

Касперский Касперский Password Manager for Business B26.0 Linux

“ Инструкция составлена на основе [официальной документации](#) и опыта эксплуатации.
Дата исправления: 01.09.2026

1. Требования к серверу

Для корректной работы Kaspersky Password Manager for Business сервер должен соответствовать следующим требованиям:
Для сервера KPM:

Параметр	Значение
CPU	4 ядра, 2.5 ГГц или выше
RAM	6 ГБ или более
Диск	Свободное место 10 ГБ или больше
ОС	Debian 11/12, Ubuntu 22.04/24.04 LTS, Astra Linux SE 1.8.3.8 / 7.6 (x64)
СУБД	MySQL 8.0, MariaDB 10.6/10.11, PostgreSQL 14.x/15.x, Postgres Pro 14.x/15.x, Platform V Pangolin 5.4.0/6.1.0, Jatoba 4.

Важно: Свободное место на диске рассчитывается по формуле $N \times S$, где N - количество планируемых пользователей, S - объем памяти, выделенный на одно хранилище. Полученное значение суммируется с минимальным значением в таблице.

Отдельно или на этом же сервере должен быть развернут KSC для установки плагина в веб интерфейс для управления KPM4B.

Kaspersky Password Manager for Business поддерживает работу со следующими версиями Kaspersky Security Center:

- Kaspersky Security Center Windows 15.1 Update 2 или выше; ([Подробнее про требования](#))
- Kaspersky Security Center Linux 15.1 Update 2 или выше. ([Подробнее про требования](#))

Важно: Если KSC устанавливается рядом с сервером KPM, на сервер KPM необходимо установить Агент администрирования KSC.

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

Порты, используемые Kaspersky Password Manager for Business					
Номер порта (по умолчанию)	Имя процесса	Имя службы	Протокол	Тип соединения	Описание
3000	dotnet.exe KL.Kpm.B2B.ServerApp.dll	Kaspersky Password Manager for Business Web API	TCP (HTTPS)	Входящее	Прием запросов от клиента Kaspersky Password Manager for Business (Synchronization API) и Kaspersky Password Manager for Business веб-плагинов (Management API).
1433	dotnet.exe KL.Kpm.B2B.ServerApp.dll	Kaspersky Password Manager for Business Web API	TCP	Исходящее	Взаимодействие с базой данных SQL Server.

3306	dotnet.exe KL.Kpm.B2B.ServerApp.dll	Kaspersky Password Manager for Business Web API	TCP	Исходящее	Взаимодействие с базой данных MySQL или MariaDB.
5432	dotnet.exe KL.Kpm.B2B.ServerApp.dll	Kaspersky Password Manager for Business Web API	TCP	Исходящее	Взаимодействие с базой данных PostgreSQL, Jatoba или Pangolin.
389	dotnet.exe KL.Kpm.B2B.ServerApp.dll	Kaspersky Password Manager for Business Web API	TCP (LDAP)	Исходящее	Взаимодействие с сервером LDAP (соединение без TLS).
636	dotnet.exe KL.Kpm.B2B.ServerApp.dll	Kaspersky Password Manager for Business Web API	TCP (LDAPS)	Исходящее	Взаимодействие с сервером LDAP (соединение с TLS).
80	dotnet.exe KL.Kpm.B2B.ServerApp.dll	Kaspersky Password Manager for Business Web API	TCP (HTTPS)	Исходящее	Взаимодействие с сервером OAuth2 (SSO).
88	dotnet.exe KL.Kpm.B2B.ServerApp.dll	Kaspersky Password Manager for Business Web API	TCP/UCP	Исходящее	Kerberos аутентификация.
5055	dotnet.exe KL.Kpm.B2B.Job Agent.dll	Kaspersky Password Manager for Business Job Agent	TCP (HTTP)	Входящее	Прием запросов на Health-Check эндпоинт.
1433	dotnet.exe KL.Kpm.B2B.Job Agent.dll	Kaspersky Password Manager for Business Job Agent	TCP	Исходящее	Взаимодействие с базой данных SQL Server.
3306	dotnet.exe KL.Kpm.B2B.Job Agent.dll	Kaspersky Password Manager for Business Job Agent	TCP	Исходящее	Взаимодействие с базой данных MySQL или MariaDB.

