Центр
Управления
Гетерогенными
Инфраструктурами

ЕХС. Инструкция по запуску продукта в демо-зоне

ООО «Клируэй Текнолоджис»

2026

Оглавление

1 Введение

Настоящий документ содержит информацию о процессе установки «Единого хранилища секретов — EXC», на ОС «Astra Linux 1.8» (далее система), а также инструкцию для доступа к уже готовому демо-стенду. На демо-стенде можно ознакомиться с функциональностью системы и протестировать её возможности.

> ⚠ Для выполнения всех действий требуются права локального администратора (Windows) или root (Linux).

2 Служба поддержки

По всем вопросам, связанных с установкой системы и доступу к демо-стенду, следует обращаться в техническую поддержку к сервисным инженерам.

Техническая поддержка работает круглосуточно и доступна по следующим каналам связи:

- Телефон: +7 (495) 142-41-42
- Email: support@clearwayintegration.com

3 Использование демо-стенда системы

3.1 Общая информация

Демо-стенд системы расположен во внутреннем контуре компании. Система развернута в минимальной версии и включает в себя сервер приложений, на котором находятся сервисы EXC, сервер Keycloak, сервер PostgreSQL, сервер Active Directory. Для доступа к демо-стенду необходимо настроить VPN, добавить в доверенные сертификаты и перейти на веб-интерфейс управления системой (см. раздел Вход в веб-интерфейс системы).

3.2 Пререквизиты

Программное обеспечение

VPN-клиент	Cisco AnyConnect Secure Mobility Client https://vpn.clearwayintegration.com
Веб-браузер	Любой современный браузер для доступа к интерфейсам управления
Операционная система	Windows или Linux (поддерживаются Debian/Ubuntu и RHEL/CentOS/Fedora)

Требования к аппаратным ресурсам

CPU	2 ядра
RAM	8 ГБ
HDD	70 ГБ

Учетные записи

	Назначение УЗ	Учетная запись	Пароль
1	VPN Адрес шлюза для VPN: 82.142.150.30	Для подключения по VPN запросите учетные данные администратора у сотрудников технической поддержки.	
2	Учетная запись для аутентификации в веб-интерфейсе EXC	consumer	DVI7KWBtdjMG

Сертификаты безопасности

Для корректной работы браузера и отсутствия ошибок SSL на компьютере, который используется для подключения к демо-стенду, необходимо установить следующие сертификаты:

- Root CA Cert (корневой сертификат);
- Sub CA Cert (промежуточный сертификат).

Целевые ресурсы

После настройки доступ осуществляется по адресу:

- Web-интерфейс EXC: https://min-ess.tst.itc.internal.

3.3 Схема развертывания компонентов продукта на демо-стенде

Ниже представлена схема компонентов системы, развернутой по адресу https://min-ess.tst.itc.internal.

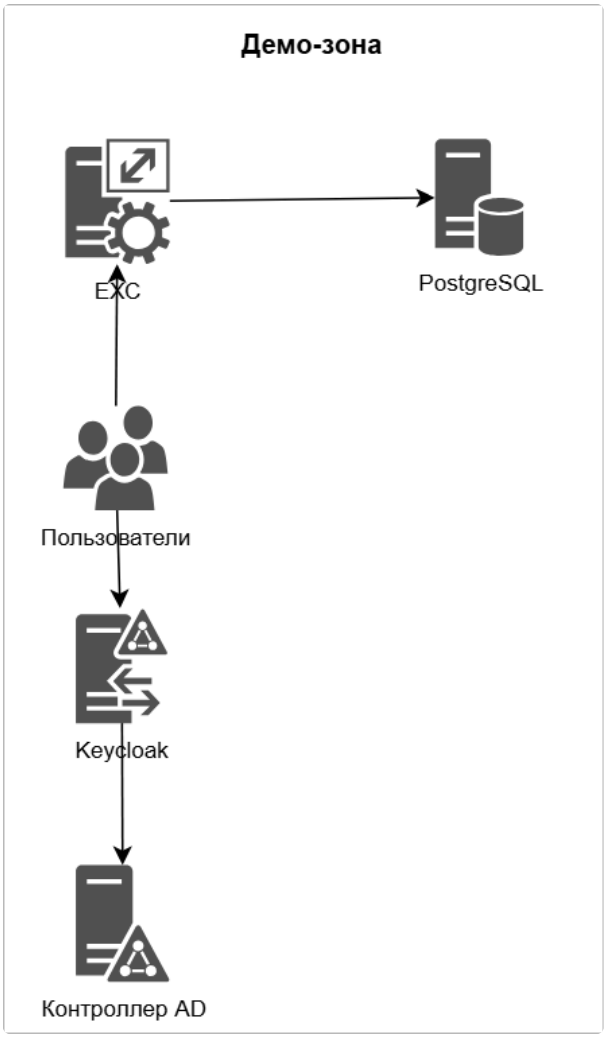


Рисунок 1 Схема компонентов EXC

1. Хост min-ess.tst.itc.internal — на этом хосте установлены компоненты EXC:

nginx	Web-сервер, реверс-прокси, балансировщик
ess	Единое хранилище секретов

2. Хост min-klck.tst.itc.internal - на этом хосте установлена система управления идентификацией и доступом Keycloak:

KeyCloak 26.0.7	Идентификация и управления доступом

3. Хост min-pgs.tst.itc.internal - на этом хосте установлена СУБД PostgreSQL:

PostgreSQL 15.14	Хранение данных

4. Список БД для функционирования данного ППО:

ess-ha
ess-transit

5. Хост min-dc.tst.itc.internal - на этом хосте установлен Контроллер AD:

ActiveDirectory	Служба каталогов

3.4 Настройка доступа к демо-стенду

Для настройки доступа к веб-интерфейсу управления системой выполните следующие шаги.

1. Запросите учетные данные для VPN у сотрудников технической поддержки.
2. Авторизуйтесь по VPN.
3. Добавьте в доверенные необходимые сертификаты для ОС Windows / ОС Linux.

3.4.1 Настройка VPN

Доступ во внутренний контур компании обеспечивается с помощью программы Cisco AnyConnect Secure Mobility Client.

Перед началом установки убедитесь, что:

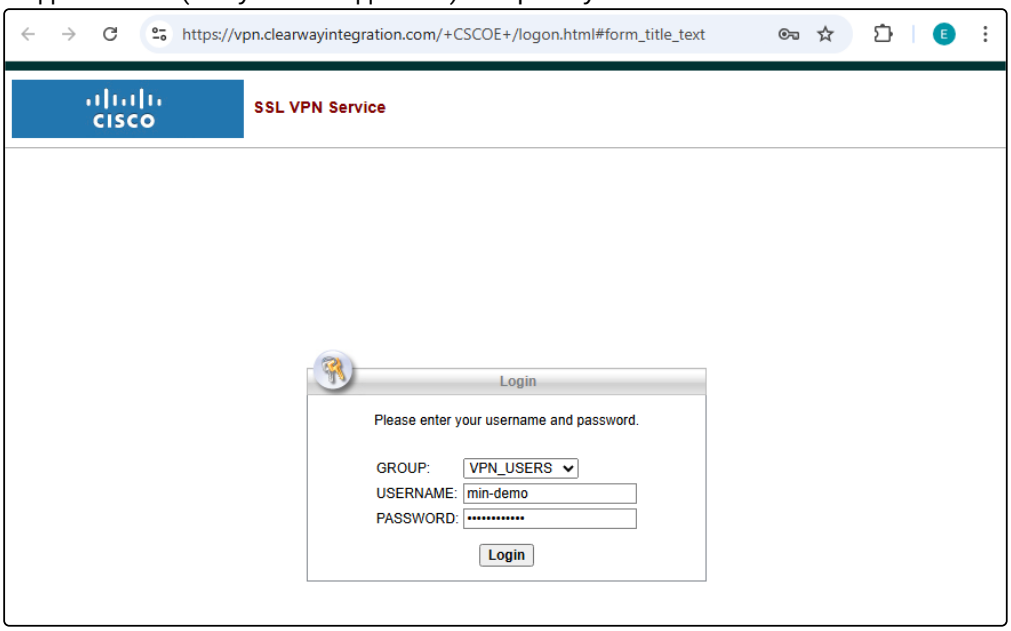
- вы выполняете инструкцию на рабочем компьютере, на котором будет осуществляться VPN-подключение к ресурсам компании;

- у вас есть права локального Администратора (Windows) или sudo (Linux/macOS);
- отключены другие VPN-соединения.

