

**Рутокен Логон для Linux.
Версия 0.1.0, итерация 2.
Руководство
администратора**



- [Общая информация](#)
- [О программном комплексе](#)
 - [Назначение](#)
 - [Состав](#)
 - [Описание компонентов](#)
 - [Описание работы](#)
- [Условия применения](#)
 - [Поддерживаемые устройства](#)
 - [Поддерживаемые платформы](#)
 - [Поддерживаемые ОС](#)
 - [Поддерживаемые контроллеры домена](#)
 - [Необходимые библиотеки и зависимости](#)
- [Настройка ПК для работы с rtlogon](#)
 - [Настройка Network manager для экрана приветствия ОС Astra Linux](#)
 - [Ввод ПК в домен](#)
 - [Active Directory](#)
 - [ОС Astra Linux](#)
 - [ОС РЕД ОС](#)
 - [ОС АЛЬТ](#)
 - [FreeIPA](#)
 - [ОС Astra Linux](#)
 - [ОС РЕД ОС](#)
 - [ОС АЛЬТ](#)
 - [ALDPro](#)
 - [ОС Astra Linux](#)
 - [Samba DC](#)
 - [ОС Astra Linux](#)
 - [ОС РЕД ОС](#)
 - [ОС АЛЬТ](#)
 - [Проверка ввода ПК в домен](#)
 - [Загрузка корневого сертификата или сертификатов цепочки доверия УЦ на ПК](#)
 - [FreeIPA и ALDPro](#)
 - [Корневой сертификат](#)
 - [Сертификаты цепочки доверия УЦ](#)
 - [Active Directory](#)
 - [Samba DC](#)

- [Установка rtlogon](#)
- [Установка библиотеки libjсPKCS11-2.so](#)
- [Команды и общие параметры rtlogon](#)
- [Обновление rtlogon](#)
- [Удаление rtlogon](#)
- [Настройка ОС для работы с 2ФА](#)
- [Реконфигурация ОС для работы с 2ФА](#)
- [Отключение настроек ОС для работы с 2ФА](#)
- [Настройка 2ФА](#)
- [Проверка настройки 2ФА](#)
- [Изменение настроек 2ФА](#)
- [Удаление 2ФА](#)
- [Создание запроса на получение сертификата, генерация самоподписанного сертификата](#)
- [Получение сертификата УЗ от УЦ](#)
 - [FreeIPA и ALDPro](#)
 - [Active Directory](#)
 - [Samba DC](#)
- [Смена PIN-кода токена](#)
- [Разблокировка PIN-кода на экране приветствия или блокировки](#)
- [Запрос информации о конфигурации rtlogon и параметрах локальной 2ФА](#)
- [Логирование работы rtlogon](#)
- [Экспорт конфигурационных файлов, лог-файлов и файла с параметрами локальной 2ФА](#)
- [Приложение 1. Сообщения об ошибках](#)

i Термины, определения и аббревиатуры

Двухфакторная аутентификация (2ФА) - тип аутентификации, при которой требуется предъявить 2 фактора. Чаще всего для 2ФА используется фактор владения (например, токен или смарт-карта) и фактор знания (например, PIN-код от устройства).

Однофакторная аутентификация (1ФА) - тип аутентификации, при которой требуется предъявить 1 фактор. Чаще всего для 1ФА используется фактор знания (пароль).

Ключевая пара - набор из открытого и закрытого ключей электронной подписи, однозначно привязанных к друг другу.

Сложный пароль - пароль размером 72 символа в кодировке ASCII (с 33 по 126 символ), хранящийся на токене. Используется для 2ФА.

Учетная запись (УЗ) - совокупность данных, однозначно определяющих пользователя ПК.

Доменная УЗ - учетная запись, зарегистрированная в доменной службе. Используется для управления доступом к сетевым ресурсам в пределах домена, таким как ПК, серверы, файлы и принтеры.

Локальная УЗ - учетная запись, которая создается и хранится на конкретном ПК и используется для доступа к его ресурсам. В отличие от доменной УЗ, локальная не предоставляет доступ к сетевым ресурсам или другим ПК в сети без дополнительной настройки.

Удостоверяющий центр (УЦ) - доверенный орган, который имеет право выпускать сертификаты электронной подписи юридическим и физическим лицам. В рамках "Рутокен Логон для Linux" выпускает сертификаты УЗ для настройки одного из типов доменной 2ФА.

Сертификат - электронный документ, который подтверждает связь электронной подписи с ее владельцем. Сертификат содержит сведения о его владельце, открытый ключ, информацию о сроке действия сертификата, информацию о выдавшем электронную подпись удостоверяющем центре, серийный номер сертификата и иные сведения.

Самоподписанный сертификат - сертификат, генерируемый и подписываемый самой УЗ, без участия УЦ.

Экран приветствия или Greeter - экран входа в операционную систему.

Экран блокировки или Lock Screen - экран блокировки текущей пользовательской сессии с полями для ввода данных УЗ.

КД - контроллер домена.

ОС - операционная система.

ПК - персональный компьютер.

Настоящее руководство администратора предназначено для сотрудников, осуществляющих системное администрирование программного комплекса «Рутокен Логон для Linux» для локальных и доменных УЗ.

Руководство определяет порядок действий при подготовке к установке, установке/удалении и настройке программного комплекса "Рутокен Логон для Linux".

Сотрудники, осуществляющие установку, настройку и обслуживание программного комплекса «Рутокен Логон для Linux», должны обладать следующими навыками и знаниями:

- знание и опыт работы с операционными системами семейства Linux на уровне администратора;
- знание и опыт администрирования компьютерных сетей;
- знание и опыт установки и настройки контроллеров домена.

О программном комплексе

> Назначение

Рутокен Логон для Linux (далее по тексту - `rtlogon`) - это программный комплекс, предназначенный для настройки, управления и использования схемы двухфакторной аутентификации пользователей в ОС семейства Linux. В качестве первого фактора аутентификации используется наличие подключенного к ПК токена, в качестве второго - секрет, хранящийся на токене, доступ к которому предоставляется только после предъявления верного PIN-кода токена.

В качестве секрета может использоваться:

- сложный пароль;
- сертификат.

`rtlogon` поддерживает следующие типы аутентификации:

- по количеству используемых факторов:
 - 2ФА:
 - по наличию подключенного к ПК токена и ключевой паре - 2ФА по сертификату;
 - по наличию подключенного к ПК токена и сложному паролю - 2ФА по сложному паролю.
 - 1ФА по паролю УЗ (настраивается вне `rtlogon`).
- по типу УЗ, для которой настраивается аутентификация:
 - локальная;
 - доменная.

> Состав

rtlogon состоит из следующих компонентов:

- rtlogon-cli;
- rtlogon_event-monitor;
- pam_rtlogon.so;
- GUI:
 - Экран приветствия (Greeter):
 - libfly-dmgreet_rtlogon.so;
 - lightdm-rtlogon-greeter.
 - Экран блокировки (Lock Screen):
 - rtlogon-lock-screen;
 - lightdm-rtlogon-greeter.
- rtlogon_log.

> Описание компонентов

- **rtlogon-cli** - консольная утилита, предназначенная для:
 - настройки ОС для работы с 2ФА;
 - реконфигурации ОС для работы с 2ФА;
 - отключения настроек ОС для работы с 2ФА;
 - создания и удаления 2ФА;
 - создания запроса на получение сертификата УЗ и генерации самоподписанного сертификата (ключевая пара при этом записывается на токен);
 - смены PIN-кода токена;
 - предоставление информации о токене, конфигурации rtlogon и параметрах настроенной локальной 2ФА;
 - экспорта лог-файлов, конфигурационных файлов и файлов с параметрами настроенной локальной 2ФА.
- **rtlogon_event-monitor** - приложение-сервис, предназначенный для:
 - контроля запуска системного экрана блокировки (Lock Screen);
 - контроля за операциями над токеном, использовавшимся при последней аутентификации;
 - выполнения политики при отключении токена от ПК во время активной пользовательской сессии.
- **pam_rtlogon.so** - PAM-модуль, интегрируемый в ОС Linux. Предназначен для аутентификации пользователя с настроенной 2ФА.

- GUI - набор компонентов, реализующих графический пользовательский интерфейс для аутентификации пользователя в ОС:
 - Экран приветствия (Greeter):
 - libfly-dmgreet_rtlogon.so - библиотека (плагин) для экрана приветствия ОС Astra Linux.
 - lightdm-rtlogon-greeter - универсальное приложение, реализующее экраны приветствия и блокировки для экранного менеджера lightdm.
 - Экран блокировки (Lock Screen):
 - rtlogon-lock-screen - приложение экрана блокировки для ОС Astra Linux.
 - lightdm-rtlogon-greeter - универсальное приложение, реализующее экраны приветствия и блокировки для экранного менеджера lightdm.
- rtlogon_log - сервер логирования.

> Описание работы

Для успешного входа в ОС пользователь должен подключить свой токен к ПК и ввести PIN-код токена.

ОС аутентифицирует пользователя на основе данных, размещённых в защищённой памяти токена: сложный пароль или ключевая пара.

rtlogon позволяет настроить политику входа в ОС для локальной аутентификации:

- вход только по сертификату;
- вход по сертификату или логину/паролю;
- вход по сложному паролю.

При доменной аутентификации политика входа в ОС настраивается на стороне КД.

Также rtlogon позволяет настроить политику ОС при отключении токена от ПК:

- вызов экрана блокировки (Lock Screen);
В этом случае для возобновления доступа необходимо снова подключить токен к ПК и ввести PIN-код токена.
- продолжение активной пользовательской сессии.

Доменная 2ФА по сертификату

Для обеспечения доменной 2ФА по сертификату необходима:

1. Генерация сертификата:
 - a. Администратор, используя rtlogon, создает и записывает на токен ключевую пару и формирует запрос на получение сертификата пользователя.
 - b. Администратор передает запрос на сертификат в УЦ.
 - c. УЦ создает сертификат пользователя и отправляет его администратору.
 - d. Администратор загружает сертификат на ПК.
2. Настройка доменной 2ФА по сертификату с использованием rtlogon, в процессе которой сертификат загружается на токен.

3. Аутентификация пользователя ПК:

- a. Пользователь получает токен и подключает его к ПК.
- b. Для входа в домен пользователь инициирует запрос на аутентификацию.
- c. КД отправляет пользователю набор данных для подписи.
- d. Пользователь вводит PIN-код токена для доступа к закрытому ключу, которым подписываются данные.
- e. Подписанные данные передаются КД.
- f. КД проверяет подпись и при положительном результате аутентифицирует пользователя.

Локальная 2ФА по сертификату

Для обеспечения локальной 2ФА по сертификату необходима:

1. Генерация сертификата.

Администратор, используя `rtlogon`, создает и записывает на токен ключевую пару, генерирует сертификат и сам его подписывает (генерирует самоподписанный сертификат).

2. Настройка локальной 2ФА по сертификату с использованием `rtlogon`, в процессе которой сертификат загружается на токен.

3. Аутентификация пользователя ПК:

- a. Пользователь получает токен и подключает его к ПК.
- b. Для входа в ОС пользователь инициирует запрос на аутентификацию.
- c. ОС отправляет пользователю набор данных для подписи.
- d. Пользователь вводит PIN-код токена для доступа к закрытому ключу, которым подписываются данные.
- e. Подписанные данные передаются ОС.
- f. ОС проверяет подпись и при положительном результате аутентифицирует пользователя.

Доменная 2ФА по сложному паролю

Для обеспечения доменной 2ФА по сложному паролю необходима:

1. Настройка доменной 2ФА по сложному паролю в `rtlogon`. В процессе настройки 2ФА осуществляется генерация сложного пароля в КД и его дублирование на токен.

2. Аутентификация пользователя:

- a. Пользователь получает токен и подключает его к ПК.
- b. Для входа в домен пользователь инициирует запрос на аутентификацию.
- c. КД отправляет запрос на предоставление сложного пароля.
- d. Пользователь вводит PIN-код токена для доступа к сложному паролю.
- e. Сложный пароль передается КД.
- f. КД проводит сверку сложных паролей и при положительном результате аутентифицирует пользователя.

Локальная 2ФА по сложному паролю

Для обеспечения локальной 2ФА по сложному паролю необходима:

1. Настройка локальной 2ФА по сложному паролю в `rtlogon`. В процессе настройки 2ФА осуществляется генерация ОС сложного пароля и его дублирование на токен.

