **Имя учетной записи PKI** введите UPN сервисной учетной записи (обязательно в формате userPrincipalName@DNSDomainName).
4. Введите доменный пароль и сохраните настройки.



Скриншот 15. Включение интеграции с Microsoft CA и указание сервисной учетной записи в KSC Web Console.

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

После сохранения параметров обновите список шаблонов сертификатов в правилах выпуска и проверьте, что Kaspersky Security Center получает данные от Microsoft CA. Затем выполните тестовый выпуск нужного типа сертификата для доменного пользователя.

Проверьте следующее:

- Windows-посредник выбран в Параметрах PKI и подключен к Kaspersky Security Center.
- Сервисная учетная запись указана в формате UPN, пароль актуален.
- Создан постоянный профиль учетной записи и в `Current User → Personal` присутствует сертификат Enrollment Agent.
- Назначено право **Log on as a service**.
- На CA есть **Issue and Manage Certificates**.
- На шаблоне Enrollment Agent есть **Read** и **Enroll**, шаблон опубликован.
- Windows-посредник и CA находятся в одном домене, сетевое соединение Агента администрирования работает.

“ i Если право **Log on as a service** задается доменной GPO, локальное изменение через `secpol.msc` может быть перезаписано. Назначьте право в соответствующей групповой политике.

8. ?????? ?????????????? ?????? PKI ?? ????????????? ??????????????

После настройки интеграции Kaspersky Security Center может использовать Microsoft CA для выпуска пользовательских сертификатов, которые затем применяются на мобильных устройствах. В KSMM через PKI предусмотрен выпуск **почтовых** и **VPN-сертификатов**. В качестве источника используется опубликованный на Microsoft CA шаблон, доступный сервисной учетной записи интеграции.

“ ⚠ Не путайте мобильный сертификат Kaspersky Security Center с сертификатом, выпущенным Microsoft CA.

В интерфейсе KSC тип **Мобильный сертификат** используется для идентификации мобильного устройства при подключении к Серверу администрирования. Выбор PKI-шаблона Microsoft CA в актуальной версии KSMM 10 предусмотрен в разделах **Почтовые сертификаты** и

VPN-сертификаты.

Таким образом, настроенная в предыдущем разделе связка выглядит следующим образом:

KSC → Агент администрирования на Windows → сервисная учетная запись → Enrollment Agent → Microsoft CA → пользовательский сертификат → мобильное устройство

8.1. ?????????? ??????? ??? ?????????? ????????????????