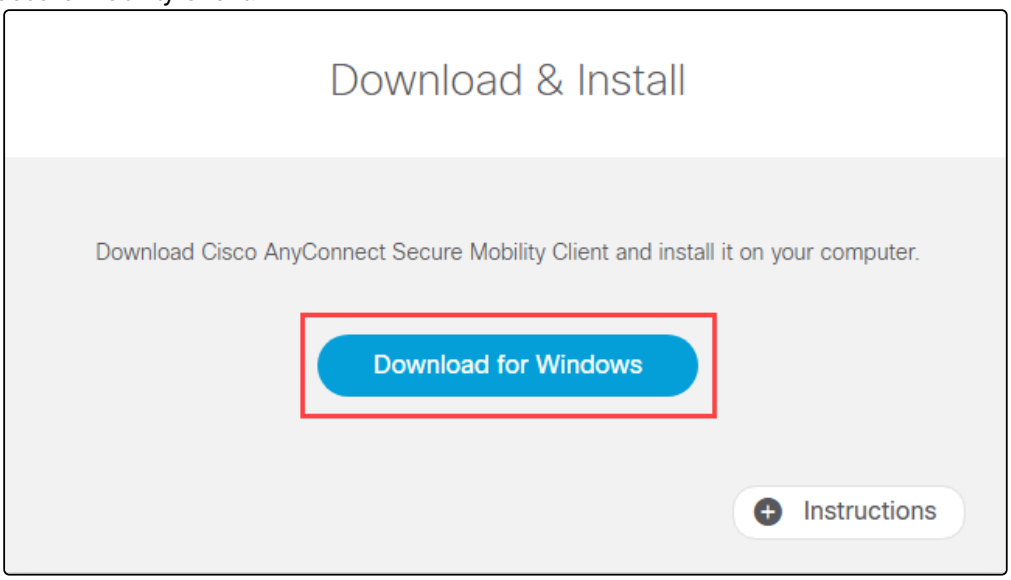
3.4.1.1 Первоначальная установка VPN-клиента

Если VPN-клиент Cisco AnyConnect уже установлен на вашем компьютере, пропустите этот раздел и перейдите к разделу Авторизация по VPN.

1. Откройте в браузере страницу https://vpn.clearwayintegration.com
   Введите логин (без указания домена) и пароль учетной записи VPN-клиента.



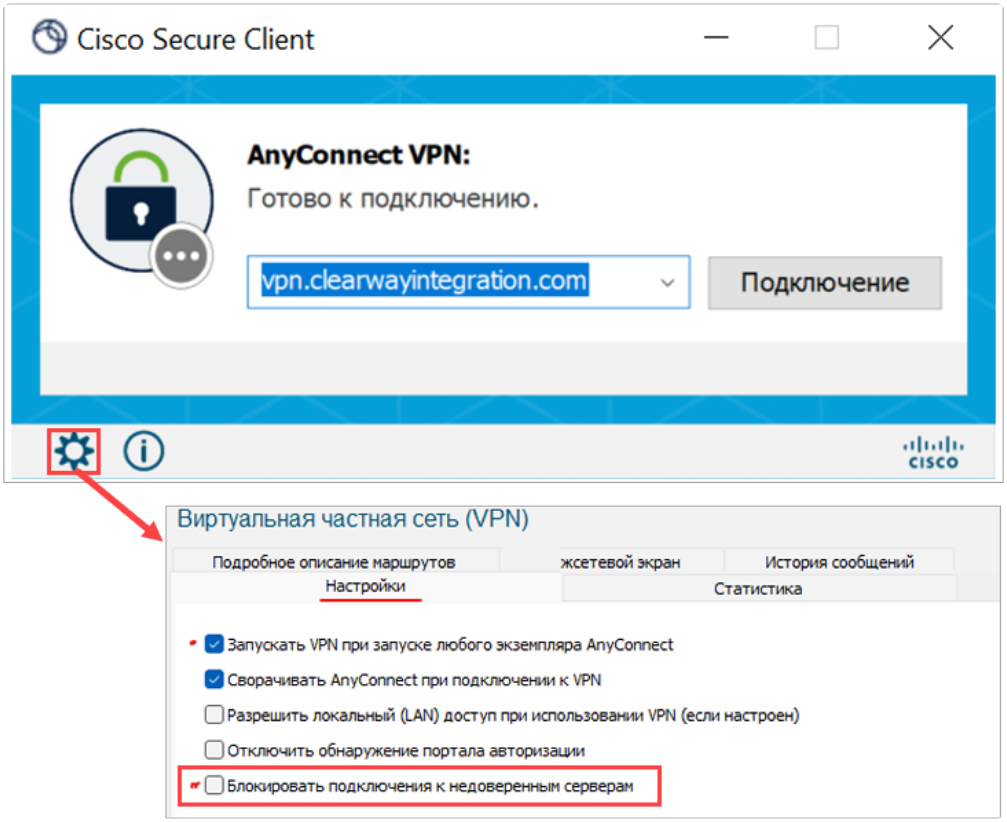
2. После успешной авторизации откроется окно с кнопкой для скачивания дистрибутива AnyConnect Secure Mobility Client.



   Клиент выбирается автоматически для той ОС, в которой открыт браузер.

3. Скачайте и установите Cisco AnyConnect, следуя указаниям мастера установки.
4. Запустите клиент Cisco AnyConnect.

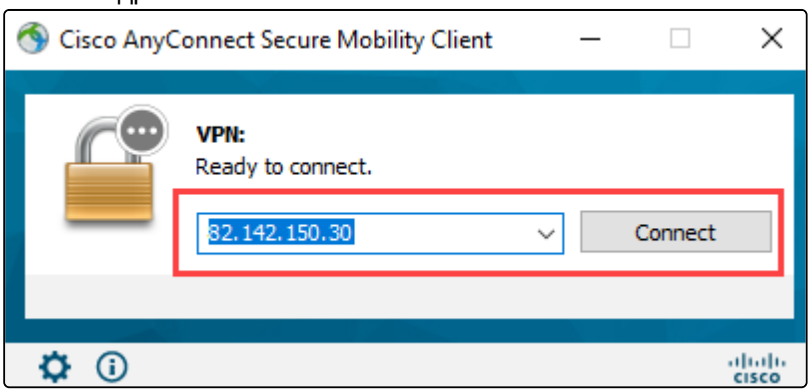
5. Откройте настройки (значок шестеренки) и снимите флажок "Блокировать подключения к недоверенным серверам", затем закройте окно настроек.



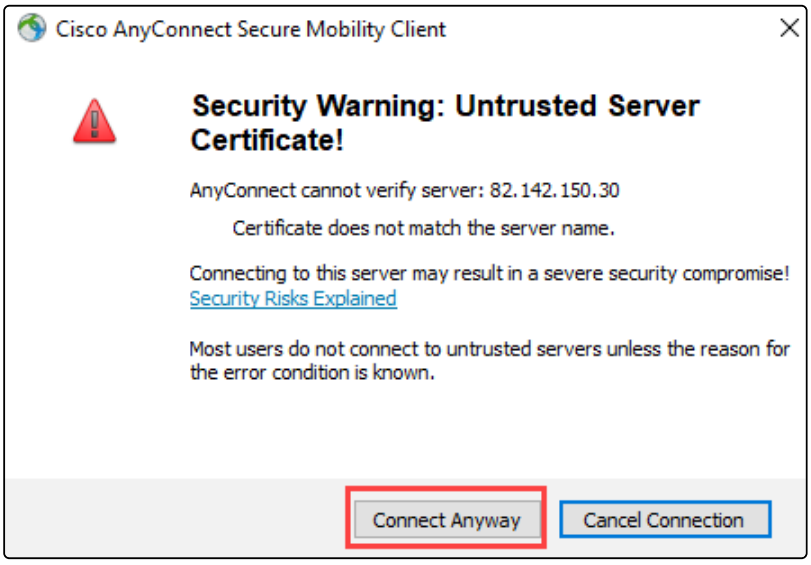
3.4.1.2 Авторизация по VPN

Для подключения к VPN выполните следующие действия.

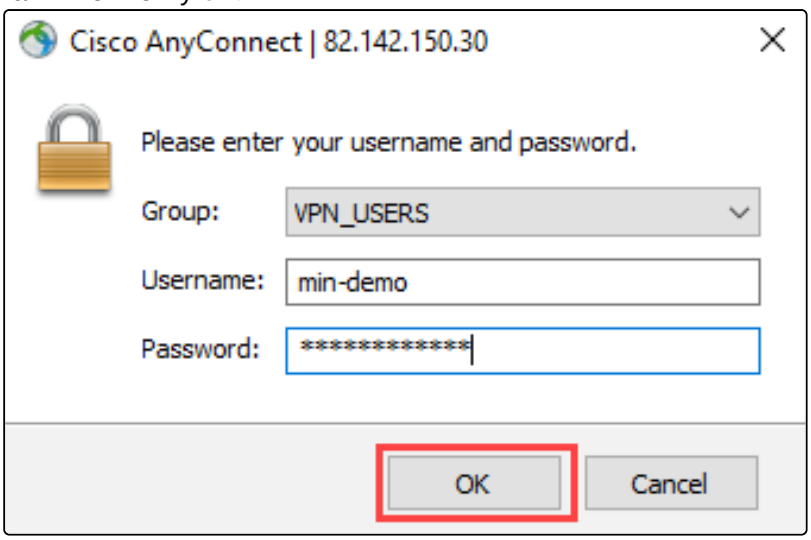
1. Запустите VPN-клиент Cisco AnyConnect.
2. Укажите адрес шлюза и нажмите **Connect**.



3. При подключении к демо-стенду вы можете увидеть предупреждение, что сертификат внутреннего корпоративного ресурса не является доверенным для вашего компьютера. Это не означает, что соединение небезопасно. Нажмите **Connect Anyway**.

