Инструкция по удаленному подключению к компьютеру ЗКВС

Казначейство России

Что должно быть у сотрудника для удаленного подключения к своему рабочему месту

Компьютер (рабочая станция) со следующими минимальными характеристиками:
Процессор с тактовой частотой не менее 1,8 ГГц;
Объем **жесткого диска** не менее 512 Мб;
Объем **оперативной памяти** не менее 512 Мб;

На котором установлено следующее программное обеспечение:
Операционная система: Windows 7 SP и выше
Не устанавливается требуемое ПО на: **Mac OS, Windows 10 Home**
Интернет-браузер «Internet Explorer» или другой
Антивирус Kaspersky или любой другой антивирус **(с последними обновлениями)**

Квалифицированный сертификат ключа проверки **электронной подписи**:
есть у каждого сотрудника УФК по КО
- используется для работы в LanDocs, ЭБ и пр.

Ваш компьютер в сети ЗКВС для доступа к нему должен быть **включен**
Для входа Вы должны знать **Имя своего компьютера в сети ЗКВС** (узнать имя компьютера можно в меню Пуск - Панель управления – Система – поле Компьютер. Например, W3900OKOIB02)

Казначейство России

Как настроить удаленное рабочее место: 6 шагов

1. Обязательно проверить **наличие работающего антивируса** на компьютере. В случае его отсутствия необходимо провести его установку. Дистрибутив антивируса Kaspersky можно взять в папке «**Kaspersky**».

2. Установить Драйвер Рутокен для носителя информации из соответствующей папки (как это сделать – на странице «**Шаг 1. Устанавливаем Драйвер Рутокен»**).

3. Установить Континент-АП для возможности установки защищенного соединения (как это сделать – на странице **«Шаг 2. Устанавливаем Континент-АП»**)

4. Создать запрос на пользовательский сертификат (как это сделать – на странице «**Шаг 3. Создаем запрос на сертификат»**)

5. Отправить запрос в адрес сотрудников ОРСиБИ по интернет-почте, получить сертификат и установить его, как отправить запрос и установить сертификат – на странице **«Шаг 4. Получаем и устанавливаем сертификат»**

6. Установить Крипто-про для возможности использования электронной подписи при подписании документов на удаленном рабочем месте в сети ЗКВС (как это сделать – на странице **«Шаг 5. Устанавливаем Крипто-про на удаленном рабочем месте»)**

7. Подключиться к своему рабочему месту в сети ЗКВС (как это сделать – на странице **«Шаг 6. Подключаемся»**). Вы сможете работать на своем компьютере ЗКВС со всеми программами с одним ограничением: в данном режиме нет возможности копировать (переносить) файлы из защищенного контура ЗКВС в открытый контур.

Шаг 1. Устанавливаем Драйвер Рутокен

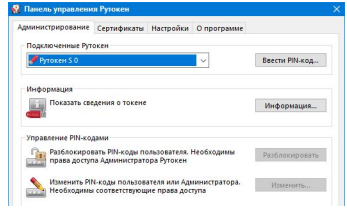
1. Из папки **«1_Драйвер Рутокен»** запустить файл **RuToken.exe** для стандартной установки или **RuToken_Тихая установка.cmd** для установки без вопросов.

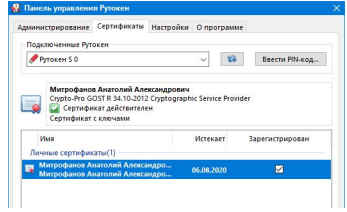
2. Для проверки установки подключить Рутокен к компьютеру, дождаться окончания установки драйвера, после этого запустить с рабочего стола ярлык **«Панель управления Рутокен».**

3. В строке «Подключенные Рутокен» должен отобразиться Ваш носитель информации.

4. На вкладке «Сертификаты» должен отобразиться Ваш ключевой контейнер на носителе.

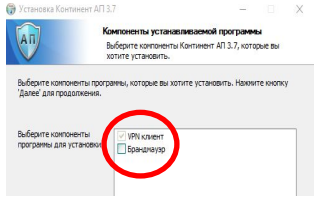
5. Вы можете перейти к следующему шагу.





Шаг 2. Устанавливаем Континент-АП

1. Из папки **«2_Континент-АП»** запустить файл **«AP_setup.exe»** для стандартной установки или **«AP_setup_Тихая установка.cmd»** для установки без вопросов.