2. Аутентификация пользователя:

- a. Пользователь получает токен и подключает его к ПК.
- b. Для входа в ОС пользователь инициирует запрос на аутентификацию.
- c. ОС отправляет запрос на предоставление сложного пароля.
- d. Пользователь вводит PIN-код токена для доступа к сложному паролю.
- e. Сложный пароль передается ОС.
- f. ОС проводит сверку сложных паролей и при положительном результате аутентифицирует пользователя.

Условия применения

> Поддерживаемые устройства



Если у токена отсутствует криптоядро, он может использоваться в rtlogon только для 2ФА со сложным паролем.

- Рутокен Lite;
- Рутокен ЭЦП;
- JaCarta ГОСТ;
- JaCarta PKI/ГОСТ.

> Поддерживаемые платформы

- x86_64;
- ARM64.

> Поддерживаемые ОС

- Astra Linux SE 1.7.2 и новее (включая работу в режиме замкнутой программной среды (ЗПС)) с уровнями защищенности:
 - Орел;
 - Воронеж;
 - Смоленск.



Для корректной работы rtlogon после обновления ОС Astra Linux необходимо выполнить [реконфигурацию ОС для работы с 2ФА](#).

- ОС Альт 8 СП, релиз 10;
- ОС Альт 8.4 СП;
- ОС Альт 10;
- РЕД ОС 7.3;
- РЕД ОС 8.

➤ Поддерживаемые контроллеры домена

- ALD Pro 2.1;
- Active Directory;
- FreeIPA 4.9.11;
- Samba DC версии:
 - 4.13.13 - для Astra Linux 1.7;
 - 4.19.12 - для РЕД ОС 7.3;
 - 4.19.7 - для ОС Альт 10;
 - 4.9.18 - для ОС Альт 8.4.

➤ Необходимые библиотеки и зависимости

- libpam версии:
 - 1.1.8 - для ОС Astra Linux;
 - 1.1.6 - для ОС Альт;
 - 1.1.8 - для ОС РЕД ОС.
- PKCS#11:
 - librtpkcs11esp.so версии 2.14.1 и новее - для устройств Рутокен;
 - libjсPKCS11-2.so версии 2.8.0 и новее - для устройств JaCarta.
- Network manager 1.8.9 и новее;
- krb5-pkinit (для доменной сети);
- sssd-1.16.4;
- pam 1.1.8;
- libc6 2.12;
- pcsc-lite 1.8.22;
- pcsc-lite-ccid 1.4.26;
- pcscd 1.8.22;
- liblightdm-qobject 1.16.7 (кроме ОС Astra Linux);
- glib2 2.46.2;
- qt5-qtbase 5.6.1;
- qt5-x11extras-common 5.6.1;
- libqt5-widgets 5.6.1;
- libqt5-concurrent 5.6.1;
- libqt5-svg 5.6.1;
- libqt5-core 5.6.1;
- lightdm 1.16.7 (кроме ОС Astra Linux);
- libqt5x11extras5 5.6.1 (только для ОС Astra Linux);
- lightdm 1.16.7 (только для ОС Astra Linux);
- liblightdm 1.16.7 (только для ОС Astra Linux);
- libglib2.0-0 2.46.2 (кроме ОС Astra Linux).

Все необходимые для rtlogon зависимости присутствуют в репозиториях поддерживаемых ОС, за исключением библиотеки libjсPKCS11-2.so. При использовании токенов Jacarta эту библиотеку необходимо установить самостоятельно.

Установка библиотеки libjсPKCS11-2.so описана в разделе [Установка библиотеки libjсPKCS11-2.so](#).

Настройка ПК для работы с rtlogon

Для работы с rtlogon необходимо:

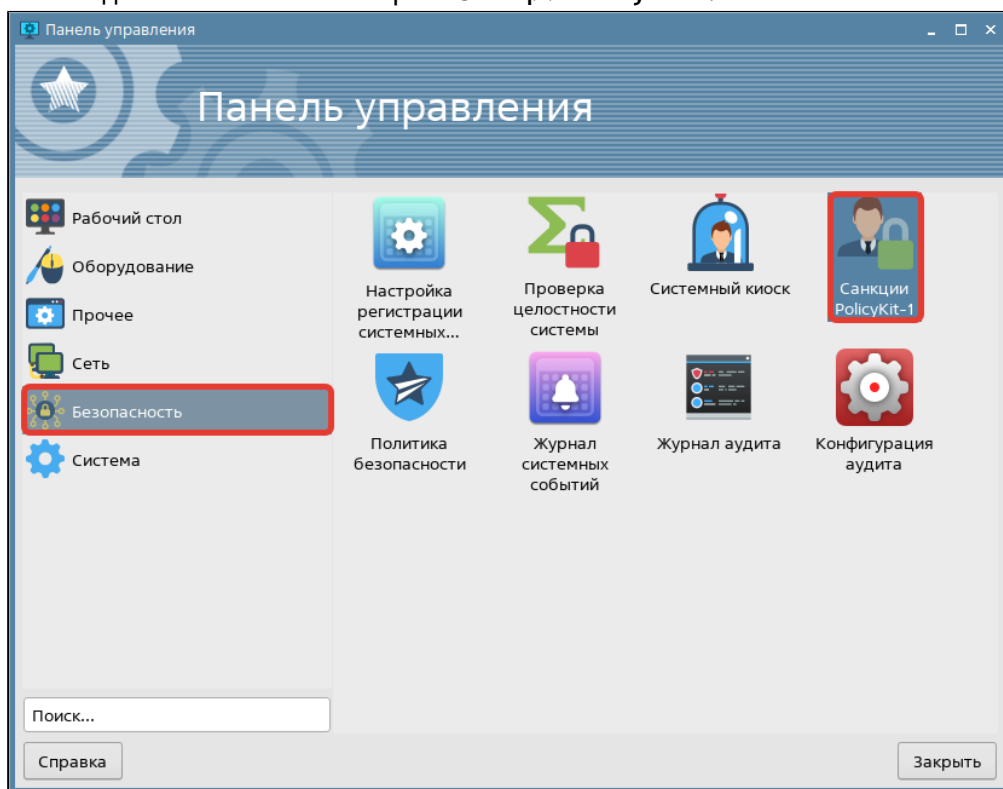
- [настроить работу Network manager для экрана приветствия](#) - для ОС Astra Linux;
- [вести ПК в домен](#) - для использования доменной 2ФА;
- [загрузить сертификат УЦ](#) - для использования доменной 2ФА.

> Настройка Network manager для экрана приветствия ОС Astra Linux

В ОС Astra Linux функциональность Network manager в экране приветствия по умолчанию недоступна.

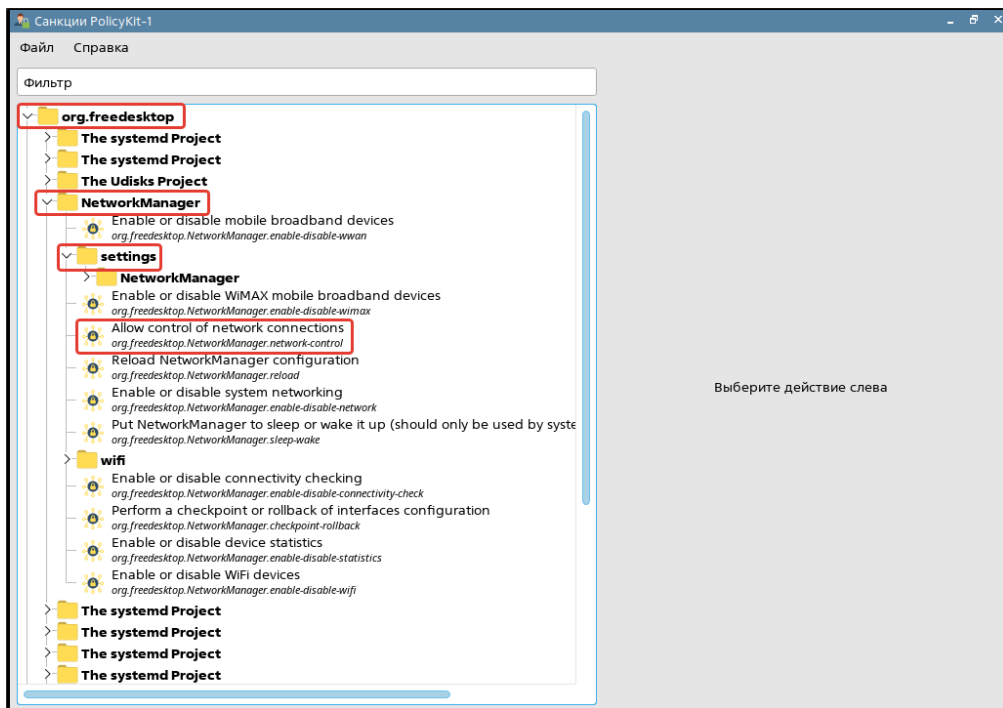
Если требуется включить в экран приветствия возможность работы с сетевым подключением, необходимо:

1. Запустить Панель управления.
2. На вкладке **Безопасность** в выбрать Санкции PolicyKit-1.

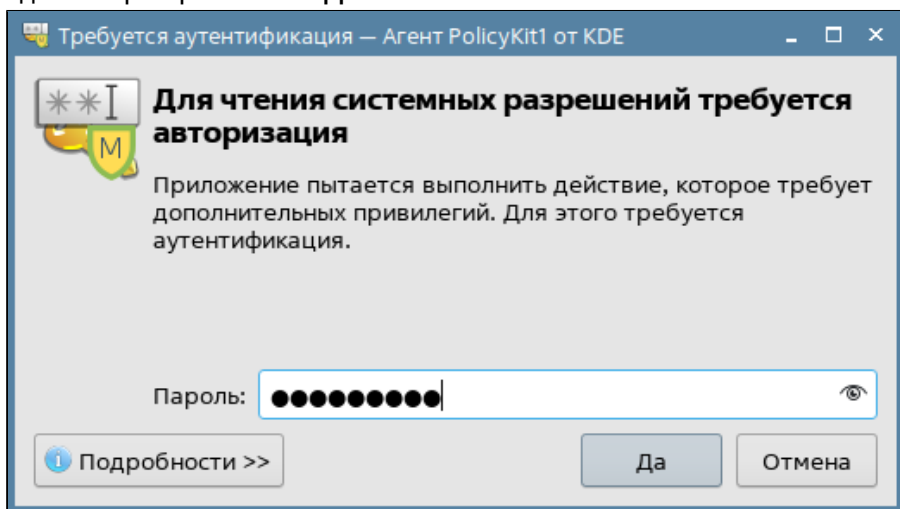


3. В открывшемся окне Санкции PolicyKit-1 выбрать org.freedesktop.

4. В раскрывшемся списке выбрать NetworkManager, далее settings, далее Allow control of network connection.

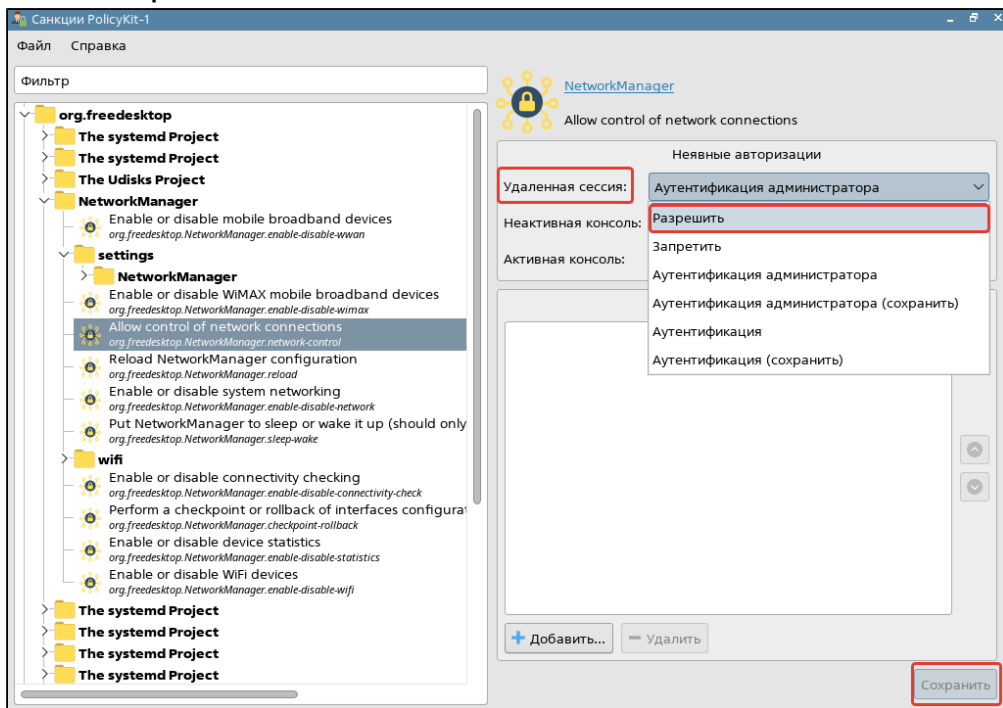


5. При открытии окна Требуется аутентификация - Агент PolicyKit1 от KDE ввести пароль администратора. Нажать Да.