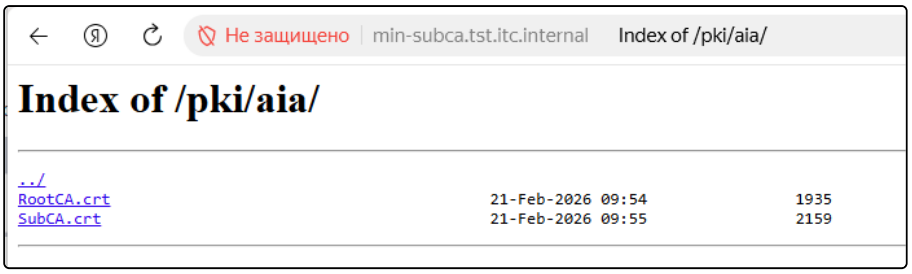


4. Укажите логин и пароль учетной записи VPN-клиента, в поле "Группа" выберите "VPN_USERS".
5. Нажмите кнопку **OK**.



3.4.2 Добавление сертификатов в доверенные

1. Откройте браузер и перейдите по ссылке http://min-subca.tst.itc.internal/pki/aia/.



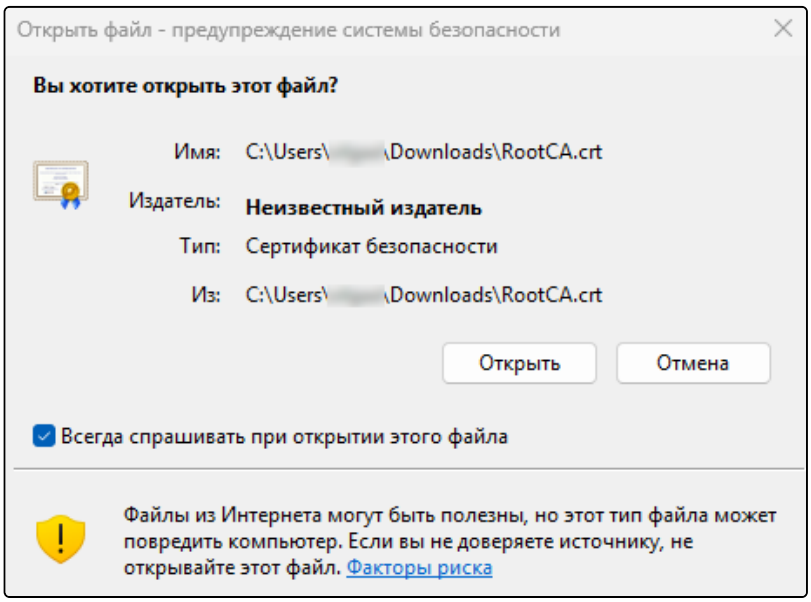
2. Скачайте на компьютер файлы сертификатов *RootCA.crt* и *SubCA.crt*.
3. Перейдите в директорию, куда вы сохранили файлы сертификатов.

4. Добавьте сертификаты, как описано ниже.
5. После добавления сертификатов закройте и заново откройте браузер, чтобы он подхватил новые сертификаты.

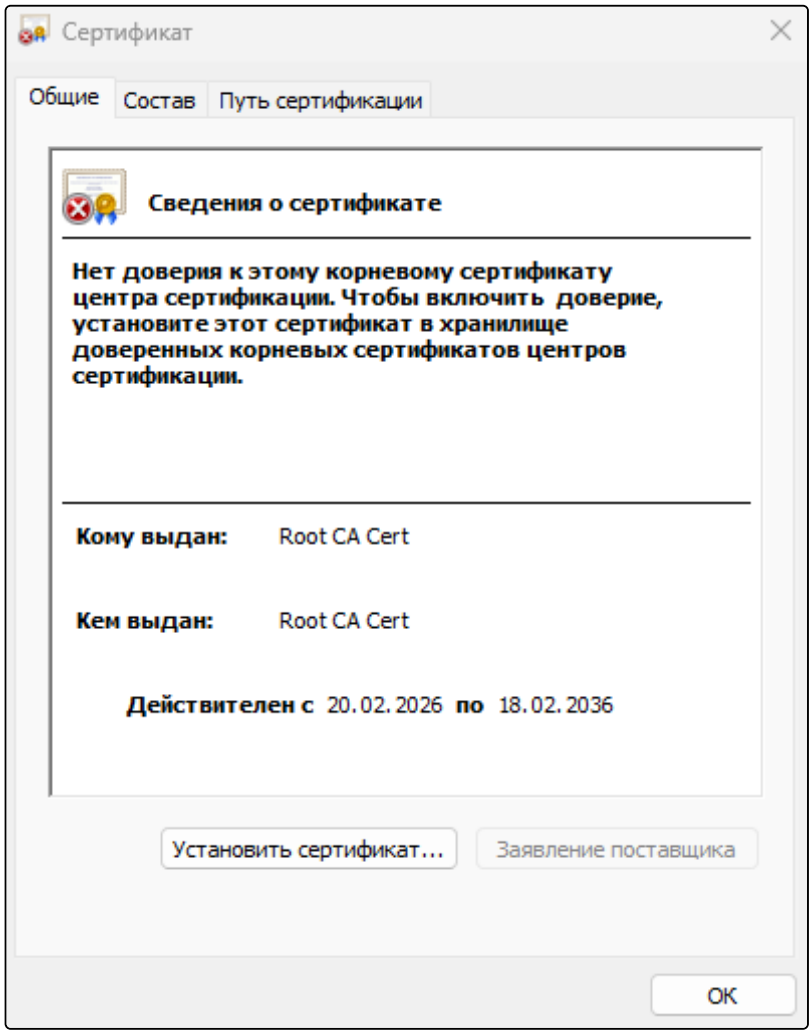
3.4.2.1 Добавление сертификатов для ОС Windows

1. Добавьте корневой сертификат *RootCA.crt* в доверенные корневые центры сертификации.

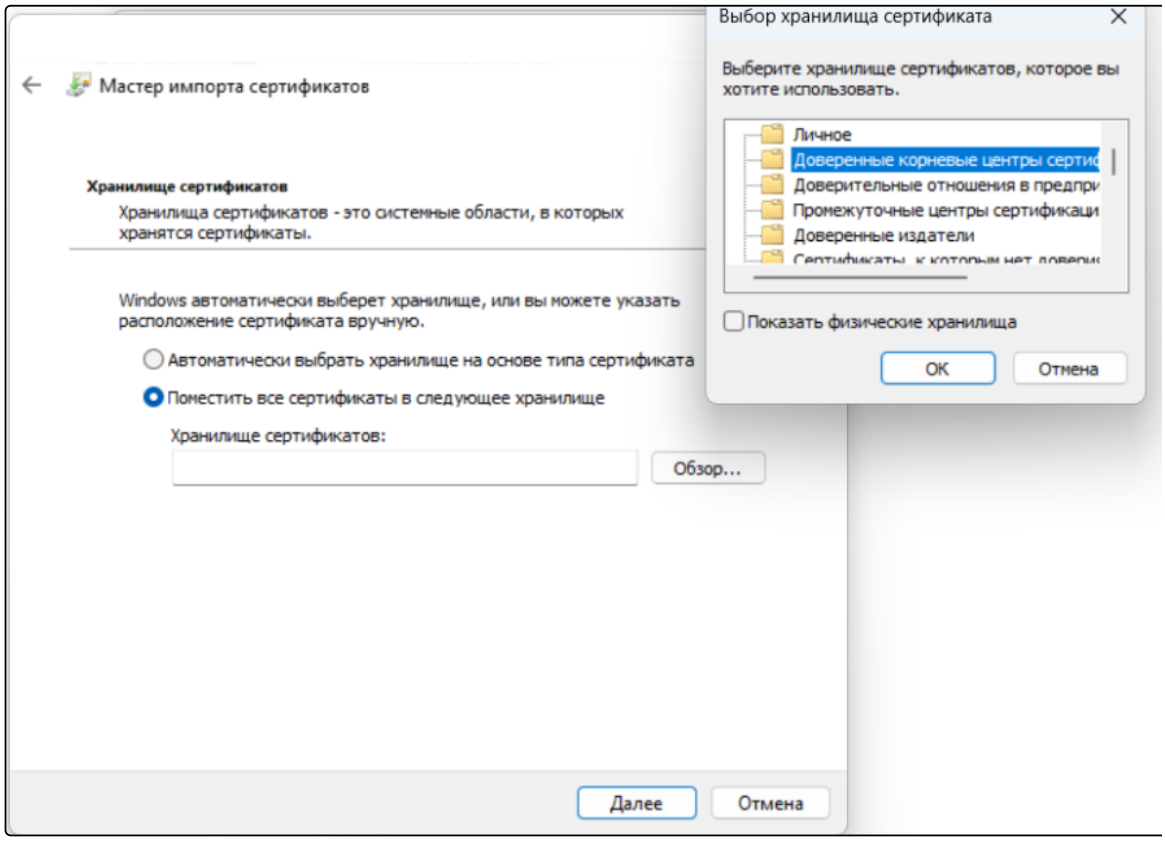
    a. Дважды нажмите на имя файла *RootCA.crt*, а затем в окне предупреждения системы безопасности нажмите **Открыть**.



    b. Нажмите **Установить сертификат**.