5432	dotnet.exe KL.Kpm.B2B.Job Agent.dll	Kaspersky Password Manager for Business Job Agent	TCP	Исходящее	Взаимодействи е с базой данных PostgreSQL, Jatoba или Pangolin.
389	dotnet.exe KL.Kpm.B2B.Job Agent.dll	Kaspersky Password Manager for Business Job Agent	TCP (LDAP)	Исходящее	Взаимодействи е с сервером LDAP (соединение без TLS).
636	dotnet.exe KL.Kpm.B2B.Job Agent.dll	Kaspersky Password Manager for Business Job Agent	TCP (LDAPS)	Исходящее	Взаимодействи е с сервером LDAP (соединение с TLS).
25	dotnet.exe KL.Kpm.B2B.Job Agent.dll	Kaspersky Password Manager for Business Job Agent	TCP (SMTP)	Исходящее	Взаимодействи е с сервером SMTP (соединение без TLS).
587	dotnet.exe KL.Kpm.B2B.Job Agent.dll	Kaspersky Password Manager for Business Job Agent	TCP (SMTPS)	Исходящее	Взаимодействи е с сервером SMTP (соединение с TLS).
88	dotnet.exe KL.Kpm.B2B.Job Agent.dll	Kaspersky Password Manager for Business Job Agent	TCP/UCP	Исходящее	Kerberos аутентификаци я.
48093	dotnet.exe KL.Kpm.B2B.Job Agent.dll	Kaspersky Password Manager for Business Job Agent	TCP (HTTP/gRPC)	Исходящее (localhost)	Прием запросов от Kaspersky Password Manager for Business Job Agent (только для Windows).
48093	kpm_licensing.e xe	Служба лицензировани я Kaspersky Password Manager for Business	TCP (HTTP/gRPC)	Исходящее (localhost)	Взаимодействи е со службой лицензировани я Kaspersky Password Manager for Business (только Windows).

3. Установка PostgreSQL

3.1 Установка PostgreSQL

PostgreSQL 15

Установка:

```
apt update
apt install postgresql -y
systemctl enable --now postgresql
```

Подключиться к PostgreSQL и задать пароль суперпользователя:

```
sudo -u postgres psql
ALTER USER postgres WITH PASSWORD 'ПАРОЛЬ';
```

При установке KPM автоматически создаст базу `KpmDb` и сервисного пользователя `KpmServiceUser` с ограниченными правами.

3.2 Настройка SMTP

SMTP-сервер используется для отправки уведомлений и кодов подтверждения пользователям. Рекомендуется использовать отдельную сервисную учётную запись с минимальными правами:

- аутентификация на SMTP-сервере;
- отправка электронных сообщений.

Для подключения потребуются: FQDN SMTP-сервера, порт и учётные данные (если используется аутентификация). Если почтовый трафик шифруется по SSL/TLS, сертификат удостоверяющего центра, которым подписан сертификат SMTP-сервера, должен быть в списке доверенных на сервере KPM.

3.3 Настройка сертификатов

Для работы KPM требуются два набора сертификатов:

Серверный сертификат (PFX) - зашифрованный контейнер с сертификатом и закрытым ключом (serverAuth). Используется для защищённого соединения между сервером KPM, клиентскими приложениями и KSC.

Сертификат аутентификации администратора (PFX) - зашифрованный контейнер с сертификатом и закрытым ключом (clientAuth). Используется для аутентификации администратора.

Требования:

- Алгоритмы ключа: RSA / ECDSA / DSA
- Хеш: SHA-256 или SHA-384
- Обязательные поля: DN, DNS или SPN, KU, EKU, SAN
- KU: KeyEncipherment + DigitalSignature
- EKU сервера: 1.3.6.1.5.5.7.3.1 (serverAuth)
- EKU администратора: 1.3.6.1.5.5.7.3.2 (clientAuth)
- Рекомендуется включать в EKU обе аутентификации (server + client)
- SAN обязательно содержит FQDN и/или IP хоста KPM
- При использовании Kerberos адрес в клиенте должен совпадать с SPN

Пример

```
#Корневой CA
openssl genrsa -out ca.key 4096
openssl req -x509 -new -nodes -key ca.key -sha256 -days 3650 \
    -out ca.crt -subj "/C=RU/O=НАЗВАНИЕ_КОМПАНИИ/CN=НАЗВАНИЕ_КОМПАНИИ Root CA"

#Серверный сертификат
openssl req -new -nodes -newkey rsa:2048 \
    -keyout server.key -out server.csr \
    -subj "/C=RU/O=НАЗВАНИЕ_КОМПАНИИ/CN=DNS_ИМЯ_СЕРВЕРА"

openssl x509 -req -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial \
    -out server.cer -days 365 -sha256 \
    -extfile <(echo "keyUsage=digitalSignature,keyEncipherment
extendedKeyUsage=serverAuth,clientAuth
subjectAltName=DNS:DNS_ИМЯ_СЕРВЕРА,IP:IP_АДРЕС_СЕРВЕРА")

openssl pkcs12 -export -legacy \
    -in server.cer -inkey server.key -certfile ca.crt \
    -out server.pfx -passout pass:ПАРОЛЬ

#Сертификат аутентификации администратора
openssl req -new -nodes -newkey rsa:2048 \
    -keyout admin.key -out admin.csr \
```

```
-subj "/C=RU/O=НАЗВАНИЕ_КОМПАНИИ/CN=kpm-admin"
```

```
openssl x509 -req -in admin.csr -CA ca.crt -CAkey ca.key -CAcreateserial \
-out admin.cer -days 365 -sha256 \
-extfile <(echo "keyUsage=digitalSignature,keyEncipherment
extendedKeyUsage=clientAuth,serverAuth
subjectAltName=DNS:DNS_ИМЯ_СЕРВЕРА,IP:IP_АДРЕС_СЕРВЕРА")

openssl pkcs12 -export -legacy \
-in admin.cer -inkey admin.key -certfile ca.crt \
-out admin.pfx -passout pass:ПАРОЛЬ
```

3.4 ?????????? ?????????? ?????????? ??????? ???????