6. В окне Санкции PolicyKit-1, в поле Удаленная сессия из выпадающего списка выбрать Разрешить.

Нажать Сохранить.



7. При открытии окна Требуется аутентификация - Агент PolicyKit1 от KDE ввести пароль администратора. Нажать Да.

8. Закрыть все окна .

> Ввод ПК в домен

Active Directory

ОС Astra Linux

Ввод ПК в домен состоит из следующих основных шагов:

1. Добавить в настройках сетевого подключения IP-адрес DNS-сервера предприятия.
2. Установить утилиту *astra-ad-sssd-client* для ввода ПК в домен.
3. Используя утилиту, ввести ПК в домен.
 Подробная инструкция по вводу ПК в домен представлена на официальном сайте <https://wiki.astralinux.ru/pages/viewpage.action?pageId=27361515>.
4. Установить поиск kerberos-имени и настроек домена через DNS. Для этого необходимо задать значение `True` следующим параметрам в разделе `[libdefaults]` файла `/etc/krb5.conf` :

```
dns_lookup_realm = True
dns_lookup_kdc = True
```

5. Перезагрузить ПК.

Для удобства ввода ПК в домен можно использовать скрипт *configure_ad.sh* для ОС Astra Linux из комплекта поставки, заменив в нем значения параметров на требуемые.

После ввода ПК в домен скрипт нужно удалить, т.к. он содержит логин и пароль администратора.

ОС РЕД ОС

Ввод ПК в домен состоит из следующих основных шагов:

1. Добавить в настройках сетевого подключения IP-адрес DNS-сервера предприятия .
2. Установить утилиту *join-to-domain* для ввода ПК в домен.
3. Используя утилиту, ввести ПК в домен.
 Подробная инструкция по вводу ПК в домен представлена на официальном сайте <https://redos.red-soft.ru/base/arm/arm-domen/arm-msad/prejoindomain/>.
4. Перезагрузить ПК.

Для удобства ввода ПК в домен можно использовать скрипт *configure_ad.sh* для ОС РЕД ОС из комплекта поставки, заменив в нем значения параметров на требуемые.

После ввода ПК в домен скрипт нужно удалить, т.к. он содержит логин и пароль администратора.

ОС Альт



Все шаги по вводу ПК в домен необходимо выполнять в одном терминале.

Ввод ПК в домен состоит из следующих основных шагов:

1. Заменить `[hostname]` на `[current_hostname.domain]` .
2. Отключить плагин *etcdnet-alt* для NetworkManager.
3. Перезапустить NetworkManager.
4. Подключиться к новому сетевому соединению.

5. Добавить в настройках сетевого подключения IP-адрес DNS-сервера предприятия .
6. Установить утилиту *task-auth-ad-sssd* для ввода ПК в домен.
7. Используя утилиту, ввести ПК в домен.
 Подробная инструкция по вводу ПК в домен представлена на официальном сайте <https://docs.altlinux.org/ru-RU/alt-education/10.0/html/alt-education/activedirectory-login--chapter.html>.
8. Перезагрузить ПК.

Для удобства ввода ПК в домен можно использовать скрипт *configure_ad.sh* для ОС Альт из комплекта поставки , заменив в нем значения параметров на требуемые.

После ввода ПК в домен скрипт нужно удалить, т.к. он содержит логин и пароль администратора.

FreeIPA

ОС Astra Linux

Ввод ПК в домен состоит из следующих основных шагов:

1. Настроить разрешение имен. В файле */etc/hosts* необходимо:
 - a. Заменить *[127.0.1.1 hostname]* на *[IP-адрес_ПК hostname.domain]*. При этом запись *hostname.domain* должна быть уникальной и отсутствовать в домене.
 - b. Добавить IP-адрес сервера FreeIPA.
2. Добавить в настройках сетевого подключения IP-адрес DNS-сервера предприятия.
3. Установить утилиту *astra-freeipa-client* для ввода ПК в домен.
4. Используя утилиту, ввести ПК в домен.
 Подробная инструкция по вводу ПК в домен представлена на официальном сайте <https://wiki.astralinux.ru/pages/viewpage.action?pageId=60359750>.
5. Перезагрузить ПК.

Для удобства ввода ПК в домен можно использовать скрипт *configure_freeipa.sh* для ОС Astra Linux из комплекта поставки , заменив в нем значения параметров на требуемые.

После ввода ПК в домен скрипт нужно удалить, т.к. он содержит логин и пароль администратора.

ОС РЕД ОС

Ввод ПК в домен состоит из следующих основных шагов:

1. Заменить *[hostname]* на *[client_name.domain]*.
2. Добавить в настройках сетевого подключения IP-адрес DNS-сервера предприятия .
3. Установить утилиту *ipa-client* для ввода ПК в домен.
4. Используя утилиту, ввести ПК в домен.
 Подробная инструкция по вводу ПК в домен представлена на официальном сайте <https://redos.red-soft.ru/base/arm/arm-domen/redos-in-ipa/>.
5. Перезагрузить ПК.

Для удобства ввода ПК в домен можно использовать скрипт *configure_freeipa.sh* для ОС РЕД ОС из комплекта поставки , заменив в нем значения параметров на требуемые.

После ввода ПК в домен скрипт нужно удалить, т.к. он содержит логин и пароль администратора.

ОС Альт

⊖ Для ОС Альт все шаги по вводу ПК в домен необходимо выполнять в одном терминале.

Ввод ПК в домен состоит из следующих основных шагов:

1. Заменить *[hostname]* на *[hostname.domain]*.
2. Отключить плагин *etcnet-alt* для NetworkManager.
3. Перезапустить NetworkManager.
4. Подключиться к новому сетевому соединению.
5. Добавить в настройках сетевого подключения IP-адрес DNS-сервера предприятия.
6. Установить утилиту *freeipa-client* для ввода ПК в домен.
7. Используя утилиту, ввести ПК в домен.

Подробная инструкция по вводу ПК в домен представлена на официальном сайте <https://docs.altlinux.org/ru-RU/alt-kworkstation/10.1/html/alt-kworkstation/ch57.html>.

8. Перезагрузить ПК.

Для удобства ввода ПК в домен можно использовать скрипт *configure_freeipa.sh* для ОС Альт из комплекта поставки, заменив в нем значения параметров на требуемые.

После ввода ПК в домен скрипт нужно удалить, т.к. он содержит логин и пароль администратора.

ALDPro

ОС Astra Linux

Ввод ПК в домен состоит из следующих основных шагов:

1. Настроить разрешения имен. В файл */etc/hosts* необходимо добавить IP-адрес КД ALDPro.
2. Добавить репозитории ALDPro в каталог */etc/apt/sources.list.d/*.
3. Добавить в настройках сетевого подключения IP-адрес DNS-сервера предприятия.
4. Установить утилиту *aldpro-client* для ввода ПК в домен.
5. Используя утилиту, ввести ПК в домен.
6. Перезагрузить ПК.

Для удобства ввода ПК в домен можно использовать скрипт *configure_ald_pro.sh* для ОС Astra Linux из комплекта поставки, заменив в нем значения параметров на требуемые.

После ввода ПК в домен скрипт нужно удалить, т.к. он содержит логин и пароль администратора.

Samba DC

ОС Astra Linux

Ввод ПК в домен состоит из следующих основных шагов:

1. Добавить в настройках сетевого подключения IP-адрес DNS-сервера предприятия.
2. Установить утилиту *astra-ad-sssd-client* для ввода ПК в домен.
3. Используя утилиту, ввести ПК в домен.

Подробная инструкция по вводу ПК в домен представлена на официальном сайте <https://wiki.astralinux.ru/pages/viewpage.action?pageId=27361515>.

4. Включить поиск kerberos-имени домена через DNS.
5. Включить поиск kerberos-настроек домена через DNS.
6. Перезагрузить ПК.

Для удобства ввода ПК в домен можно использовать скрипт `configure_samba.sh` для ОС Astra Linux из комплекта поставки, заменив в нем значения параметров на требуемые.

После ввода ПК в домен скрипт нужно удалить, т.к. он содержит логин и пароль администратора.

ОС РЕД ОС

Ввод ПК в домен состоит из следующих основных шагов:

1. Добавить в настройках сетевого подключения IP-адрес DNS-сервера предприятия.
2. Установить утилиту `join-to-domain` для ввода ПК в домен.
3. Используя утилиту, ввести ПК в домен.
Подробная инструкция по вводу ПК в домен представлена на официальном сайте <https://redos.red-soft.ru/base/arm/arm-domen/arm-msad/prejoindomain/>.
4. Перезагрузить ПК.

Для удобства ввода ПК в домен можно использовать скрипт `configure_samba.sh` для ОС РЕД ОС из комплекта поставки, заменив в нем значения параметров на требуемые.

После ввода ПК в домен скрипт нужно удалить, т.к. он содержит логин и пароль администратора.

ОС Альт



Все шаги по вводу ПК в домен необходимо выполнять в одном терминале.

Ввод ПК в домен состоит из следующих основных шагов:

1. Заменить `[hostname]` на `[current_hostname.domain]`.
2. Отключить плагин `etnet-alt` для NetworkManager.
3. Перезапустить NetworkManager.
4. Подключиться к новому сетевому соединению.
5. Добавить в настройках сетевого подключения IP-адрес DNS-сервера предприятия.
6. Установить утилиту `task-auth-ad-sssds` для ввода ПК в домен.
7. Используя утилиту, ввести ПК в домен.
Подробная инструкция по вводу ПК в домен представлена на официальном сайте <https://docs.altlinux.org/ru-RU/alt-education/10.0/html/alt-education/activedirectory-login--chapter.html>.
8. Перезагрузить ПК.

Для удобства ввода ПК в домен можно использовать скрипт `configure_samba.sh` для ОС Альт из комплекта поставки, заменив в нем значения параметров на требуемые.

После ввода ПК в домен скрипт нужно удалить, т.к. он содержит логин и пароль администратора.

> Проверка ввода ПК в домен

Чтобы проверить, введен ли ПК в домен, необходимо:

1. Открыть файл `/etc/sss/sss.conf`.
2. Убедиться, что в секции `[sss]` параметру `domains` присвоено значение.

Пример.

```
[sss]
domains = some.domain
```

> Загрузка корневого сертификата или сертификатов цепочки доверия УЦ на ПК

Если сертификат является промежуточным среди сертификатов цепочки доверия УЦ, то файл сертификатов цепочки на ПК должен содержать все промежуточные сертификаты до корневого, который его выписал.

Для этого необходимо выполнить команду:

```
cat cert1.pem cert2.pem cert3.pem >> ca_certs.pem
```

FreeIPA и ALDPro

Корневой сертификат

Корневой сертификат автоматически загружается на ПК в процессе [ввода ПК в домен](#). Дополнительных действий выполнять не требуется.

Сертификаты цепочки доверия УЦ

Чтобы получить список всех сертификатов цепочки доверия УЦ, необходимо выполнить команду:

```
ipa ca-find
```

В результате в терминале появится список с названием всех сертификатов.

