РУТОКЕН

Рутокен Логон для Linux

Версия 1.1.0

Руководство администратора



© 2026 Компания «Актив»

- Общая информация 5
- О программном комплексе 6
  - Назначение 6
  - Состав 7
  - Описание компонентов 8
  - Описание работы 8
- Поддерживаемое окружение 12
  - Поддерживаемые устройства 12
  - Поддерживаемые программные аутентификаторы 12
  - Поддерживаемые архитектуры процессоров 12
  - Поддерживаемые ОС 13
  - Поддерживаемые графические окружения 13
  - Поддерживаемые контроллеры домена 14
  - Необходимые библиотеки, зависимости и утилиты 14
  - Поддерживаемые считыватели отпечатков пальцев 15
- Лицензирование продукта 15
  - Общая информация 15
  - Установка сервера лицензирования 16
  - Удаление сервера лицензирования 17
  - Активация лицензии 18
    - В графическом режиме Мастера лицензий Guardant 18
    - В консольном режиме Мастера лицензий Guardant 19
  - Открепление лицензии rtlogon для другого компьютера 21
    - Открепление лицензии 21
    - Добавление открепленной лицензии на целевой компьютер 22
- Предварительная настройка компьютера для работы с доменной МФА 23
  - Настройка Network manager для экрана приветствия ОС Astra Linux 23
  - Ввод компьютера в домен 25
    - Active Directory 25
    - FreeIPA 28
    - ALDPro 31
    - Samba DC 32

- РЕД АДМ 35
- Dynamic Directory 35
- Проверка ввода компьютера в домен 35
- Загрузка корневого сертификата или сертификатов цепочки доверия УЦ на компьютер 36
  - FreeIPA, Dynamic Directory и ALDPro 36
    - Корневой сертификат 36
    - Сертификаты цепочки доверия УЦ 36
  - Active Directory 37
  - Samba DC и РЕД АДМ 37
- Поддержка коротких доменных имен УЗ 38
- Установка rtlogon 38
- Установка библиотеки libjcPKCS11-2.so 39
- Подготовка к настройке 3ФА 41
  - Установка rtbiocomponents 41
  - Установка rtbioadmin 42
  - Добавление биометрических отпечатков пальцев на Рутокен 43
  - Замена биометрических отпечатков пальцев на Рутокене 44
- Команды и общие параметры rtlogon 45
- Обновление rtlogon 46
- Удаление rtlogon 46
- Настройка ОС для работы с МФА 47
- Реконфигурация ОС для работы с МФА 50
- Отключение настроек ОС для работы с МФА 52
- Скрипт массового развертывания rtlogon 52
- Проверка сертификатов пользователей на статус «отозванный» 54
  - CRL 54
  - OCSP 55
- Настройка работы с OTP 56
- Настройка МФА 58
- Минимальные права администратора для смены сложного пароля 63
- Проверка настройки МФА 67

- Изменение настроек МФА 68
- Удаление МФА 69
- Кеширование УЗ 72
- Создание запроса на получение сертификата, генерация самоподписанного сертификата 73
- Получение сертификата УЗ от УЦ 78
  - FreeIPA, Dynamic Directory и ALDPro 78
  - Active Directory 78
  - Samba DC и РЕД АДМ 80
- Проверка готовности компьютера к МФА 80
  - Требования к скриптам 80
  - Примеры скриптов 82
  - Запуск скриптов пользователем 82
  - Логирование проверок 83
- Смена PIN-кода токена 85
- Разблокировка PIN-кода на экране приветствия или экране блокировки ... 86
- Запрос информации о конфигурации rtlogon и параметрах локальной МФА 87
- Логирование работы rtlogon 92
  - rtlogon_log 92
  - syslog 92
- Экспорт конфигурационных файлов, лог-файлов и файла с параметрами локальной МФА 93
- Приложение 1. Ошибки 96
  - Ошибки, выводимые в GUI 96
  - Ошибки, выводимые в терминале 101

Общая информация

Термины, определения и аббревиатуры

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

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

Трехфакторная аутентификация (3ФА) — тип аутентификации, при которой требуется предъявить 3 фактора. Чаще всего для 3ФА используется фактор владения ключевым носителем (например, токен или смарт-карта), фактор знания (например, PIN-код от устройства) и фактор свойства владельца ключевого носителя (например, отпечаток пальца).

Многофакторная аутентификация (МФА) — тип аутентификации, для которой требуется предъявить более одного фактора.

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

Сложный пароль — пароль размером 72 произвольных символа, хранящийся на ключевом носителе. Используется для 2ФА.

Учетная запись (УЗ) — совокупность данных, однозначно определяющих пользователя компьютера.

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

Локальная УЗ — учетная запись, которая создается и хранится на конкретном компьютере и используется для доступа к его ресурсам. В отличие от доменной УЗ, локальная не предоставляет доступ к сетевым ресурсам или другим компьютерам 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 МФА.

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.

CRL (Certificate Revocation List) — список отозванных сертификатов, публикуемый центром сертификации (CA) для указания, какие сертификаты были аннулированы до истечения срока их действия. Этот список используется для проверки действительности сертификатов и обеспечения безопасности.

OCSP (Online Certificate Status Protocol) — протокол, используемый для проверки статуса отзыва цифровых сертификатов в режиме реального времени.

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.

Лицензия — набор условий, в рамках которых пользователю разрешено использовать защищенное ПО.

Сервер лицензирования — многофункциональный сервис, который используется как инструмент для контроля за количеством подключений к сетевым лицензиям, а также для откреплення лицензий и использования их на компьютерах пользователей, находящихся вне сети.

Мастер лицензий Guardant — утилита, предназначенная для активации, переноса и обновления программных лицензий.

Пользовательский скрипт — скрипт для установки и настройки rtlogon на компьютере пользователя с параметрами, заданными администратором в скрипте массового развертывания.

Пользовательский дистрибутив — комплект для автоматического разворачивания и настройки rtlogon на компьютере пользователя. Включает в себя дистрибутив rtlogon, пользовательский скрипт, корневой сертификат или сертификаты цепочки доверия УЦ.

OTP (One Time Password) — одноразовый пароль, действительный только для одного сеанса аутентификации. Используется для усиления аутентификации по паролю.

КД — контроллер домена.

ОС — операционная система.

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 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:

- 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 многофакторной аутентификации пользователей в ОС семейства Linux.

rtlogon позволяет легко настраивать и управлять многофакторной аутентификацией на компьютерах пользователей.

В качестве факторов аутентификации используются:

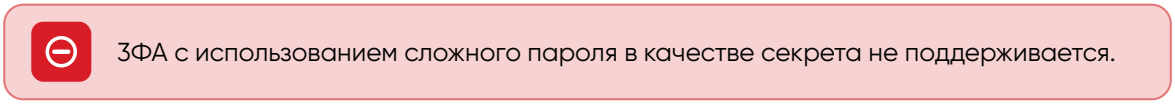
- наличие у пользователя ключевого носителя;

- знание пользователем PIN-кода ключевого носителя для доступа к секрету, хранящемуся на нем. В качестве секрета может использоваться:
  - сложный пароль;
  - закрытый ключ ключевой пары.
- свойство владельца ключевого носителя — биометрический отпечаток пальца.

Обязательными факторами аутентификации являются наличие ключевого носителя и знание PIN-кода. Использование биометрического отпечатка пальца настраивается администратором в дополнение к этим факторам.

rtlogon поддерживает следующие типы аутентификации:

- по количеству используемых факторов:
  - МФА:
    - 3ФА. В качестве секрета при этом используется закрытый ключ ключевой пары;

    - 2ФА. В зависимости от типа секрета:
      - 2ФА по сертификату;
      - 2ФА по сложному паролю.
    - 2ФА по логину, паролю УЗ и одноразовому паролю (One-Time Password — OTP) — настраивается вне rtlogon.
  - 1ФА по логину и 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-lockpam.
- rtlogon_log.

Описание компонентов

- **rtlogon-cli** — консольная утилита, предназначенная для:
  - настройки ОС для работы с МФА;
  - реконфигурации ОС для работы с МФА;
  - отключения настроек ОС для работы с МФА;
  - создания и удаления МФА;
  - создания запроса на получение сертификата УЗ и генерации самоподписанного сертификата (ключевая пара при этом записывается на ключевой носитель);
  - смены PIN-кода;
  - предоставление информации о ключевом носителе, конфигурации rtlogon и параметрах настроенной локальной МФА;
  - сбора лог-файлов с информацией о системе и ее логами;
  - экспорта лог-файлов, конфигурационных файлов и файлов с параметрами настроенной локальной МФА.
- **rtlogon_ event- monitor** — приложение-сервис, предназначенное для:
  - контроля запуска системного экрана блокировки (Lock Screen);
  - контроля за операциями над ключевым носителем, использовавшимся при последней аутентификации;
  - выполнения политики ОС при отключении ключевого носителя от компьютера во время активной пользовательской сессии.
- **pam_ rtlogon. so** — PAM-модуль, интегрируемый в ОС Linux. Предназначен для аутентификации пользователя с настроенной МФА;
- **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-lockpam** — PAM-приложение для экрана блокировки ОС Astra Linux.
- **rtlogon_log** — сервер логирования.

Описание работы

Для успешного входа в ОС пользователь должен:

- подключить свой ключевой носитель к компьютеру и ввести PIN-код;
  ИЛИ
- подключить свой ключевой носитель и считыватель отпечатков пальцев к компьютеру, ввести PIN-код и приложить свой палец к подключенному считывателю.

ОС аутентифицирует пользователя на основе данных, размещенных в защищенной памяти ключевого носителя: сложный пароль или ключевая пара.

rtlogon позволяет задать следующие способы входа в ОС для локальной МФА:

- 3ФА:
  - только по сертификату,
  - по сертификату или логину/паролю.
- 2ФА:
  - только по сертификату,
  - по сертификату или логину/паролю,
  - по сложному паролю.

Для доменной МФА способ входа в ОС настраивается на стороне КД.

Также rtlogon позволяет настроить политику ОС при отключении ключевого носителя от компьютера:

- вызов экрана блокировки,
- продолжение активной пользовательской сессии.

Дополнительно rtlogon поддерживает вход в ОС для доменной УЗ по логину, паролю и одноразовому паролю (OTP), если такой вид аутентификации настроен в домене — доменная 2ФА с OTP.

Доменная 3ФА

Для реализации доменной 3ФА необходимо сначала выполнить ее настройку, а потом провести аутентификацию пользователя.

Настройка доменной 3ФА выполняется по следующей схеме:

1. С помощью ПО **Рутокен БИО. Программа администратора** администратор сохраняет на ключевом носителе биометрические отпечатки пальцев пользователя.
2. Администратор создает и записывает на ключевой носитель ключевую пару с пометкой, что она используется для аутентификации по биометрии, и формирует запрос на получение сертификата.
3. Администратор передает сформированный запрос в УЦ.
4. УЦ создает сертификат пользователя.
5. Администратор настраивает доменную 3ФА с использованием rtlogon, в процессе которой сертификат пользователя загружается на ключевой носитель.

Процесс аутентификации пользователя выполняется по следующей схеме:

1. Пользователь подключает к компьютеру считыватель отпечатков пальцев.
2. Пользователь получает ключевой носитель и подключает его к компьютеру.
3. Пользователь вводит PIN-код и прикладывает палец к считывателю, после чего в системе инициируется запрос на аутентификацию и отправляется КД.
4. После получения запроса КД отправляет на компьютер набор данных для подписи.
5. С помощью закрытого ключа, хранящегося на ключевом носителе, данные подписываются и возвращаются КД.
6. КД проверяет подпись и при положительном результате аутентифицирует пользователя.

Локальная 3ФА

Для реализации локальной 3ФА необходимо сначала выполнить ее настройку, а потом провести аутентификацию пользователя.

Настройка локальной 3ФА выполняется по следующей схеме:

1. С помощью ПО **Рутокен БИО. Программа администратора** администратор сохраняет на ключевом носителе биометрические отпечатки пальцев пользователя.
2. Администратор создает и записывает на ключевой носитель ключевую пару с пометкой, что она используется для аутентификации по биометрии, создает сертификат и сам его подписывает (генерирует самоподписанный сертификат).
3. Администратор настраивает локальную 3ФА с использованием rtlogon, в процессе которой сертификат загружается на ключевой носитель.

Процесс аутентификации пользователя выполняется по следующей схеме:

1. Пользователь подключает к компьютеру считыватель отпечатков пальцев.
2. Пользователь получает ключевой носитель и подключает его к компьютеру.
3. Пользователь вводит PIN-код и прикладывает палец к считывателю, после чего в системе инициируется запрос на аутентификацию.
4. Система формирует набор данных для подписи.
5. С помощью закрытого ключа, хранящегося на ключевом носителе, данные подписываются.
6. Система проверяет подпись и при положительном результате аутентифицирует пользователя.

Доменная 2ФА по сертификату

Для реализации доменной 2ФА по сертификату необходимо сначала выполнить ее настройку, а потом провести аутентификацию пользователя.

Настройка доменной 2ФА по сертификату выполняется по следующей схеме:

1. Администратор создает и записывает на ключевой носитель ключевую пару и формирует запрос на получение сертификата пользователя.

   Генерация ключевой пары на ключевом носителе может выполняться не только с использованием rtlogon, но и альтернативными инструментами: УЦ, система управления жизненным циклом ключей и сертификатов Рутокен Keybox и т.п.

2. Администратор передает сформированный запрос в УЦ.
3. УЦ создает сертификат пользователя.
4. Администратор настраивает доменную 2ФА по сертификату с использованием rtlogon, в процессе которой сертификат пользователя загружается на ключевой носитель.

Процесс аутентификации пользователя выполняется по следующей схеме:

1. Пользователь получает ключевой носитель и подключает его к компьютеру.
2. Пользователь вводит PIN-код, после чего в системе инициируется запрос на аутентификацию и отправляется КД.
3. После получения запроса КД отправляет на компьютер набор данных для подписи.

4. С помощью закрытого ключа, хранящегося на ключевом носителе, данные подписываются и возвращаются КД.
5. КД проверяет подпись и при положительном результате аутентифицирует пользователя.

Локальная 2ФА по сертификату

Для реализации локальной 2ФА по сертификату необходимо сначала выполнить ее настройку, а потом провести аутентификацию пользователя.

Настройка локальной 2ФА по сертификату выполняется по следующей схеме:

1. Администратор создает и записывает на ключевой носитель ключевую пару, создает сертификат и сам его подписывает (генерирует самоподписанный сертификат).

   Генерация ключевой пары на ключевом носителе может выполняться не только с использованием rtlogon, но и альтернативными инструментами: УЦ, система управления жизненным циклом ключей и сертификатов Рутокен Keybox и т.п.

2. Администратор настраивает локальную 2ФА по сертификату с использованием rtlogon, в процессе которой сертификат загружается на ключевой носитель.

Процесс аутентификации пользователя выполняется по следующей схеме:

1. Пользователь получает ключевой носитель и подключает его к компьютеру.
2. Пользователь вводит PIN-код, после чего в системе инициируется запрос на аутентификацию.
3. Система формирует набор данных для подписи.
4. С помощью закрытого ключа, хранящегося на ключевом носителе, данные подписываются.
5. Система проверяет подпись и при положительном результате аутентифицирует пользователя.

Доменная 2ФА по сложному паролю

Для реализации доменной 2ФА по сложному паролю необходимо сначала выполнить ее настройку, а потом провести аутентификацию пользователя.

Настройка доменной 2ФА по сложному паролю выполняется с помощью rtlogon. В процессе настройки в КД генерируется сложный пароль и дублируется на ключевой носитель.

Процесс аутентификации пользователя выполняется по следующей схеме:

1. Пользователь получает ключевой носитель и подключает его к компьютеру.
2. Пользователь вводит PIN-код, после чего в системе инициируется запрос на аутентификацию и отправляется КД.
3. После получения запроса КД отправляет свой запрос на предоставление сложного пароля.
4. Сложный пароль, хранящийся на ключевом носителе, передается КД.
5. КД проводит сверку сложных паролей и при положительном результате аутентифицирует пользователя.

Локальная 2ФА по сложному паролю

Для реализации локальной 2ФА по сложному паролю необходимо сначала выполнить ее настройку, а потом провести аутентификацию пользователя.

Настройка локальной 2ФА по сложному паролю выполняется с помощью rtlogon. В процессе настройки в системе генерируется сложный пароль и дублируется на ключевой носитель.

Процесс аутентификации пользователя выполняется по следующей схеме:

1. Пользователь получает ключевой носитель и подключает его к компьютеру.
2. Пользователь вводит PIN-код, после чего в системе инициируется запрос на аутентификацию.
3. Система проводит сверку сложного пароля, хранящегося на ключевом носителе, и сложного пароля, хранящегося в системе, и при положительном результате аутентифицирует пользователя.

Поддерживаемое окружение

Поддерживаемые устройства



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

- Рутокен Lite;
- устройства Рутокен ЭЦП 2.0;
- устройства Рутокен ЭЦП 3.0, включая Рутокен ЭЦП 3.0 3120 Touch и Рутокен ЭЦП 3.0 3250 БИО ;
- Рутокен OTP;
- JaCarta ГОСТ;
- JaCarta PKI/ГОСТ.

Поддерживаемые программные аутентификаторы

Яндекс ID.

Поддерживаемые архитектуры процессоров

- x86_64,
- ARM64.



3ФА не поддерживается для архитектуры процессора ARM64.

Поддерживаемые ОС

- Astra Linux SE 1.7.2 и новее, SE 1.8.1 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 версий ниже 1.7.8 и 1.8.3 необходимо выполнить команду rtlogon-cli reconfigure без указания параметров.

- ОС Альт 8 СП, релиз 10;
- ОС Альт 8.4 СП;
- ОС Альт 10.0;
- ОС Альт 11.0;
- РЕД ОС 7.3;
- РЕД ОС 8;
- РОСА Хром 12.4;
- Debian 13;
- Ubuntu 24.04;
- ОСнова версии 2.14;
- ОСнова версии 3.1.