Для запуска служб КРМ необходимо создать непривилегированного пользователя и группу безопасности:

```
adduser kpm
groupadd kpmadmins
gpsswd -a kpm kpmadmins
usermod -g kpmadmins kpm
```

Имя пользователя и группы указываются при настройке `kpmctl postinstall`. Службы КРМ (`kpm-api`, `kpm-worker`, `kpm-licensing`) будут запускаться от имени этой учётной записи.

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

1. Скачайте установочный файл с [сайта "Лаборатории Касперского"](#).
2. Выберите файл, соответствующий дистрибутиву Linux, установленному на вашем устройстве: Debian x64 | Server.
3. Перенесите скачанный файл на сервер КРМ.
4. Перейдите в папку с файлом.

Для установки сервера Kaspersky Password Manager for Business необходимо выполнить команды, приведенные в инструкциях ниже, под учетной записью пользователя с правами `root`.

5. Запустите установку сервера Kaspersky Password Manager for Business:

```
apt install kpmserver_<version number>-<build_version>_amd64.deb  
или  
dpkg -i kpmserver_<version number>-<build_version>_amd64.deb
```

6. Запустите настройки сервера Kaspersky Password Manager for Business в интерактивном режиме:

```
sudo /opt/kaspersky/kpmserver/kpmctl/kpmctl postinstall
```

Скрипт последовательно запрашивает значения необходимых параметров для настройки сервера Kaspersky Password Manager for Business, проверяет каждый ввод и генерирует итоговый файл *appsettings.json*.

Мастер интерактивной настройки проведет вас через следующие этапы конфигурации:

1. Принятие Лицензионного соглашения.
2. Принятие Политики конфиденциальности.
3. Настройка использования параметров из ранее сохраненной резервной копии, если она доступна.
 - Указание пути для сохранения резервной копии.
 - Указание пароля резервной копии.
4. Настройка службы лицензирования.
5. Указание группы безопасности для служб сервера Kaspersky Password Manager for Business.
6. Указание имени аккаунта службы.
7. Выбор способа аутентификации (Domain, Basic, или OAuth).
 - Если выбрана аутентификация с помощью SSO:
 - Указание URL центра авторизации (Authority).
 - Указание идентификатора клиента (Audience).
 - Если выбрана доменная аутентификация:
 - Указание домена LDAP.
 - Указание сервера LDAP.
 - Включение или отключение SSL для соединения с LDAP.
 - Указание порта LDAP-сервера.
 - Указание типа аутентификации LDAP. Для базовой аутентификации укажите имя пользователя и пароль LDAP.
8. Если доменная аутентификация отключена, включите или отключите **LDAP User Status Check**. Если проверка статуса включена, перейдите к шагу 7.
9. Выбор типа базы данных.
10. Настройка подключения к базе данных:

- Указание типа базы данных.
- Указание адреса базы данных.
- Указание номера порта базы данных.
- Указание имени базы данных.
- Указание логина базы данных.
- Указание пароля базы данных.

11. Указание адреса электронной почты отправителя SMTP.
12. Указание адреса сервера SMTP.
13. Включение или отключение SSL для SMTP-соединения.
14. Указание порта SMTP-сервера.
15. Указание типа аутентификации SMTP.
16. Указание имени пользователя SMTP.
17. Указание пароля пользователя SMTP.
18. Указание порта сервера Kaspersky Password Manager for Business.
19. Указание PFX-контейнера для сервера Kaspersky Password Manager for Business.
20. Указание пароля для PFX-контейнера.
21. Указание сертификата сервера Kaspersky Password Manager for Business.
22. Указание пароля организации.
23. Подтверждение пароля организации.

Не рекомендуется повторно запускать процедуру первоначальной настройки. Для обновления файлов конфигурации используйте команду `kpmctl modify`.

5. Настройка KSC

5.1 Настройка агента администрирования

Для управления устройствами организации требуется установить на сервер KPM и на клиентские устройства Агент администрирования. Вы можете установить Агент администрирования [удаленно](#), [в интерактивном режиме](#) или [в тихом режиме](#).

Удаленная установка Агента администрирования

1. Перейдите во вкладку Инсталляционные пакеты в веб-интерфейсе KSC. Выберите Добавить:

KSC FOC Linux

Навигация консоли

Мониторинг

Управление активами

Управление уязвимостями

Задачи

Приложения и службы

Пользователи и роли

Хранилища

Управление программным обеспечением

Инсталляционные пакеты

Приложения "Лаборатории"

KSC FOC Linux

Управляемые устройства

Инсталляционные пакеты

Скрыть иерархиюKSC FOC Linux

+ Добавить

X Удалить

Обновить

+ Развернуть

Просмотреть список автономно

Поиск...

Имя	Статус инсталляционн...	Источник
Все готово к установке		
iOS MDM Server for Linux x64 deb (English)_15.4.0.2019	Все готово к установке	АО "Лабо...
KES 14.0.0.504 LE	Все готово к установке	АО "Лабо...
Kaspersky Endpoint Security для Windows 12.12.0 (Русский) (Lite encryption)_12.12.0	Все готово к установке	АО "Лабо...
Kaspersky Endpoint Security for Mac (Русский)_12.2.1.191	Все готово к установке	АО "Лабо...
Агент администрирования Kaspersky Security Center для Windows (16) (Русский)_16	Все готово к установке	АО "Лабо...
Kaspersky Endpoint Security 12.4 для Linux (Русский)_12.4.0.1225	Все готово к установке	АО "Лабо...
Kaspersky Network Agent for Linux (Русский)_16.3.0.1207	Все готово к установке	АО "Лабо...