2. При стандартной установке следуйте рекомендациям инсталлятора, кроме следующих особенностей:
   - необходимо **СНЯТЬ галку** с компоненты **«Брандмауэр»** в разделе «**Компоненты устанавливаемой программы**»,

3. Обязательно **перегрузите** компьютер

4. Дальше не удивляйтесь – для продолжения установки Вам предложат несколько раз нажать на левую кнопку «мыши», целясь в передвигающуюся по экрану **мишень.** Это необходимо для формирования случайного числа, используе программой

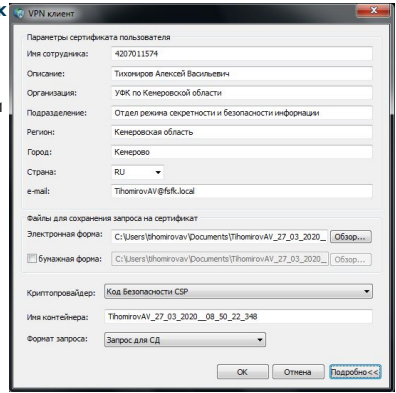
5. Вы закончили установку Континент-АП. Чтобы проверить себя - на панели задач Windows, в трее (группа значков рядом с часами) найдите **значок VPN-клиента** и, нажав на него правой кнопкой мыши, проверьте, что выбран «**Криптопровайдер по умолчанию» Код Безопасности CSP**.

6. Вы можете перейти к следующему шагу.

Казначейство России

Шаг 3. Создаем запрос на сертификат аутентификации Континент АП

1. На панели задач Windows, в трее (группа значков рядом с часами) найдите **значок VPN-клиента** и, нажав на него правой кнопкой мыши, выберете «Сертификаты/**Создать запрос на пользовательский сертификат»**.



2. Заполните **форму запроса** своими **личными данными как в примере справа**. При заполнении обратите внимание на следующее:

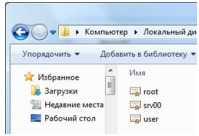
- при указании электронной почты - укажите Вашу почту в домене @fsfk.local (например MitrofanovAA@sfk.local)
- при заполнении поля **«Электронная форма»** выберете путь, где будет сохранен сформированный электронный запрос и укажите имя файла с расширением «.req» так, чтобы Вам было его легко потом найти (например, "ФИО.req")
- после заполнения основных полей формы нажмите кнопку «Подробно» и проверьте, что в поле **«Криптопровайдер»** указано «Код Безопасности SCP» и нажмите «Ок».

3. И снова мы увидим **мишень**.
Нажмите на нее несколько раз, пока создается контейнер.
4. Введите **пароль** для контейнера и **запомните его**. Выберете место хранение закрытого ключа – **Рутокен**, при отсутствии – **Реестр Windows**. Нажмите ОК. Запрос на сертификат будет успешно создан и размещен по адресу, который Вы указали ранее в поле «Электронная форма»
5. Вы можете перейти к следующему шагу

Казначейство России

Шаг 4. Устанавливаем сертификат аутентификации Континент АП

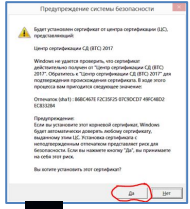
1. С использованием **своей** интернет-почты отправьте созданный на шаге 2 **файл-запрос с расширением «.req»** на адрес сотрудник ОРСиБИ УФК: rsibi_ufk39@mail.ru



В **теме** укажите «**Запрос от <ФИО> <отдел>**»
В **тексте** напишите свой контактный телефон - 8-9XX-XXX-XXXX.
Не забудьте к письму прикрепить созданный файл с расширением **«.req»**

2. В ответ Вы получите архив, содержащий 3 файла, которые необходимо сохранить в удобном для Вас месте.

3. Для установки сертификата на панели задач Windows нажмите на **значок VPN-клиента** и выберите пункт меню **«Сертификаты/Установить сертификат пользователя»**, укажите в нем полученный ранее файл **user.cer** и следуйте далее предложениям инсталлятора. При отсутствии на компьютере корневого сертификата – согласитесь с автоматической его установкой. Подтвердите установку корневого сертификата.