Поддерживаемые графические окружения

- для ОС Astra Linux — Fly;
- для ОС Альт:
  - KDE;
  - Mate.
- для ОС РЕД ОС:
  - Mate;
  - Cinnamon;
  - KDE.
- для ОС РОСА Хром — KDE Plasma;
- для ОС Debian — KDE Plasma.



Графическое окружение GNOME не поддерживается для экранов приветствия и блокировки rtlogon.

Для работы с GNOME необходимо использовать системный экран GDM.

Поддерживаемые контроллеры домена

- ALD Pro 2.1, 2.4;
- Active Directory;
- FreeIPA 4.9.11;
- Samba DC версии:
  - 4.13.13 и новее — для Astra Linux 1.7;
  - 4.19.12 и новее — для РЕД ОС 7.3;
  - 4.19.7 и новее — для ОС Альт 10;
  - 4.9.18 и новее — для ОС Альт 8 СП, релиз 10.
- Dynamic Directory 4.13.0 и новее;
- РЕД АДМ 2.0.1 и новее.

Необходимые библиотеки, зависимости и утилиты

- libpam версии:
  - 1.1.8 — для ОС Astra Linux;
  - 1.1.6 — для ОС Альт;
  - 1.1.8 — для ОС РЕД ОС.
- PKCS#11:
  - librtpkcs11ecp.so версии 2.18 и новее — для устройств Рутокен;
  - libjcPKCS11-2.so версии 2.8.0 и новее — для устройств JaCarta.
- Network manager 1.8.9 и новее;
- krb5-pkinit (для доменной сети);
- krb5-user (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 (кроме ОС Astra Linux);
- 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 и новее (кроме ОС Astra Linux);
- libqt5x11extras5 5.6.1 (только для ОС Astra Linux);
- libglib2.0-0 2.46.2 (кроме ОС Astra Linux);
- для работы с биометрией — дистрибутив rtbiocomponents версии 1.1.0, в состав которого входит:
  - FAPI;
  - FSSM;
  - BioLib.

Все необходимые для rtlogon зависимости присутствуют в репозиториях поддерживаемых ОС, за исключением:

- библиотеки libjcPKCS11-2.so;
- rtbiocomponents.

Установка библиотеки libjcPKCS11-2.so описана в разделе Установка библиотеки libjcPKCS11-2.so.

Установка rtbiocomponents описана в разделе Установка rtbiocomponents.

Поддерживаемые считыватели отпечатков пальцев

- Futronic FS-80H,
- Futronic FS-80,
- Папилон ДС-21С.

Лицензирование продукта

Общая информация

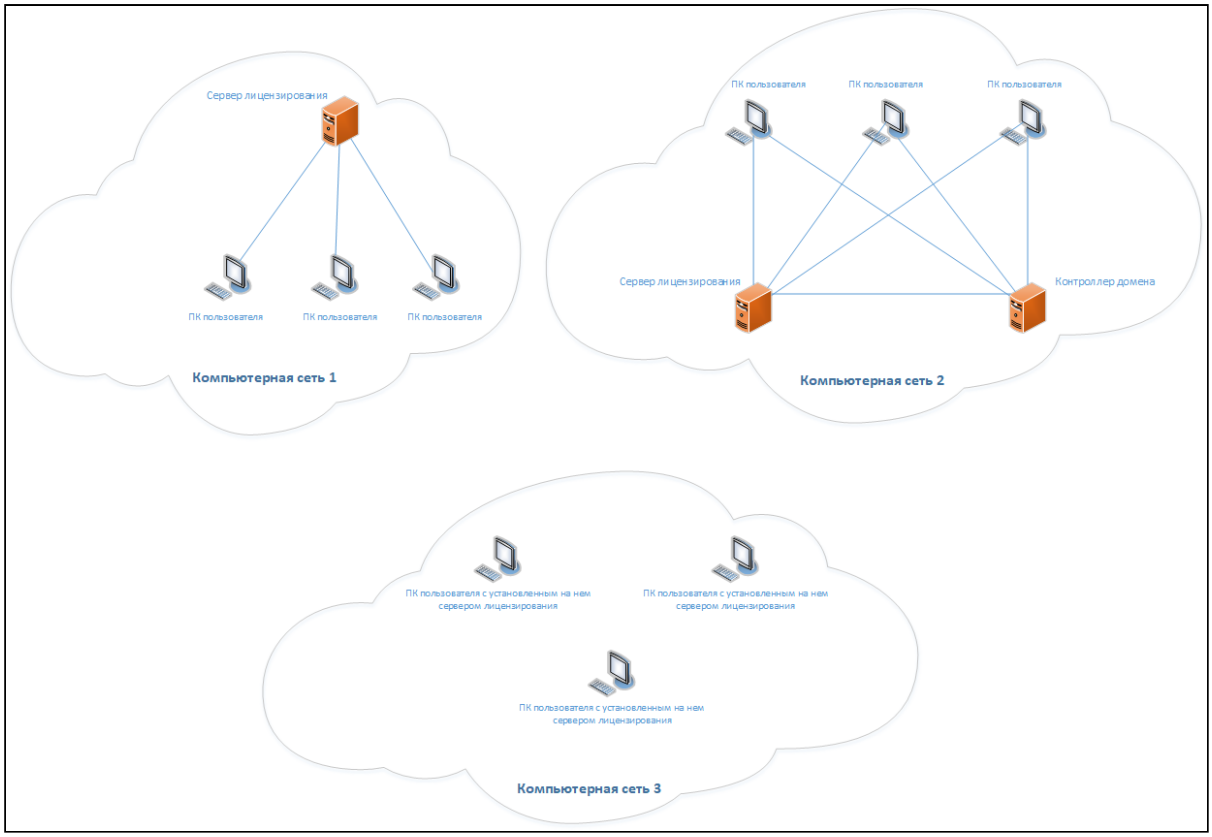
rtlogon поддерживает следующие типы лицензий:

- стандартная — предоставляет доступ ко всем функциям rtlogon, кроме 3ФА;
- дополнительная лицензия — предоставляет доступ к настройке и использованию 3ФА.

Чтобы иметь возможность работать с rtlogon, в сети должен быть развернут сервер лицензирования и активирована на нем лицензия.

Выбор компьютера для установки сервера лицензирования зависит от используемого сценария аутентификации:

- если rtlogon будет использоваться только для локальной аутентификации на распределенных компьютерах, то рекомендуется устанавливать сервер лицензирования на каждый компьютер пользователя;
- если rtlogon будет использоваться для доменной или локальной аутентификации на компьютерах внутри одной сети, то рекомендуется устанавливать сервер лицензирования на отдельный компьютер.



Для корректной работы механизма лицензирования rtlogon необходимо, чтобы все компьютеры пользователей имели сетевое соединение с компьютером сервера лицензирования по порту 3189.

Чтобы подготовить сервер лицензирования и активировать лицензию:

1. Установите сервер лицензирования в сети.
2. С помощью Мастера лицензий Guardant активируйте лицензию rtlogon на сервере лицензирования.

Установка сервера лицензирования

В ОС Альт установку/удаление сервера лицензирования необходимо выполнять от имени root.

Чтобы установить сервер лицензирования:

1. Скачайте с официального сайта Компании «Актив» (https://www.rutoken.ru/support/download/rutoken-logon-for-linux/) установочный пакет Guardant Control Center для необходимой ОС и архитектуры процессора компьютера.
2. Откройте терминал.
3. Перейдите в каталог расположения установочного пакета Guardant Control Center — grdcontrol.

4. Введите в терминале команду:

Astra Linux and deb-based distributives

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

Alt Linux

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

RED OS and rpm-based distributives

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

5. При запросе введите пароль администратора.

Установка сервера лицензирования завершена.

Подробная информация о Guardant Control Center представлена на официальном сайте https://dev.guardant.ru/display/GSLK/Guardant+Control+Center.

Удаление сервера лицензирования

Чтобы удалить сервер лицензирования, введите в терминале команду:

Astra Linux and deb-based distributives

```
sudo apt-get remove grdcontrol
```

Alt Linux

```
apt-get remove grdcontrol
```

RED OS and rpm-based distributives

```
sudo dnf remove grdcontrol
```

Активация лицензии

Для активации лицензии rtlogon используется утилита **Мастер лицензий Guardant**.

Утилита устанавливается автоматически в процессе установки сервера лицензирования и располагается в каталоге */opt/guardant/grdcontrol*.

Мастер лицензий Guardant может работать в двух режимах: графический и консольный.

Подробная информация о Мастере лицензий Guardant представлена на официальном сайте https://dev.guardant.ru/pages/viewpage.action?pageId=85492642.

В графическом режиме Мастера лицензий Guardant

Чтобы активировать лицензию rtlogon в графическом режиме Мастера лицензий Guardant:

1. Откройте терминал и введите в нем команду:

   ```
   /opt/guardant/grdcontrol/license_wizard
   ```

2. В открывшемся окне **Мастер лицензий Guardant** нажмите **Настройки**.
3. В разделе **Настройки**, в поле **Адрес сервера лицензий**, введите адрес https://getlicense.guardant.ru/.
4. Установите переключатель **Проверять обновления лицензий при запуске автоматически** в активное положение.
5. Нажмите **←Назад**.
6. Нажмите кнопку **+Активация лицензии**.
7. В поле **На каком компьютере вы хотите использовать лицензию?** выберите **На этом**.
8. Если компьютер, на котором выполняется активация лицензии, имеет соединение с сетью Интернет:
   a. В поле **Серийный номер** введите полученный серийный номер программного ключа Guardant DL.
   b. Нажмите **Получить лицензию**.
9. Если компьютер, на котором выполняется активация лицензии, не имеет соединение с сетью Интернет:
   a. Нажмите на ссылку **Оффлайн активация**.
   b. Выберите вкладку **Новая лицензия** и нажмите **Сохранить**.
   c. Сохраните файл запроса.
   d. Нажмите **Продолжить**.
   e. Перенесите файл запроса на компьютер, который имеет соединение с сетью Интернет.
   f. Запустите на том компьютере Мастер лицензий Guardant.
   g. Повторите п. 2-6.
   h. В поле **На каком компьютере вы хотите использовать лицензию?** выберите **На другом**.
   i. Нажмите **Продолжить**.
   j. Нажмите **Выбрать файл** и откройте перенесенный на этот компьютер файл запроса.
   k. Введите в поле полученный серийный номер программного ключа Guardant DL.

l. Нажмите **Активировать новую лицензию**.

m. В поле **Готово** нажмите **Сохранить**.

n. Сохраните файл лицензии и перенесите его на компьютер, у которого нет соединения с сетью Интернет.

o. Если Мастер лицензий Guardant был закрыт на этом компьютере:

   i. Повторите п. 1, 6, 7.

   ii. Нажмите на ссылку **Оффлайн активация**.

   iii. Нажмите **Продолжить**.

   iv. Нажмите **Продолжить, у меня есть лицензия**.

   v. Нажмите **Выбрать файл**.

   vi. Выберите файл лицензии и нажмите **Открыть**.

p. Если Мастер лицензий Guardant не был закрыт на этом компьютере:

   i. Нажмите **Продолжить, у меня есть лицензия**.

   ii. Нажмите **Выбрать файл**.

   iii. Выберите файл лицензии и нажмите **Открыть**.

Лицензия активирована.

В консольном режиме Мастера лицензий Guardant

Чтобы активировать лицензию для rtlogon в консольном режиме Мастера лицензий Guardant:

1. Если компьютер, на котором выполняется активация лицензии, имеет соединение с сетью Интернет:

   a. Откройте терминал и введите в нем команду:

```
/opt/guardant/grdcontrol/license_wizard --console --activate
[серийный номер программного ключа Guardant DL] --host
https://getlicense.guardant.ru:443
```

   Пример.

```
/opt/guardant/grdcontrol/license_wizard --console --activate
sV112L-AzxhvH-BiGeWJ-EbHe6q-487Va8 --host
https://getlicense.guardant.ru:443
```

2. Если компьютер, на котором выполняется активация лицензии, не имеет соединение с сетью Интернет:

   a. Создайте запрос на активацию лицензии. Для этого откройте терминал и введите в нем команду:

```
/opt/guardant/grdcontrol/license_wizard --console
--activate-request [путь к файлу запроса на активацию лицензии]/
[имя файла].request
```

Пример.

```
/opt/guardant/grdcontrol/license_wizard --console
--activate-request /home/user/test.request
```

b. Перенесите на компьютер, у которого есть соединение с сетью Интернет, созданный файл запроса.

c. На компьютере с доступом в сеть Интернет откройте терминал и введите команду:

```
/opt/guardant/grdcontroal/license_wizard --console
--activate-response [серийный номер программного ключа Guardant
DL] [путь к файлу запроса на активацию лицензии]/[имя
файла].request [путь к файлу лицензии]/[имя файла].response
--host https://getlicense.guardant.ru:443
```

Пример.

```
/opt/guardant/grdcontrol/license_wizard --console
--activate-response sV112L-AzxhvH-BiGeWJ-EbHe6q-487Va8
/home/user/Downloads/test.request
/home/user/Downloads/test_license.response
--host https://getlicense.guardant.ru:443
```

d. Перенесите на первоначальный компьютер полученный в предыдущем пункте файл лицензии.

e. На первоначальном компьютере введите в терминале команду:

```
/opt/guardant/grdcontrol/license_wizard --console
--activate-offline [путь к файлу лицензии]/[имя файла].response
```

Пример.

```
/opt/guardant/grdcontrol/license_wizard --console
--activate-offline /home/user/test_license.response
```

Лицензия активирована.

Открепление лицензии rtlogon для другого компьютера

Чтобы открепить лицензию rtlogon для другого компьютера:

1. Открепите лицензию от компьютера, на котором она на текущий момент используется (далее — исходный компьютер) .
2. Добавьте открепленную лицензию на компьютер, на котором планируется ее дальнейшее использование (далее — целевой компьютер).

Подробная информация об откреплении и переносе лицензии приведена на сайте https://dev.guardant.ru/pages/viewpage.action?pageId=152666466.

Открепление лицензии

Чтобы открепить лицензию:

1. На целевом компьютере:
   a. Установите сервер лицензирования.
   b. Откройте веб-интерфейс сервера лицензирования — введите в адресной строке браузера http://127.0.0.1:3189.
   c. В правом верхнем углу интерфейса нажмите на значок .
   d. На открывшейся странице **Цифровой отпечаток компьютера «название целевого компьютера»** нажмите кнопку **Сохранить цифровой отпечаток**.
   Файл с цифровым отпечатком целевого компьютера *fingerprint.json* сохранится в папке *Загрузки*.
2. Перенесите полученный файл с цифровым отпечатком целевого компьютера на исходный компьютер.
3. На исходном компьютере:
   a. Откройте веб-интерфейс сервера лицензирования — введите в адресной строке браузера http://127.0.0.1:3189.
   b. В правом верхнем углу интерфейса нажмите на значок .
   c. В поле **Пароль** введите пароль администратора сервера лицензирования.

      По умолчанию пароль администратора сервера лицензирования — **admin**.

   d. В настройках выберите раздел **Открепление лицензий**.
   e. Нажмите кнопку **+ Добавить отпечаток ПК**.
   f. Выберите перенесенный ранее файл с цифровым отпечатком целевого компьютера — *fingerprint.json*.
   g. В поле **Максимальный период открепления** укажите максимальное количество дней, по истечении которых переносимая лицензия вернется на исходный компьютер. По умолчанию задано 30 дней.
   h. Нажмите кнопку **Сохранить изменения**.
   i. Перейдите на вкладку **Ключи**.

j. Найдите лицензию, которую нужно открепить, и напротив нее нажмите на значок  .

k. На открывшейся странице **Открепление лицензии** укажите параметры открепления:

- в поле **Где будет использоваться лицензия** установите переключатель в положение **На другом**;
- в выпадающем списке **Компьютер** выберите имя целевого компьютера;
- в поле **Дата окончания использования** укажите дату окончания действия открепленной лицензии на целевом компьютере или в поле **или количество дней, включая сегодня** укажите количество дней, в течение которых открепленная лицензия будет действовать на целевом компьютере.

> Срок действия открепленной лицензии на целевом компьютере не должен превышать срок действия самой лицензии.

l. Справа нажмите кнопку **Открепить лицензию**.

m. В окне **Необходима авторизация** введите пароль администратора сервера лицензирования и нажмите кнопку **Войти**.

n. На открывшейся странице **Готово! Осталось отправить файл с лицензией** нажмите кнопку **Сохранить**.
Файл с откреплённой лицензией *license-[имя целевого компьютера].json* сохранится в папке *Загрузки*.

4. Перенесите откреплённую лицензию на целевой компьютер.

Добавление откреплённой лицензии на целевой компьютер

Чтобы добавить откреплённую лицензию на целевой компьютер:

1. На целевом компьютере откройте веб-интерфейс сервера лицензирования — введите в адресной строке браузера http://127.0.0.1:3189.
2. Перейдите на вкладку **Ключи**.
3. В правом верхнем углу нажмите на значок  .
4. На открывшейся странице **Добавление откреплённой лицензии** нажмите кнопку **Выбрать**.
5. Выберите файл откреплённой лицензии.
6. В окне **Необходима авторизация** введите пароль администратора сервера лицензирования и нажмите кнопку **Войти**.
Перенесенная лицензия появится в списке ключей сервера лицензирования на целевом компьютере.

Предварительная настройка компьютера для работы с доменной МФА

Для работы с доменной МФА необходимо:

- настроить Network manager для ОС Astra Linux (опционально) – если необходима возможность управления сетью из экрана приветствия;

> Для ОС ОСнова возможность управления сетью из экрана приветствия не поддерживается.

- ввести компьютер в домен;
- загрузить корневой сертификат или сертификаты цепочки доверия УЦ.