2. Выберите пункт Создать инсталляционный пакет для приложения Лаборатория касперского:

Мастер создания инсталляционного пакета

Выбор типа инсталляционного пакета

☒ Создать инсталляционный пакет для приложения "Лаборатории Касперского"

☐ Создать инсталляционный пакет из файла

☐ Выбрать приложение из базы "Лаборатории Касперского" для создания инсталляционного пакета

☐ Создать инсталляционный пакет для задачи "Удаленное выполнение скриптов" на основе архива ZIP с файлом manifest.json

3. Найдите последнюю версию и требуемый язык приложения. Скачайте нужный дистрибутив:

Текущие версии приложений

Группировать по: ОС (изменить группировку, используя фильтр)

Область защиты	Тип	Имя	Версия	Последняя версия	ОС	Язык	Добавлен
Linux							
Администрирование	Дистрибутив	Kaspersky Network Agent for Linux Legacy (Русский)	16.3.0.1207	Да	Linux	ru	24.07.2026 21:01:10
Администрирование	Дистрибутив	Kaspersky Network Agent for Linux (Русский)	16.3.0.1207	Да	Linux	ru	24.07.2026 21:01:10
Промышленные сети	Веб-плагин	Kaspersky Industrial CyberSecurity for Networks	4.5.1.12	Да	Linux	ru	15.07.2026 21:01:10
macOS							

Kaspersky Network Agent for Linux (Русский)