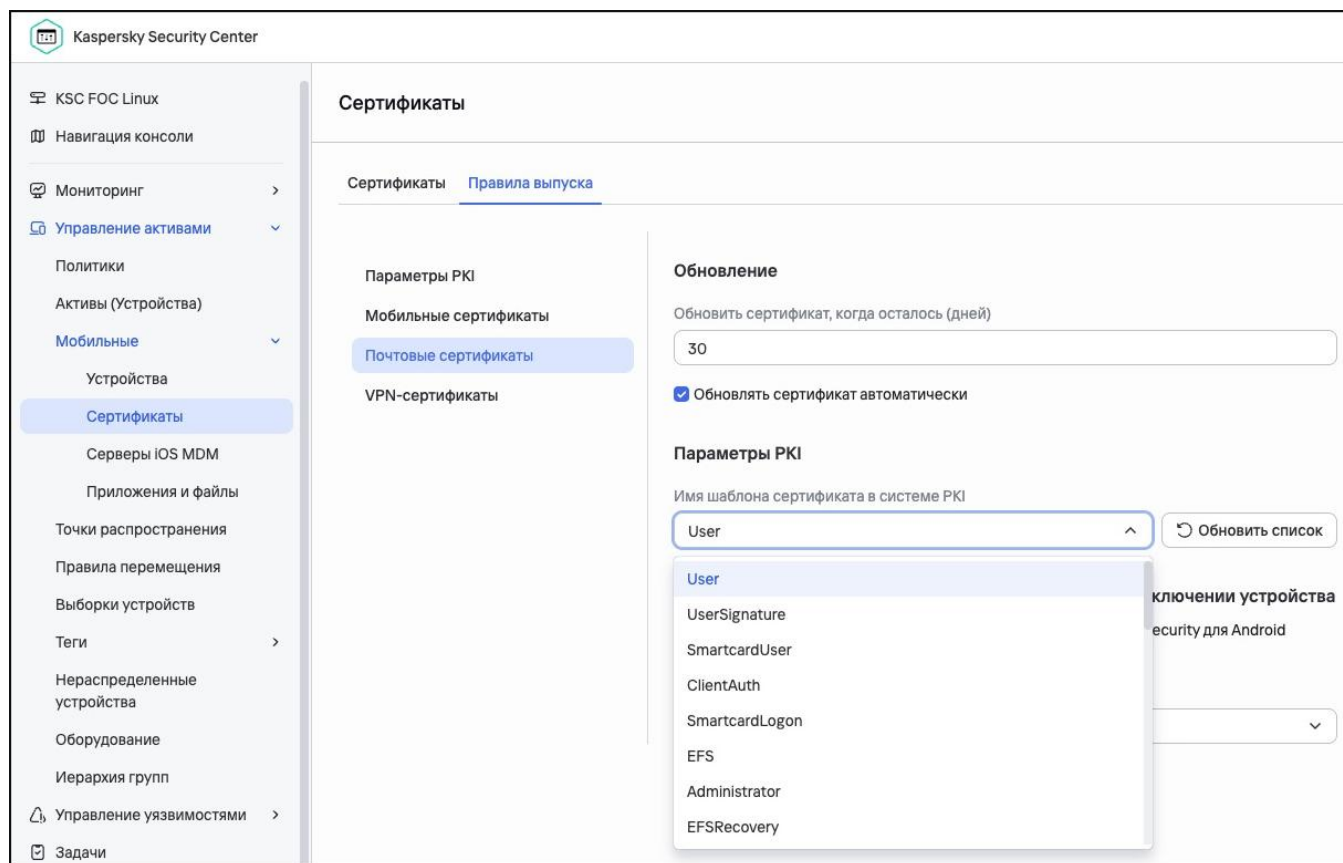
Перейдите:

Активы (Устройства) → Мобильные → Сертификаты → Правила выпуска

Откройте раздел **Почтовые сертификаты** или **VPN-сертификаты** в зависимости от требуемого сценария.

Перед использованием убедитесь, что шаблон опубликован на СА и его параметры соответствуют назначению сертификата: требованиям VPN-шлюза, Exchange, Wi-Fi или другого сервиса.

В блоке **Параметры PKI** обновите список шаблонов и в поле **Имя шаблона сертификата в системе PKI** выберите шаблон Microsoft CA, предназначенный для выпуска пользовательских сертификатов. Именно этот шаблон Kaspersky Security Center будет использовать при формировании запроса в СА.



Скриншот 16. Выбор шаблона сертификата.

“ ⚠ Речь идет не о шаблоне **Enrollment Agent**, который мы настраивали ранее. Enrollment Agent необходим сервисной учетной записи KSC для выполнения регистрации сертификатов от имени пользователей. На этом этапе выбирается **целевой шаблон**, сертификаты которого должны получать пользователи мобильных устройств.

8.2. ?????????? ?????????????????????? ????????? ????????????????????

Для почтовых и VPN-сертификатов Kaspersky Security Center может автоматически отправлять запрос в Microsoft CA при подключении мобильного устройства.

В соответствующем разделе **Правила выпуска** включите автоматический выпуск для нужного типа устройств:

- **Выпускать для устройств под управлением Kaspersky Endpoint Security для Android;**

- **Выпускать для iOS MDM-устройств.**

Для сертификатов iOS дополнительно указывается **псевдоним сертификата**. Этот псевдоним связывает выпущенный сертификат с настройками политики, например с конфигурацией корпоративной почты, VPN или Wi-Fi.