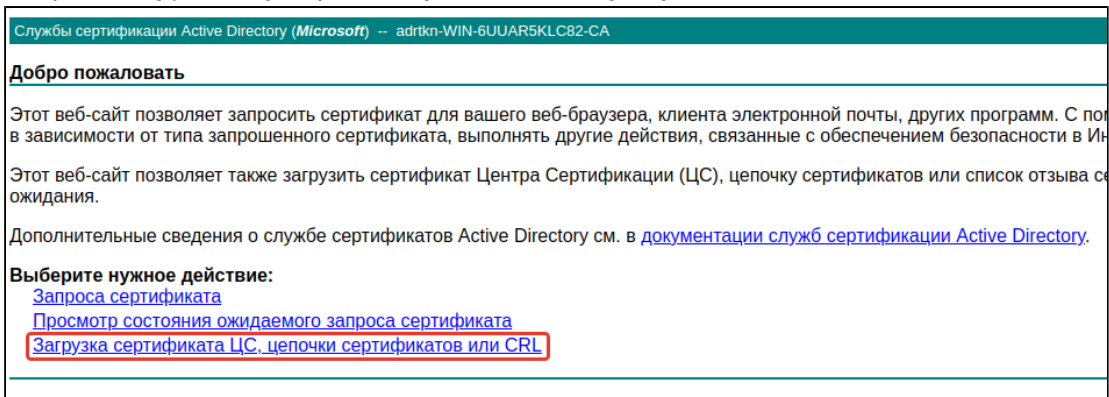
Чтобы загрузить на ПК все сертификаты, необходимо выполнить команду:

```
ipa ca-show "$CA_NAME" --chain --certificate-out chain.pem
```

Active Directory

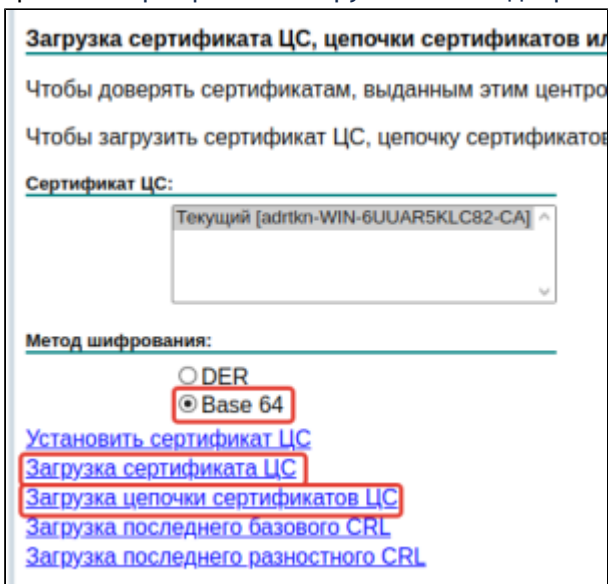
Для загрузки корневого сертификата или сертификатов цепочки доверия УЦ на ПК необходимо:

1. Зайти на веб-интерфейс УЦ КД. Адрес по умолчанию `https://[domain]/certsrv`.
2. Выбрать **Загрузка сертификата ЦС, цепочки сертификатов или CRL**.



3. В поле **Метод шифрования** выбрать **Base 64**.
4. Выбрать **Загрузка сертификата ЦС** или **Загрузка цепочки сертификатов ЦС**. Загрузка на ПК начнется автоматически.

Цепочка сертификатов загружается в виде файла - контейнера формата p7b.



Дополнительно для сертификатов цепочки доверия УЦ:

5. Извлечь сертификаты из контейнера. Для этого можно использовать утилиту `openssl`.
6. Собрать сертификаты цепочки в один файл с помощью команды `cat`.

Пример.

```
cat cert1.pem cert2.pem cert3.pem >> ca_certs.pem
```

Samba DC

КД Samba DC не имеет встроенного УЦ.

Схема загрузки корневого сертификата или сертификатов цепочки доверия УЦ на ПК пользователя зависит от выбранных администратором УЦ и выполненных на них настроек.

Установка rtlogon

1. Скопировать с поставочного диска или скачать с официального сайта Компании "Актив" установочный пакет rtlogon для необходимой платформы ПК и ОС:
 - a. rutokenlogon-[версия rtlogon]-astra1_arm64.deb - для ОС Astra Linux на ARM64;
 - b. rutokenlogon_[версия rtlogon]-astra1_amd64.deb - для ОС Astra Linux на x86_64;
 - c. rutokenlogon-[версия rtlogon]-alt1.aarch64.rpm - для ОС Альт на ARM64;
 - d. rutokenlogon-[версия rtlogon]-alt1.x86_64.rpm - для ОС Альт на x86_64;
 - e. rutokenlogon-[версия rtlogon]-1.aarch64.rpm - для ОС РЕД ОС и rpm-based дистрибутивов на ARM64;
 - f. rutokenlogon-[версия rtlogon]-1.x86_64.rpm - для ОС РЕД ОС и rpm-based дистрибутивов на x86_64;
 - g. rutokenlogon_[версия rtlogon]-1_arm64.deb - для deb-based дистрибутивов на ARM64;
 - h. rutokenlogon_[версия rtlogon]-1_amd64.deb - для deb-based дистрибутивов на x86_64.
2. Открыть терминал.
3. Перейти в каталог расположения установочного пакета.
4. Ввести в терминале команду:

```
Astra Linux and deb-based distributives
```

```
sudo apt install ./[the name of the installation package rtlogon].deb
```

```
Alt Linux
```

```
sudo apt-get install ./[the name of the installation package rtlogon].rpm
```

```
RED OS and rpm-based distributives
```

```
sudo dnf install ./[the name of the installation package rtlogon].rpm
```

5. При запросе ввести пароль администратора.
6. При запросе подтвердить выполнение операции, нажав **Enter** или введя **Д**.
7. Дождаться окончания установки.
8. Ввести в терминале команду:

```
rtlogon-cli --version
```

9. Проверить наличие в терминале сообщения с номером установленной версии rtlogon.

```
user@B3381-PC:~$ rtlogon-cli --version
0.1.0
user@B3381-PC:~$ █
```

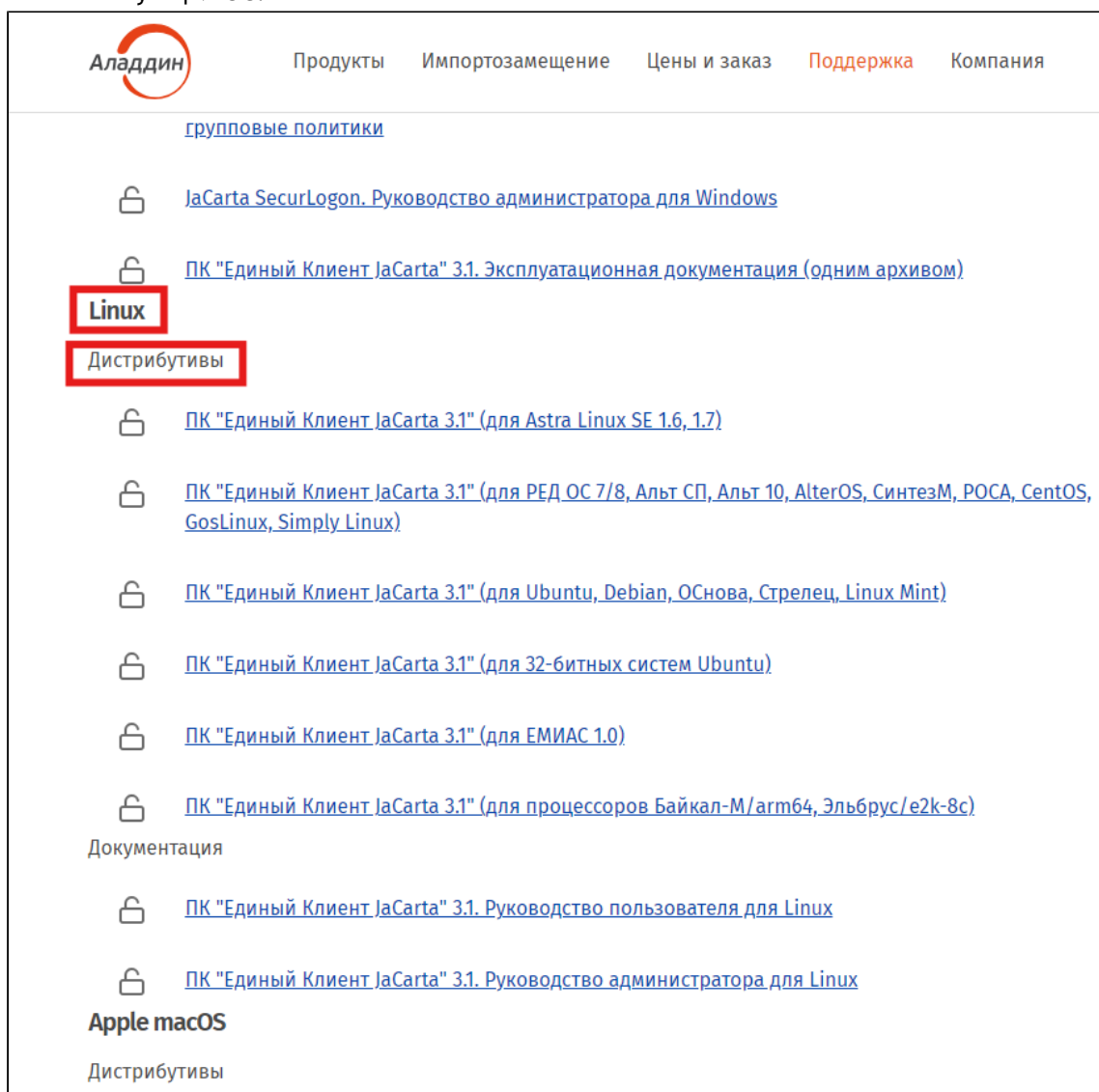
Установка rtlogon завершена.

Установка библиотеки libjcPKCS11-2.so

Для работы rtlogon с устройствами JaCarta необходимо скачать и установить библиотеку libjcPKCS11-2.so.

Для этого:

1. Перейти на сайт <https://www.aladdin-rd.ru/support/downloads/jacarta/>.
2. На странице в разделе **Linux Дистрибутивы** выбрать ПК "Единый Клиент JaCarta 3.1" для соответствующей ОС.



3. На открывшейся странице нажать кнопку **Скачать**.
4. Распаковать скачанный архив.
5. Открыть терминал.
6. Перейти в терминале в каталог распакованного архива.

7. Ввести команду:

Astra Linux and deb-based distributives

```
sudo apt install ./jcpkcs11-2[*].deb
```

Alt Linux

```
sudo apt-get install ./jcpkcs11-2[*].rpm
```

RED OS and rpm-based distributives

```
sudo dnf install ./jcpkcs11-2[*].rpm
```

8. Переместить библиотеку *libjсPKCS11-2.so* из каталога */usr/lib* в каталог */opt/aktivco/rtlogon/lib*:

```
sudo cp /usr/lib/libjсPKCS11-2.so /opt/aktivco/rtlogon/lib/
```

Установка библиотеки завершена.

Команды и общие параметры rtlogon


Команда /параметр	Описание
Команды	
configure	Настройка ОС для работы с 2ФА
reconfigure	Реконфигурация ОС для работы с 2ФА
unconfigure	Отключение настроек ОС для работы с 2ФА
setup-auth	Настройка 2ФА
unsetup-auth	Удаление 2ФА
create-cert	Создание запроса на получение сертификата, генерация самоподписанного сертификата
change-pin	Смена PIN-кода токена
collect-log	Экспорт конфигурационных файлов, лог-файлов и файла с параметрами локальной 2ФА
info	Запрос информации о конфигурации rtlogon и параметрах локальной 2ФА
Параметры	
-h или --help	Получение перечня команд и общих параметров rtlogon. При вызове с любой командой rtlogon выводит перечень ее параметров
--version	Получение информации о версии установленного rtlogon

Обновление rtlogon

Для обновления rtlogon необходимо:


1. [Удалить старый пакет rtlogon с ПК.](#)
2. [Установить новый пакет rtlogon.](#)


Удаление rtlogon

 При удалении rtlogon могут быть удалены все его зависимости, в том числе экранный менеджер lightdm. Удаление экранного менеджера lightdm из графической сессии, при входе в которую он использовался, приведет к закрытию текущей сессии пользователя и необходимости перезагрузить ПК.

Также при удалении rtlogon можно потерять доступ к УЗ с настроенной 2ФА по сложному паролю.

Поэтому **перед удалением rtlogon рекомендуется [отключить настройки ОС для работы с 2ФА](#) и перезагрузить ПК.**

 Если конфигурационный файл rtlogon.conf был поврежден, то перед удалением rtlogon в ОС Альт и ОС РЕД ОС, необходимо вручную восстановить конфигурационный файл, используя бэкап, или отключить настройки ОС для работы с 2ФА, выполнив команду [rtlogon-cli unconfigure](#).

 После удаления rtlogon администратор должен заново задать пароли для входа в ОС УЗ, у которых была настроена 2ФА со сложным паролем.

Для удаления rtlogon необходимо:

1. Ввести команду:

Astra Linux and deb-based distributives

```
sudo apt remove rutokenlogon
```

Alt Linux

```
sudo apt-get remove rutokenlogon
```

RED OS and rpm-based distributives

```
sudo dnf remove rutokenlogon
```

2. При запросе ввести пароль администратора.

3. Проверить, что rtlogon был удален с ПК:

а. Ввести команду:

```
Astra Linux and deb-based distributives
```

```
dpkg -s rutokenlogon
```

```
RED OS, Alt Linux and rpm-based distributives
```

```
rpm -q rutokenlogon
```

б. Убедиться, что в терминале выводится пустая строка.