Область защиты

Администрирование

Тип

Используется в управляемой сети

Версия

Добавлен

ОС

Язык

Дистрибутив

16.3.0.1207

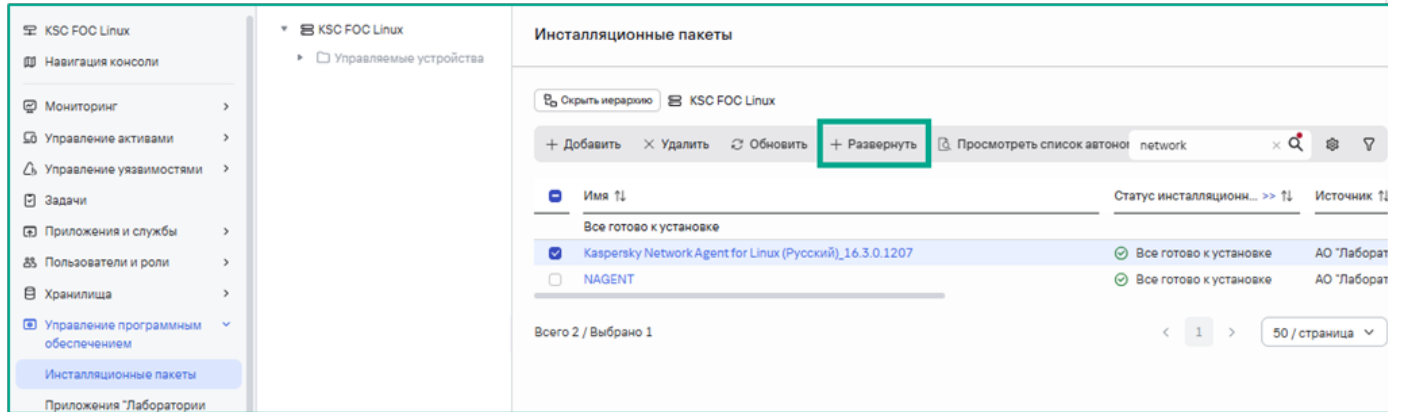
24.07.2026 21:01:10

Linux

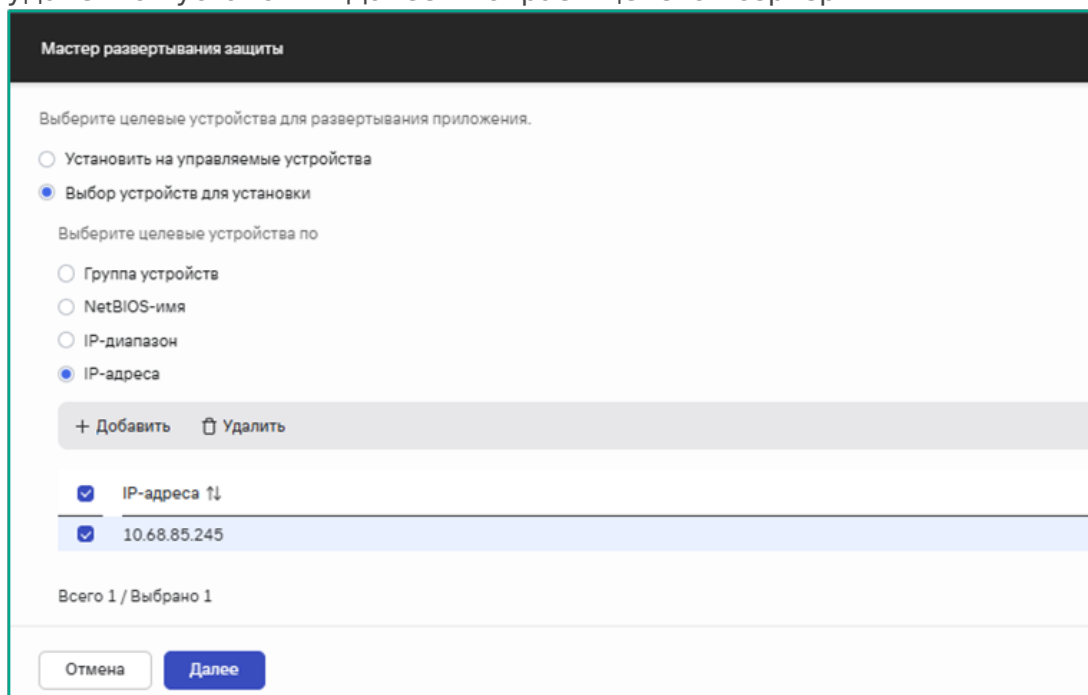
ru

Скачивание завершено

4. Перейдите обратно во вкладку Инсталляционные пакеты и найдите нужный дистрибутив. Выберите Развернуть:



5. В Мастере развертывания защиты выбираем Метод - С использованием задачи удаленной установки. Далее выбираем целевой сервер KPM:



6. В параметрах выбираем установку Средствами операционной системы:

The screenshot shows the 'Master of Protection Deployment' window with the 'Remote Installation Parameters' tab selected. The 'Task type' is 'Remote installation' and the 'Task name' is 'Task of remote application installation'. Under 'Forcefully download the installation package', the option 'By means of the operating system with the help of distribution points' is selected. A note states this parameter is necessary for Windows installation without the management agent. Other options like 'Do not install if already installed' and 'Assign installation to Active Directory group policies' are also visible. Navigation buttons 'Back' and 'Next' are at the bottom.

Мастер развертывания защиты

Параметры задачи удаленной установки

Тип задачи
Удаленная установка
Kaspersky Network Agent for Linux (Русский)_16.3.0.1207

Название задачи
Задача удаленной установки приложения

Длина имени задачи в этом поле ввода не может превышать 100 символов.

Принудительно скачать инсталляционный пакет

☐ С помощью Агента администрирования

☐ Средствами операционной системы с помощью точек распространения

Этот параметр необходим при установке приложения для Windows на устройство без Агента администрирования. [Узнать больше](#)

☒ Средствами операционной системы с помощью Сервера администрирования

☒ Не устанавливать приложение, если оно уже установлено

☐ Назначить установку инсталляционного пакета в групповых политиках Active Directory

Назад Далее

7. Далее идем по шагам Мастера развертывания защиты. Вводим учетную запись с правами на установку:

The screenshot shows the 'Master of Protection Deployment' window with the 'Select accounts for device access' step. The option 'Account is required (Management agent is not used)' is selected. A modal dialog titled 'Account details' is open, showing fields for 'Type' (Local or domain account), 'Username' (Administrator), and 'Password'. The 'OK' button is highlighted.

Мастер развертывания защиты

Выбор учетных записей для доступа к устройствам

☐ Учетная запись не требуется (Агент администрирования уже установлен)

☒ Учетная запись требуется (Агент администрирования не используется)

+ Добавить / Изменить / ↑ Вверх / ↓ Вниз / × Удалить

Имя ↑ Тип ↑

Нет информации

Всего 0

Назад Далее

Учетная запись

Тип
Локальная или доменная учетная запись

Учетная запись
Administrator

Формат доменной учетной записи: "domain\user" или "user@domain"

Пароль
.....

OK Отмена

8. Запускаем задачу после завершения работы мастера.

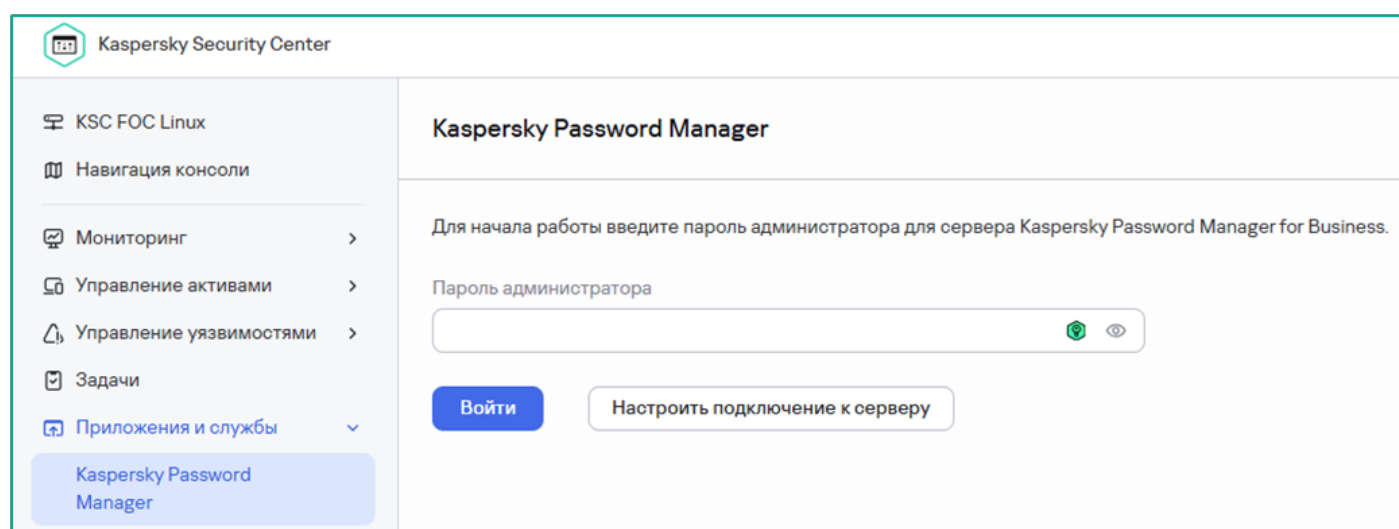
5.2 ?????????? ???-?????????