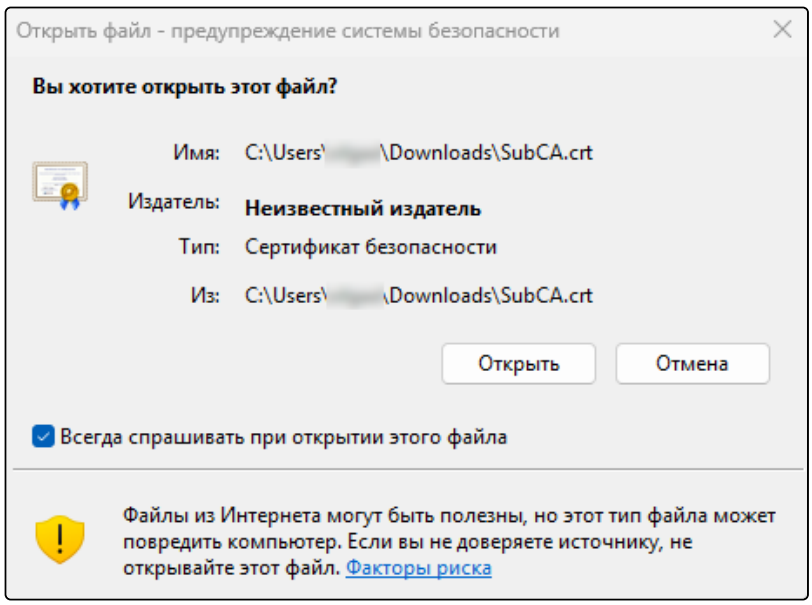
c. Нажмите **Далее**, выберите пункты, как показано на рисунке ниже. Затем нажмите **Далее**.



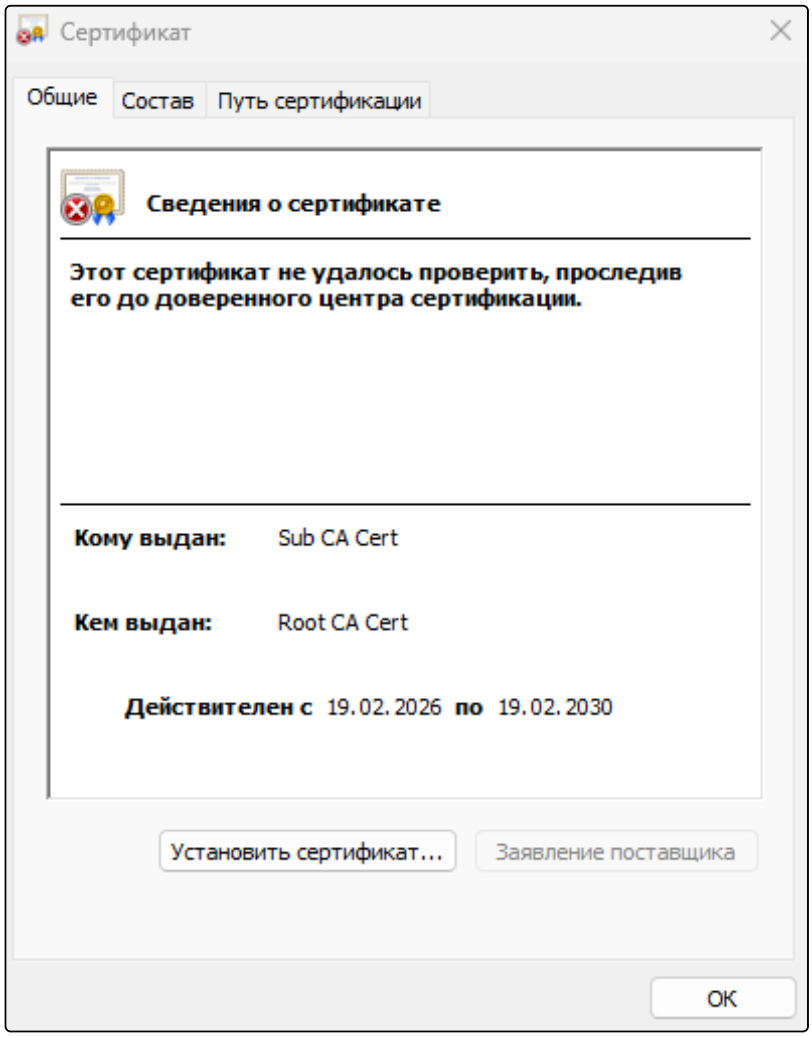
d. Нажмите **Готово**, а затем в окне предупреждения системы безопасности нажмите **Да**.

2. Добавьте промежуточный сертификат *SubCA.crt* в промежуточные центры сертификации:

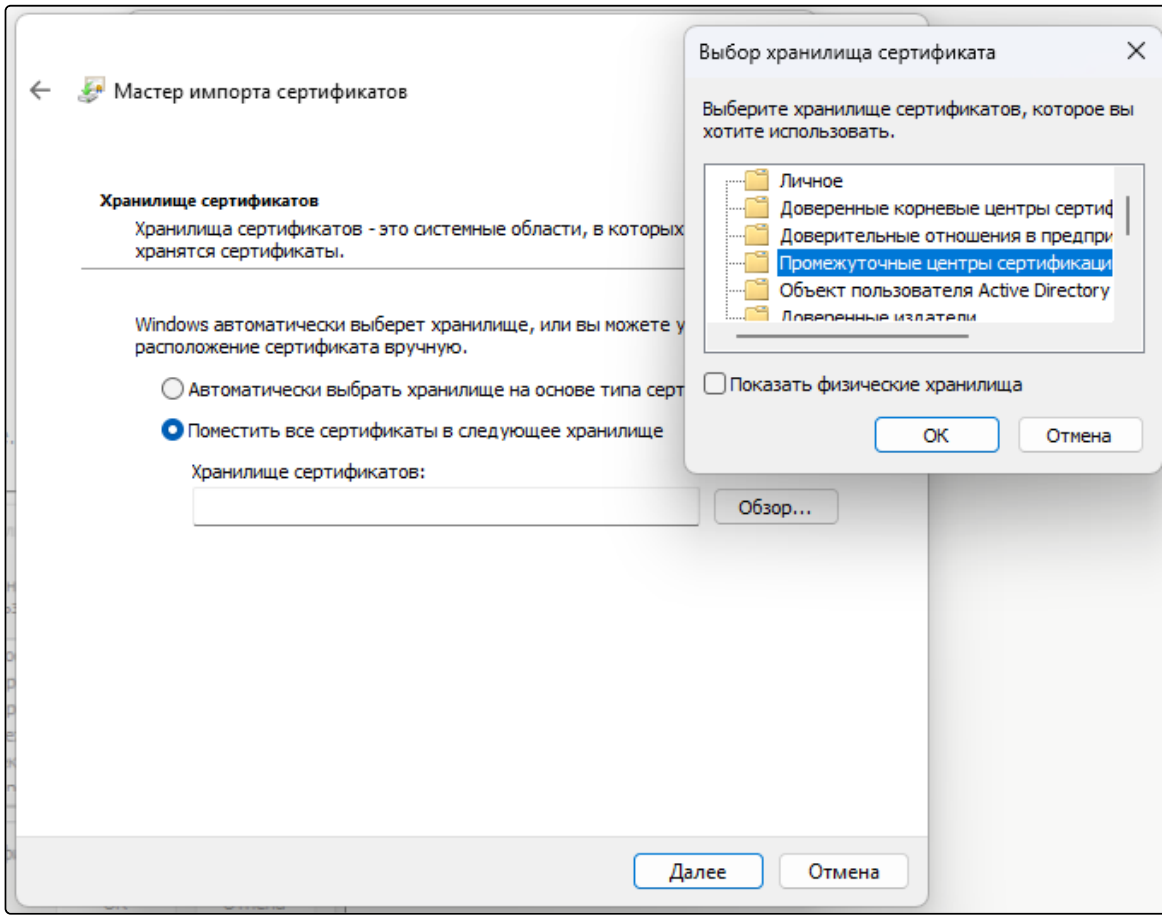
a. Дважды нажмите на имя файла *SubCA.crt*, а затем в окне предупреждения системы безопасности нажмите **Открыть**.



b. Нажмите **Установить сертификат**.



c. Нажмите **Далее**, выберите пункты, как показано на рисунке ниже. Затем нажмите **Далее**.



d. Нажмите **Готово**, а затем в окне предупреждения системы безопасности нажмите **Да**.

3.4.2.2 Добавление сертификата для ОС Linux

3.4.2.2.1 Метод 1. Использование update-ca-certificates (Debian/Ubuntu)

1. Скопируйте сертификат в нужную директорию:

```
sudo cp your-ca-certificate.crt /usr/local/share/ca-certificates/
```

2. Обновите хранилище сертификатов:

```
sudo update-ca-certificates
```

3. Проверьте добавление сертификата:

```
ls -la /etc/ssl/certs/ | grep your-certificate
```

3.4.2.2.2 Метод 2. Ручное добавление (RHEL/CentOS/Fedora)

1. Скопируйте сертификат:

```
sudo cp your-ca-certificate.crt /etc/pki/ca-trust/source/anchors/
```

2. Обновите хранилище сертификатов:

```
sudo update-ca-trust
```

3. Проверьте добавление сертификата:

```
ls -la /etc/pki/ca-trust/extracted/openssl/
```

3.5 Вход в веб-интерфейс демо-стенда

Для начала работы с веб-интерфейсом системы выполните следующие шаги:

Предварительные требования
Убедитесь, что ваше рабочее место подключено к корпоративной сети через VPN (см. раздел Настройка доступа), так как адрес находится во внутреннем контуре.