Параметры PKI

Мобильные сертификаты

Почтовые сертификаты

VPN-сертификаты

Обновление

Обновить сертификат, когда осталось (дней)

30

☒ Обновлять сертификат автоматически

Параметры PKI

Имя шаблона сертификата в системе PKI

User

Обновить список

Автоматический выпуск почтового сертификата при подключении устройства

☒ Выпускать для устройств под управлением Kaspersky Endpoint Security для Android

☒ Выпускать для iOS MDM-устройств

Псевдоним сертификата*

Почтовый сертификат 1

Скриншот 17. Включение автовыпуска сертификата.

“□ Для постоянной эксплуатации автоматический выпуск обычно удобнее ручного: после регистрации устройства KSC сам инициирует обращение через Windows-посредник к Microsoft CA и получает сертификат для соответствующего доменного пользователя.

В тех же правилах можно включить **автоматическое обновление** сертификатов и указать, за сколько дней до окончания срока действия KSC должен инициировать перевыпуск.

8.3. ??????? ??????? ?????????????? ?????? ??????? KSC

Для проверки интеграции или единичного выпуска сертификат можно запросить вручную.

Перейдите [Активы \(Устройства\) → Мобильные → Сертификаты](#)

Нажмите **Добавить**. Откроется **Мастер выпуска сертификата**. Набор шагов мастера может различаться в зависимости от типа сертификата, операционной системы и настроенных правил выпуска.

Выполните следующие действия:

1. На шаге **Тип сертификата** выберите **Почтовый сертификат** или **VPN-сертификат**.
2. Укажите операционную систему целевого устройства — **Android** или **iOS**.
3. Для Android при необходимости выберите вариант подключения с использованием или без использования мобильного сертификата KSC.
4. На шаге **Пользователи** выберите доменного пользователя, для которого будет выпущен сертификат.
5. На шаге выбора источника сертификата установите **Интегрировать выпуск с Microsoft CA через PKI**.
6. В поле **Шаблон PKI** выберите требуемый шаблон, импортированный из Microsoft CA.
7. Укажите способ передачи пользователю информации, необходимой для установки сертификата.
8. На последнем шаге проверьте параметры и нажмите **Подтвердить и выпустить сертификат**.

Если PKI настроена правильно, KSC передаст запрос на выбранный Windows-узел. Агент администрирования запустит операцию от имени указанной в настройках PKI доменной сервисной учетной записи, а Microsoft CA выпустит пользовательский сертификат на основании выбранного шаблона.

После завершения мастера новый сертификат появится в общем списке **Активы** (Устройства) → Мобильные → Сертификаты

Мобильные / Сертификаты

Сертификаты Правила выпуска

Мобильные сертификаты: 611

+ Добавить

Обновить

Удалить

Изменить псевдоним

☐	Дата выпуска	Имя пользователя	Статус	Тип
☐	01.10.2026, 13:17:15	Sergey	Сертификат применен	VPN
☐	01.10.2026, 12:04:33	Sergey	Сертификат применен	Почтовый
☐	30.09.2026, 17:00:05	Sergey	Сертификат выпущен	Мобильный

Информация о сертификате

Имя пользователя

Sergey

Статус

Сертификат применен

Тип

VPN

Протокол

Kaspersky Endpoint Security

Источник

PKI

Дата истечения

01.10.2027, 13:07:17

Дата выпуска

01.10.2026, 13:17:15

Последнее изменение статуса

01.10.2026, 13:17:32

Псевдоним

Автоматическое обновление включено

Да

Отпечаток

88 B4 D6 03 B7 CB 22 28 1C

Скриншот 18. Просмотр параметров сертификата.