Веб-плагин необходимо установить в Kaspersky Security Center Web Console для управления приложением.

Чтобы вручную установить веб-плагин Kaspersky Password Manager for Business в Kaspersky Security Center Web Console, выполните следующие действия:

1. Скачайте .zip файл веб-плагина с [сайта "Лаборатории Касперского"](#).
2. Распакуйте файл .zip на компьютер, на котором установлена Kaspersky Security Center Web Console.
3. Откройте Kaspersky Security Center Web Console.
4. В главном меню перейдите в Параметры → Веб-плагины.
5. Нажмите на кнопку Добавить из файла.
6. Загрузите plugin.zip файл веб-плагина и signature.txt.
7. Нажмите Добавить.

Веб-плагин добавляется из файла и отображается в списке управления веб-плагинами. В боковой панели появляется отдельный вкладка с управлением KPM.



5.3 ?????????? ???-????????

Мастер быстрой установки запускается сразу после установки веб-плагина Kaspersky Password Manager for Business, что позволяет быстро настроить:

- Подключение к серверу Kaspersky Password Manager for Business
- Параметры политики Kaspersky Password Manager for Business
- Создание инсталляционного пакета Kaspersky Password Manager for Business

Если мастер был закрыт раньше времени, к этим действиям можно вернуться из отдельной вкладки управления KPM.

Чтобы указать параметры подключения к серверу Kaspersky Password Manager for Business:

1. Укажите полное доменное имя (FQDN) или IP-адрес устройства, на котором размещен сервер Kaspersky Password Manager for Business и которое доступно в сети, например: `https://kpm-server.example.com` или `https://192.168.1.100`.

2. Укажите номер порта сервера, указанный при настройке HTTPS. Номер порта должен быть в диапазоне от 0 до 65535. (Значение по умолчанию – 3000).

3. Загрузите открытый сертификат сервера (PEM/CER/DER).

Пример

Как начать использовать Kaspersky Password Manager for Business

1

Настройте соединение с сервером Kaspersky Password Manager for Business

2

Настроить политики

3

Создать установочный пакет

4

Настроить дополнительные политики и установить Kaspersky Password Manager for Business

Настройте соединение с сервером Kaspersky Password Manager for Business

Сервер Kaspersky Password Manager for Business обеспечивает синхронизацию, лицензирование, аутентификацию и хранение секретов. На этом шаге введите параметры подключения к серверу, чтобы администратор мог просматривать и управлять пользователями и их хранилищами через консоль.

Установите сервер Kaspersky Password Manager for Business

Прежде чем настраивать подключение, убедитесь, что сервер Kaspersky Password Manager for Business установлен и готов к работе. Подробнее смотрите в разделе [Справка](#)

[Как установить сервер Kaspersky Password Manager for Business](#)

Настройте подключение к серверу Kaspersky Password Manager for Business

Здесь необходимо указать настройки подключения к серверу Kaspersky Password Manager for Business.

Адрес сервера*

Порт*

Сертификат сервера*

Сертификат успешно загружен.

Кому выдан

localhost

Кем выдан

localhost

Действителен с

03.06.2026 01:08:40

Действителен по

03.06.2027 01:08:40

Авторизация на сервере Kaspersky Password Manager for Business

Здесь необходимо загрузить и расшифровать текущий PFX-контейнер, используя его пароль, а затем установить пароль администратора для сервера Kaspersky Password Manager for Business.*

2.50 KB

X

Пароль к закрытой части ключа для PFX-контейнера

Позже

Продолжить

4. Загрузите сертификат аутентификации администратора в формате PFX и пароль для контейнера PFX.

Пример

Авторизация на сервере Kaspersky Password Manager for Business

Здесь необходимо загрузить и расшифровать текущий PFX-контейнер, используя его пароль, а затем установить пароль администратора для сервера Kaspersky Password Manager for Business.*

2.50 KB X

Пароль к закрытой части ключа для PFX-контейнера

Установить пароль администратора*

Рекомендуется выбрать пароль длиной не менее 16 символов и соблюсти все требования к паролям для Kaspersky Password Manager for Business.