Порядок действий

1. Откройте используемый веб-браузер (например, Google Chrome, MS Edge или Яндекс.Браузер).
2. В адресную строку введите следующую ссылку и нажмите **Enter**: https://min-ess.tst.itc.internal.
3. В появившемся окне выберите метод «Логин & Пароль», введите логин и пароль учетной записи для аутентификации в веб-интерфейсе EXC из таблицы Учетные записи и нажмите кнопку входа для доступа к главной странице системы.

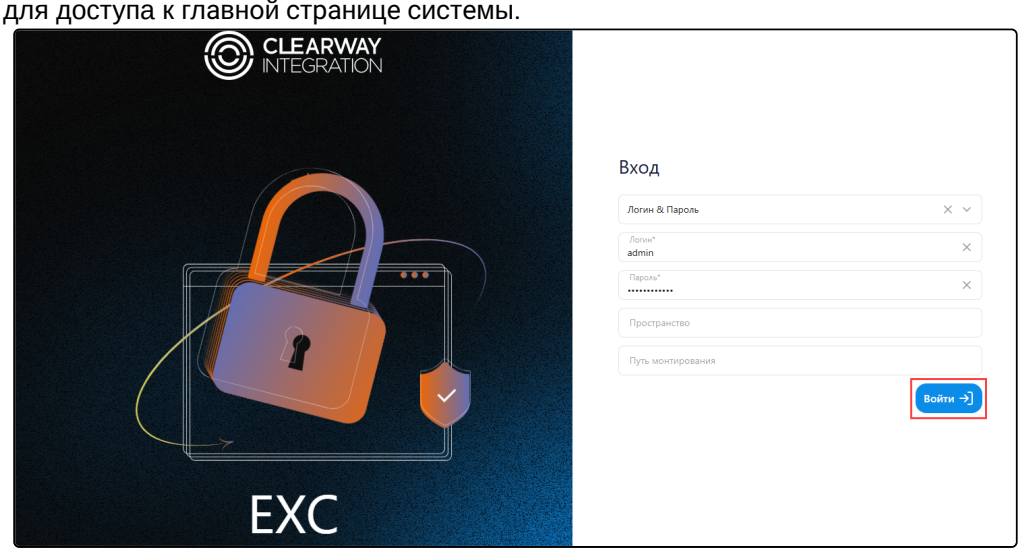


Рисунок 2 Вход в систему EXC

Откроется главная страница портала EXC:

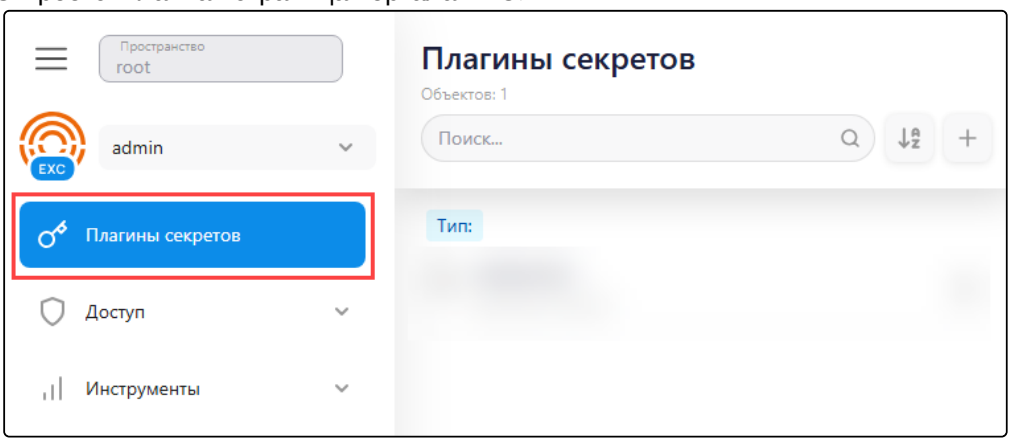


Рисунок 3 Главная страница портала EXC

3.6 Подключение к демо-стенду через SSH

Для подключения к демо-стенду через SSH запросите учетные данные администратора у сотрудников технической поддержки.

Для подключения можно использовать стандартный SSH-клиент (OpenSSH), который вызывается через командную строку (cmd) для Windows, или использовать стандартный терминал для Linux.

1. Ввести команду для подключение к машине демо-стенда по SSH:

```
ssh min-ess.tst.itc.internal -l administrator
```

2. Согласиться на добавление сервера в known_hosts, вписав в строке yes.

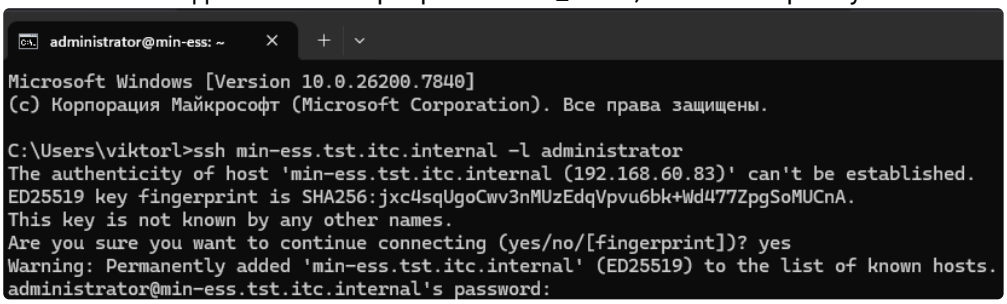


Рисунок 4 Добавление сервера в know_hosts

3. Ввести пароль от учетной записи administrator.
4. При успешном подключении будет информация о предыдущем входе пользователя и в начале строки появится имя пользователя и имя сервера:

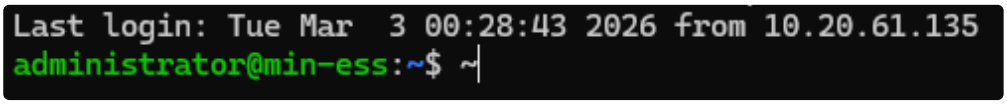


Рисунок 5 Успешное подключение по ssh

4 Проверка работы ПО

4.1 Сценарий использования системы

4.1.1 Активация плагина секретов Key-Value

1. Перейдите в веб-интерфейс управления системой (см. раздел Вход в веб-интерфейс системы).

2. Откройте раздел «Плагины секретов»
В главном меню перейдите в раздел «Плагины секретов».

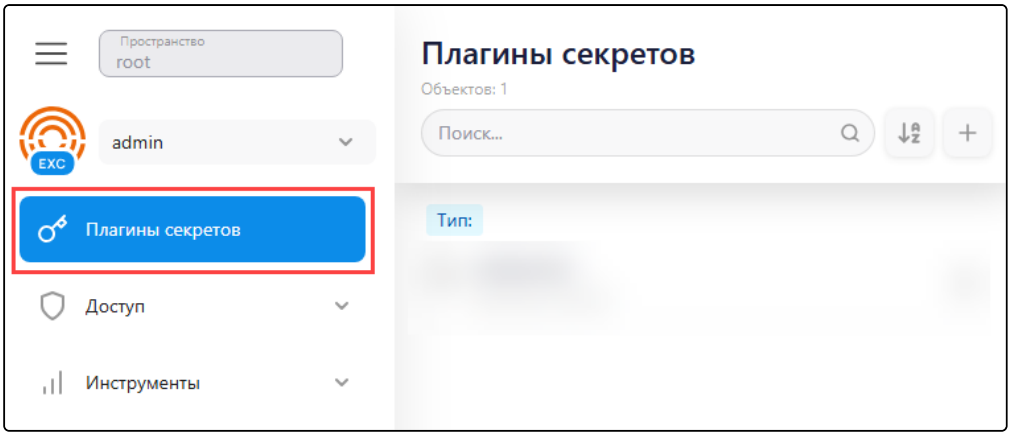


Рисунок 6 Переход в раздел «Плагины секретов»

3. Приступите к созданию нового плагина
Нажмите кнопку «**+**» в правом верхнем углу панели.

Рисунок 7 Создание плагина

4. Выберите тип плагина
В списке доступных универсальных плагинов выберите «KV».