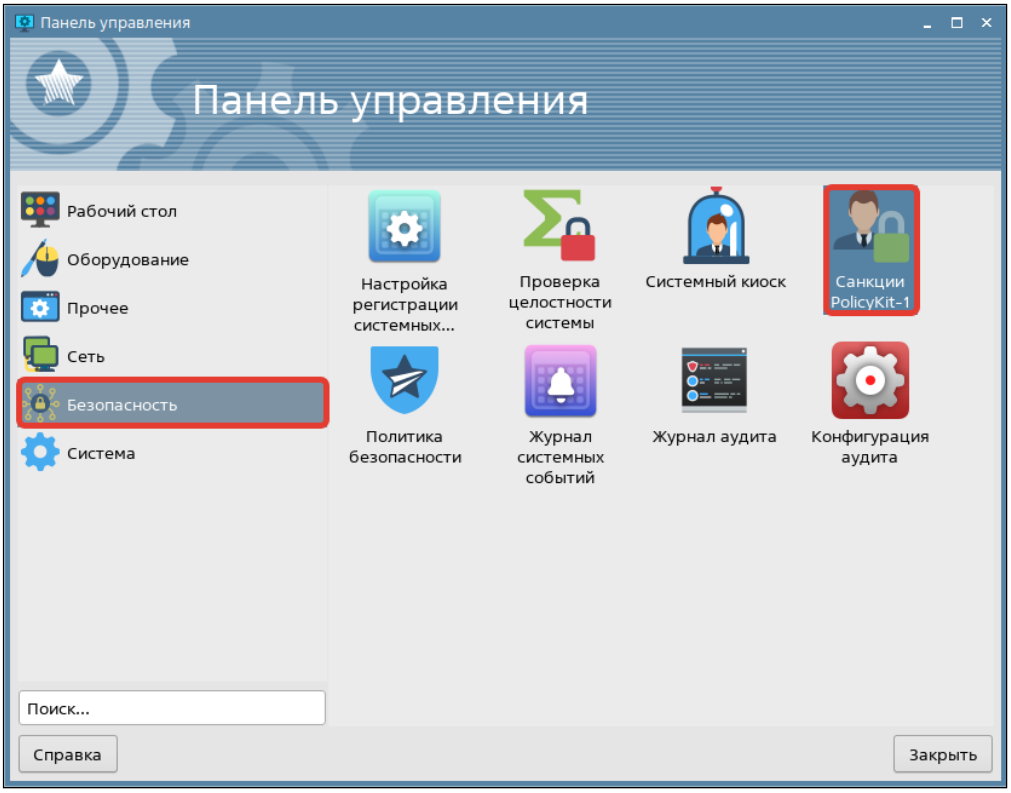
> В целях поддержания безопасности сети предприятия рекомендуется для ввода компьютера в домен использовать УЗ, имеющую права только на выполнение этой операции.

Настройка Network manager для экрана приветствия ОС Astra Linux

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

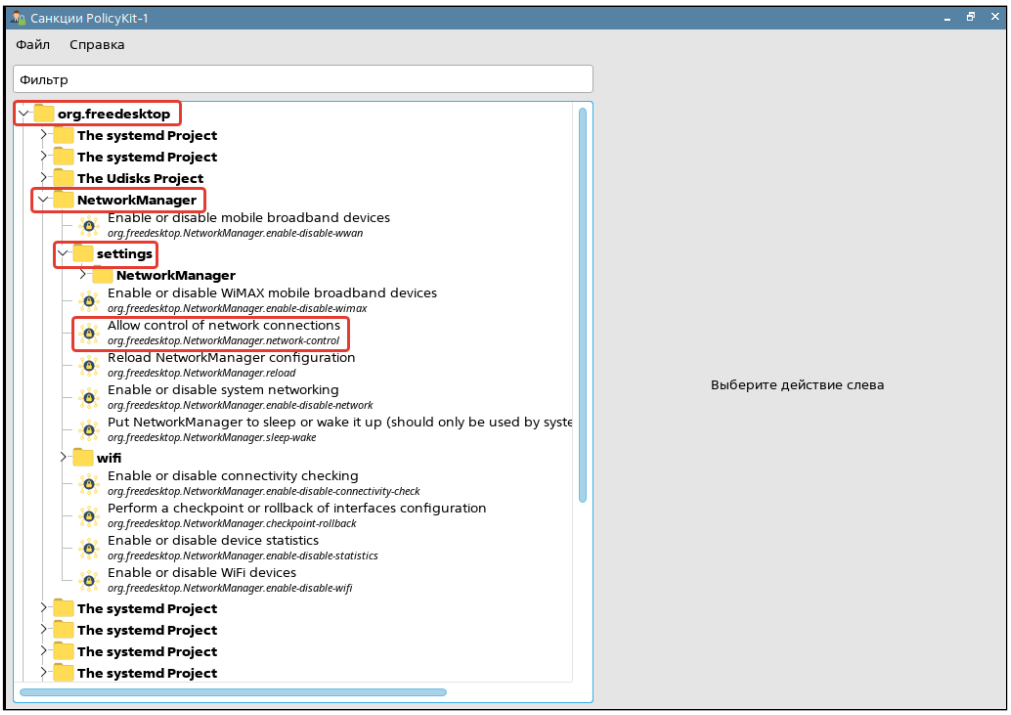
Чтобы включить возможность управления сетевыми подключениями через экран приветствия:

1. Запустите **Панель управления**.
2. На вкладке **Безопасность** выберите **Санкции PolicyKit-1**.

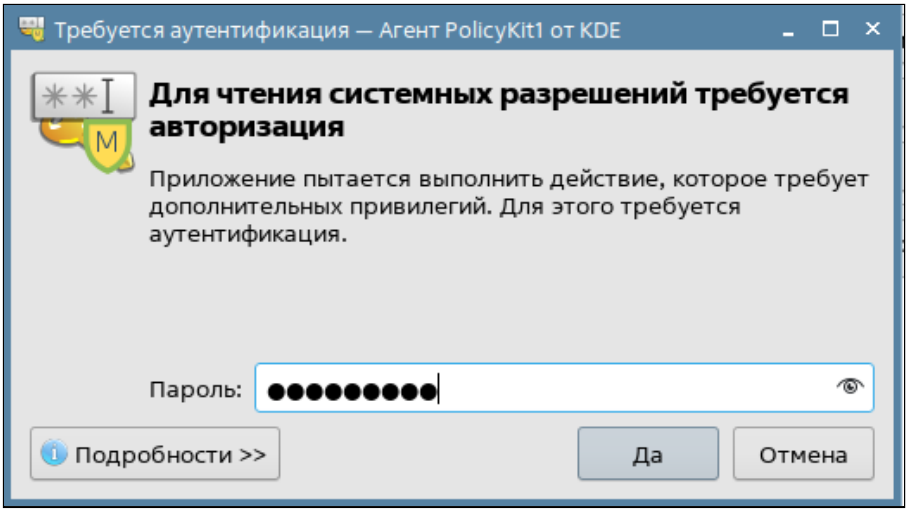


3. В открывшемся окне **Санкции PolicyKit-1** выберите **org.freedesktop**.

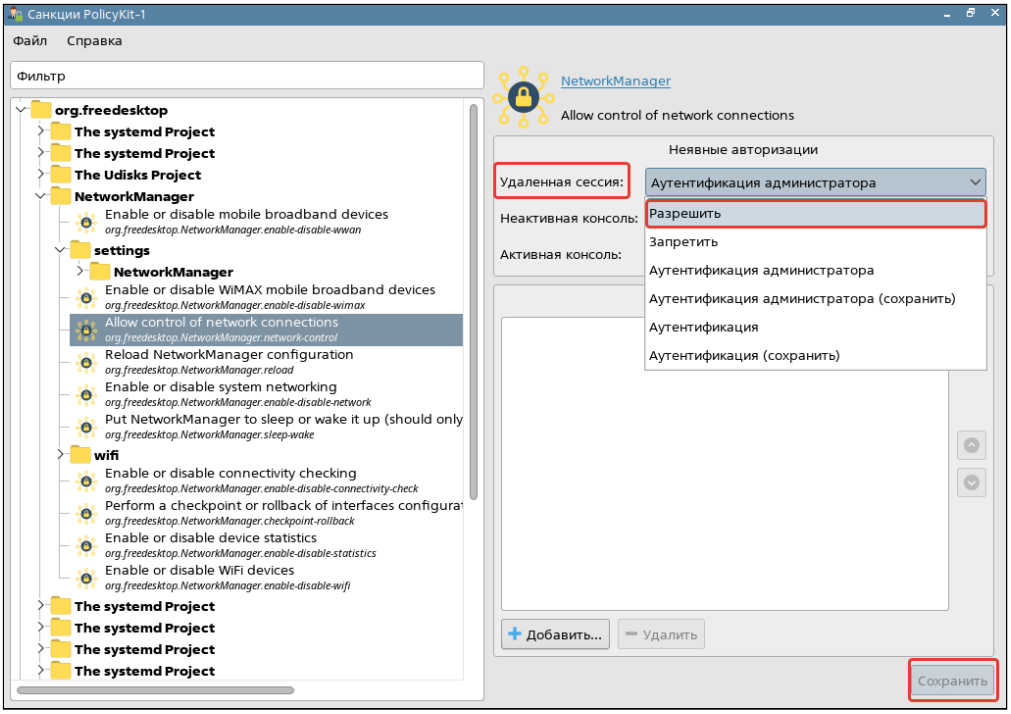
4. В раскрывшемся списке выберите **NetworkManager**, далее **settings**, далее **Allow control of network connection**.



5. При открытии окна **Требуется аутентификация – Агент PolicyKit1 от KDE** введите пароль УЗ. Нажмите **Да**.



6. В окне **Санкции PolicyKit-1**, в поле **Удаленная сессия** из выпадающего списка выберите **Разрешить**. Нажмите **Сохранить**.



7. При открытии окна **Требуется аутентификация – Агент PolicyKit1 от KDE** введите пароль УЗ. Нажмите **Да**.
8. Закройте все окна.

Ввод компьютера в домен

Active Directory

ОС Astra Linux

Чтобы ввести компьютер в домен:

1. Добавьте в настройки сетевого подключения IP-адрес DNS-сервера предприятия.
2. Установите утилиту **astra-ad-sssd-client** для ввода компьютера в домен.
3. Используя утилиту, введите компьютер в домен.
   Подробное описание ввода компьютера в домен приведено в технической документации на ОС Astra Linux.
4. Установите 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. Перезагрузите компьютер.

Для удобства ввода компьютера в домен можно использовать скрипт *configure_ad.sh* для ОС Astra Linux из комплекта поставки.
Для этого необходимо присвоить значения указанным параметрам скрипта и запустить его. Или можно сразу запустить скрипт, значения параметров при этом вводятся вручную по запросам.

Параметр скрипта	Описание параметра
`SERVER_IP`	IP-адрес сервера КД
`DOMAIN`	Название домена
`ADMIN_USERNAME`	Логин УЗ, обладающей правами для ввода компьютера в домен
`ADMIN_PASSWORD`	Пароль УЗ, обладающей правами для ввода компьютера в домен

ОС РЕД ОС

Чтобы ввести компьютер в домен:

1. Добавьте в настройки сетевого подключения IP-адрес DNS-сервера предприятия.
2. Установите утилиту **join-to-domain** для ввода компьютера в домен.
3. Используя утилиту, введите компьютер в домен.
   Подробное описание ввода компьютера в домен приведено в технической документации на ОС РЕД ОС.
4. Перезагрузите компьютер.

Для удобства ввода компьютера в домен можно использовать скрипт *configure_ad.sh* для ОС РЕД ОС из комплекта поставки.
Для этого необходимо присвоить значения указанным параметрам скрипта и запустить его. Или можно сразу запустить скрипт, значения параметров при этом вводятся вручную по запросам.

Параметр скрипта	Описание параметра
`SERVER_IP`	IP-адрес сервера КД
`DOMAIN`	Название домена
`ADMIN_USERNAME`	Логин УЗ, обладающей правами для ввода компьютера в домен
`ADMIN_PASSWORD`	Пароль УЗ, обладающей правами для ввода компьютера в домен

ОС Альт

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

Чтобы ввести компьютер в домен:

1. Замените `[hostname]` на `[current_hostname.domain]`.
2. Отключите плагин **etcnet-alt** для NetworkManager.
3. Перезапустите NetworkManager.

4. Подключитесь к новому сетевому соединению.
5. Добавьте в настройки сетевого подключения IP-адрес DNS-сервера предприятия.
6. Установите утилиту **task-auth-ad-sssd** для ввода компьютера в домен.
7. Используя утилиту, введите компьютер в домен.
   Подробное описание ввода компьютера в домен приведено в технической документации на ОС Альт.
8. Перезагрузите компьютер.

Для удобства ввода компьютера в домен можно использовать скрипт *configure_ad.sh* для ОС Альт из комплекта поставки.
Для этого необходимо присвоить значения указанным параметрам скрипта и запустить его. Или можно сразу запустить скрипт, значения параметров при этом вводятся вручную по запросам.

Параметр скрипта	Описание параметра
SERVER_IP	IP-адрес сервера КД
DOMAIN	Название домена
ADMIN_USERNAME	Логин УЗ, обладающей правами для ввода компьютера в домен
ADMIN_PASSWORD	Пароль УЗ, обладающей правами для ввода компьютера в домен
BIOS_NAME	Название BIOS домена

ОС РОСА Хром

Подробное описание ввода компьютера в домен приведено в технической документации на ОС РОСА Хром.

Для удобства ввода компьютера в домен можно использовать скрипт *configure_ad.sh* для ОС РОСА Хром из комплекта поставки.
Для этого необходимо присвоить значения указанным параметрам скрипта и запустить его. Или можно сразу запустить скрипт, значения параметров при этом вводятся вручную по запросам.

Параметр	Описание параметра
SERVER_IP	IP-адрес сервера КД
DOMAIN	Название домена
ADMIN_USERNAME	Логин УЗ, обладающей правами для ввода компьютера в домен
ADMIN_PASSWORD	Пароль УЗ, обладающей правами для ввода компьютера в домен

ОС Debian, Ubuntu

Подробное описание ввода компьютера в домен приведено в технической документации на ОС Debian, Ubuntu.

Для удобства ввода компьютера в домен можно использовать скрипт *configure_ad.sh* для ОС Debian, Ubuntu из комплекта поставки.
Для этого необходимо присвоить значения указанным параметрам скрипта и запустить его. Или можно сразу запустить скрипт, значения параметров при этом вводятся вручную по запросам.

Параметр	Описание параметра
`SERVER_IP`	IP-адрес сервера КД
`DOMAIN`	Название домена
`ADMIN_USERNAME`	Логин УЗ, обладающей правами для ввода компьютера в домен
`ADMIN_PASSWORD`	Пароль УЗ, обладающей правами для ввода компьютера в домен

FreeIPA

ОС Astra Linux

Чтобы ввести компьютер в домен:

1. Настройте разрешение имен. Для этого в файле */etc/hosts*:
    a. Замените `[127.0.1.1 hostname]` на `[IP-адрес_компьютера hostname.domain]`. При этом запись `hostname.domain` должна быть уникальной и отсутствовать в домене.
    b. Добавьте IP-адрес сервера FreeIPA.
2. Добавьте в настройки сетевого подключения IP-адрес DNS-сервера предприятия.
3. Установите утилиту **astra-freeipa-client** для ввода компьютера в домен.
4. Используя утилиту, введите компьютер в домен.
   Подробное описание ввода компьютера в домен приведено в технической документации на ОС Astra Linux.
5. Перезагрузите компьютер.

Для удобства ввода компьютера в домен можно использовать скрипт *configure_freeipa.sh* для ОС Astra Linux из комплекта поставки.
Для этого необходимо присвоить значения указанным параметрам скрипта и запустить его. Или можно сразу запустить скрипт, значения параметров при этом вводятся вручную по запросам.

Параметр	Описание параметра
SERVER	URL-адрес сервера КД
SERVER_IP	IP-адрес сервера КД
DOMAIN	Название домена
ADMIN_USERNAME	Логин УЗ, обладающей правами для ввода компьютера в домен
ADMIN_PASSWORD	Пароль УЗ, обладающей правами для ввода компьютера в домен

ОС РЕД ОС

Чтобы ввести компьютер в домен:

1. Замените `[hostname]` на `[client_name.domain]`.
2. Добавьте в настройки сетевого подключения IP-адрес DNS-сервера предприятия.
3. Установите утилиту **ipa-client** для ввода компьютера в домен.
4. Используя утилиту, введите компьютер в домен.
   Подробное описание ввода компьютера в домен приведено в технической документации на ОС РЕД ОС.
5. Перезагрузите компьютер.

Для удобства ввода компьютера в домен можно использовать скрипт *configure_freeipa.sh* для ОС РЕД ОС из комплекта поставки.

Для этого необходимо присвоить значения указанным параметрам скрипта и запустить его. Или можно сразу запустить скрипт, значения параметров при этом вводятся вручную по запросам.

Параметр	Описание параметра
SERVER	URL-адрес сервера КД
SERVER_IP	IP-адрес сервера КД
DOMAIN	Название домена
ADMIN_USERNAME	Логин УЗ, обладающей правами для ввода компьютера в домен
ADMIN_PASSWORD	Пароль УЗ, обладающей правами для ввода компьютера в домен

ОС Альт

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

Чтобы ввести компьютер в домен:

1. Замените `[hostname]` на `[hostname.domain]`.
2. Отключите плагин **etcnet-alt** для NetworkManager.
3. Перезапустите NetworkManager.
4. Подключитесь к новому сетевому соединению.
5. Добавьте в настройки сетевого подключения IP-адрес DNS-сервера предприятия.
6. Установите утилиту **freeipa-client** для ввода компьютера в домен.
7. Используя утилиту, введите компьютер в домен.
   Подробное описание ввода компьютера в домен приведено в технической документации на ОС Альт.
8. Перезагрузите компьютер.