Подтвердить пароль администратора*

Позже Продолжить

5. Установите пароль администратора, который будет использоваться для аутентификации на сервере Kaspersky Password Manager for Business и доступа к веб-странице администрирования плагина Kaspersky Password Manager for Business.

6. Нажмите Продолжить.

5.4 ?????????? ?????????? KPM

На втором шаге мастера настраивается политика для клиентов KPM: правила восстановления мастер-пароля, требования к сложности паролей и дополнительные параметры безопасности.

Как начать использовать Kaspersky Password Manager for Business

1. Настройте соединение с сервером Kaspersky Password Manager for Business

2. **Настроить политики**

3. Создать установочный пакет

4. Настроить дополнительные политики и установить Kaspersky Password Manager for Business

Настройте политики сервера Kaspersky Password Manager for Business

To deploy Kaspersky Password Manager for Business on client machines and ensure proper functionality of the application, install Kaspersky Password Manager Server

1. Настроить политики вы можете в соответствующем разделе Kaspersky Security Center Web Console:
[Перейти в Активы \(Устройства\) —> Политики и профили политик](#)

Электронная почта администратора*

Укажите политику по восстановлению мастер-пароля
 Политика восстановления мастер-пароля позволяет сбрасывать пароль пользователя.

Выберите политику*

☒ **Запретить восстановление паролей**
 Если мастер-пароль потерян, его невозможно восстановить через администратора. Это повышает безопасность.

☐ По желанию пользователей
 Пользователь сам решает, что для него важнее — повышенная безопасность или восстановление пароля.

☐ Обязательно для всех пользователей
 Позволяет пользователям запрашивать восстановление мастер-пароля у администратора.

Требования к сложности мастер-пароля Принудительно ☒

Здесь вы можете указать требования к безопасности для мастер-паролей, паролей учетных записей сервера при базовой аутентификации, а также настроить Генератор паролей, если он используется для создания этих паролей.

Количество символов

☒ Обязательно использовать цифры
☒ Обязательно использовать строчные буквы
☒ Обязательно использовать заглавные буквы
☐ Обязательно использовать специальные символы

Требования к генерации паролей

Здесь вы можете указать настройки для Генератора паролей, которые будут применяться для паролей в хранилище пользователя.

Количество символов

☒ Использовать цифры

Пропустить Создать политику

5.5 ?????????? ?????????????? ?????????????? KPM

Удаленная установка клиентского приложения

1. Скачайте клиентское приложение с [сайта "Лаборатории Касперского"](#).
2. Перейдите во вкладку Инсталляционные пакеты в веб-интерфейсе KSC. Выберите Добавить:

The screenshot shows the KSC FOC Linux web interface. On the left is a navigation menu with options like 'Monitoring', 'Device Management', 'Vulnerability Management', 'Tasks', 'Applications and Services', 'Users and Roles', 'Storage', and 'Program Management'. The 'Program Management' section is expanded, showing 'Installation Packages'. The main area is titled 'Installation Packages' and contains a table of packages. A green box highlights the '+ Добавить' (Add) button. Below the table, there are buttons for 'Удалить' (Delete), 'Обновить' (Update), 'Развернуть' (Expand), and 'Просмотреть список автономных' (View list of offline).

Имя	Статус инсталляционн...	Источник
Все готово к установке		
IOS MDM Server for Linux x64 deb (English)_15.4.0.2019	✓ Все готово к установке	АО "Лабора
KES 14.0.0.504 LE	✓ Все готово к установке	АО "Лабора
Kaspersky Endpoint Security для Windows 12.12.0 (Русский) (Lite encryption)_12.12.0 >>	✓ Все готово к установке	АО "Лабора
Kaspersky Endpoint Security for Mac (Русский)_12.2.1.191	✓ Все готово к установке	АО "Лабора
Агент администрирования Kaspersky Security Center для Windows (16) (Русский)_16 >>	✓ Все готово к установке	АО "Лабора
Kaspersky Endpoint Security 12.4 для Linux (Русский)_12.4.0.1225	✓ Все готово к установке	АО "Лабора
Kaspersky Network Agent for Linux (Русский) 16.3.0.1207	✓ Все готово к установке	АО "Лабора

3. Выберите пункт Создать инсталляционный пакет из файла:

The screenshot shows the 'Master of creating installation package' form. It has a title bar 'Мастер создания инсталляционного пакета'. Below it, there is a section 'Выбор типа инсталляционного пакета' (Choose package type) with four radio button options. The second option, 'Создать инсталляционный пакет из файла' (Create installation package from file), is selected. At the bottom, there are two buttons: 'Отмена' (Cancel) and 'Далее' (Next).