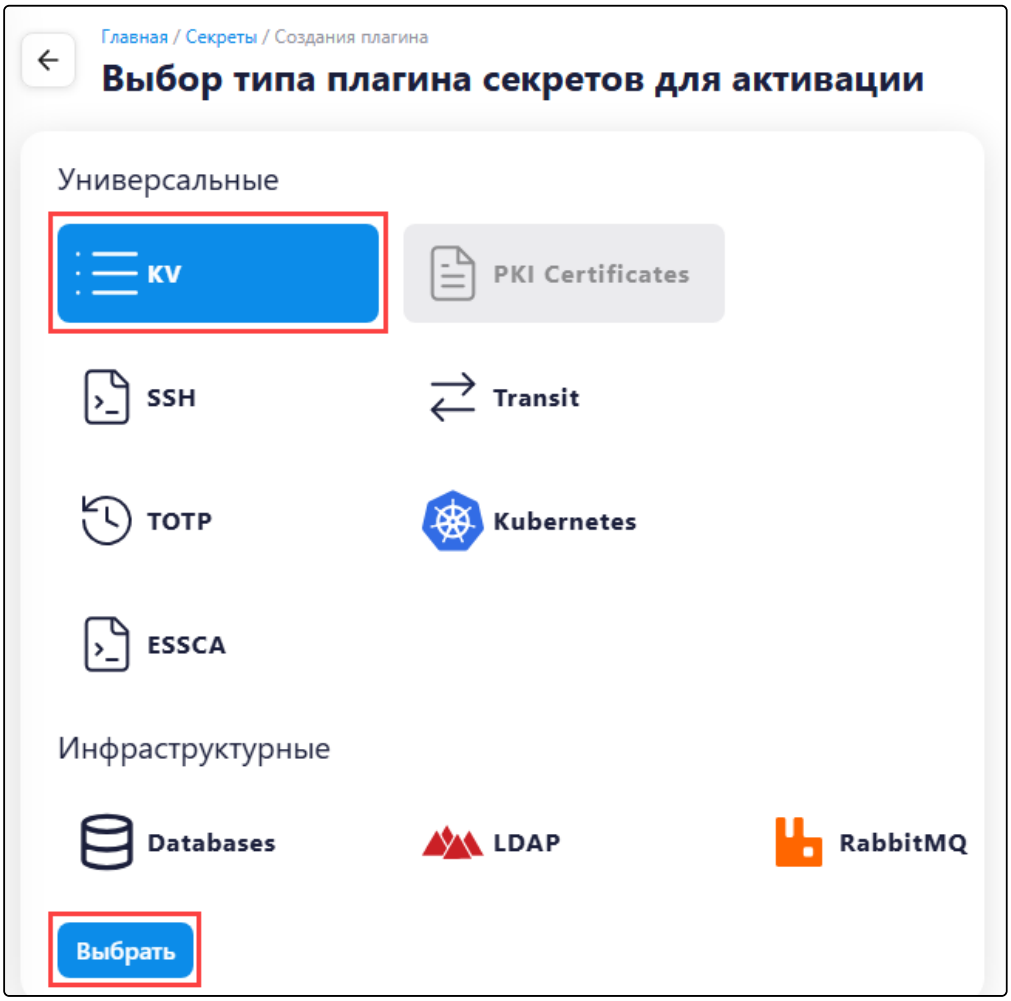


Рисунок 8 Выбор типа плагина

5. Укажите путь для плагина
В поле «Путь» введите уникальный корневой адрес для плагина.

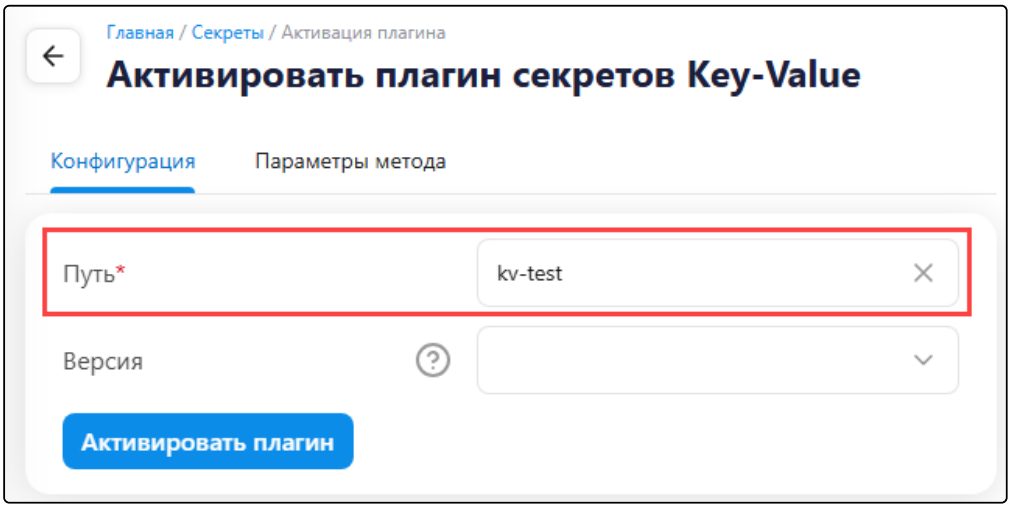


Рисунок 9 Ввод уникального корневого адреса для плагина

6. Выберите версию плагина
В поле «Версия» укажите значение 1 — это версия с плоской структурой данных.

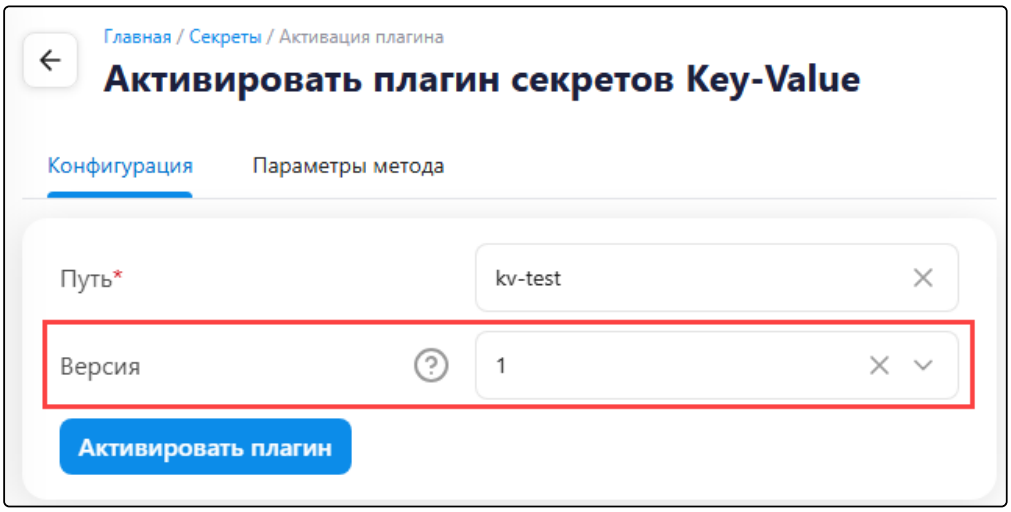


Рисунок 10 Выбор версии плагина

7. Активируйте плагин
Нажмите кнопку **Активировать плагин**.

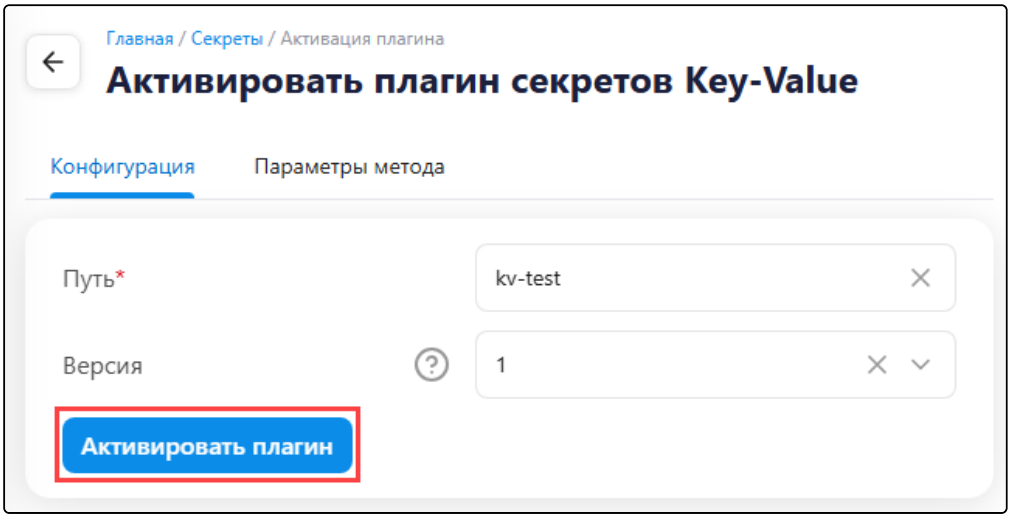


Рисунок 11 Активация плагина секретов

8. Плагин активирован
В правом верхнем углу окна появится уведомление «Метод успешно создан».

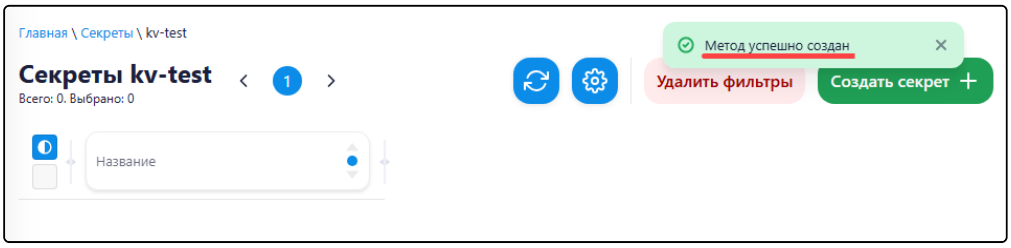


Рисунок 12 Плагин успешно активирован

4.1.2 Создание секрета

9. Вернитесь к списку плагинов
Перейдите обратно в раздел «Плагины секретов», чтобы увидеть обновленный список.