Для удобства ввода компьютера в домен можно использовать скрипт *configure_freeipa.sh* для ОС Альт из комплекта поставки.
Для этого необходимо присвоить значения указанным параметрам скрипта и запустить его. Или можно сразу запустить скрипт, значения параметров при этом вводятся вручную по запросам.

Параметр	Описание параметра
`SERVER`	URL-адрес сервера КД
`SERVER_IP`	IP-адрес сервера КД
`DOMAIN`	Название домена
`ADMIN_USERNAME`	Логин УЗ, обладающей правами для ввода компьютера в домен
`ADMIN_PASSWORD`	Пароль УЗ, обладающей правами для ввода компьютера в домен

ОС РОСА Хром

Подробное описание ввода компьютера в домен приведено в технической документации на ОС РОСА Хром.

Для удобства ввода компьютера в домен можно использовать скрипт *configure_freeipa.sh* для ОС РОСА Хром из комплекта поставки.
Для этого необходимо присвоить значения указанным параметрам скрипта и запустить его. Или можно сразу запустить скрипт, значения параметров при этом вводятся вручную по запросам.

Параметр	Описание параметра
`SERVER`	URL-адрес сервера КД
`SERVER_IP`	IP-адрес сервера КД
`DOMAIN`	Название домена

Параметр	Описание параметра
ADMIN_USERNAME	Логин УЗ, обладающей правами для ввода компьютера в домен
ADMIN_PASSWORD	Пароль УЗ, обладающей правами для ввода компьютера в домен

ОС Debian, Ubuntu

Подробное описание ввода компьютера в домен приведено в технической документации на ОС Debian, Ubuntu.

Для удобства ввода компьютера в домен можно использовать скрипт *configure_freeipa.sh* для ОС Debian, Ubuntu из комплекта поставки.
Для этого необходимо присвоить значения указанным параметрам скрипта и запустить его. Или можно сразу запустить скрипт, значения параметров при этом вводятся вручную по запросам.

Параметр	Описание параметра
SERVER	URL-адрес сервера КД
SERVER_IP	IP-адрес сервера КД
DOMAIN	Название домена
ADMIN_USERNAME	Логин УЗ, обладающей правами для ввода компьютера в домен
ADMIN_PASSWORD	Пароль УЗ, обладающей правами для ввода компьютера в домен

ALDPro

ОС Astra Linux

Чтобы ввести компьютер в домен:

1. Настройте разрешения имен. В файл */etc/hosts* необходимо добавить IP-адрес КД ALDPro.
2. Добавьте репозитории ALDPro в каталог */etc/apt/sources.list.d/*.
3. Добавьте в настройки сетевого подключения IP-адрес DNS-сервера предприятия.
4. Установите утилиту **aldpro-client** для ввода компьютера в домен.
5. Используя утилиту, введите компьютер в домен.
6. Перезагрузите компьютер.

Для удобства ввода компьютера в домен можно использовать скрипт *configure_ald_pro.sh* для ОС Astra Linux из комплекта поставки.
Для этого необходимо присвоить значения указанным параметрам скрипта и запустить его. Или можно сразу запустить скрипт, значения параметров при этом вводятся вручную по запросам.

Параметр	Описание параметра
SERVER	URL-адрес сервера КД
SERVER_IP	IP-адрес сервера КД
DOMAIN	Название домена
ADMIN_USERNAME	Логин УЗ, обладающей правами для ввода компьютера в домен
ADMIN_PASSWORD	Пароль УЗ, обладающей правами для ввода компьютера в домен
ALDPRO_VERSION	Версия ALDPro

Samba DC

ОС Astra Linux

Чтобы ввести компьютер в домен:

1. Добавьте в настройки сетевого подключения IP-адрес DNS-сервера предприятия.
2. Установите утилиту **astra-ad-sssd-client** для ввода компьютера в домен.
3. Используя утилиту, введите компьютер в домен.
   Подробное описание ввода компьютера в домен приведено в технической документации на ОС Astra Linux.
4. Включите поиск kerberos-имени домена через DNS.
5. Включите поиск kerberos-настроек домена через DNS.
6. Перезагрузите компьютер.

Для удобства ввода компьютера в домен можно использовать скрипт *configure_samba.sh* для ОС Astra Linux из комплекта поставки.
Для этого необходимо присвоить значения указанным параметрам скрипта и запустить его. Или можно сразу запустить скрипт, значения параметров при этом вводятся вручную по запросам.

Параметр	Описание параметра
SERVER_IP	IP-адрес сервера КД
DOMAIN	Название домена
ADMIN_USERNAME	Логин УЗ, обладающей правами для ввода компьютера в домен
ADMIN_PASSWORD	Пароль УЗ, обладающей правами для ввода компьютера в домен

ОС РЕД ОС

Чтобы ввести компьютер в домен:

1. Добавьте в настройки сетевого подключения IP-адрес DNS-сервера предприятия.
2. Установите утилиту **join-to-domain** для ввода компьютера в домен.
3. Используя утилиту, введите компьютер в домен.
   Подробное описание ввода компьютера в домен приведено в технической документации на ОС РЕД ОС.
4. Перезагрузите компьютер.

Для удобства ввода компьютера в домен можно использовать скрипт *configure_samba.sh* для ОС РЕД ОС из комплекта поставки.
Для этого необходимо присвоить значения указанным параметрам скрипта и запустить его. Или можно сразу запустить скрипт, значения параметров при этом вводятся вручную по запросам.

Параметр	Описание параметра
`SERVER_IP`	IP-адрес сервера КД
`DOMAIN`	Название домена
`ADMIN_USERNAME`	Логин УЗ, обладающей правами для ввода компьютера в домен
`ADMIN_PASSWORD`	Пароль УЗ, обладающей правами для ввода компьютера в домен

ОС Альт

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

Чтобы ввести компьютер в домен:

1. Замените `[hostname]` на `[current_hostname.domain]`.
2. Отключите плагин **etcnet-alt** для NetworkManager.
3. Перезапустите NetworkManager.
4. Подключитесь к новому сетевому соединению.
5. Добавьте в настройки сетевого подключения IP-адрес DNS-сервера предприятия.
6. Установите утилиту **task-auth-ad-sssd** для ввода компьютера в домен.
7. Используя утилиту, введите компьютер в домен.
   Подробное описание ввода компьютера в домен приведено в технической документации на ОС Альт.
8. Перезагрузите компьютер.

Для удобства ввода компьютер в домен можно использовать скрипт *configure_samba.sh* для ОС Альт из комплекта поставки.
Для этого необходимо присвоить значения указанным параметрам скрипта и запустить его. Или можно сразу запустить скрипт, значения параметров при этом вводятся вручную по запросам.

Параметр	Описание параметра
SERVER	URL-адрес сервера КД
DOMAIN	Название домена
ADMIN_USERNAME	Логин УЗ, обладающей правами для ввода компьютера в домен
ADMIN_PASSWORD	Пароль УЗ, обладающей правами для ввода компьютера в домен
BIOS_NAME	Название BIOS домена

ОС РОСА Хром

Подробное описание ввода компьютера в домен приведено в технической документации на ОС РОСА Хром.

Для удобства ввода компьютера в домен можно использовать скрипт *configure_samba.sh* для ОС РОСА Хром из комплекта поставки.
Для этого необходимо присвоить значения указанным параметрам скрипта и запустить его. Или можно сразу запустить скрипт, значения параметров при этом вводятся вручную по запросам.

Параметр	Описание параметра
SERVER_IP	IP-адрес сервера КД
DOMAIN	Название домена
ADMIN_USERNAME	Логин УЗ, обладающей правами для ввода компьютера в домен
ADMIN_PASSWORD	Пароль УЗ, обладающей правами для ввода компьютера в домен

ОС Debian, Ubuntu

Подробное описание ввода компьютера в домен приведено в технической документации на ОС Debian, Ubuntu.

Для удобства ввода компьютера в домен можно использовать скрипт *configure_samba.sh* для ОС Debian, Ubuntu из комплекта поставки.
Для этого необходимо присвоить значения указанным параметрам скрипта и запустить его. Или можно сразу запустить скрипт, значения параметров при этом вводятся вручную по запросам.

Параметр	Описание параметра
SERVER_IP	IP-адрес сервера КД
DOMAIN	Название домена
ADMIN_USERNAME	Логин УЗ, обладающей правами для ввода компьютера в домен
ADMIN_PASSWORD	Пароль УЗ, обладающей правами для ввода компьютера в домен

РЕД АДМ

Чтобы ввести компьютер в домен, необходимо воспользоваться технической документацией к РЕД АДМ.

Dynamic Directory

ОС РОСА Хром

Подробное описание ввода компьютера в домен приведено в технической документации на ОС РОСА Хром.

Для удобства ввода компьютера в домен можно использовать скрипт *configure_freeipa.sh* для ОС РОСА Хром из комплекта поставки.
Для этого необходимо присвоить значения указанным параметрам скрипта и запустить его. Или можно сразу запустить скрипт, значения параметров при этом вводятся вручную по запросам.

Параметр	Описание параметра
`SERVER`	URL-адрес сервера КД
`SERVER_IP`	IP-адрес сервера КД
`DOMAIN`	Название домена
`ADMIN_USERNAME`	Логин УЗ, обладающей правами для ввода компьютера в домен
`ADMIN_PASSWORD`	Пароль УЗ, обладающей правами для ввода компьютера в домен

Проверка ввода компьютера в домен

Чтобы проверить, введен ли компьютер в домен:

1. Откройте файл */etc/sssd/sssd.conf*.
2. Убедитесь, что в секции `[sssd]` параметру `domains` присвоено значение.

Пример.

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

Загрузка корневого сертификата или сертификатов цепочки доверия УЦ на компьютер

Если сертификат является промежуточным в цепочке доверия УЦ, то файл сертификата УЦ на компьютере должен содержать все промежуточные сертификаты до корневого.

> ⚠ Если сертификат пользователя содержит поле **Certificate Authority Information Access** с адресом сервера корневых сертификатов, то промежуточные сертификаты можно не указывать при настройке ОС для работы с МФА.

Составить файл со всеми доверенными сертификатами можно 2-мя способами.

1 способ.

Записать все сертификаты в один файл с помощью команды `cat`:

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

2 способ.

Загрузить сертификаты в контейнер в формате p7b.

FreeIPA, Dynamic Directory и ALDPro

Корневой сертификат

Корневой сертификат автоматически загружается на компьютер в процессе ввода компьютера в домен. Дополнительных действий выполнять не требуется.

Сертификаты цепочки доверия УЦ

Для загрузки сертификатов цепочки доверия УЦ на компьютер:

1. Введите команду:

   ```
   ipa ca-find
   ```

   В терминале появится список с названием всех сертификатов.

2. Введите команду:

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

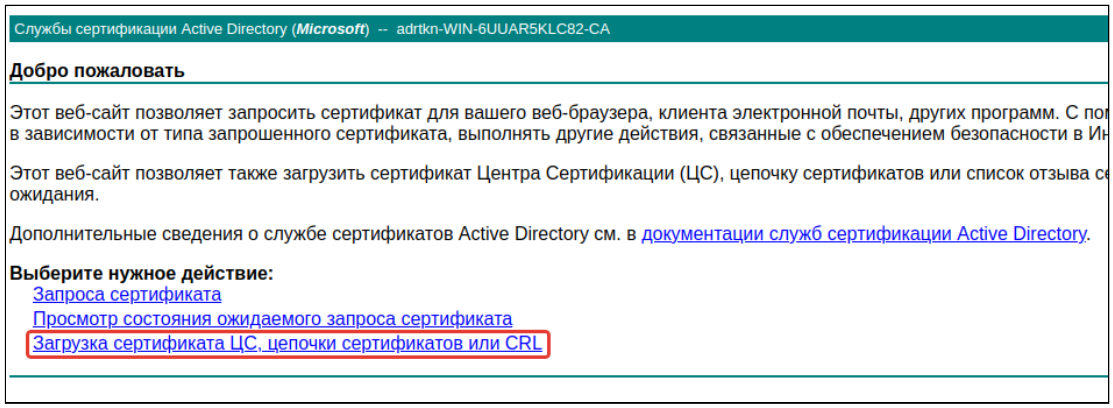
   На компьютер будут загружены все сертификаты цепочки доверия УЦ.

3. Запишите все сертификаты в один файл с помощью команды `cat` или используйте контейнер p7b.

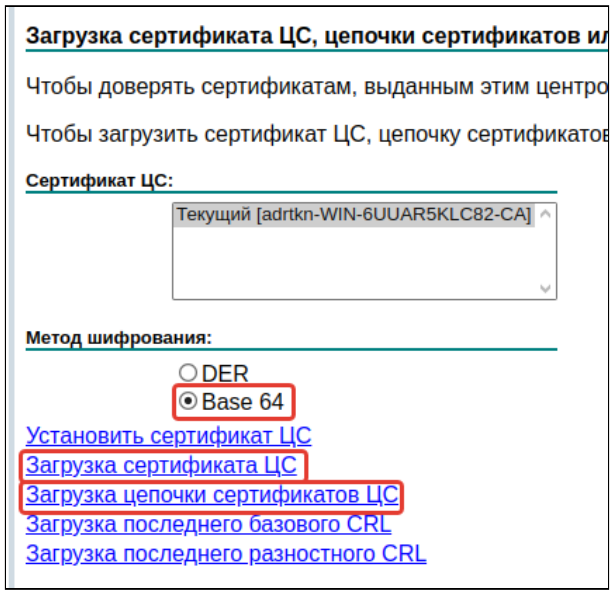
Active Directory

Для загрузки корневого сертификата или сертификатов цепочки доверия УЦ на компьютер:

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



3. В поле **Метод шифрования** выберите **Base 64**.
4. Выберите **Загрузка сертификата ЦС** или **Загрузка цепочки сертификатов ЦС**. Загрузка на компьютер начнется автоматически.
   Цепочка сертификатов загружается в виде файла – контейнера формата p7b.



Если присутствует необходимость извлечь сертификаты из контейнера, можно воспользоваться утилитой **openssl**.

Samba DC и РЕД АДМ

Эти КД не имеют встроенного УЦ.

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

Поддержка коротких доменных имен УЗ

rtlogon поддерживает использование коротких доменных имен для следующих типов аутентификации:

- 1ФА по логину и паролю УЗ;
- 2ФА по логину, паролю и OTP.

Возможность использовать короткие доменные имена задается в конфигурационном файле */etc/sssd/sssd.conf* параметром `use_fully_qualified_names`.

Этот параметр может принимать следующие значения:

- False (значение по умолчанию) — использование коротких доменных имен разрешено;

  Короткое доменное имя не должно совпадать с локальным именем пользователя. В противном случае при попытке аутентификации rtlogon выдаст ошибку.

- True — использование коротких доменных имен запрещено. Пользователь может вводить только полное доменное имя (FQDN).

Установка rtlogon

В ОС Альт установку/удаление rtlogon необходимо выполнять от имени root.

Чтобы установить rtlogon:

1. Скачайте с официального сайта Компании «Актив» (https://www.rutoken.ru/support/download/rutoken-logon-for-linux/) установочный пакет rtlogon для необходимой ОС и архитектуры процессора компьютера.
2. Откройте терминал.
3. Перейдите в каталог расположения установочного пакета.
4. Введите в терминале команду:

   Astra Linux and deb-based distributives

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

   Alt Linux

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

   RED OS and rpm-based distributives

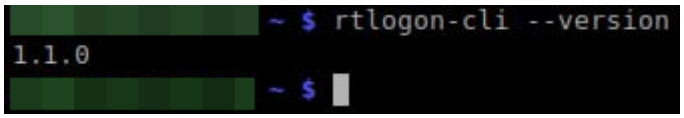
   ```
   sudo dnf install ./[the name of the installation package rtlogon].rpm
   ```

5. При запросе введите пароль администратора.

6. При запросе подтвердите продолжение установки.
7. Дождитесь окончания установки.
8. Введите в терминале команду:

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

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

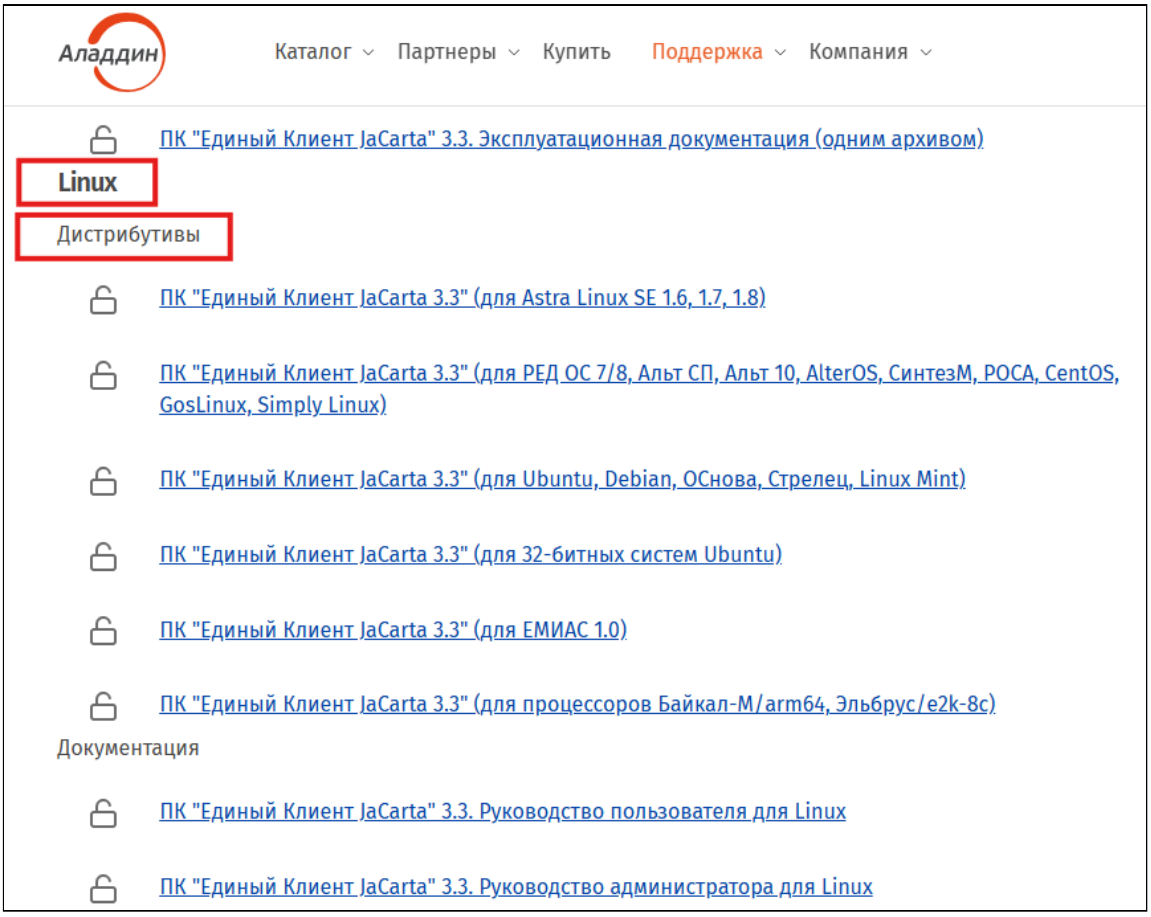


Установка rtlogon завершена.