Удаление rtlogon с ПК завершено.

Настройка ОС для работы с 2ФА

При настройке ОС выполняются следующие операции:

- сбор данных о механизме отключения ПК и блокировки сессии;
- изменение конфигурации PAM-модулей ОС для внедрения pam_rtlogon.so;
- внедрение плагина для экрана приветствия и экрана блокировки (для ОС Astra Linux и дистрибутивов, поддерживающих экранный менеджер lightDM);
- конфигурирование pam_sssd (для доменной аутентификации).



В плагине для экрана приветствия, основывающимся на экранном менеджере lightDM, поддерживаются языки раскладки клавиатуры, которые были добавлены через localectl.

При вызове экрана блокировки в дистрибутивах, поддерживающих скринсейверы, возможно его произвольное открытие в другом tty.

Для проверки поддержки ОС скринсейвера используется команда `[gui]-screensaver-command --query`.




Перед настройкой ОС для работы с доменной 2ФА по сертификату на ПК должен быть [загружен корневой сертификат или сертификаты цепочки доверия УЦ](#).

Для настройки ОС необходимо ввести в терминале команду:

```
rtlogon-cli configure [command parameters]
```


Command parameters

Параметр	Описание	Значение по умолчанию	Наличие параметра в команде	Условие применения
<code>--domain arg</code>	Тип КД. Допустимые значения: ipa, aldprow, ad, samba	-	Обязательно	Необходимо настроить ОС для работы с доменной 2ФА
<code>--local</code>	Настройка ОС для работы с локальной 2ФА	-	Обязательно	Необходимо настроить ОС для работы с локальной 2ФА <div style="border: 1px solid red; padding: 5px; background-color: #ffe6e6;"> <p> Запрещена одновременная установка с параметром <code>--domain</code>.</p> <p>Эти 2 параметра являются взаимоисключающими.</p> </div>
<code>--ca-cert arg</code>	Путь к файлу, содержащему корневой сертификат или сертификаты цепочки доверия УЦ	<code>/etc/ipa/ca.crt</code>	Опционально	Необходимо настроить ОС для работы с доменной 2ФА по сертификату
<code>--use-system-gui arg</code>	Использование системных экранов приветствия и блокировки. Допустимые значения: yes, no	no	Опционально	Если необходимо использовать системные экраны приветствия и блокировки, указывать значение yes . Если необходимо использовать экраны приветствия и блокировки rtlogon , указывать значение no

Примеры

```
sudo rtlogon-cli configure --local --use-system-gui yes
//OS setup for local 2FA; using system Greeter and Lock Screen
sudo rtlogon-cli configure --domain ad --ca-cert ert.pem
//OS setup for domain certificate 2FA
```


Реконфигурация ОС для работы с 2ФА

 Перед изменением настроек ОС должна быть сконфигурирована для работы с 2ФА, т.е. должна быть выполнена команда [rtlogon-cli configure](#).

Для реконфигурации ОС необходимо ввести в терминале команду:

```
sudo rtlogon-cli reconfigure [command parameters]
```

Command parameters

Параметр	Описание	Наличие параметра в команде	Условие применения
--domain arg	Тип КД. Допустимые значения: ipa, aldro, ad, samba	Опционально	Необходимо настроить ОС для работы с доменной 2ФА
--local	Настройка ОС для работы с локальной 2ФА	Опционально	Необходимо настроить ОС для работы с локальной 2ФА <div style="border: 1px solid red; padding: 5px; background-color: #ffe6e6;"> <p> Запрещена одновременная установка с параметром --domain. Эти 2 параметра являются взаимоисключающими.</p> </div>
--ca-cert arg	Путь к файлу, содержащему корневой сертификат или сертификаты цепочки доверия УЦ	Опционально	Необходимо настроить ОС для работы с доменной 2ФА по сертификату

Параметр	Описание	Наличие параметра в команде	Условие применения
<code>--use-system-gui arg</code>	Использование системных экранов приветствия и блокировки. Допустимые значения: <code>yes</code> , <code>no</code>	Опционально	Если необходимо использовать системные экраны приветствия и блокировки, указывать значение yes Если необходимо использовать экраны приветствия и блокировки rtlogon , указывать значение no

Если команда вызывается без параметров, то для настройки ОС будут использоваться значения, указанные в конфигурационном файле `rtlogon.conf`.

Реконфигурацию ОС без указания параметров рекомендуется использовать в следующих случаях:

- после выхода из строя ОС;
- после обновления ОС (для Astra Linux).

Отключение настроек ОС для работы с 2ФА

Для отключения настроек ОС необходимо ввести в терминале команду:

```
sudo rtlogon-cli unconfigure
```

Если файл `rtlogon.conf` не повреждён, то в результате выполнения этой команды вернется в исходное состояние:

- конфигурация PAM-модулей системы и `pam_sssd`;
- плагин для системных экранов приветствия и блокировки.

⊖ После выполнения команды `sudo rtlogon-cli unconfigure` для локальных УЗ необходимо заново настроить 2ФА.

Настройка 2ФА

⊖ Перед настройкой доменной 2ФА ОС должна быть сконфигурирована для работы с этим типом аутентификации т.е. должна быть выполнена команда [rtlogon-cli configure](#) с доменными параметрами.

⊖ Для настройки доменной 2ФА необходимо, чтобы время на ПК совпадало с серверным.

Для настройки 2ФА необходимо:


1. Подключить токен к компьютеру.
2. Для настройки доменной 2ФА по сертификату:
 - a. [Создать запрос на получение сертификата.](#)
 - b. [Получить сертификат УЗ от УЦ.](#)
3. Для настройки локальной 2ФА по сертификату - [сгенерировать самоподписанный сертификат](#);
4. Ввести в терминале команду:

```
sudo rtlogon-cli setup-auth [command parameters]
```


ⓘ При помощи команды `rtlogon-cli setup-auth` можно настраивать 2ФА для другого ПК (с указанием соответствующего домена). В этом случае команда вводится без `sudo`.


Command parameters

Параметр	Описание	Значение по умолчанию	Наличие параметра в команде	Условия применения
Общие параметры				
-l arg или --login arg	Логин УЗ, для которой настраивается 2ФА	-	Обязательно	
-d arg или --domain arg	Имя домена, в котором зарегистрирована УЗ	-	Опционально	Для доменных УЗ

Параметр	Описание	Значение по умолчанию	Наличие параметра в команде	Условия применения
<code>--disconnect-policy arg</code>	<p>Политика ОС при отключении токена от ПК.</p> <p>Возможные значения:</p> <ul style="list-style-type: none"> ■ lock - вызов экрана блокировки; ■ none - продолжение текущей сессии 	lock	Опционально	Необходимо отключить вызов экрана блокировки при отключении токена от ПК
<code>--token-id arg</code>	<p>Идентификатор токена, к которому применяется команда</p> <div style="border: 1px solid #add8e6; padding: 10px; margin-top: 10px;"> <p> Как правило, идентификатор токена - это его серийный номер. Для некоторых моделей (комбинированные устройства JaCarta-2 PKI/ГОСТ и т.п.) - это серийный номер и постфикс, обозначающий апплет (-PKI/-GOST и т.п.).</p> <p>Для просмотра информации об идентификаторе токена необходимо вызвать команду rtlogon-cli info.</p> </div>	-	Опционально	К ПК подключено несколько токенов или один комбинированный токен

Параметр	Описание	Значение по умолчанию	Наличие параметра в команде	Условия применения
-p arg или --pin arg	PIN-код токена, к которому применяется команда. При вводе PIN-код отображается в явном виде	-	Опционально	Необходимо явно указать PIN-код токена. Если не указать параметр, после ввода команды в терминале появится запрос на ввод PIN-кода. При вводе PIN-код не отображается
Параметры настройки 2ФА по сложному паролю				
--passwd	Признак настройки 2ФА по сложному паролю	-	Обязательно	
-e arg или --expire-days arg	Количество дней до регенерации сложного пароля	-	Опционально	Необходимо задать количество дней до регенерации сложного пароля. Если параметр не указан, регенерация сложного пароля не производится
--domain-admin arg	Логин администратора	-	Опционально	Настройка доменной 2ФА по сложному паролю
Параметры настройки 2ФА по сертификату				
-c arg или --cert arg	Путь к сертификату УЗ. В случае, когда сертификат располагается в текущей директории, допускается указывать только его наименование	-	Обязательно	

Параметр	Описание	Значение по умолчанию	Наличие параметра в команде	Условия применения
--login-policy arg	<p>Политика входа в ОС.</p> <p>Возможные значения:</p> <ul style="list-style-type: none"> ■ certonly - только по сертификату и наличию подключенного токена; ■ certandpass - по сертификату и наличию подключенного токена или по логину/паролю УЗ. Выбор осуществляется при входе в ОС <div style="border: 1px solid red; padding: 5px; margin-top: 10px;"> <p> Для администратора может быть установлен только certandpass.</p> </div>	certonly	Опционально	<p>Настройка локальной 2ФА по сертификату.</p> <p>Необходимо изменить политику входа в ОС</p>

 Рекомендуется для смены политики ОС при отключении токена от ПК после выполнения команды перезагрузить ПК.

Примеры:

Local certificate 2FA

```
sudo rtlogon-cli setup-auth --login user2 --cert cert.pem --disconnect-policy lock --login-policy certonly
// Login is only by certificate 2FA; OS policy when token and PC are disconnected is block session
sudo rtlogon-cli setup-auth -l user -c cert.pem --disconnect-policy none --login-policy certandpass
// Login is by account login/password or certificate 2FA
```

Local strong password 2FA

```
sudo rtlogon-cli setup-auth --login user2 --passwd --disconnect-policy none
```


Domain certificate 2FA

```
rtlogon-cli setup-auth -c cert.pem --domain "$DOMAIN" --login "$DOMAIN_USER"
```

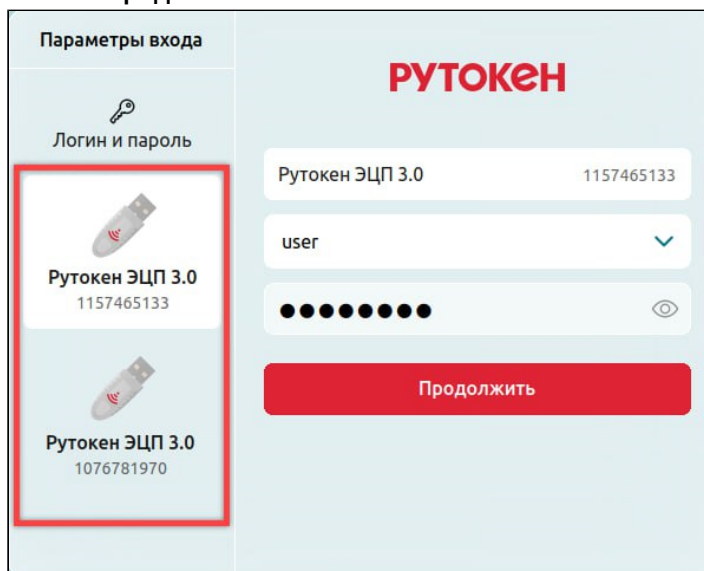
Domain strong password 2FA

```
rtlogon-cli setup-auth --domain "$DOMAIN" --login "$DOMAIN_USER" --passwd -p 12341234
// enter domain admin login and password
rtlogon-cli setup-auth --domain "$DOMAIN" --login "$DOMAIN_USER" --passwd -p 12341234 --domain-admin "$DOMAIN_ADMIN"
// enter domain admin password
rtlogon-cli setup-auth --domain "$DOMAIN" --login "$DOMAIN_USER" --passwd -p 12341234 --domain-type <ipa|aldpro|ad>
// enter domain type
```

Проверка настройки 2ФА

Для проверки настроек 2ФА необходимо:

1. Завершить текущую сессию.
2. Переподключить токен к ПК.
3. На экране приветствия **tlogon**:
 - a. Выбрать в списке устройств необходимый токен.
 - b. В раскрывающемся списке **Логин** выбрать логин необходимой УЗ.
 - c. Ввести PIN-код токена в поле **PIN-код**.
 - d. Нажать **Продолжить**.



4. На системном экране приветствия:
 - a. Ввести логин УЗ.
 - b. Ввести PIN-код токена.

Если 2ФА была настроенная корректно, пользователь успешно войдет в ОС.

Изменение настроек 2ФА

Для изменения настроек 2ФА необходимо снова вызвать команду [rtlogon-cli setup-auth](#) с указанием нужным параметров.