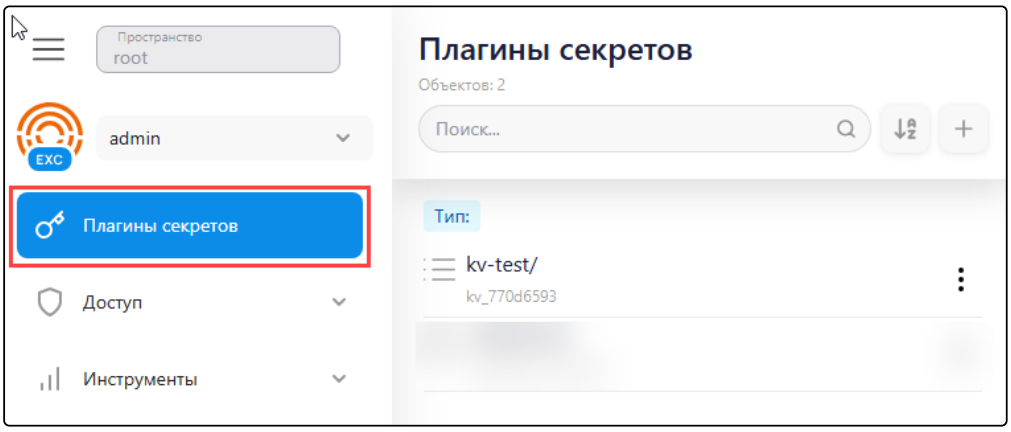


Рисунок 13 Переход в раздел «Плагины секретов»

10. Откройте плагин KV
В списке активированных плагинов нажмите на созданный плагин KV.

Рисунок 14 Выбор плагина в списке активированных

11. Приступите к созданию секрета
В разделе выбранного плагина нажмите кнопку **Создать секрет**.

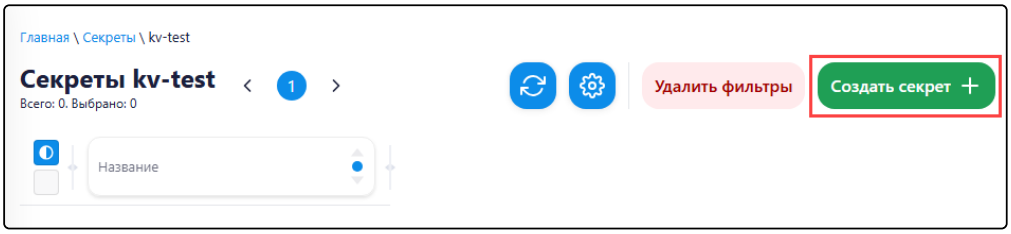


Рисунок 15 Создание секрета

12. Введите идентификатор секрета
В поле «Название» укажите имя секрета (ключ верхнего уровня).

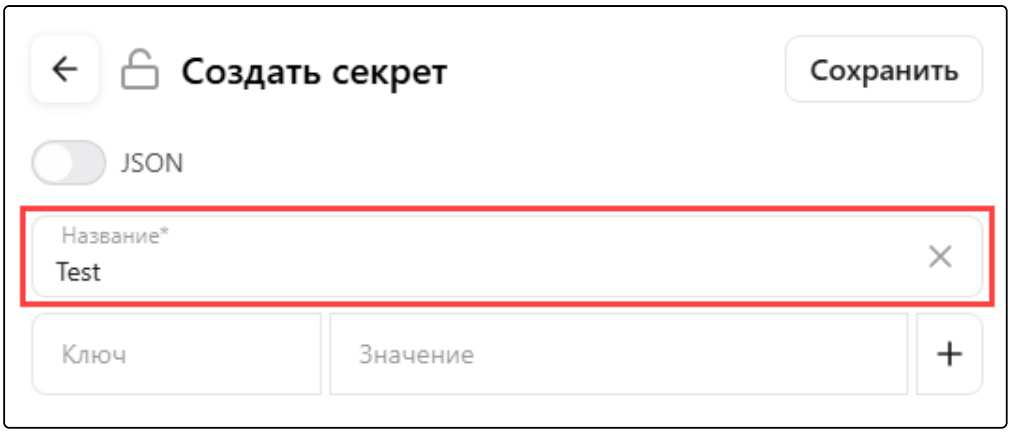


Рисунок 16 Ввод названия секрета

13. Добавьте пару «ключ-значение»
Заполните поля:

- «Ключ» — идентификатор параметра;
- «Значение» — fewf23 (для тестового примера).

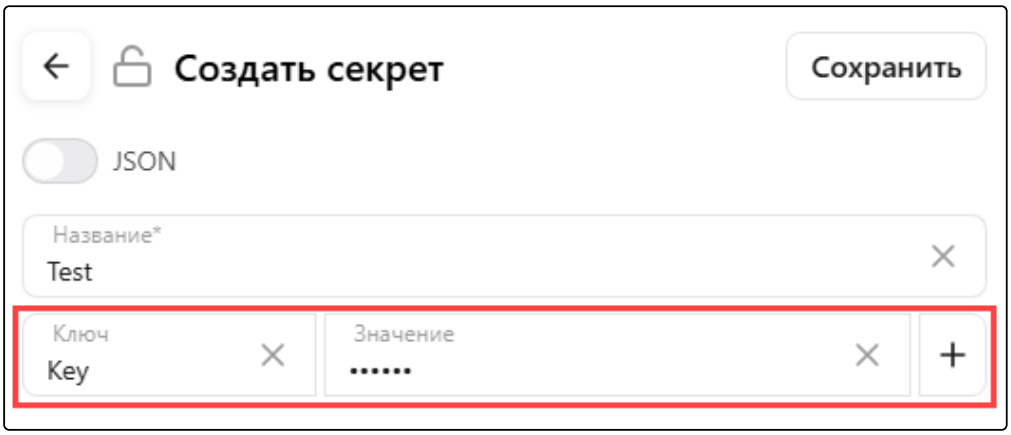


Рисунок 17 Заполнение пары «ключ-значение»

14. Сохраните секрет
Нажмите кнопку **Сохранить** в правом верхнем углу.

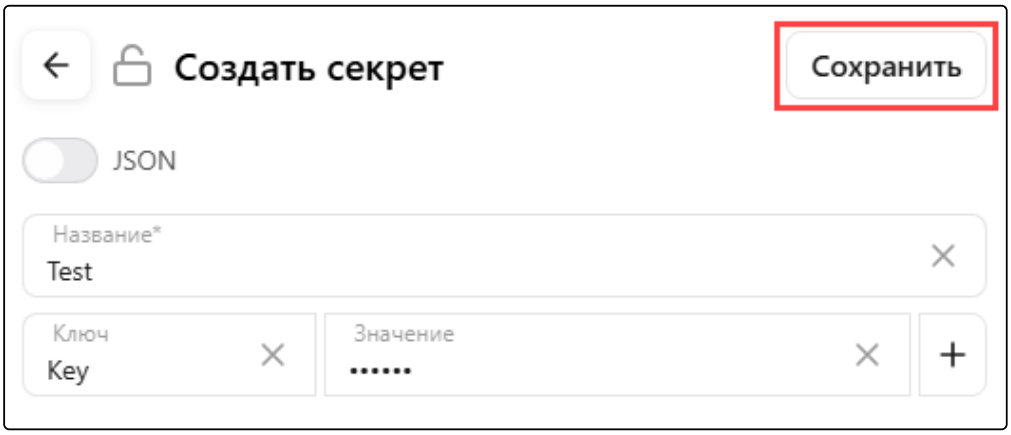


Рисунок 18 Сохранение секрета

15. Секрет добавлен
В списке секретов появится новый.

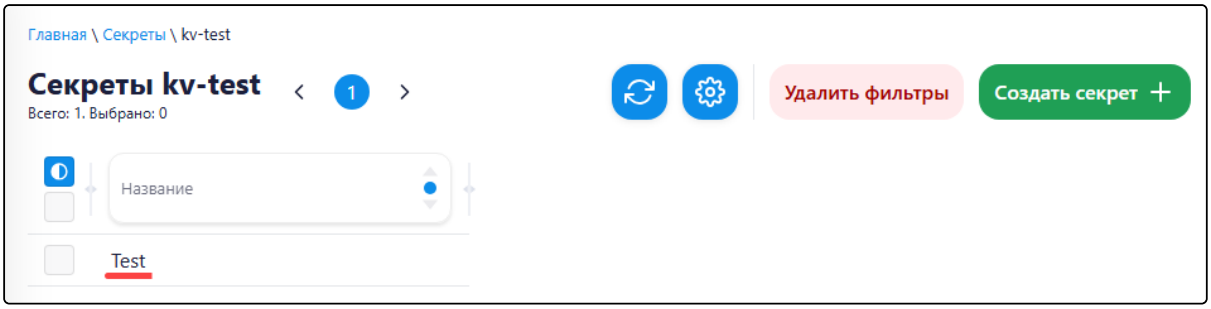


Рисунок 19 Обновленный список секретов

4.1.3 Просмотр секрета

16. Откройте секрет
В списке секретов нажмите на созданную запись, чтобы перейти к детальному просмотру.

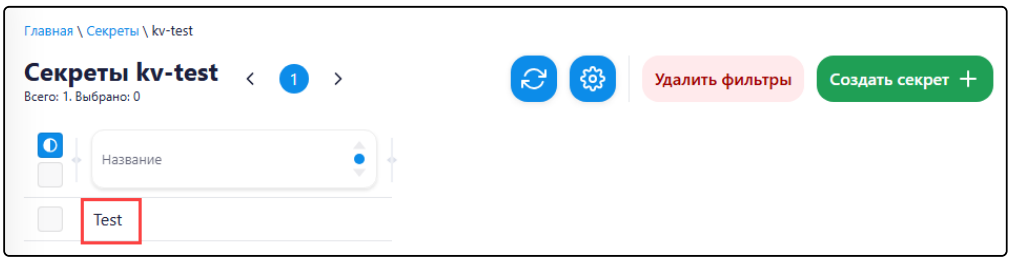


Рисунок 20 Переход к просмотру секрета

17. Проверьте данные
В правой боковой панели окна нажмите на иконку «глаз» справа от поля значения, чтобы отобразить скрытое содержимое и убедиться в корректности сохраненных данных.