Установка библиотеки libjcPKCS11-2.so

Чтобы работать с устройствами JaCarta, необходимо скачать и установить библиотеку libjcPKCS11-2.so:

1. Зайдите на сайт https://www.aladdin-rd.ru/support/downloads/jacarta/.
2. На странице в разделе **Linux Дистрибутивы** выберите **ПК "Единый Клиент JaCarta 3.3"** для соответствующей ОС.



3. На открывшейся странице нажмите кнопку **Скачать**.

4. Распакуйте скачанный архив.
5. Откройте терминал.
6. Перейдите в терминале в каталог распакованного архива.
7. Введите 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. Переместите библиотеку libjcPKCS11-2.so из каталога */usr/lib64* в каталог */opt/aktivco/rtlogon/pkcs*:

```
sudo cp /usr/lib64/libjcPKCS11-2.so /opt/aktivco/rtlogon/pkcs/
```

Установка библиотеки завершена.

Подготовка к настройке 3ФА

Чтобы работать с 3ФА, на компьютере пользователя должен быть установлен rtbiocomponents.

rtbiocomponents и 3ФА не поддерживаются для архитектуры процессора ARM64.

Чтобы добавить биометрические отпечатки пальцев пользователя на Рутокен, на компьютере администратора должны быть установлены:

- rtbiocomponents,
- ПО **Рутокен БИО. Программа администратора** — rtbioadmin,
- драйверы для используемого считывателя отпечатков пальцев.

Установка rtbiocomponents

Скачать rtbiocomponents можно на сайте Компании «Актив» — https://www.rutoken.ru/support/download/rutoken-bio/#components.

Чтобы установить rtbiocomponents на компьютер:

1. Откройте терминал и перейдите в каталог расположения дистрибутива.
2. Введите в терминале команду:

Astra Linux and deb-based distributives

```
sudo apt install ./rtbio_<версия>_amd64.deb
```

RED OS and rpm-based distributives

```
sudo dnf install rtbio_<версия>.x86_64.rpm
```

Alt Linux

```
su -c "apt-get install ./rtbio_<версия>-alt1.x86_64.rpm"
```

3. При запросе введите пароль администратора.

Установка rtbiocomponents завершена.

Установка rtbioadmin

Скачать rtbioadmin мо жно на сайте Компании «Актив» — https://www.rutoken.ru/support/download/rutoken-bio/#admin.

Установить rtbioadmin можно двумя способами:

- с помощью стандартной команды установки приложений,
- с помощью скрипта.

Чтобы установить rtbioadmin на компьютер с помощью стандартной команды установки приложений:

1. Установите на компьютере rtbiocomponents.
2. Откройте терминал и перейдите в каталог расположения скачанного rtbioadmin.
3. Введите в терминале команду:

   Astra Linux and deb-based distributives

   ```
   sudo apt install ./rtbioadmin_<версия>_amd64.deb
   ```

   RED OS and rpm-based distributives

   ```
   sudo dnf install ./rtbioadmin-<версия>.x86_64.rpm
   ```

   Alt Linux

   ```
   su -c "apt-get install ./rtbioadmin-<версия>.x86_64.rpm"
   ```

4. По запросу введите пароль администратора.

Установка rtbioadmin завершена.

Чтобы установить rtbioadmin на компьютер с помощью скрипта:

1. Откройте терминал и перейдите в каталог расположения скачанного rtbioadmin.
2. Введите в терминале команду:

   ```
   sudo ./install.sh
   ```

   rtbiocomponents установятся автоматически в процессе установки rtadmin.

Установка rtbioadmin завершена.

Подробнее процесс установки rtbioadmin описан в **Руководстве по работе с Рутокен БИО. Программа администратора**.

Добавление биометрических отпечатков пальцев на Рутокен

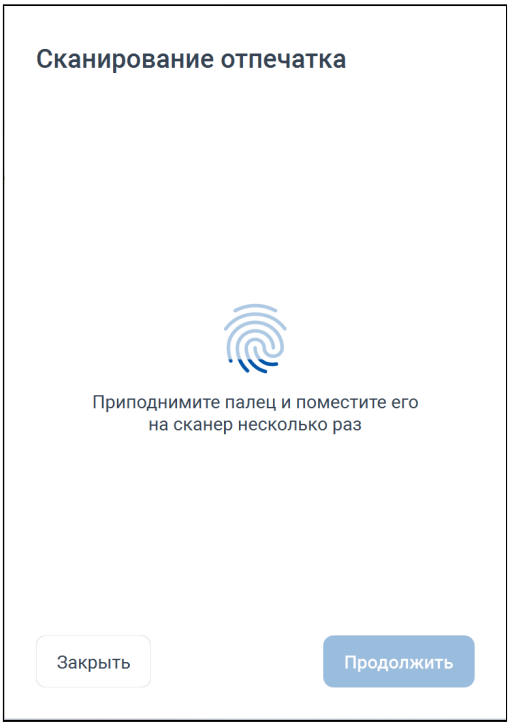
> 3ФА с использованием биометрических отпечатков пальцев поддерживается только для Рутокен ЭЦП 3.0 3250 БИО.
>
> Добавлять отпечатки пальцев на Рутокен можно только при отсутствии на нем добавленных ранее отпечатков.

Чтобы на компьютере администратора добавить биометрические отпечатки пальцев пользователей на Рутокен:

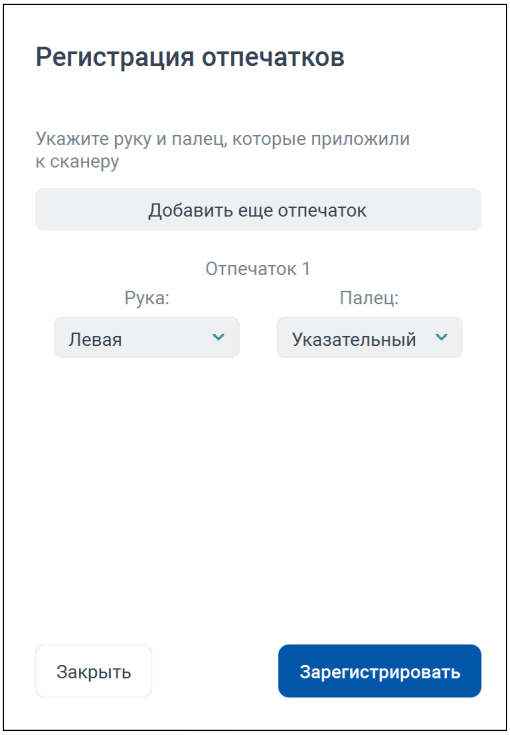
1. Установите rtbioadmin.
2. Установите на компьютер драйверы для считывателя отпечатков пальцев.
3. Подключите к компьютеру Рутокен.
4. Подключите к компьютеру считыватель отпечатков пальцев.
5. Откройте терминал и перейдите в каталог расположения файла запуска rtbioadmin.
6. Введите в терминале команду для запуска программы:

```
rtbioadmin
```

7. На боковой панели окна программы выберите нужный Рутокен.
8. Нажмите на вкладку **Отпечатки**.
9. На вкладке нажмите на кнопку **Войти**.
10. Введите PIN-код Администратора Рутокена.
11. В правом верхнем углу нажмите на значок +.
12. Следуя подсказкам в программе, с помощью считывателя отсканируйте отпечаток пальца пользователя.



13. Нажмите кнопку **Продолжить**.
14. На странице **Регистрация отпечатков**, в раскрывающихся списках **Рука** и **Палец**, выберите руку и палец пользователя, отпечаток которого добавляется.



15. Если необходимо добавить еще отпечатки пользователя, то нажмите кнопку **Добавить еще отпечаток** и повторите п. 12-14.

> На Рутокен ЭЦП 3.0 3250 БИО можно добавить до трех отпечатков пальцев.

16. Нажмите кнопку **Зарегистрироваться**.
17. Нажмите кнопку **Закрыть**.

Отпечатки пальцев пользователя будут добавлены на Рутокен.

Подробнее процесс добавления отпечатков описан в документе **Руководство по работе с Рутокен БИО. Программа администратора**.

Замена биометрических отпечатков пальцев на Рутокене

Чтобы заменить биометрические отпечатки пользователя на Рутокене:

1. Удалите их с Рутокена, отформатировав устройство.

> При форматировании Рутокена все пользовательские данные с него будут удалены, а его настройки вернутся к заводскому состоянию.

2. Добавьте новые отпечатки.

Команды и общие параметры rtlogon

Команда/параметр	Описание
Команды	
`configure`	Настройка ОС для работы с МФА
`reconfigure`	Реконфигурация ОС для работы с МФА
`unconfigure`	Отключение настроек ОС для работы с МФА
`setup-auth`	Настройка МФА
`unsetup-auth`	Удаление МФА
`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 МФА
`info`	Запрос информации о конфигурации rtlogon и параметрах локальной МФА
Параметры	

`-h`
или
`--help`
	Получение перечня команд и общих параметров rtlogon.
	При вызове с командой выводит перечень ее параметров

`--version`	Получение информации о версии установленного rtlogon

Обновление rtlogon

Для обновления rtlogon необходимо установить новый пакет. Старый пакет при этом удалять не требуется.

Удаление rtlogon

Особенности и ограничения при удалении rtlogon:

- запрещается самостоятельно, без использования средств rtlogon, удалять или изменять:
  - конфигурационный файл rtlogon — */etc/rtlogon/rtlogon.conf*;
  - файл, содержащий записи об УЗ с настроенной локальной МФА — */etc/rtlogon/localAuthDesc*.
- для удаления rtlogon необходимо использовать средства самого rtlogon;
- для удаления rtlogon в ОС Альт и ОС РЕД ОС необходим корректный (неповрежденный) файл *rtlogon.conf*.
  Если есть вероятность повреждения файла из-за выхода из строя жесткого диска или действий администратора, рекомендуется после установки и настройки rtlogon сделать бэкап файла */etc/rtlogon/rtlogon.conf*.
- для удаления rtlogon с поврежденным *rtlogon.conf* рекомендуется:
  - вручную восстановить *rtlogon.conf*, используя бэкап;
  - если восстановить файл *rtlogon.conf* невозможно:
    a. Отключить настройки ОС для работы с МФА.
    В этом случае исходная конфигурация PAM-модулей и/или исходный плагин ОС для системных экранов приветствия и блокировки могут не восстановиться.
    b. Удалить rtlogon.
- 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 МФА и перезагрузить компьютер.
  После удаления rtlogon администратор должен заново задать пароли для входа в ОС УЗ, у которых была настроена 2ФА со сложным паролем.

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 компьютер.

В ОС Альт установку/удаление rtlogon необходимо выполнять от имени root.

Чтобы удалить rtlogon:

1. Если ранее была настроена МФА, удалите ее.
2. Если ранее была настроена ОС для работы с МФА, отключите эти настройки.

3. Введите команду:

Astra Linux and deb-based distributives

```
sudo apt remove rutokenlogon
```

Alt Linux

```
apt-get remove rutokenlogon
```

RED OS and rpm-based distributives

```
sudo dnf remove rutokenlogon
```

4. При запросе введите пароль администратора.

Удаление rtlogon с компьютера завершено.

Настройка ОС для работы с МФА

В процессе настройки ОС автоматически выполняются следующие операции:

- настройка сервиса rtlogon_event-monitor;
- 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, основывающемся на экранном менеджере LightDM, поддерживаются языки раскладки клавиатуры, которые были добавлены через localectl.
>
> При вызове экрана блокировки в дистрибутивах, поддерживающих скринсейверы, возможно его непроизвольное открытие в другом tty.
>
> Для проверки поддержки ОС скринсейвера используется команда `[gui]-screensaver-command --query`.

Перед настройкой ОС для работы с МФА:

- должен быть установлен в сети или на компьютере пользователя сервер лицензирования;
- на сервере лицензирования должна быть активирована лицензия rtlogon для работы с соответствующей МФА;
- время на компьютере должно совпадать с серверным;
- для доменной 2ФА по сертификату и доменной 3ФА на компьютер пользователя должен быть загружен корневой сертификат и сертификаты цепочки доверия промежуточных УЦ, если они есть;
- для доменной 2ФА по сложному паролю на компьютере пользователя должен быть сгенерирован самоподписанный сертификат.

Чтобы настроить ОС для работы с МФА, введите в терминале команду:

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

Command parameters

Параметр	Описание	Значение по умолчанию	Наличие параметра в команде	Условие применения
`--domain arg`	Тип КД. Допустимые значения: • ipa, • aldpro, • ad, • samba, • rosadd, • redadm	-	Обязательно	Необходимо настроить ОС для работы с **доменной** МФА. ⊖ Не может применяться совместно с параметром `--local`. Эти 2 параметра являются взаимоисключающими
`--local`	Настройка ОС для работы с локальной МФА	-	Обязательно	Необходимо настроить ОС для работы с **локальной** МФА. ⊖ Не может применяться совместно с параметром `--domain`. Эти 2 параметра являются взаимоисключающими
`--license-server arg`	Адрес сервера лицензирования. В качестве адреса можно указать: • IP-адрес, • DNS-имя. Для локального сервера лицензирования: • IP-адрес – 127.0.0.1, • DNS-имя – localhost	-	Обязательно	Всегда

Параметр	Описание	Значение по умолчанию	Наличие параметра в команде	Условие применения
`--ca-cert arg`	Путь к файлу, содержащему: • корневой сертификат, • сертификаты цепочки доверия УЦ, • самоподписанный сертификат	/etc/ipa/ca.crt	Опционально	Необходимо настроить ОС для работы с доменной МФА
`--use-system-gui arg`	Использование системных экранов приветствия и блокировки. Допустимые значения: • yes — использовать системные экраны приветствия и блокировки, • no — использовать экраны приветствия и блокировки rtlogon	no	Опционально	Если необходимо использовать **системные** экраны приветствия и блокировки, указывать значение **yes**. Если необходимо использовать экраны приветствия и блокировки **rtlogon**, указывать значение **no**

При выборе системных экранов приветствия и блокировки в настройках ОС для работы с МФА возможно появление следующих ограничений на экранах:

- недоступна разблокировка PIN-кода;
- недоступен просмотр списка пользователей на токене, под которыми можно войти в систему;
- недоступны настройки сети;
- некорректный вывод запроса на предоставление PIN-кода для аутентификации – система запрашивает PIN-код, а на экран выводится сообщение с запросом пароля.

Поэтому при настройке **необходимо указывать использование экранов приветствия и блокировки rtlogon для всех ОС, кроме Astra Linux SE 1.8.1 – 1.8.4**. Эта ОС работает только с системными экранами приветствия и блокировки.

Если есть вероятность повреждения конфигурационного файла rtlogon из-за выхода из строя жесткого диска или действий администратора, рекомендуется после настройки или реконфигурации ОС для работы с МФА сделать бэкап файла */etc/rtlogon/rtlogon.conf*.

Неповрежденный файл *rtlogon.conf* необходим для корректного удаления rtlogon.

Внесение изменений вручную в файл *rtlogon.conf* запрещено. Повреждение файла может привести к невозможности использования rtlogon.

Пример.

```
sudo rtlogon-cli configure --local --license-server 127.0.0.1 --use-system-
gui yes
//OS setup for local MFA; using system Greeter and Lock Screen
sudo rtlogon-cli configure --domain ad --license-server TEST-PC --ca-cert
cert.pem
//OS setup for domain MFA; using rtlogon Greeter and Lock Screen
```

Реконфигурация ОС для работы с МФА

Перед изменением настроек ОС должна быть сконфигурирована для работы с МФА, т.е. должна быть выполнена команда rtlogon-cli configure.

Для реконфигурации ОС введите 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, • aldpro, • ad, • samba, • rosadd, • redadm	Опционально	Необходимо настроить ОС для работы с **доменной** МФА. Не может применяться совместно с параметром `--local`. Эти 2 параметра являются взаимоисключающими
`--local`	Настройка ОС для работы с локальной МФА	Опционально	Необходимо настроить ОС для работы с **локальной** МФА. Не может применяться совместно с параметром `--domain`. Эти 2 параметра являются взаимоисключающими

Параметр	Описание	Наличие параметра в команде	Условие применения
`--license-server`	Адрес сервера лицензирования. В качестве адреса можно указать: • IP-адрес, • DNS-имя. Для локального сервера лицензирования: • IP-адрес – 127.0.0.1, • DNS-имя – localhost	Опционально	Необходимо изменить адрес сервера лицензирования
`--ca-cert arg`	Путь к файлу, содержащему: • корневой сертификат, • сертификаты цепочки доверия УЦ, • самоподписанный сертификат	Опционально	Необходимо настроить ОС для работы с доменной МФА
`--use-system-gui arg`	Использование системных экранов приветствия и блокировки. Допустимые значения: • yes — использовать системные экраны приветствия и блокировки, • no — использовать экраны приветствия и блокировки rtlogon	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 */etc/rtlogon/rtlogon.conf*.