1. На панели задач Windows, в трее (группа значков рядом с часами) найдите **значок VPN-клиента** и, нажав на него правой кнопкой мыши, выберете «Настройка соединения/**Континент АП».**
2. В открывшемся окне введите любой из следующих адресов серверов доступа:

- **3900-sd-01.roskazna.ru** *(предпочтительный)*
- **3900-sd-02.roskazna.ru** *(предпочтительный)*
- **3900-sd-03.roskazna.ru** (в день издания сертификата подключаться только к этому серверу)
- **3900-sd-04.roskazna.ru**

Казначейство России

Шаг 5. Устанавливаем Крипто-про на удаленном рабочем месте:

1. Запустите файл **КриптоПро.exe** из папки **«3_КриптоПро»**

2. Следуйте рекомендациям инсталлятора

3. Перезагрузите компьютер

4. Вставьте в компьютер свой **Рутокен**, на которым хранится Ваш сертификат электронной подписи (который Вы используете на рабочем месте для подписания документов LanDocs и прочее).

5. Для **проверки корректности** установки запустите программу **Крипто-Про**, перейдите на закладку «Сервис» и там в разделе «Сертификаты в контейнере закрытого ключа» нажмите «Просмотреть сертификаты в контейнере» и далее - «Обзор». Проверьте, что Ваши сертификаты есть в списке. Не выбирайте сертификаты и нажмите «Отмена».

6. Из папки **«4_Корневые сертификаты»** открывайте файлы по порядку. В каждом окне нажмите **«Установить сертификат».**

7. Следуя рекомендациям мастера импорта на 2 шаге нужно выбрать пункт **«Поместить сертификат в хранилище»** и через кнопку **«Обзор»** выбрать:
   - для 1 сертификата – **«Доверенные корневые центры сертификации»**;
   - для 2 и 3 сертификатов – **«Промежуточные центры сертификации».**

8. Вы можете перейти к следующему шагу.

Казначейство России

Шаг 6. Подключаемся

1. На панели задач Windows нажмите на **значок VPN-клиента**  и выберите пункт меню **«Подключить ….** ».
2. Выберите свой сертификат (обычно – это 3900-… и срок окончания действия сертификата например 28-06-2021).
3. Будет осуществлен поиск закрытого ключа аутентификации. Введите пароль к контейнеру, не ставьте галку «Запомнить пароль»!
4. Согласитесь с предложением занести сертификаты в списки разрешенных.
5. Через несколько минут значок **VPN-клиента** станет зеленым – это обозначает, что Вы установили соединение.
6. Из меню **«Пуск»** - **«Все программы»** - **«Стандартные»** запустить **«Подключение к удаленному рабочему столу»**
7. В поле **«Компьютер»** укажите указанный ниже адрес и продолжите подключение, соглашаясь на вопросы от инсталлятора:

   10.39.1.56:3415

   При появлении следующего окна нажмите «больше не выводить запрос..» и «подключить».
6. В появившемся далее окне введите:

   Имя пользователя: **Ваша учетная запись ЗКВС**

   Пароль: **Ваш пароль от ЗКВС** (пароль тот же под которым заходите в свой ЗКВС компьютер)
7. Если Вы все сделали правильно, то увидите виртуальный терминальный сервер (рабочий стол), на котором запустите ярлык **«Подключение к удаленному рабочему столу»**

   В появившемся окне введите **имя своего компьютера в сети ЗКВС** (например, W3900okoib02 и еще раз **Ваш пароль от ЗКВС**
8. Вы можете работать в своем ЗКВС компьютере в режиме **«терминального доступа»**. Выход из режима и настройка экрана терминального доступа осуществляется в верхней части открывшегося экрана.

Казначейство России

Если возникли проблемы:

Контактные телефоны администраторов:

Отдел РСиБИ:
Тихомиров Алексей Васильевич
8-905-900-7812
Опалев Кирилл Николаевич
8-923-613-4233
Оленников Виталий Евгеньевич
8-950-272-7517

ФИО	Номер телефона сотового	28.03.2020	29.03.2020
Митрофанов Анатолий Александрович	+79505730020	да	да
Бауэр Светлана Николаевна	+79235356611	да	да
Лобышев Сергей Павлович	+79089463062	нет	да
Гусева Нина Михайловна	+79234983546	да	да
Стремякова Елена Алексеевна	+79236062568	нет	да
Беркутова Елена Викторовна	+79234908630	нет	да
Винокурова Вера Викторовна	+79515867413	нет	да
Чеснокова Ирина Евгеньевна	+79039843039	да	да
Алигерский Сергей Николаевич	+79069287313	да	да
Носов Алексей Александрович	83842719084	Да	Нет
Леонненко Евгения Анатольевна	83842719150	Да	Нет
Кривоногов Евгений Владиславович	89505765654	Да	Нет
Дятлов Антон Павлович	83842719180	Да	Нет

Успешной удаленной работы!