Удаление 2ФА

- ⊖ Перед удалением доменной 2ФА ОС должна быть сконфигурирована для работы с этим типом аутентификации т.е. должна быть выполнена команда [rtlogon-cli configure](#) с доменными параметрами.

Для удаления 2ФА необходимо:


1. Если требуется удалить 2ФА для УЗ только с токена или с токена и ПК, необходимо подключить токен к ПК. В противном случае данный пункт пропустить.
2. Ввести в терминале команду:

```
sudo rtlogon-cli unsetup-auth [command parameters]
```

3. При запросе дважды ввести новый пароль для УЗ.

- ⓘ При помощи команды `rtlogon-cli unsetup-auth` можно удалить 2ФА для УЗ другого ПК (при помощи указания домена или id ПК). В этом случае команда вводится без `sudo`.

Command parameters

Параметр	Описание	Значение по умолчанию	Наличие параметра в команде	Условие применения
-l arg или --login arg	Логин УЗ, для которой удаляется 2ФА	-	Обязательно	
-d arg или --domain arg	Имя домена, в котором зарегистрирована УЗ	-	Опционально	Для доменных УЗ
--host-id arg	Идентификатор ПК, к которому привязана УЗ	-	Опционально	Удаление 2ФА для УЗ, привязанной к другому ПК с идентификатором <i>host-id</i>
--token-id arg	Идентификатор токена, к которому применяется команда <div data-bbox="405 1155 783 2040" style="border: 1px solid #add8e6; padding: 10px; background-color: #e6f2ff;"> <p> Как правило, идентификатор токена - это его серийный номер. Для некоторых моделей (комбинированные устройства JaCarta-2 PKI/ГОСТ и т.п.) - это серийный номер и постфикс, обозначающий апплет (-PKI/-GOST и т.п.).</p> <p>Для просмотра информации об идентификаторе токена необходимо вызвать команду rtlogon-cli info</p> </div>	-	Опционально	К ПК подключено несколько токенов или один комбинированный токен

Параметр	Описание	Значение по умолчанию	Наличие параметра в команде	Условие применения
-p arg или --pin arg	PIN-код токена, к которому применяется команда. При вводе PIN-код отображается в явном виде	-	Опционально	Необходимо явно указать PIN-код токена. Если не указать параметр, после ввода команды в терминале появится запрос на ввод PIN-кода. При вводе PIN-код не отображается
--ignore-token	Удалить 2ФА для УЗ только с ПК. На токене 2ФА для УЗ сохраняется	-	Опционально	Для локальных УЗ
--keep-cert-and-key	Удалить 2ФА для УЗ с ПК и токена с сохранением ключевой пары и сертификата	-	Опционально	Удаление 2ФА для УЗ с ПК и токена с сохранением ключевой пары и сертификата
--only-on-token	Удалить 2ФА для УЗ только с токена. На ПК 2ФА для УЗ сохраняется	-	Опционально	Удаление 2ФА для УЗ только с токена
--domain-admin arg	Логин администратора	-	Опционально	Удаление доменной 2ФА по сложному паролю для УЗ



Если вызвать команду `rtlogon-cli unsetup-auth` без следующих параметров, то 2ФА для УЗ удаляется и с токена, и с ПК:

- `--ignore-token;`
- `--keep-cert-and-key;`
- `--only-on-token.`

Ключевая пара и сертификат при этом не сохраняются.

Примеры:

Remove local 2FA

```
sudo rtlogon-cli unsetup-auth -l "$LOCAL_USER" --pin <PIN-code>
```

Remove domain 2FA

```
rtlogon-cli unsetup-auth -l "$DOMAIN_CERT_USER" -d "$DOMAIN" --pin <PIN-code>
rtlogon-cli unsetup-auth -l "$DOMAIN_PASSWD_USER" -d "$DOMAIN" --pin <PIN-code>
// enter domain admin login and password
rtlogon-cli unsetup-auth -l "$DOMAIN_PASSWD_USER" -d "$DOMAIN" --pin <PIN-code> --domain-admin "$DOMAI
N_ADMIN"
// enter domain admin password
rtlogon-cli unsetup-auth -l "$DOMAIN_PASSWD_USER" -d "$DOMAIN" --pin <PIN-code> --domain-type
<ipa|aldpro|ad>
// enter domain type
```

Remove local 2FA for other PC

```
rtlogon-cli unsetup-auth -l "$LOCAL_USER" --host-id "$HOST_ID" --pin <PIN-code>
```

Remove domain 2FA with key pair and certificate saved


```
rtlogon-cli unsetup-auth -l "$DOMAIN_USER" -d "$DOMAIN" --keep-cert-and-key --pin <PIN-code>
```

Создание запроса на получение сертификата, генерация самоподписанного сертификата

1. Подключить токен к ПК.
2. Ввести в терминале команду:

```
rtlogon-cli create-cert [certificate parameters] [token parameters] [certificate content]
```

Command parameters

Параметр	Описание	Значение по умолчанию	Наличие параметра в команде	Условие применения
Certificate parameters				
-a arg или --alg arg	Криптоалгоритм создания сертификата. Доступные значения: <ul style="list-style-type: none"> ■ rsa; ■ gost256; ■ gost512 	rsa с длиной ключа 2048	Опционально	Необходимо изменить криптоалгоритм с rsa на другой доступный
-s или --self-signed	Признак генерации самоподписанного сертификата	-	Опционально	Генерация самоподписанного сертификата
-o arg или --output arg	Путь к сохраняемому на ПК сертификату. В случае, если сертификат будет располагаться в текущей директории, допускается указывать только его наименование <div style="border: 1px solid #f08080; padding: 10px; margin-top: 10px;"> <p> rtlogon поддерживает следующие форматы сертификатов:</p> <ul style="list-style-type: none"> ■ pem; ■ der </div>	-	Обязательно	
Token parameters				

Параметр	Описание	Значение по умолчанию	Наличие параметра в команде	Условие применения
--token-id arg	<p>Идентификатор токена, к которому применяется команда</p> <div style="border: 1px solid #add8e6; padding: 10px; margin: 10px 0;"> <p>i Как правило, идентификатор токена - это его серийный номер. Для некоторых моделей (комбинированные устройства JaCarta-2 PKI /ГОСТ и т.п.) - это серийный номер и постфикс, обозначающий апплет (-PKI/-GOST и т.п.).</p> <p>Для просмотра информации об идентификаторе токена необходимо вызвать команду rtlogon-cli info.</p> </div>	-	Опционально	Если к ПК подключено несколько токенов или один комбинированный токен
-p arg или --pin arg	<p>PIN-код токена, к которому применяется команда.</p> <p>При вводе PIN-код отображается в явном виде</p>	-	Опционально	<p>Необходимо явно указать PIN-код токена.</p> <p>Если не указать параметр, после ввода команды в терминале появится запрос на ввод PIN-кода. При вводе PIN-код не отображается</p>
Certificate content				
--dn CN arg	<p>Фамилия владельца УЗ. Указывается одним словом. Используемый алфавит: латинский</p>	-	Обязательно	
--dn C arg	<p>Страна. Для обозначения используется двухбуквенный код страны в соответствии с ISO 3166</p>	RU	Опционально	Необходимо изменить название страны

Параметр	Описание	Значение по умолчанию	Наличие параметра в команде	Условие применения
--dn ST arg	Область (край и т.д.). Указывается одним словом. Используемый алфавит: латинский	-	Опционально	Необходимо указать название области
--dn STREET arg	Улица. Указывается одним словом. Используемый алфавит: латинский	-	Опционально	Необходимо указать название улицы
--dn L arg	Город. Указывается одним словом. Используемый алфавит: латинский	-	Опционально	Необходимо указать название города
--dn O arg	Название организации. Указывается одним словом. Используемый алфавит: латинский	-	Опционально	Необходимо указать название организации
--days arg	Время действия сертификата (в днях). Максимальное значение: 5500 дней . Датой начала действия сертификата является дата выполнения команды <code>create-cert</code>	1095 дней (3 года)	Опционально	Для самоподписанного сертификата. Необходимо изменить срок его действия

Пример

Create self-signed certificate

```
rtlogon-cli create-cert -s -o cert.pem -p 12345678 --dn CN Petrova --dn C BB --dn ST Lilovaja --dn L Saratov --dn O Pulse --days 365
```

Create a request for a certificate

```
rtlogon-cli create-cert -a gost256 -o cert.pem -p 12345678 --dn CN Petrova --dn C BB
```


Request file content

```

-----BEGIN CERTIFICATE-----
MIIEsDCCApGCAQAwDQYJKoZIhvcNAQELBQAwHjEPMA0GA1UEAwGyWxkcHJvMQsw
CQYDVQQGEwJVSTAEFw0yNDA5MDkxNDQ5NTRaFw0yNzA5MDkxNDQ5NTRaMB4xDzAN
BgNVBAMMBmFsZHBzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVz
DWAwwGIIKAAoICAQDHGEBEgZKouPLusCh80U/r8c5q0gNSzV83GzJJRjLzo5fcUK7p
eNzTx2dPQL6moUrLQrpgAiFW08ZsI42S4QAg8A8+AL58nNnrmdCbahc j8LPvY9uZ
u3SV08bts4PfH6kqk9xgX5LVOrXvFw2k4a+A+7h+n/9fWDy1aRv+8Au9whN6XRaj
Mr6a4HzF22ohpxwRRL8HVWA33Kxrpvt3OsnG7Tw50tpNXyKl jppQRoIJJSwsZ0Kwn
+6kIAh2T6L6odQmToA/cJi5IjHcuRx7Pef3qOqHj0CiojARY24Hkx7p8SsYddfvx
D8TN6gov1/FJ7QJNqkPkYr6bCr6 jAoS6XzP8VoMV7ftj3JUONJRqrdVL4imR7 jwE
qcMV1uLfi8W2d3eIesr0jpTAWLT19ObK7gH61HR10NQIgrYgDnV04ZKq8b4R13
bi6c0/Aq/c7MiB1TIF5nT4NG8zio7u3xTdyRELZb6As5eqTRWpI0wMdQvhtbLmtQ
XbFR9CEQmZhAllP4CTvCN/bAEIA6BpHJdq8dXVPOYHQ7OCFmvOLEDvrBjQiPdhhZ
p1Lr4sFrrPrj4vEA/Fz7z0KmlN8wGZIxBrPRvCGeuBF5A8bgxhOMubZjibEagt2+
m4QC6Zo5KJRsZVWgiR9qnWr+bV3wPPNvbbQvJchSy8bAastvz06VIJt6QIDAQAB
MA0GCSqGSIB3DQEBEwUAA4ICAQBLI8Jx0+z+vfyPUIdnCrOPubp7XiWw76pXQIno
B9suGdXkHytahq0am7+9A3E3rmgyNh8tvOkSmkmCM2cMMreeHWlpSiQp58J5tEiT
uZGpp1Ap+FQpFRYqQQ7Ibzhmi2sb5qQ2C01q+2+QGEMySxKIt+idLhmp+Hf2xK+m
1D9vqQLdJ5W1TqpvsxcNI9ybSwl8qtM0qs9xWbRP+M9G0FGrvZR2pYhVzQYOYVWh
V6wRDxMDzqKeh3vzOdcIi22b06FxA1DQ5qI6xIuE0JmGiplPzgK0TKCnr8YFSQ9W
fjA+Unfu+rED1kf/j3a2ErmqdAvfYAlgyNjNluq907NGMzMolzJr0KmGSOQESXW0
9ohhxxQdl8cOg/zqZWbvXjv5WaELsblVEF0dS1wFetva0PVCsua3eITX/loWvhZR
n7spWnYfKpVMgwyKraoFAC/2h0N88v2XvetnA0YvYOLxeolHt1FWvLWsdkiD1Wk+
3yXuNsFvA+s/uzO/HchGMvF7Q1IeWhdwsriGgGbjpJn5VMiKnLvykJbC07X1fZmo
pWe4wEkG5h7FTZlOmYwbNvbfDFgTudmaSnTiydNxjFND0pekVqRPCu7XDuv4BexE
3qeL36190tSCznEfhfZvPfu2unEBi1NkRQ/Gmqt00KmIDKcAwjgwxKU1IZ6801YO
qR4Lxg==
-----END CERTIFICATE-----

```

Получение сертификата УЗ от УЦ

> FreeIPA и ALDPro

После создания запроса на получение сертификата необходимо ввести следующие команды:

```

kinit [admin login]

ipa cert-request [the path to the certificate request file] --principal [domain account login for
which certificate is being issued] --ca [certification center type] --profile-id [certification
center ID profile] --certificate-out [certificate name]

kdestroy

```

При запросе ввести пароль администратора.