Реконфигурацию ОС без указания параметров рекомендуется использовать в следующих случаях:

- после выхода из строя ОС;
- после обновления ОС (для Astra Linux);
- при появлении сообщения об отсутствии лицензии с поддержкой биометрии, хотя она была получена и активирована на сервере лицензирования.



Рекомендуется использовать экраны приветствия и блокировки rtlogon.

Отключение настроек ОС для работы с МФА

Если для УЗ была настроена локальная 2ФА по сложному паролю, то перед отключением настроек ОС для работы с МФА необходимо выполнить команду rtlogon-cli unsetup-auth для этих УЗ.

Чтобы отключить настройки ОС для работы с МФА, введите в терминале команду:

```
sudo rtlogon-cli unconfigure
```

Если конфигурационный файл */etc/rtlogon/rtlogon.conf* не поврежден, то в результате выполнения этой команды вернутся в исходное состояние:

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

Скрипт массового развертывания rtlogon

Для централизованной установки rtlogon на компьютеры пользователей можно использовать скрипт массового развертывания.

Скрипт поддерживается только для доменной МФА.

В результате использования скрипта на компьютере администратора будет сформирован пользовательский дистрибутив, в состав которого будут входить:

- дистрибутив rtlogon для указанной ОС пользователя,
- пользовательский скрипт — *rutokenlogon_distributive.sh*,
- корневой сертификат, или сертификаты цепочки доверия УЦ, или самоподписанный сертификат.

Далее пользовательский дистрибутив необходимо перенести на компьютер пользователя и запустить пользовательский скрипт, входящий в его состав.

В результате использования пользовательского скрипта на компьютере пользователя:

- будет установлен rtlogon,
- настроена ОС для работы с доменной МФА.

Чтобы централизовано установить rtlogon на компьютеры пользователей:

1. Скачайте с сайта https://www.rutoken.ru/support/download/rutoken-logon-for-linux/ **Скрипты для массового развертывания и ввода ПК в домен**.
2. Распакуйте скачанный архив.
3. Откройте в любом текстовом редакторе файл *widespread_deploy.sh*.

4. Задайте значения следующим параметрам:

Параметр	Описание параметра	Пример
RUTOKENLOGON_PACKAGE	Абсолютный или относительный путь до дистрибутива rtlogon, который будет устанавливаться на компьютерах пользователей	RUTOKENLOGON_PACKAGE='/home/user/Downloads/rutokenlogon_1.1.0-1_amd64.deb'
GRDCONTROL_PACKAGE	Абсолютный или относительный путь до дистрибутива сервера лицензирования. ⊖ Если сервер лицензирования будет установлен на отдельный компьютер в сети, то значение параметру не задается	GRDCONTROL_PACKAGE='/home/user/Downloads/grdcontrol-4.4.3_amd64.deb'
USER_DISTRIBUTIVE_OUPUT_DIR	Абсолютный или относительный путь, по которому будет сохранен пользовательский дистрибутив rtlogon	USER_DISTRIBUTIVE_OUPUT_DIR="$(pwd)"
DOMAIN_TYPE	Тип домена, в который входит компьютер пользователя. Может принимать значения: • ipa, • samba, • aldpro, • ad	DOMAIN_TYPE="ipa"
PATH_TO_CA	Путь до сертификатов, загруженных на компьютер администратора: • корневого, • сертификатов цепочки доверия УЦ, • самоподписанного	PATH_TO_CA="/home/user/Downloads/certificate.pem"
OCSP_URL	Адрес OCSP сервера	OCSP_URL="192.168.1.10"
CRL_URL	Адрес, по которому можно выгрузить CRL	CRL_URL="192.168.1.10"
LICENSE_SERVER_URL	Адрес сервера лицензирования, на котором активирована лицензия rtlogon	LICENSE_SERVER_URL="192.168.1.5"

5. Сохраните изменения в скрипте.

6. Запустите скрипт:

```
./widespread_deploy.sh
```

По окончании работы скрипта будет сформирован пользовательский дистрибутив *rutokenlogon_distributive_deployment.tar.*

7. Перенесите пользовательский дистрибутив на компьютер пользователя.
8. На компьютере пользователя:
    a. Распакуйте пользовательский дистрибутив.
    b. Запустите пользовательский скрипт:

```
./rutokenlogon_distributive.sh
```

    c. При запросе данных в терминале введите соответствующую информацию.

В результате на компьютере пользователя будет установлен rtlogon и настроена ОС для работы с доменной МФА.

Проверка сертификатов пользователей на статус «отозванный»

rtlogon поддерживает функцию проверки сертификатов пользователей на статус «отозванный».

Проверка может выполняться с помощью CRL или OCSP.

CRL

Чтобы включить проверку сертификатов с помощью CRL:

1. Загрузите на компьютер CRL-файл(ы).
2. Проверьте, что на компьютер загружен корневой сертификат УЦ и сертификаты промежуточных УЦ цепочки доверия.
3. Откройте файл */etc/sssd/sssd.conf*.
4. В секции `[sssd]`, в параметр `certificate_verification` добавьте опцию `crl_file` и задайте для нее путь к CRL-файлу.

    Поддерживается только pem-формат CRL-файла.

5. Для игнорирования проверки в случае истечения срока действия CRL-файла добавьте в параметр `certificate_verification` опцию `soft_crl`.

    Опцию игнорирования ошибок в цепочке доверия `partial_chain` не рекомендуется включать при работе в домене в связи с его некорректной работой с kerberos.

6. Сохраните изменения в файле.
7. Выполните команду `rtlogon-cli reconfigure` без параметров.

Если опция `crl_file` отсутствует, проверка сертификата пользователя на статус «отозванный» не выполняется.

Пример.

```
[sssd]
certificate_verification = soft_crl, crl_file = /PATH/TO/CRL/FILE, ...
```

OCSP

Включить проверку сертификата на статус «отозванный» с помощью OCSP можно 2-мя способами.

1 способ.

URL-адрес сервера OCSP задан в сертификате пользователя, корневом сертификате или сертификате промежуточного УЦ.

2 способ.

1. Откройте файл */etc/sssd/sssd.conf*.
2. В секции `[sssd]`, в параметр `certificate_verification` добавьте опцию `ocsp_default_responder` и задайте для нее URL-адрес сервера OCSP.
3. Для игнорирования проверки при недоступности сервера OCSP добавьте в параметр `certificate_verification` опцию `soft_ocsp`.
4. Для отключения проверки сертификата добавьте в параметр `certificate_verification` опцию `no_ocsp`.
5. Сохраните изменения в файле.
6. Выполните команду `rtlogon-cli reconfigure` без параметров.

Пример.

```
/// enabling verification via the sssd.conf and ignoring verification
[sssd]
certificate_verification = soft_ocsp, ocsp_default_responder = /OCSP/SERVER/
ADDRESS, ...

/// disabling verification
[sssd]
certificate_verification = no_oscp

/// ignoring verification. The OCSP server URL is specified in the
certificate
[sssd]
certificate_verification = soft_ocsp
```

Настройка работы с OTP

2ФА с использованием OTP поддерживается только для КД Freel PA, Dynamic Directory и ALDPro.

Возможность использования доменной 2ФА с OTP настраивается средствами домена.

Чтобы настроить вход доменного пользователя по Рутокен OTP или Яндекс ID (далее — TOTP-токены):

1. Добавьте TOTP-токен в домен, введя команду:

```
ipa otptoken-add [TOKEN_ID] [command parameters]
```

Command parameters

Параметр	Описание	Значение по умолчанию	Наличие параметра в команде	Условие применения
`TOKEN_ID`	Идентификатор TOTP-токена в домене. В качестве идентификатора может использоваться: • имя токена; • серийный номер токена – для Рутокена OTP; • логин пользователя в домене, для которого настраивается TOTP-токен	uuid	Опционально	Необходимо изменить идентификатор TOTP-токена, используемый по умолчанию
Command parameters				
`--owner arg`	Пользователь TOTP-токена. Указывается логин УЗ пользователя без имени домена, для которого настраивается доменная 2ФА с OTP	Логин администратора домена, который вызывает данную команду	Опционально	Необходимо настроить доменную 2ФА с OTP для другого пользователя
`--algo arg` или `-a arg`	Алгоритм хеширования, на основе которого вырабатываются одноразовые пароли. Может принимать значения: • sha1, • sha256	sha1	Опционально	Необходимо изменить алгоритм, используемый по умолчанию

Параметр	Описание	Значение по умолчанию	Наличие параметра в команде	Условие применения
`--interval arg` или `--int arg`	Время действия одноразового пароля (в секундах) до его перегенерации. Может принимать значения: • 30, • 60	30	Опционально	Необходимо изменить время действия, используемое по умолчанию
`--digits arg`	Длина одноразового пароля rtlogon поддерживает длину одноразового пароля равную только 6 цифрам	6	Опционально	-
`--type arg`	Тип токена, для которого выполняется настройка. Может принимать значения: • totp, • TOTP	TOTP	Опционально	-
`--key arg`	Секретный ключ TOTP-токена в формате base32	-	Опционально	TOTP-токен уже был настроен до добавления в домен
`--no-qrcode`	Не генерировать QR-код с настройками TOTP-токена	-	Опционально	TOTP-токен уже был настроен до добавления в домен

Пример .

The TOTP token wasn't configured before being added to the domain

```
ipa otptoken-add --type totp --algo sha256 --digits 6 --interval 30
--owner "$DOMAIN_USER" "$OTP_SERIAL"
```

The TOTP token was configured before being added to the domain

```
ipa otptoken-add --type totp --algo sha256 --digits 6 --interval 30
--owner "$DOMAIN_USER"
--key key_value --no-qrcode "$OTP_SERIAL"
```

2. Если TOTP-токен ранее не был настроен:
    a. Отсканируйте в Приложении для инициализации устройств Рутокен OTP или Яндекс ID полученный в результате выполнения предыдущей команды QR-код.
    b. Подключите устройство к приложению и выполните его настройку — для Рутокен OTP.
3. Разрешите использование TOTP-токена для входа в систему, введя одну из команд:

Команда	Применение команды
`ipa user-mod [m_login] --user-auth-type otp`	В домене настроена политика входа в систему по паролю УЗ
`ipa user-mod [m_login] --user-auth-type otp --user-auth-type pkinit`	В домене настроена политика входа в систему по сертификату или паролю УЗ

Чтобы отменить вход доменного пользователя по Рутокен OTP или Яндекс ID, введите команду:

```
ipa otptoken-del [TOKEN_ID]
```

Пример.

```
ipa otptoken-del "$OTP_SERIAL"
```

Работу с OTP можно также настроить, используя графический интерфейс КД.

Настройка МФА

Перед настройкой доменной МФА должна быть выполнена команда rtlogon-cli configure с доменными параметрами.

Для настройки МФА:

1. Подключите токен к компьютеру.
2. Для настройки доменной 2ФА по сертификату или доменной 3ФА:
    a. Создайте запрос на получение сертификата.
    b. Получите сертификат УЗ от УЦ.
3. Для настройки локальной 2ФА по сертификату, доменной 2ФА по сложному паролю или локальной 3ФА – сгенерируйте самоподписанный сертификат.
4. Введите в терминале команду:

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

При помощи команды `rtlogon-cli setup-auth` можно настраивать МФА для другого компьютера (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 МФА	-	Обязательно	
`-d arg` или `--domain arg`	Имя домена, в котором зарегистрирована УЗ	-	Опционально	Необходимо обязательно указывать этот параметр **для доменных УЗ**
`--disconnect-policy arg`	Политика ОС при отключении токена от компьютера. Возможные значения: • **lock** – вызов экрана блокировки; • **none** – продолжение текущей сессии	lock	Опционально	Необходимо отключить вызов экрана блокировки при отключении токена от компьютера
`--token-id arg` или `-t arg`	Идентификатор токена, к которому применяется команда. ⓘ 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.). Для просмотра информации об идентификаторе токена необходимо вызвать команду rtlogon-cli info	-	Опционально	К компьютеру 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 отображаться не будет

Параметры настройки 2ФА по сложному паролю				
`--passwd`	Признак настройки 2ФА по сложному паролю	-	Обязательно	

`-e arg`
или
`--expire-days arg`
	Количество дней до перегенерации сложного пароля	-	Опционально	Настройка локальной 2ФА по сложному паролю.
				Необходимо задать количество дней до перегенерации сложного пароля.
				Если параметр не указан, перегенерация сложного пароля не выполняется. Время действия сложного пароля при этом не ограничено

`--domain-admin arg`	Логин администратора	-	Опционально	Настройка доменной 2ФА по сложному паролю. Указание учетной записи администратора используется для изменения пароля пользователя на контроллере домена

Параметр	Описание	Значение по умолчанию	Наличие параметра в команде	Условия применения
Параметры настройки 2ФА по сертификату или 3ФА				

`-c arg`
или
`--cert arg`
	Путь к сертификату УЗ.
	В случае когда сертификат располагается в текущей директории, допускается указывать только его наименование.
	Поддерживаются следующие форматы сертификата:
	• pem,
	• der
		-	Обязательно	

`--login-policy arg`	Политика входа в ОС.
	Возможные значения:
	• **certonly**:
	  ◦ для 2ФА — только по сертификату и наличию подключенного токена;
	  ◦ для 3ФА — только по сертификату, наличию подключенного токена и биометрическому отпечатку пальца.
	• **certandpass**:
	  ◦ для 2ФА — по сертификату и наличию подключенного токена или по логину/паролю УЗ;
	  ◦ для 3ФА — по сертификату, наличию подключенного токена и биометрическому отпечатку пальца или по логину/паролю УЗ.
	Выбор осуществляется при входе в ОС.
	⊖ Для администратора может быть установлен только **certandpass**
		certonly	Опционально	Настройка локальной 2ФА по сертификату или локальной 3ФА.
				Необходимо изменить политику входа в ОС

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

Пример:

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
```

Минимальные права администратора для смены сложного пароля

Для смены сложного пароля в настроенной доменной 2ФА по сложному паролю администратор должен соответствовать требованиям, указанным в таблице.

КД	Требования для администратора
Active Directory	Должен входить в одну из следующих групп домена: - Account Operators; - Domain Admins; - любая группа, имеющая право **Reset password**. Право **Reset password** назначается группе через настройку **Delegation of Control** контейнера или OU домена

КД	Требования для администратора

ALDPro	Должен иметь доступ к LDAP-операции **Modify** для других записей.
	
	Для добавления необходимых прав можно воспользоваться следующими командами, заменив в них данные на необходимые:
	
	`ipa group-add passwd-admins --desc="Password Administrators"`
	
	`ipa env | grep basedn`
	`// the base domain NAME will be displayed in the terminal, for example:`
	`// basedn: dc=ald,dc=test`
	
	`nano password-admin.ldif`
	`// add the following lines to the file:`
	`// dn: cn=global_policy,cn=ALD.TEST,cn=kerberos,dc=ald,dc=test`
	`// changetype: modify`
	`// add: passwordAdminDN`
	`// passwordAdminDN: cn=passwd-admins,cn=groups,cn=accounts,dc=ald,dc=test`
	
	`ldapmodify -Y GSSAPI -H ldap://[LDAP server address] -f password-admin.ldif`
	
	`nano password-aci.ldif`
	`// add the following lines to the file:`
	`// dn: dc=ald,dc=test`
	`// changetype: modify`
	`// add: aci`
	`// aci: (targetattr="userPassword")(version 3.0;`
	`// acl "Allow passwd-admins reset passwords";`
	`// allow (write)`
	`// groupdn="ldap:///cn=passwd-admins,cn=groups,cn=accounts,dc=ald,dc=test";)`
	
	`ldapmodify -Y GSSAPI -H ldap://[LDAP server address] -f password-aci.ldif`
	
	`ipa user-add testuser --first="testuser" --last="testuser" --password`
	
	`ipa group-add-member passwd-admins --users=testuser`

КД	Требования для администратора

Samba DC и РЕД АДМ	Должен входить в одну из следующих групп домена:
	• Domain Admins;
	• любая группа, имеющая право **Reset password**.
	
	Право **Reset password** можно назначить следующим образом:
	1. Зайти в КД под УЗ **root**.
	2. Ввести следующие команды, заменив в них данные на необходимые:
	`samba-tool ou create "OU=ManagedUsers,DC=samba,DC=test"`
	`samba-tool user create user1 123456 --userou="OU=ManagedUsers"`
	`samba-tool user create user2 123456 --userou="OU=ManagedUsers"`
	`samba-tool user create admin5 654321`
	`samba-tool user show admin5 | grep -i objectsid`
	`// The administrator's SID for admin5 will be displayed in the terminal:`
	`// objectSid: [SID]`
	`samba-tool dsacl set --objectdn="OU=ManagedUsers,DC=samba,DC=loc" --sddl="(OA;CIIO;CR;00299570-246d-11d0-a768-00aa006e0529;;[The administrator's SID for admin5])(OA;CIIO;WP;bf967a0a-0de6-11d0-a285-00aa003049e2;;[The administrator's SID for admin5])"`
	3. Выйти из УЗ **root** и ввести команду:
	`sudo samba-tool user setpassword user1 --newpassword='NewStrongPassword' -U "NETBIOS\\admin5" -H ldap://[domain controller address]`

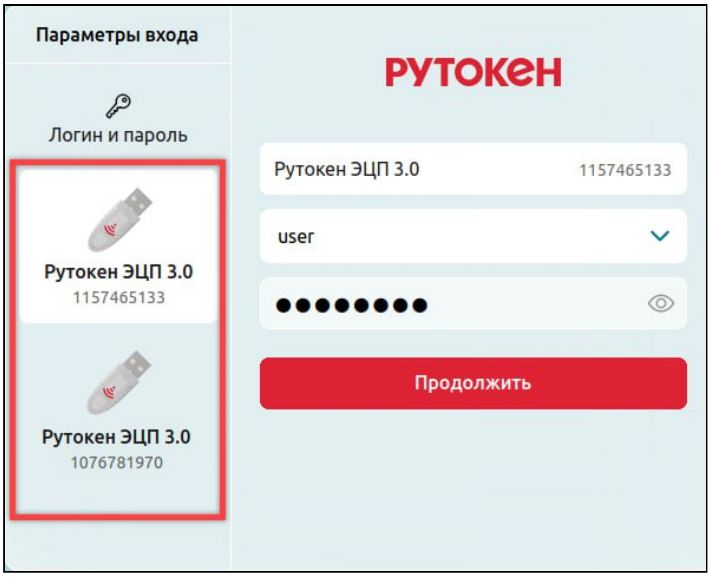
КД	Требования для администратора

FreeIPA, и Dynamic Directory	Должен входить в одну из следующих групп домена:
	• Password Administrators;
	• любая группа, имеющая право **Reset password** для нужного пользователя.
	Создать группу и назначить ей право **Reset password** можно с помощью следующих команд:
	`ipa permission-add "Permission_name" \`
	`--type=user \`
	`--right=write \`
	`--attrs=userPassword`
	
	`ipa privilege-add "Reset Password Privilege"`
	
	`ipa privilege-add-permission "Reset Password Privilege" \`
	`--permissions="Reset Password Permission"`
	
	`ipa role-add "Reset Password Role"`
	
	`ipa role-add-privilege "Reset Password Role" \`
	`--privileges="Reset Password Privilege"`
	
	`ipa role-add-member "Reset Password Role" \`
	`--groups=testgroup`

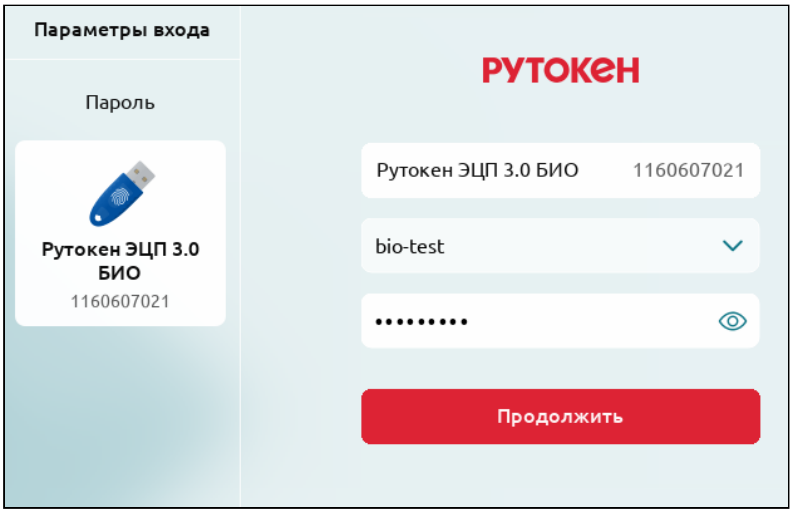
Проверка настройки МФА

Для проверки настроек МФА:

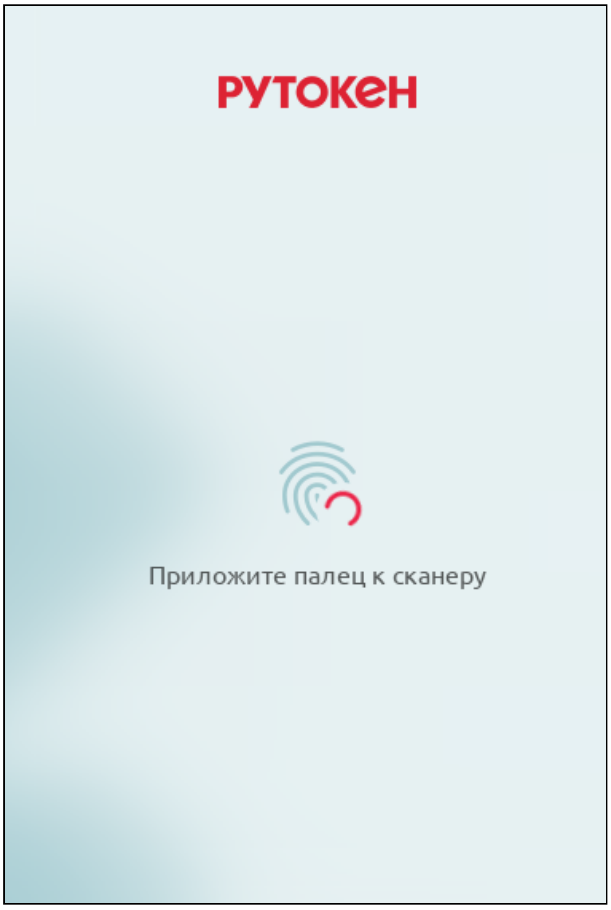
1. Завершите текущую сессию.
2. Подключите ключевой носитель к компьютеру.
3. Если была настроена 3ФА, подключите к компьютеру считыватель отпечатков пальцев.
4. На **экране приветствия rtlogon**:
    a. Выберите в списке устройств необходимый ключевой носитель.
    b. Если была настроена 2ФА:
        i. В раскрывающемся списке **Логин** выберите логин необходимой УЗ.
        ii. Введите PIN-код токена в поле **PIN-код**.
        iii. Нажмите **Продолжить**.



    c. Если была настроена 3ФА:
        i. В раскрывающемся списке **Логин** выберите логин необходимой УЗ.
        ii. Введите PIN-код токена в поле **PIN-код**.
        iii. Нажмите кнопку **Продолжить**.



iv. Когда появится сообщение "Приложите палец к сканеру", приложите палец к подключенному считывателю отпечатков пальцев.



5. На **системном экране приветствия**:
   a. Если была настроена 2ФА:
      i. Введите логин УЗ.
      ii. Введите PIN-код.
   b. Если была настроена 3ФА:
      i. Введите логин УЗ.
      ii. Введите PIN-код.
      iii. Приложите палец к считывателю отпечатков пальцев

Если МФА была настроена корректно, будет выполнен успешный вход в систему.

Изменение настроек МФА

Чтобы изменить настройки МФА, необходимо снова вызвать команду rtlogon-cli setup-auth с указанием нужным параметров.

Удаление МФА

Чтобы удалить МФА:

1. Если требуется удалить МФА для УЗ только с токена или с токена и компьютера, подключите токен к компьютеру.
2. Введите в терминале команду:

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

3. Если МФА будет удаляться с токена, введите PIN-код токена.
4. Если для УЗ была настроена 2ФА по сложному паролю, при запросе введите дважды новый пароль для УЗ.

При помощи команды `rtlogon-cli unsetup-auth` можно удалить МФА для УЗ другого компьютера (при помощи указания домена или идентификатора компьютера). 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 МФА	-	Обязательно	
`-d arg` или `--domain arg`	Имя домена, в котором зарегистрирована УЗ	-	Опционально	Для доменных УЗ
`--host-id arg`	Идентификатор компьютера, к которому привязана УЗ	-	Опционально	Удаление МФА для УЗ, привязанной к другому компьютеру с идентификатором *host-id*. В этом случае записи об УЗ с настроенной МФА удаляются только с токена. Необходимо также указать параметр `--only-on-token`

Параметр	Описание	Значение по умолчанию	Наличие параметра в команде	Условие применения

`--token-id arg`
или
`-t arg`
	Идентификатор токена, к которому применяется команда.
	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.).
	Для просмотра информации об идентификаторе токена необходимо вызвать команду rtlogon-cli info
		-	Опционально	К компьютеру подключено несколько токенов или один комбинированный токен

`-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 отображаться не будет

`--ignore-token`	Удалить МФА для УЗ только с компьютера. На токене МФА для УЗ сохраняется	-	Опционально	Для локальных УЗ
`--keep-cert-and-key`	Удалить МФА для УЗ с компьютера и токена с сохранением ключевой пары и сертификата	-	Опционально	Удаление МФА для УЗ с компьютера и токена с сохранением ключевой пары и сертификата
`--only-on-token`	Удалить МФА для УЗ только с токена. На компьютере МФА для УЗ сохраняется	-	Опционально	Удаление МФА 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 МФА для УЗ удаляется и с токена, и с компьютера:

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

Ключевая пара и сертификат при этом не сохраняются.

Пример:

Remove local MFA

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

Remove domain MFA

```
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 "$DOMAIN_ADMIN"
// enter domain admin password
```

Remove local MFA for other PC

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

Remove domain MFA with key pair and certificate saved

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

Кеширование УЗ

В rtlogon для sssd по умолчанию включена функция кеширования УЗ с настроенной доменной МФА.

Кеширование доменных УЗ позволяет пользователям аутентифицироваться в свою УЗ даже при отсутствии соединения с КД.

Кеширование задается следующими параметрами:

```
[sssd]
certificate_verification = soft_ocsp, soft_crl, ...

# вместо <domain_name> указывается имя домена
[domain/<domain_name>]
cache_credentials = True
krb5_store_password_if_offline = True
```

Чтобы отключить кеширование УЗ, введите в терминале следующие команды:

```
mkdir -p /etc/sssd/conf.d/
cat >> /etc/sssd/conf.d/60-disable_offile_auth.conf <<EOF
[sssd]
certificate_verification =
# вместо <domain_name> указывается имя домена
[domain/<domain_name>]
cache_credentials = False
krb5_store_password_if_offline = False
EOF

chown root:root /etc/sssd/conf.d/60-disable_offile_auth.conf
chmod 600 /etc/sssd/conf.d/60-disable_offile_auth.conf

systemctl restart sssd
```

Создание запроса на получение сертификата, генерация самоподписанного сертификата

Чтобы создать запрос на получение сертификата или сгенерировать самоподписанный сертификат:

1. Подключите токен к компьютеру.
2. Введите в терминале команду:

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

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:
	▪ rsa,
	▪ gost256,
	▪ gost512
		rsa с длиной ключа 2048	Опционально	Необходимо изменить криптоалгоритм с rsa на другой доступный.
				⊖ Домены поддерживают работу только с криптоалгоритмом RSA

`-s`
или
`--self-signed`
	Атрибут, указывающий, что генерируется самоподписанный сертификат	-	Опционально	Генерация самоподписанного сертификата

`-o arg`
или
`--output arg`
	Путь к сохраняемому на компьютере сертификату.
	В случае, если сертификат будет располагаться в текущей директории, допускается указывать только его наименование
		-	Обязательно	

Параметр	Описание	Значение по умолчанию	Наличие параметра в команде	Условие применения
Token parameters				

`-t arg`
или
`--token-id arg`
	Идентификатор токена, к которому применяется команда.
	ⓘ 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.).
	Для просмотра информации об идентификаторе токена необходимо вызвать команду rtlogon-cli info
		-	Опционально	Если к компьютеру подключено несколько токенов или один комбинированный токен

`-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

Параметр	Описание	Значение по умолчанию	Наличие параметра в команде	Условие применения
Certificate content				
`--dn CN arg`	Common Name (CN) субъекта сертификата — имя пользователя. Формат записи имени пользователя зависит от типа МФА. Если имя пользователя будет указано в неверном формате, то при аутентификации сертификат пользователя не будет найден. Для локальной МФА имя пользователя может принимать любое значение. Для доменной МФА имя пользователя может принимать следующие значения: • в КД FreeIPA, ALD Pro, Dynamic Directory — имя пользователя в домене; • в КД AD — имя пользователя может принимать любое значение. ⊖ Для доменной МФА с КД FreeIPA, ALD Pro, Dynamic Directory параметр `--dn CN` необходимо использовать совместно с параметром `--dn O`, который содержит имя домена. Пример. CN = ivanov O = RTKN.TEST	-	Обязательно	
`--dn C arg`	Страна. Для обозначения используется двухбуквенный код страны в соответствии с ISO 3166	RU	Опционально	Необходимо изменить название страны
`--dn ST arg`	Область (край и т.д.). Указывается одним словом. Используемый алфавит: латинский	-	Опционально	Необходимо указать название области

Параметр	Описание	Значение по умолчанию	Наличие параметра в команде	Условие применения
`--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 ⊖ Для доменной МФА с КД FreeIPA, ALD Pro параметр представляет собой имя домена	-	Опционально	Необходимо указать название организации
`--days arg`	Время действия сертификата (в днях). Максимальное значение: **5500 дней**. Датой начала действия сертификата является дата выполнения команды `create-cert`	1095 дней (3 года)	Опционально	Для самоподписанного сертификата. Необходимо изменить срок его действия
bio parameter				
`--bio`	Атрибут, указывающий, что сертификат или запрос на сертификат предназначен для настройки аутентификации по биометрии	-	Опционально	Если будет настраиваться аутентификация по биометрии

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 -o cert.pem -p 12345678 --dn CN Petrova --dn O
RTKN.TEST
```

Request file content

```
-----BEGIN CERTIFICATE-----
MIIEsDCCApgCAQAwDQYJKoZIhvcNAQELBQAwHjEPMA0GA1UEAwwGYWxkcHJvMQsw
CQYDVQQGEwJSVTAeFw0yNDA5MDkxNDQ5NTRaFw0yNzA5MDkxNDQ5NTRaMB4xDzAN
BgNVBAMMBmFsZHBybzELMAkGA1UEBhMCUlUwggIiMA0GCSqGSIb3DQEBAQUAA4IC
DwAwggIKAoICAQDHGEBEgZXouPLusCh80U/r8c5q0gNSzV83GzJJRJlzo5fcUK7p
eNzTx2dPQL6moUrLQrpgAiFW08ZsI42S4QAg8A8+AL58nNnrdmCbahcj8LPvY9uZ
u3SVO8bts4PfH6kqk9xgX5LVOrXvFw2k4a+A+7h+n/9fWDy1aRv+8Au9whN6XRaj
Mr6a4HzF22ohpxwRRL8HVWA33Kxrpvt3OsnG7Tw50tpNXyKljpQRoIJJSwsZ0Kwn
+6kIAh2T6L6odQmToA/cJi5IjHcuRx7Pef3qOqHj0CiojARY24Hkx7p8SsYddfvx
D8TN6gov1/FJ7QJNqkPkYr6bCr6jAoS6XzP8VoMV7fTj3JUONJRqrdVL4imR7jwE
qcMV1uLFi8W2d3eIesr0jpTAWLT19ObK7gH61HR10NQIgrrYGdRnV04ZKq8b4R13
bI6c0/Aq/c7MiB1TIF5nT4NG8zio7u3xTdyRELZb6As5eqTRWpI0wMdQvhtbLmtQ
XbFR9CEQmZhAllP4CTvCN/bAEIA6BpHJdq8dXVPOYHQ7OCFmvOLEDvrBjQiPdhbZ
p1Lr4sFrrPrj4vEA/Fz7z0KmlN8wGZIxBrPRvCGeuBF5A8bgxhOMubZJibEagt2+
m4QC6Zo5KJRszVWgiR9qnWr+bV3wPPNvbbQvJchSy8bAAstvrz06VIJt6QIDAQAB
MA0GCSqGSIb3DQEBCwUAA4ICAQBLI8Jx0+z+vfyPUIdnCrOPubp7XiWw76pXQIno
B9suGdXkHytahq0am7+9A3E3rmgyNh8tvOkSmkmCM2cMMreeHW1pSiQp58J5tEiT
uZGpplAp+FQpFRYqQQ7Ibzhmi2sb5qQ2C01q+2+QGEmySxKIt+idLhmP+Hf2xK+m
1D9vqQLdJ5WlTqpvscxNI9ybSwl8qtM0qs9xWbRP+M9G0FGrvZR2pYhVzQYOYVWh
V6wRDxMDzgKeh3vzOdcIi22b06FxA1DQ5qI6xIuE0JmGiplPzgK0TKCnr8YFSQ9W
fjA+Unfu+rED1kf/j3a2ErmqdAvfYAlgyNJNluq9O7NGMzMolzJr0KmGSOQESXW0
9ohhxxQdl8cOg/zqZWbvxjv5WaELsblVEF0dS1wFetva0PVCSuA3eITX/loWvhZR
n7spWnYfkpVMgwYKrAofAc/2h0N88v2XvetnA0YvYOLxeolHt1FWvLWsdkiD1Wk+
3yXuNsFvA+s/uzO/HchGMvF7QlIeWhdwsriGgGbjpjn5VMIknLvykJbC07X1fZmo
pWe4wEkG5h7FTZ1omYwbNvbfdFgTudmaSnTiydNxjFND0pekVqRPCu7XDuV4BexE
3qeL3619OtSCznEfhfZvPfu2unEBi1NkRQ/Gmqt00KmIDKcAwjgwxKU1IZ68OlYO
qR4Lxg==
-----END CERTIFICATE-----
```

Получение сертификата УЗ от УЦ

FreeIPA, Dynamic Directory и ALDPro

После создания запроса на получение сертификата введите в терминале 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 введите пароль администратора.