Для него можно проверить пользователя, статус, тип, источник, дату выпуска, дату окончания срока действия, псевдоним и отпечаток.

“ ⚠ **Пользователь должен корректно разрешаться в домене.** При попытке выпуска сертификата владельцу мобильного устройства, который не является доменным пользователем, операция через PKI может завершиться ошибкой.

8.4. ? ?????????? ?????????????? ?? Android

На Android почтовые и VPN-сертификаты передаются через Kaspersky Endpoint Security для Android. На корпоративных устройствах и устройствах с корпоративным контейнером такие сертификаты могут устанавливаться автоматически. Для почтового сертификата должна быть заранее настроена учетная запись Exchange ActiveSync.

VPN-сертификат также можно установить в личное хранилище сертификатов Android. В этом случае пользователь получает уведомление в Kaspersky Endpoint Security и подтверждает установку сертификата. Приложение отображает пароль сертификата, после чего Android запрашивает его при импорте. [Справка](#)

Таким образом, в случае Android важно различать два процесса, что **выпуск сертификата происходит централизованно в KSC через Microsoft CA**, а непосредственная установка и использование сертификата зависят от режима управления устройством и настроек политики.

8.5. ? ?????????????????? ?????????????????? ?? iOS MDM

Для iOS MDM выпущенному сертификату можно назначить **псевдоним**. Затем этот псевдоним выбирается в параметрах соответствующей политики — например, при настройке корпоративной почты, Exchange, VPN или Wi-Fi. [Справка](#)

Иными словами, сам факт успешного выпуска сертификата еще не означает, что iOS автоматически начнет использовать его для конкретного подключения. Необходимо связать сертификат по псевдониму с нужной конфигурацией.

Практически схема выглядит так Microsoft CA → KSC → сертификат пользователя → псевдоним → профиль iOS MDM → Mail / VPN / Wi-Fi

Это удобно, поскольку администратор может централизованно определить, какой тип сертификата должен применяться конкретной корпоративной настройкой.

8.6. ???????? ?????????? ?????? ????????????

PKI

Если интеграция с Microsoft CA формально включена, но сертификат не выпускается, проверяйте цепочку от KSC до CA целиком. На практике чаще всего проблема находится в одном из следующих мест:

- Windows-посредник недоступен из KSC или Агент администрирования не синхронизирован;
- изменился пароль сервисной учетной записи;
- у нее отсутствует **Log on as a service**;
- сертификат Enrollment Agent отсутствует именно в `Current User → Personal` сервисной учетной записи на выбранном Windows-узле;
- Enrollment Agent истек или не содержит требуемого назначения;
- целевой шаблон не опубликован на Microsoft CA;
- шаблон не отображается в KSC после **Обновить список**;
- сервисной учетной записи или Enrollment Agent запрещена регистрация сертификатов по выбранному шаблону;
- пользователь мобильного устройства не является корректным доменным пользователем;
- параметры Subject/SAN или EKU шаблона не соответствуют требованиям VPN, Exchange или Wi-Fi.

“□ Для первичной проверки интеграции удобнее сначала выполнить **ручной выпуск одного сертификата**. Если он успешно появляется одновременно в KSC и в `Issued Certificates` Microsoft CA, после этого можно включать автоматическую выдачу для Android и iOS.

??????????

После выполнения этих шагов Kaspersky Security Center Linux может автоматически передавать через промежуточный Windows-узел запросы в Microsoft CA и использовать PKI как источник сертификатов для поддерживаемых сценариев Kaspersky Secure Mobility Management.

??????????

- Официальная справка Kaspersky: <https://support.kaspersky.ru/secure-mobility-management/10.0/286898>
- Настройка правил выпуска сертификатов: <https://support.kaspersky.ru/secure-mobility-management/10.0/287322>

Revision #4

Created 1 October 2026 13:20:24 by Сергей

Updated 1 October 2026 20:14:36 by Сергей