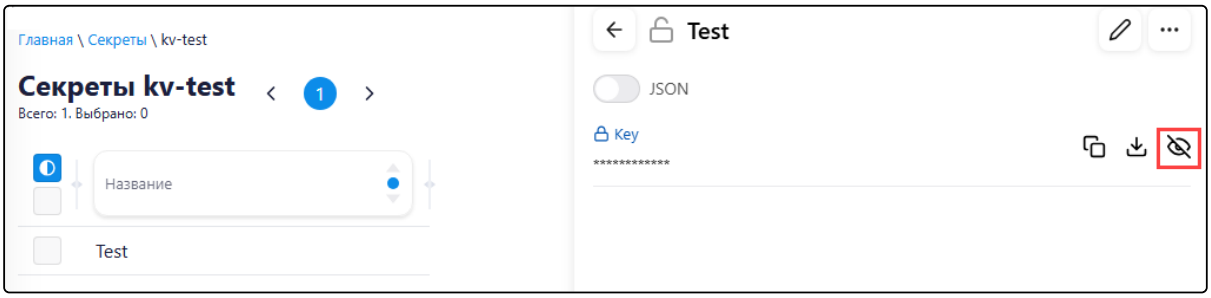


Рисунок 21 Проверка данных секрета

4.1.4 Удаление секрета

18. Скройте панель просмотра секрета
Перейдите назад для отображения доступных действий для списка секретов.

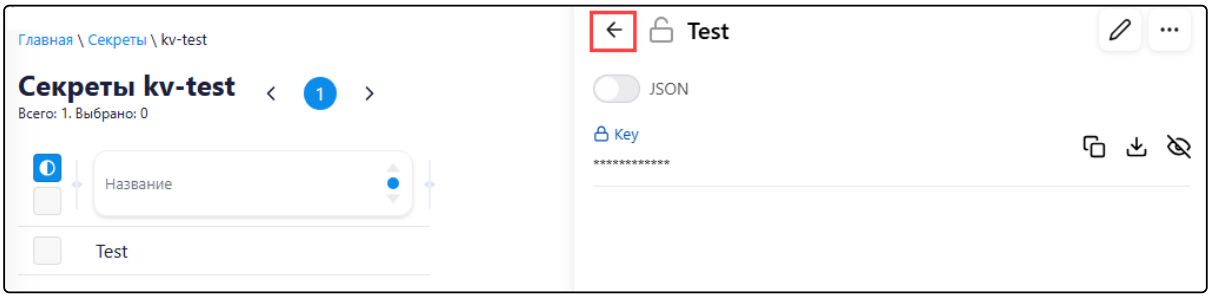


Рисунок 22 Скрытие панели просмотра секрета

19. Выберите секрет для удаления
Установите флажок слева от названия секрета, который нужно удалить.

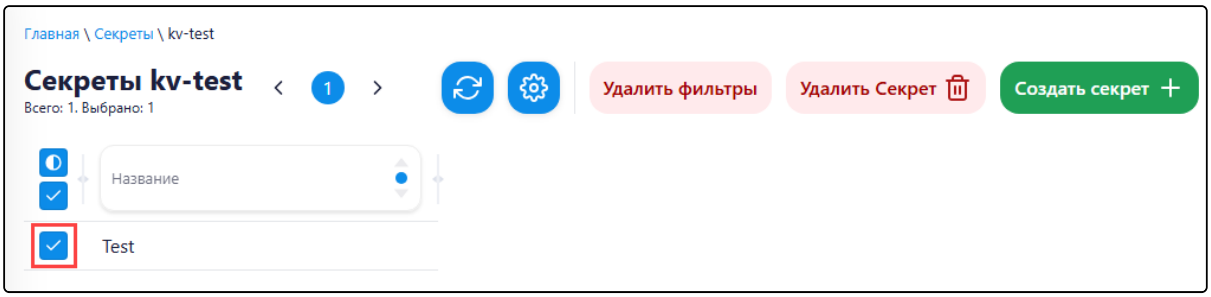


Рисунок 23 Выбор секрета в списке

20. Удалите секрет
Нажмите кнопку **Удалить секрет** в правом верхнем углу.

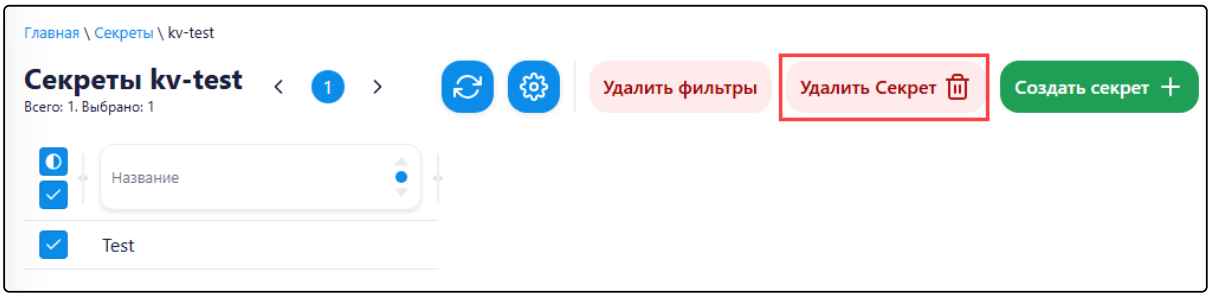


Рисунок 24 Удаление секрета

21. Подтверждение удаления
Подтвердите действие, нажав кнопку **Да** в появившемся диалоговом окне.

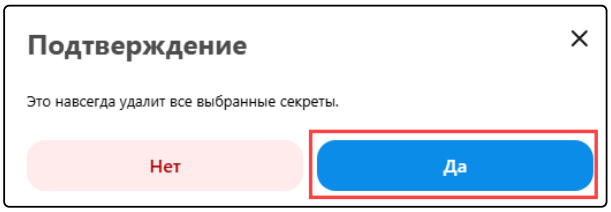


Рисунок 25 Подтверждение удаления секрета

22. Секрет удален
В правом верхнем углу окна появится уведомление «Секреты успешно удалены».

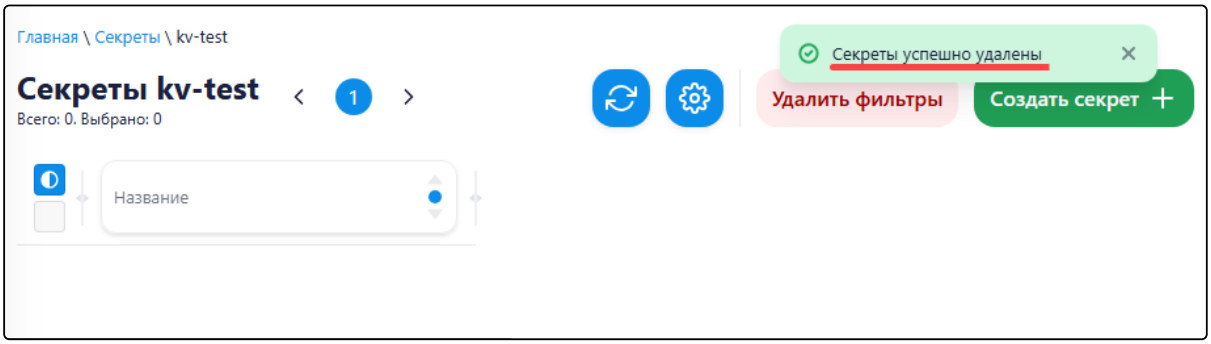


Рисунок 26 Секрет успешно удален

4.2 Проверка статуса сервисов

Для проверки статуса сервисов запросите учетные данные администратора у сотрудников технической поддержки.

1. Авторизоваться по ssh:

```
ssh min-ess.tst.itc.internal -l administrator
```

2. Перейти в контекст пользователя:

```
sudo -su itc-svc
```

3. Проверить статус работы сервисов командой:

```
systemctl list-units --user --type=service
```

4. Ожидаемый результат: отображает 2 запущенных сервиса со статусом Active: active (running). ПО запущено и функционирует.

```
administrator@min-ess:~$ sudo -su itc-svc
[sudo] пароль для administrator:
itc-svc@min-ess:/home/administrator$ systemctl list-units --user --type=service
  UNIT                LOAD   ACTIVE SUB     DESCRIPTION
  ess-ha.service      loaded active running ESS HA Server
  ess-transit.service loaded active running ESS Transit Server

LOAD   = Reflects whether the unit definition was properly loaded.
ACTIVE = The high-level unit activation state, i.e. generalization of SUB.
SUB    = The low-level unit activation state, values depend on unit type.
2 loaded units listed. Pass --all to see loaded but inactive units, too.
To show all installed unit files use 'systemctl list-unit-files'.
itc-svc@min-ess:/home/administrator$
```

Рисунок 27 Запущенные службы EXC

5 Самостоятельная установка

5.1 Системные требования

Подробный набор требований для развертывания системы содержится в документе «Описание технической архитектуры программного обеспечения» в разделе «Физическая архитектура».

5.2 Инструкции по установке

Подробные инструкции для развертывания компонентов системы запросите у сотрудников технической поддержки.