Пример

```
kinit admin

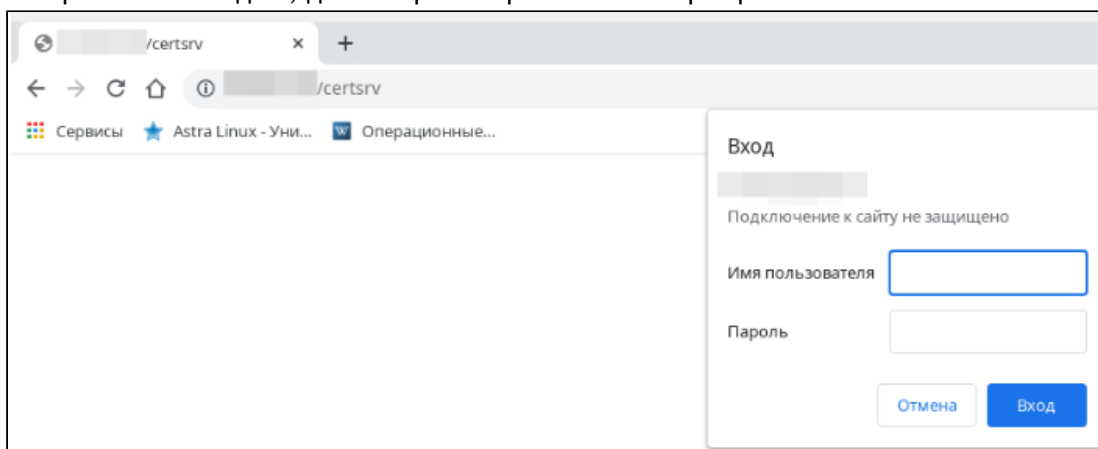
ipa cert-request ./cert.req --principal user3 --ca ipa --profile-id caIPAServiceCert --certificate-
out cert.pem

kdestroy
```

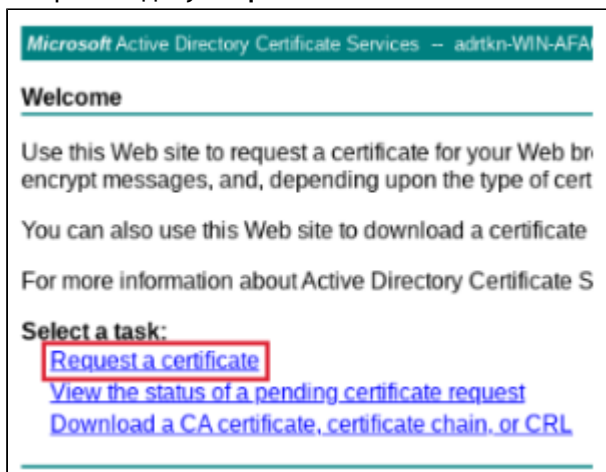
> Active Directory

После создания запроса на получение сертификата необходимо:

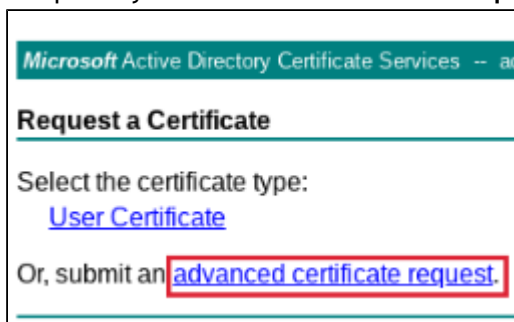
1. Зайти на веб-интерфейс УЦ КД. По умолчанию адрес имеет следующий вид:
https://[domain]/certsrv.
2. Авторизоваться под УЗ, для которой запрашивается сертификат.



3. Выбрать задачу **Request a certificate**.



4. Выбрать пункт **advanced certificate request**.



5. Вставить в поле **Saved Request** содержимое файла запроса сертификата (включая надписи BEGIN CERTIFICATE, END CERTIFICATE).
6. Выбрать в качестве шаблона **User**.
7. Нажать **Submit**.

8. В поле Certificate Issued выбрать **Base 64 encoded** и нажать **Download certificate**. Загрузка сертификата УЗ на ПК начнется автоматически.

> Samba DC

После создания запроса на на получение сертификата необходимо:

1. Отправить запрос на УЦ.
Форма и способ отправки запроса зависят от выбранного и настроенного администратором УЦ.
2. Подписать запрос на стороне УЦ.
Способ подписания зависит от заданных администратором настроек УЦ.
3. Скопировать подписанный сертификат УЗ на ПК.

Смена PIN-кода токена

rtlogon поддерживает возможность смены PIN-кода токена, заданного по умолчанию.

Сменить PIN-код можно при первичном входе в ОС, или его может сменить администратор.

Для смены PIN-кода администратором необходимо:

1. Подключить токен к ПК.
2. Ввести в терминале команду:

```
rtlogon-cli change-pin [token parameters]
```

3. Ввести текущий PIN-код токена.
4. Ввести дважды новый PIN-код токена.

Token parameters

Параметр	Описание	Значение по умолчанию	Наличие параметра в команде	Условие применения
--token-id arg	<p>Идентификатор токена, к которому применяется команда</p> <div style="border: 1px solid #add8e6; padding: 10px; margin: 10px 0;"> <p>i Как правило, идентификатор токена - это его серийный номер. Для некоторых моделей (комбинированные устройства JaCarta-2 PKI /ГОСТ и т.п.) - это серийный номер и постфикс, обозначающий апплет (-PKI/-GOST и т.п.).</p> <p>Для просмотра информации об идентификаторе токена необходимо вызвать команду rtlogon-cli info.</p> </div>	-	Опционально	Если к ПК подключено несколько токенов или один комбинированный токен

Примеры

User PIN code changing for one connected token

```
rtlogon-cli change-pin
Enter token (3f2a50b2) PIN-code:
Enter new PIN-code:
Repeat new PIN-code:
PIN-code changed succesfully
```

User PIN code changing for several connected tokens

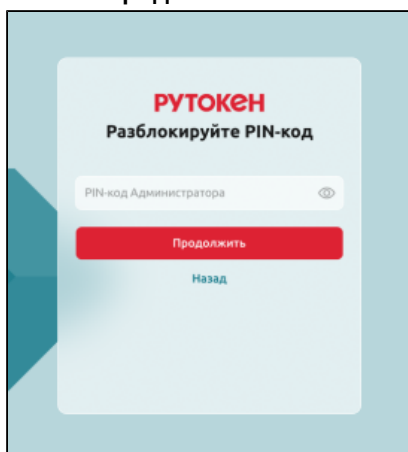
```
rtlogon-cli change-pin --token-id 3f2a50b2
Enter token (3f2a50b2) PIN-code:
Enter new PIN-code:
Repeat new PIN-code:
PIN-code changed succesfully
```

Разблокировка PIN-кода на экране приветствия или блокировки

rtlogon поддерживает разблокировку PIN-код токена на экране приветствия только при использовании GUI rtlogon.

Чтобы выполнить разблокировку, необходимо:

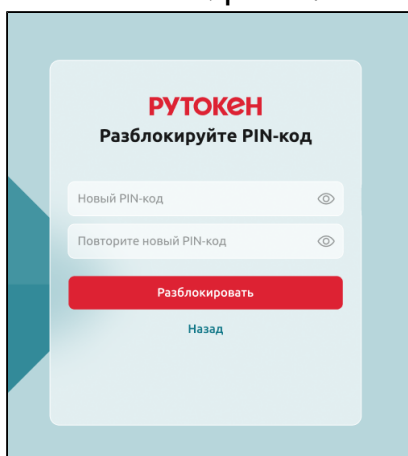
1. Ввести PIN-код Администратора токена в поле **PIN-код Администратора**.
2. Нажать **Продолжить**.



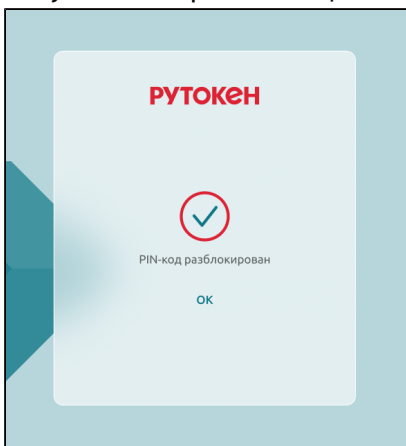
3. Ввести новый PIN-код в поле **Новый PIN-код**.

i Администратор может ввести для токена PIN-код по умолчанию (например, для Рутокена - 12345678). В этом случае при последующем входе в систему rtlogon попросит пользователя сменить PIN-код по умолчанию на другой.

4. Продублировать новый PIN-код в поле **Повторите новый PIN-код**.
5. Нажать **Разблокировать**.



6. Получить на экране сообщение о том, что PIN-код разблокирован.



7. Повторить вход в систему с новым PIN-кодом.

Запрос информации о конфигурации rtlogon и параметрах локальной 2ФА

rtlogon поддерживает вывод в терминале информации:

- о своих настройках;
- настроенной локальной 2ФА для текущего ПК;
- 2ФА, хранящуюся на токене.

Для получения информации необходимо:

1. Подключить токен к ПК (если необходимо вывести информацию об 2ФА, хранящуюся на токене).
2. Ввести в терминале команду:

```
rtlogon-cli info [command parameter]
```

Command parameter

Параметр	Описание	Значение по умолчанию	Наличие параметра в команде	Условие применения
-v или --verbose	Выводит расширенную информацию.	-	Опционально	Получение расширенной информации

Стандартная информация содержит:

- информацию о библиотеке:
 - pkcs11 Rutoken (librtpkcs11esp);
 - pkcs11 JaCarta (libjсPKCS11-2).
- идентификатор ПК;
- логин УЗ, для которой настроена локальная 2ФА;
- идентификатор токена, используемого для 2ФА;
- тип настроенной 2ФА;
- политику входа в ОС для 2ФА по сертификату;
- идентификатор подключенного к ПК токена;
- политику ОС при отключении токена от ПК.

Расширенная информация содержит:

- стандартную информацию;
- идентификатор объекта токена, в котором хранится секрет;
- содержимое сертификата.