Мастер создания инсталляционного пакета

Выбор типа инсталляционного пакета

- ☐ Создать инсталляционный пакет для приложения "Лаборатории Касперского"
- ☒ Создать инсталляционный пакет из файла
- ☐ Выбрать приложение из базы "Лаборатории Касперского" для создания инсталляционного пакета
- ☐ Создать инсталляционный пакет для задачи "Удаленное выполнение скриптов" на основе архива ZIP с файлом manifest.json

Отмена Далее

4. Подгружаем ранее скачанный архив с клиентом:

The screenshot shows the 'Master of creating installation package' form. It has a title bar 'Мастер создания инсталляционного пакета'. Below it, there is a section 'Новый пользовательский инсталляционный пакет' (New user installation package). It contains a text input field for 'Имя пакета' (Package name) with the value 'Новый инсталляционный пакет'. Below that, there is a section 'Выберите файл инсталляционного пакета, который вы хотите загрузить (поддерживаются форматы файлов ZIP, CAB, TAR и TAR.GZ)' (Choose the installation package file you want to upload). It contains a file upload field with the value 'kpmb_win_26.0.0.775_ru.zip'. At the bottom, there are two buttons: 'Назад' (Back) and 'Далее' (Next).

Мастер создания инсталляционного пакета

Новый пользовательский инсталляционный пакет

Имя пакета

Новый инсталляционный пакет

Выберите файл инсталляционного пакета, который вы хотите загрузить (поддерживаются форматы файлов ZIP, CAB, TAR и TAR.GZ)

kpmb_win_26.0.0.775_ru.zip

Обзор

Назад Далее

5. После того, как Мастер создаст пакет, перейдите обратно во вкладку
Инсталляционные пакеты и найдите нужный дистрибутив. Выберите Развернуть:

KSC FOC Linux

Навигация консоли

Мониторинг >

Управление активами >

Управление уязвимостями >

Задачи

Приложения и службы >

Пользователи и роли >

Хранилища >

Управление программным обеспечением

Инсталляционные пакеты

KSC FOC Linux

Управляемые устройства

Инсталляционные пакеты

Скрыть иерархию

KSC FOC Linux

+ Добавить

Удалить

Обновить

+ Развернуть

Просмотреть список автономных

Новый

Настройки

Фильтр

Имя ↑↓

Статус инсталляционн... >> ↑↓

Источник ↑

Все готово к установке

Новый инсталляционный пакет

Все готово к установке

АО "Лаборатория"

Всего 1 / Выбрано 1

< 1 >

50 / страница

6. В Мастере развертывания защиты выбираем Метод - С использованием задачи удаленной установки. Выбираем нужную версию агента администрирования: Агент администрирования Kaspersky Security Center для Windows. Если в списке нет нужной версии, то добавляем ее через выбор Добавить.

Мастер развертывания защиты

Выберите Агент администрирования, который будет установлен с установочным пакетом.

+ Добавить

✎ Изменить

⊞

Инсталляционные пакеты ↑↓

☐

Агент администрирования Kaspersky Security Center для Windows (16) (Русский)

☒

Агент администрирования Kaspersky Security Center для Windows (16) (Русский)

Всего 2 / Выбрано 1

Приложение: Агент администрирования Kaspersky Security Center для Windows (16) (Русский)

Версия: 16.3.0.1207

Язык: ru

Далее

7. Далее выбираем целевое устройство или выборку устройств:

Мастер развертывания защиты

Выберите целевое устройство

☐ Группа устройств

☐ NetBIOS-имя

☒ IP-диапазон

☐ IP-адреса

+ Добавить

✎ Удалить

☒

IP-диапазон ↑↓

☒

10.68.85.200 - 10.68.85.220

Отмена

Далее

8. В параметрах выбираем установку Средствами операционной системы, если агент администрирования ранее не был установлен:

9. Далее идем по шагам Мастера развертывания защиты. Вводим учетную запись с правами на установку:

10. Запустить задачу после завершения работы мастера.

????? 6. ????????????? ??????????

Чтобы добавить лицензионный ключ или код активации в хранилище Сервера администрирования:

1. Откройте Kaspersky Security Center Web Console.
2. В главном меню перейдите в Операции → Лицензирование → Лицензии "Лаборатории Касперского".
3. Нажмите на кнопку Добавить.
4. Выберите, что вы хотите добавить:
 - Добавить файл ключа
Нажмите на Выберите файл ключа и перейдите к файлу .key, который вы хотите добавить.
 - Ввести код активации
Укажите код активации в текстовом поле и нажмите на кнопку Отправить.
5. Выберите Автоматически распространять лицензионный ключ на управляемые устройства:

938C				
Общие	Устройства	О клиенте	Служба технической поддержки	Ограничения
Лицензионный ключ	938C			
Название лицензии	Kaspersky Password Manager for B2B European Edition. 10-14 User 1 year NFR License			
Тип лицензии	Коммерческая			
Срок действия (сут)	368			
Дата окончания срока действия лицензии	20.08.2027 03:00:00			
Дата окончания лицензионного ключа	20.08.2027 03:00:00			
Ограничение	14			
Используется Сервером администрирования	Не используется			
☒ Автоматически распространять лицензионный ключ на управляемые устройства				
Сохранить Отмена				

6. Нажмите на кнопку Закрыть.

Лицензионный ключ добавлен в хранилище Сервера администрирования и автоматически распространяется на все совместимые устройства.

Базовая настройка сервера Kaspersky Password Manager for Business завершена. На данном этапе выполнено: установка и настройка сервера KPM, настройка веб-плагина в KSC, настройка политики и развёртывание клиентского приложения на рабочие станции.

Revision #5

Created 1 September 2026 08:29:07 by Анна

Updated 2 September 2026 12:48:41 by Анна