Пример

```
//Standard information
rtlogon-cli info
Global config:
  pkcs11 Rutoken: found (Rutoken ECP PKCS #11 library, Manufacturer: Aktiv Co., Ver.: 2.14)
  pkcs11 JaCarta: found (JaCarta PKCS#11 module, Manufacturer: Aladdin R.D., Ver.: 2.9)
  host id: 0473082c-277c-4ff4-bc4e-492d311ca99a

Local users with configured rtlogon 2FA:
Record #0:
  user: user
  token-id: 3f2a50b2
  auth type: certificate
  login policy: certificate and password auth
Record #1:
  user: test
  token-id: 3f2a50b2
  auth type: strong password
  login policy: no policy

Token #0 (3f2a50b2):
Record #0:
  user: user
  host id: 0473082c-277c-4ff4-bc4e-492d311ca99a
  auth type: certificate
  disconnection type: lock
Record #1:
  user: test
  host id: 0473082c-277c-4ff4-bc4e-492d311ca99a
  auth type: strong password
  disconnection type: lock
```

```
//Extended information
rtlogon-cli info -v
Global config:
  pkcs11 Rutoken: found (Rutoken ECP PKCS #11 library, Manufacturer: Aktiv Co., Ver.: 2.14)
  pkcs11 JaCarta: found (JaCarta PKCS#11 module, Manufacturer: Aladdin R.D., Ver.: 2.9)
  host id: 0473082c-277c-4ff4-bc4e-492d311ca99a

Local users with configured rtlogon 2FA:
Record #0:
  user: user
  token-id: 3f2a50b2
  auth type: certificate
  login policy: certificate and password auth
  object id: bc5a8ff7-7fe1-4bb5-a5a1-ca4520e932e2
  cert body:
-----BEGIN CERTIFICATE-----
MIICtDCCAzwCAQAwDQYJKoZIhvcNAQELBQAwIDERMA8GA1UEAwIU21kb3JvdmEx\CzAJBgNVBAYTAKJZMB4XDTI
0MDgxMzA5NDAxMloXDTI3MDgxMzA5NDAxMlowIDER\NMA8GA1UEAwIU21kb3JvdmExCzAJBgNVBAYTAKJZMIIBIjAN
BgkqhkiG9w0BAQEF\NAOCQAQ8AMIIBCgKCAQEAR4KCR8nLut3ZSQZBhml+wwCde+pTZRoBihTdT7l18Yvb\nq5DVXWb
F/yL1nYRiDQyKLDkGuUhm5oWdCJsD7Gm3kvvMUer7nUHQC7lrCUPsTxXe\n52Z4Sg/WPVFyaCbSKZ0N6otxyIPrMr17
Z7jHG2elRGtUxYF7j3IdCIaNONlyTCdT\nrNBaHCpDAV/uDwiK3f4gmt2D/CGdOXgbxfhEHemvzqpCpyL/J7knTsA8Y
6PLJiyT\nc/DwBHYYEWAUmuemMOiv9pfx7qd+IK5qeVkJqy5uTJ0sy5Y9Kpv0QYH3/Qlbf2k\njH8/+wTAJbIL/3lt
oAQ9NpIKXodKgm6sno/+tYQBQIDAQABMA0GCSqGSIb3DQEB\NcUAAA4IBAQS7Tgd48eTHOdoWDERhm6eABYwRnkYi
VTYyrqsqP0PHnvs2cFxCPOd\nlzCzGW0aI+Lsqdlj/If6KahdlNAWbwy/0f04sQmOLAiv0e7a9QEZFwXwKfvxksJ\n
x5NPLb6Vi6c0KrXq3fYRTWbzdDE3WDinKxTeQyRbPCnJXsa9qvH8QERA+J3FEe3u\n0kEs8hwQHKqWcmLP01QMxEXZY
AeNQTqsA3x9lhrTphtpOKYbYY1r8HecJT5iuwFY\ndlUppYh3VZIoD5jc8InbTQwPN4xeeLpQLLZ0/vvHkh5Irumct1
XbUZOL9ERkzLVp\ngTc874Ms1sx4d3FeTuvDTpOv1KmTNIbr
-----END CERTIFICATE-----
Record #1:
  user: test
  token-id: 3f2a50b2
  auth type: strong password
  login policy: no policy
  object id: 28558443-f368-43b6-831b-61a2b574da14

Token #0 (3f2a50b2):
Record #0:
  user: user
  host id: 0473082c-277c-4ff4-bc4e-492d311ca99a
  auth type: certificate
  disconnection type: lock
  object id: bc5a8ff7-7fe1-4bb5-a5a1-ca4520e932e2
  cert body:
-----BEGIN CERTIFICATE-----
MIICtDCCAzwCAQAwDQYJKoZIhvcNAQELBQAwIDERMA8GA1UEAwIU21kb3JvdmEx\CzAJBgNVBAYTAKJZMB4XDTI
0MDgxMzA5NDAxMloXDTI3MDgxMzA5NDAxMlowIDER\NMA8GA1UEAwIU21kb3JvdmExCzAJBgNVBAYTAKJZMIIBIjAN
BgkqhkiG9w0BAQEF\NAOCQAQ8AMIIBCgKCAQEAR4KCR8nLut3ZSQZBhml+wwCde+pTZRoBihTdT7l18Yvb\nq5DVXWb
F/yL1nYRiDQyKLDkGuUhm5oWdCJsD7Gm3kvvMUer7nUHQC7lrCUPsTxXe\n52Z4Sg/WPVFyaCbSKZ0N6otxyIPrMr17
Z7jHG2elRGtUxYF7j3IdCIaNONlyTCdT\nrNBaHCpDAV/uDwiK3f4gmt2D/CGdOXgbxfhEHemvzqpCpyL/J7knTsA8Y
6PLJiyT\nc/DwBHYYEWAUmuemMOiv9pfx7qd+IK5qeVkJqy5uTJ0sy5Y9Kpv0QYH3/Qlbf2k\njH8/+wTAJbIL/3lt
oAQ9NpIKXodKgm6sno/+tYQBQIDAQABMA0GCSqGSIb3DQEB\NcUAAA4IBAQS7Tgd48eTHOdoWDERhm6eABYwRnkYi
VTYyrqsqP0PHnvs2cFxCPOd\nlzCzGW0aI+Lsqdlj/If6KahdlNAWbwy/0f04sQmOLAiv0e7a9QEZFwXwKfvxksJ\n
x5NPLb6Vi6c0KrXq3fYRTWbzdDE3WDinKxTeQyRbPCnJXsa9qvH8QERA+J3FEe3u\n0kEs8hwQHKqWcmLP01QMxEXZY
AeNQTqsA3x9lhrTphtpOKYbYY1r8HecJT5iuwFY\ndlUppYh3VZIoD5jc8InbTQwPN4xeeLpQLLZ0/vvHkh5Irumct1
XbUZOL9ERkzLVp\ngTc874Ms1sx4d3FeTuvDTpOv1KmTNIbr
-----END CERTIFICATE-----
```



```
Record #1:
  user: test
  host id: 0473082c-277c-4ff4-bc4e-492d311ca99a
  auth type: strong password
  disconnection type: lock
  object id: 28558443-f368-43b6-831b-61a2b574da14
```

Логирование работы rtlogon

Записи о работе rtlogon сохраняются в лог-файл *rtlogon.log*, расположенный в каталоге */var/log*.

Логирование включено по умолчанию. Доступ к лог-файлу осуществляется по правам администратора.

В лог-файл записываются данные о следующих событиях безопасности:

- успешная/неуспешная аутентификация пользователя;
- регенерация сложного пароля;
- изменение PIN-кода по умолчанию.

Эти данные дополнительно записываются рат-модулем в файл */var/log/auth.log*.

Экспорт конфигурационных файлов, лог-файлов и файла с параметрами локальной 2ФА


Для этого необходимо:

1. Ввести в терминале команду:

```
sudo rtlogon-cli collect-log [command parameter]
```

2. При запросе ввести пароль администратора.

Command parameter

Параметр	Описание	Значение по умолчанию	Наличие параметра в команде	Условие применения
-o arg или --output arg	Путь к выгружаемому архиву (содержит имя архива). <div style="border: 1px solid #add8e6; padding: 5px; width: fit-content;">  Имя выгружаемого архива определяет пользователь. </div>	-	Обязательно	

Выгруженный архив содержит следующие файлы:

- state_info.txt - со следующей информацией:
 - параметры конфигурации rtlogon;
 - данные об установленных библиотеках PKCS#11;
 - записи локальной 2ФА;
 - записи 2ФА, хранящиеся на токене;
 - описание публичных объектов на токенах (объекты данных, сертификаты, публичные ключи).
- installed_deb_packages.txt или installed_rpm_packages.txt - файл с информацией об установленном пакете;
- лог-файлы:
 - /var/log/auth.log - лог-файл аутентификаций;
 - /var/log/fly-dm.log - лог-файл модуля fly-dm;
 - /var/log/rtlogon.log - лог-файл rtlogon;
 - /var/log/messages - системный лог-файл;
 - /var/log/syslog - системный лог-файл;
 - /var/log/sss/ - лог-файлы служб SSSD.
- /etc/rtlogon/rtlogon.conf - конфигурационный файл rtlogon;
- /etc/rtlogon/localAuthDesc - файл УЗ, для которых настроена локальная 2ФА;
- конфигурационные файлы компонентов ПО:
 - /etc/X11/fly-dm/fly-dmrc/ - настройка экранного менеджера fly-dm ;
 - /etc/pam.d/ - конфигурационные файлы PAM;
 - /etc/selinux/config - информация о конфигурации подсистемы SELinux;
 - /etc/sss/ - конфигурационные файлы sssd ;
 - /etc/krb5* - конфигурационные файлы Kerberos;
 - /etc/control/ - настройки подсистемы control - утилиты ОС Альт ;
 - /etc/samba/ - настройка samba ;
 - /etc/lightdm/ - настройка экранного менеджера lightdm ;
 - /etc/*-release - информация о дистрибутиве ОС ;
 - /usr/share/p11-kit/modules/ - информация о настройке модулей p11-kit ;
 - /usr/share/fly-wm/theme.master/themerc - параметры конфигурации оконного менеджера fly-wm ;
 - /usr/share/authselect/ - конфигурация authselect ;
 - /usr/share/pam-configs/ - конфигурация pam-auth-update ;
 - /usr/share/xsessions/ - описание X11 графических оболочек.

Приложение 1. Сообщения об ошибках

Ошибка	Описание
Application couldn't be configured. Join PC to a domain first	Необходимо добавить ПК в домен
Application couldn't be configured. Missing required parameter '--local' or '--domain'.	При настройке ОС для работы с 2ФА не был указан один из параметров: '--local' или '--domain'
Application has already been configured. To change the configuration, run the reconfigure command	ОС уже настроена для работы с 2ФА. Чтобы изменить настройки используете команду <code>rtlogon-cli reconfigure</code>
Application hasn't been configured yet. Run the configure command first	Приложение не было сконфигурировано. Сначала выполните команду <code>rtlogon-cli configure</code>
Application isn't configured for domain operations. Use the option '--domain' to specify the domain type	ОС не была сконфигурирована для работы с доменной 2ФА. Используйте параметр <code>--domain arg</code> для задания типа домена
Application parameters have not been changed. Application was not reconfigured	Настройки ОС для работы с 2ФА не были изменены
CN argument required	При вызове команды <code>rtlogon-cli create-cert</code> не был указан аргумент параметра <code>dn -- CN</code>
Can't change PIN-code	Не удалось сменить PIN-код
Can't determine domain name	Не удалось определить имя домена при настройке аутентификации
Can't determine kdc hostname	Не удалось определить имя КД при настройке аутентификации
Can't find rtlogon configuration file. Try run: <code>rtlogon-cli configure</code>	При выполнении команды не был найден файл <code>rtlogon.conf</code>
Can't set strong password for user in system	Не удалось установить новый сложный пароль
Couldn't find CA certificates in configuration files. Use the option '--ca-cert' to provide it manually	В конфигурации <code>rtlogon</code> не найден файл, содержащий корневой сертификат или сертификаты цепочки доверия УЦ. Добавьте его, используя параметр <code>--ca-cert arg</code>
Couldn't parse the rtlogon configuration file	Не удалось считать конфигурационный файл
Couldn't read the specified CA certificates	Корневой сертификат или сертификат цепочки доверия УЦ, содержащийся в указанном администратором файле, не является сертификатом
dn argument required	При вызове команды <code>rtlogon-cli create-cert</code> не был указан параметр <code>dn</code>

Ошибка	Описание
Entered PIN-codes do not match! Try again	Введенные PIN-коды не совпадают
Incorrect domain type	Указан неверный тип домена при вызове команды <code>configure</code>
Invalid path to CA certificates	Неверно указан путь к файлу сертификата УЦ (цепочки сертификатов)
More than one token inserted. Please, specify in command token serial number	К ПК подключено несколько токенов. Необходимо указать идентификатор токена (<code>token id</code>) в параметрах вводимой команды
Network manager is not available	Утилита <code>Network manager</code> недоступна, не настроена соответствующая политика. Данная ошибка характерна для ОС <code>Astra Linux</code>
New PIN-code does not comply with PIN-code policy	Невозможно получить минимальную длину PIN-кода токена, указанную в политиках качества. Или Вводимый PIN-код не соответствует политикам качества
New PIN-code does not match PIN-code policy: PIN-code must contain at least X characters	Длина нового PIN-кода меньше минимальной, установленной в политиках качества
New PIN-code has invalid length	Невозможно получить минимальную длину PIN-кода, установленную на токене (<code>token info</code>)
PIN-code can only be changed by the Administrator	PIN-код токена может изменить только администратор
PIN-code incorrect	Введен неверный PIN-код
PIN-code length must be between X and Y characters	Длина нового PIN-кода токена находится за пределами допустимого диапазона: от X до Y включительно
This PIN-code has already been used	Вводимый PIN-код содержится в истории PIN-кодов
Unable to connect to <network_name>	Отсутствует подключение к сети
Unconfiguration was canceled	Отключение настроек ОС для работы 2ФА было прервано. Администратор не подтвердил продолжение выполнения команды <code>rtlogon-cli unconfigure</code>
Unknown domain type	В файле <code>rtlogon.conf</code> неверно указан тип настроенного домена
You couldn't setup cert auth with "cert only" policy for administrators (root and users having access to sudo). Use policy "cert and password"	Запрещена установка политики входа в систему "certonly" при настройке локальной 2ФА по сертификату для администратора или суперпользователя системы. Необходимо установить политику входа "cert and password"

Ошибка	Описание
<p>You couldn't setup strong password auth for administrators (root and users having access to sudo).</p> <p>Use cert auth with policy "cert and password"</p>	<p>Запрещена настройка локальной 2ФА по сложному паролю для администратора или суперпользователя системы.</p> <p>Необходимо настроить локальную 2ФА по сертификату с политикой входа "cert and password"</p>