Пример.

```
kinit admin

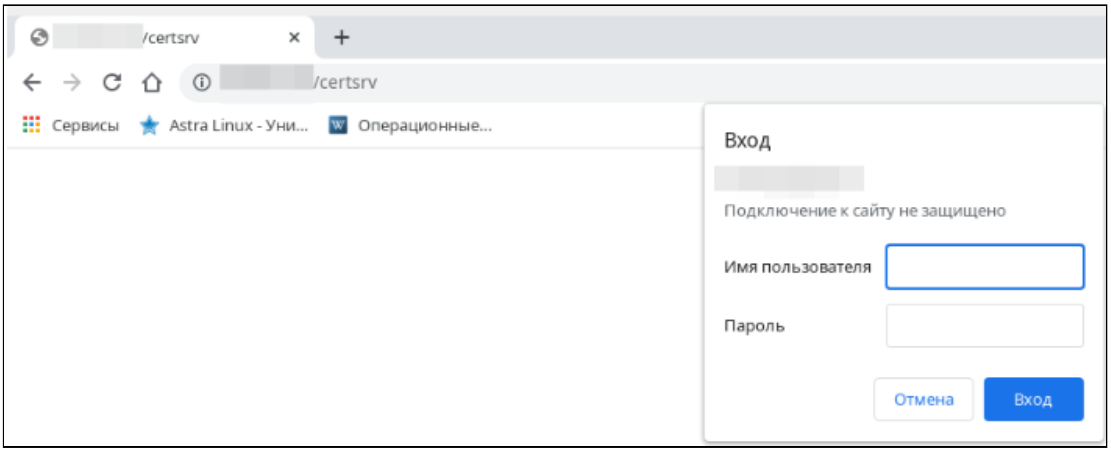
ipa cert-request ./cert.req --principal user3 --ca ipa --profile-id
caIPAserviceCert --certificate-out cert.pem

kdestroy
```

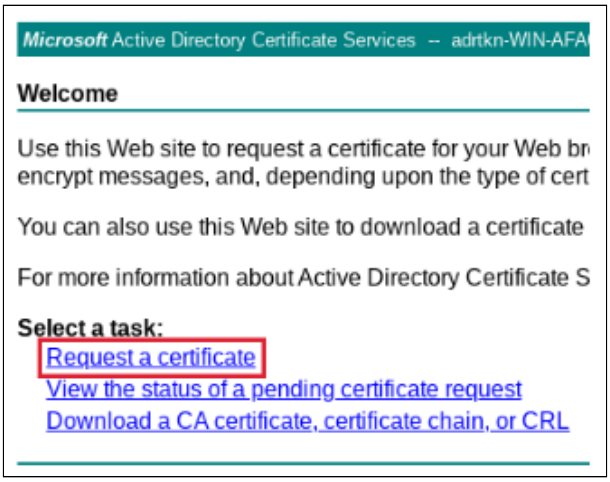
Active Directory

После создания запроса на получение сертификата:

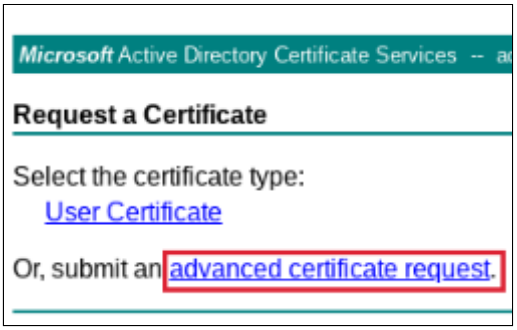
1. Зайдите на веб-интерфейс УЦ КД. По умолчанию адрес имеет следующий вид: *https://[domain]/certsrv.*
2. Авторизуйтесь под УЗ, для которой запрашивается сертификат.



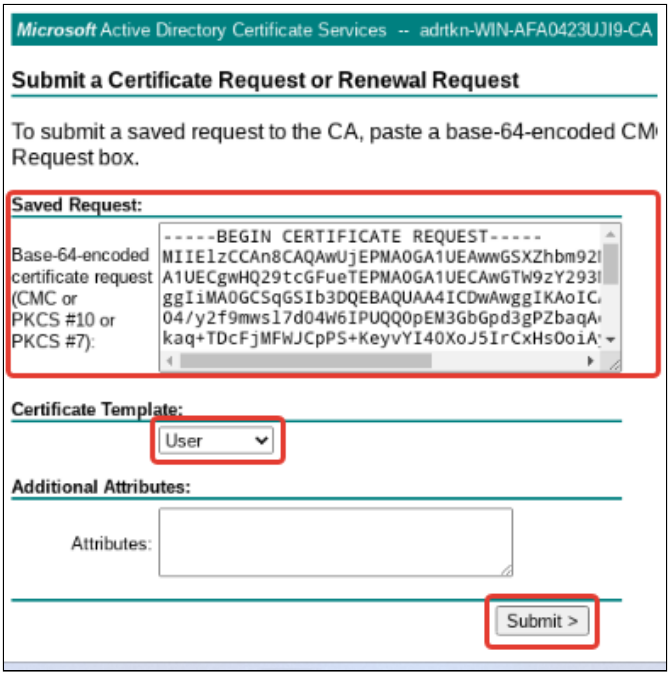
3. Выберите задачу **Request a certificate**.



4. Выберите пункт **advanced certificate request**.



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



8. В поле Certificate Issued выберите **Base 64 encoded** и нажмите **Download certificate**. Загрузка сертификата УЗ на компьютер начнется автоматически.

Samba DC и РЕД АДМ

После создания запроса на на получение сертификата:

1. Отправьте запрос на УЦ.
   Форма и способ отправки запроса зависят от выбранного и настроенного администратором УЦ.
2. Подпишите запрос на стороне УЦ.
   Способ подписания зависит от заданных администратором настроек УЦ.
3. Скопируйте подписанный сертификат УЗ на компьютер.

Проверка готовности компьютера к МФА

В rtlogon доступна функциональность проверки компьютера на готовность к МФА, которая реализована в виде скриптов проверок.

Скрипты устанавливаются в каталог */etc/rtlogon/gui_checks/*.

Каждой проверке соответствует один скрипт. Можно использовать скрипты, которые поставляются в качестве примеров вместе с rtlogon, изменять их или создавать свои согласно требованиям к скриптам.

Требования к скриптам

Для того, чтобы rtlogon мог взаимодействовать со скриптами, они должны удовлетворять следующим требованиям:

- скрипты должны быть установлены в каталог */etc/rtlogon/gui_checks/*;
- права доступа к скриптам и каталогу со скриптами должны быть `rwxr-xr-x` (запрещено вносить изменения всем, кроме владельца root);
- у пользователя экрана приветствия должны быть права на:
  - просмотр списка файлов в каталоге */etc/rtlogon/gui_checks/*;
  - чтение и запуск скриптов из каталога */etc/rtlogon/gui_checks/*.
- название файла скрипта должно начинаться с префикса `check-`;
- скрипт должен передавать rtlogon свой уникальный идентификатор;
- скрипт должен передавать rtlogon свое локализованное имя;
- если опциональные параметры заданы, они должны иметь значение из диапазона допустимых значений;
- скрипты должны завершать работу с одним из следующих кодов возврата:
  - 0 — проверяемая функциональность доступна.
    Соответствует зеленому индикатору в пользовательском интерфейсе;
  - 1 — проверяемая функциональность недоступна.
    Соответствует красному индикатору в пользовательском интерфейсе;
  - любой другой код в диапазоне от 2 до 255 включительно – внутренняя ошибка, которая не позволяет определить, доступна ли тестируемая функциональность.
    Соответствует желтому индикатору в пользовательском интерфейсе.

Параметры конфигурации скриптов

Параметр	Описание	Значение по умолчанию	Наличие параметра в скрипте
`timeout`	Максимальное время выполнения скрипта (в секундах). Допустимые значения: [0-60]	60	Опционально
`name`	Локализованное имя скрипта. Используется для отображения в пользовательском интерфейсе	-	Обязательно
`execution_interval`	Таймаут для возможности повторного запуска скрипта пользователем (в секундах). Допустимые значения: [0-60]	0	Опционально

Если в скрипте не указано значение опционального параметра, будет использовано значение по умолчанию.

Интерфейс скриптов

Все скрипты проверки имеют единый интерфейс:

```
user@host12:~/logon$ ./gui_checks/check-dc.sh --info
{
"timeout": 60,
"execution_interval": 60,
"name": "Доступность контроллера домена"
}

user@host12:~/logon$ ./gui_checks/check-dc.sh --check
...
```

При вызове с флагом `--info` скрипт должен передавать данные rtlogon (максимальное время выполнения, частоту возможности запуска, уникальный идентификатор, локализованное имя) в формате JSON.

При вызове с флагом `--check` скрипт вызывает проверку.

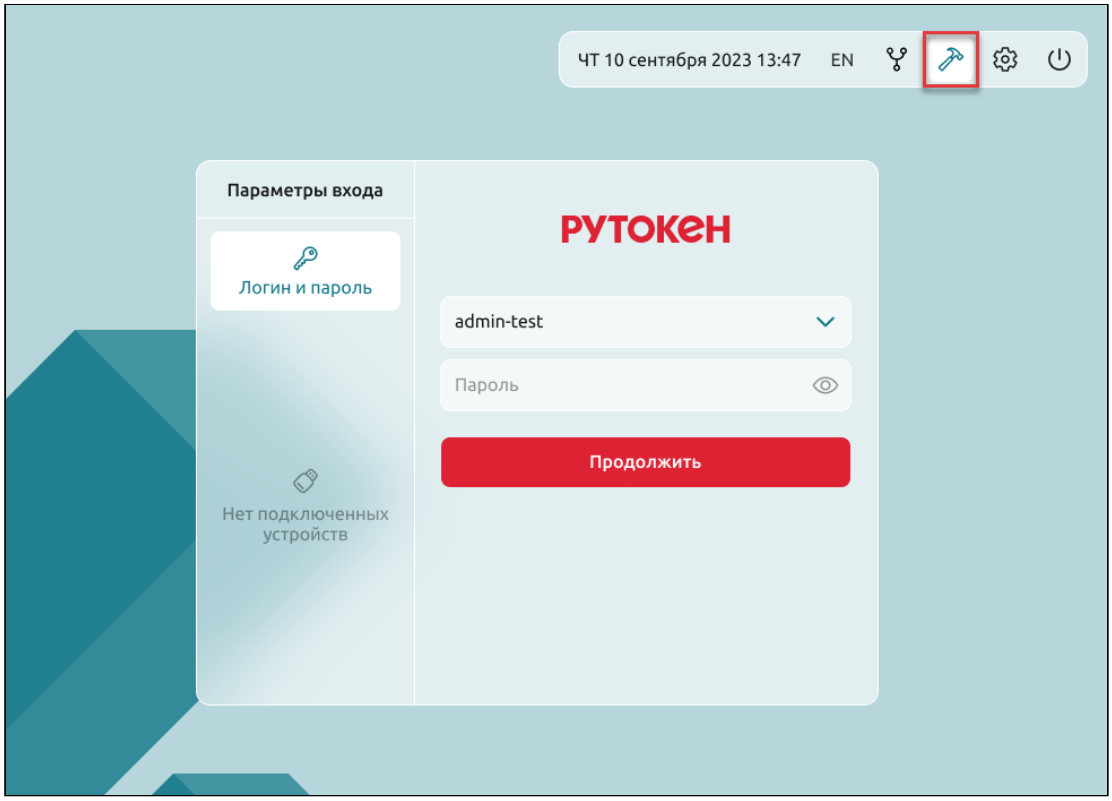
Примеры скриптов

rtlogon поставляется вместе с тремя скриптами проверок, которые при необходимости можно изменить, использовать как основу для создания новых скриптов или заменить на собственные:

- `check-dc.sh` – проверка доступности КД;
- `check-krb.sh` – проверка работоспособности КД.
  Скрипт вызывает команду `kinit`, которая запрашивает у службы KDC КД билет TGT (Ticket-Granting Ticket) и сохраняет его в кеше Kerberos. Успешное получение TGT подтверждает, что КД доступен и обрабатывает запросы аутентификации Kerberos;
- `check-crl.sh` – проверка статуса CRL.

Запуск скриптов пользователем

Скрипты проверок запускаются из меню инструментов диагностики с помощью значка , который находится на панели инструментов в правом верхнем углу экрана приветствия. При нажатии на этот значок отображается список доступных проверок.

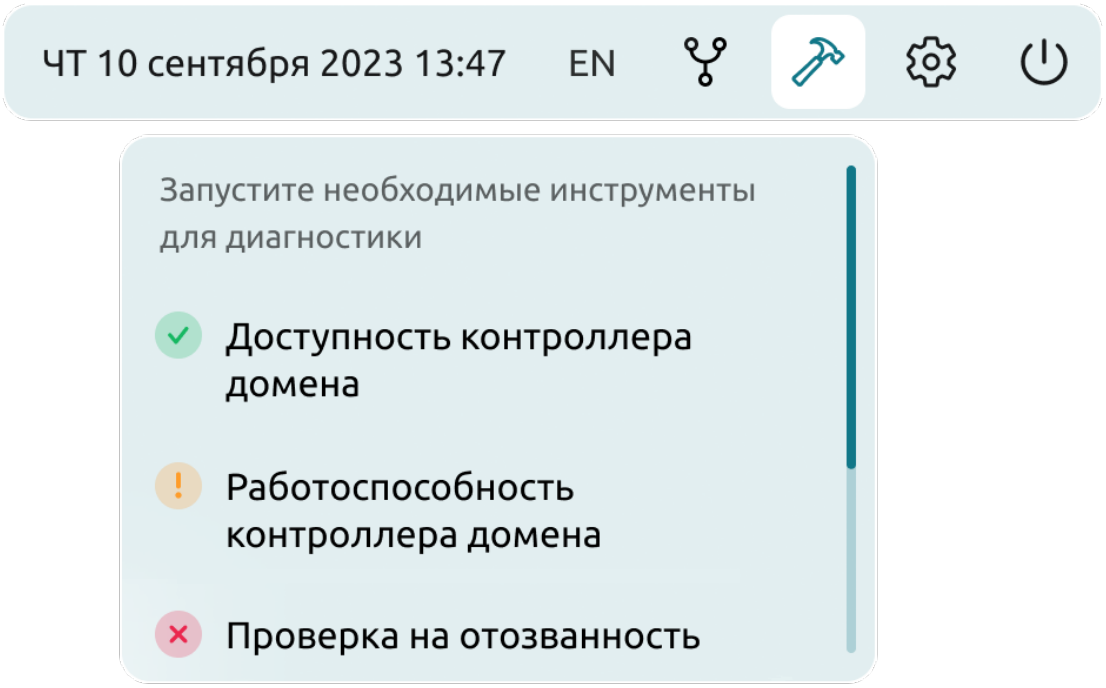


При нажатии на элемент списка происходит запуск соответствующего скрипта.

Результат работы скрипта отображается в виде цветного индикатора, соответствующего одному из значений:

- зеленый индикатор – проверка прошла, скрипт передал код возврата 0. Проверяемая функциональность доступна;
- красный индикатор – проверка не прошла, скрипт передал код возврата 1. Проверяемая функциональность недоступна;

- желтый индикатор – возникла внутренняя ошибка выполнения скрипта, скрипт передал код возврата, отличный от 0 или 1. Статус проверяемой функциональности определить не удалось.



Результаты проверок сохраняются и отображаются при следующем открытии раскрывающегося списка.

Если каталог */etc/rtlogon/gui_checks/* пустой или в нем нет скриптов, удовлетворяющих требованиям, вместо списка проверок отобразится сообщение «Инструменты для диагностики недоступны».

Логирование проверок

События проверок записываются в лог-файл в соответствии с процессом, описанным в разделе Логирование работы rtlogon.

Примеры записей результатов работы скриптов в лог-файле:

Return code 0

```
2025-08-22 15:08:46 fly-dm-greeter[1073]: INFO:"User check '" +
Domain controller connection status + "' started"

2025-08-22 15:08:46 fly-dm-greeter[1073]: INFO:"User check '" +
Domain controller connection status + "' succeded"
```

Return code 1

```
2025-08-22 15:08:46 fly-dm-greeter[1073]: INFO:"User check '" +
Domain controller connection status + "' started"
```

```
2025-08-22 15:08:46 fly-dm-greeter[1073]: INFO: User check '" +
Domain controller connection status + "' failed with code:1
```

Return code other than 0 and 1

```
2025-08-22 15:08:46 fly-dm-greeter[1073]: INFO:"User check '" +
Domain controller connection status + "' started"

2025-08-22 15:08:46 fly-dm-greeter[1073]: INFO: User check '" +
Domain controller connection status + "' failed with code:2
```

Scripts are missing

```
2025-08-22 15:08:46 fly-dm-greeter[1073]: INFO: Diagnostics tools are not
available
```

Смена PIN-кода токена

Чтобы сменить PIN-код токена:

1. Подключите токен к компьютеру.
2. Введите в терминале команду:

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

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

Token parameters

Параметр	Описание	Значение по умолчанию	Наличие параметра в команде	Условие применения

`--token-id arg`
или
`-t arg`
	Идентификатор токена, к которому применяется команда.
	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.).
	Для просмотра информации об идентификаторе токена необходимо вызвать команду rtlogon-cli info
		-	Опционально	Если к компьютеру подключено несколько токенов или один комбинированный токен

Пример:

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 экране блокировки

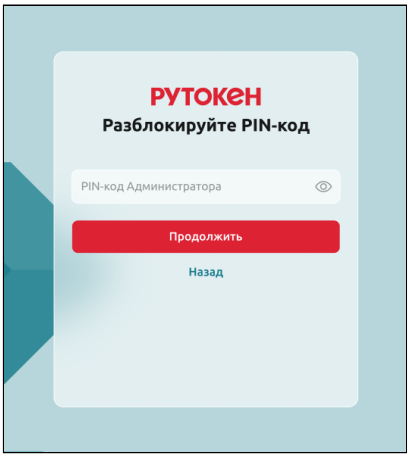
rtlogon поддерживает разблокировку PIN-кода токена на экране приветствия или экране блокировки только при выполнении следующих условий:

- используется GUI rtlogon;
- PIN-код токена может менять пользователь или администратор токена.

Разблокировка PIN-кода не поддерживается на ключевых носителях JaCarta ГОСТ. Чтобы разблокировать эти устройства, необходимо обратиться к их производителю.

Чтобы выполнить разблокировку:

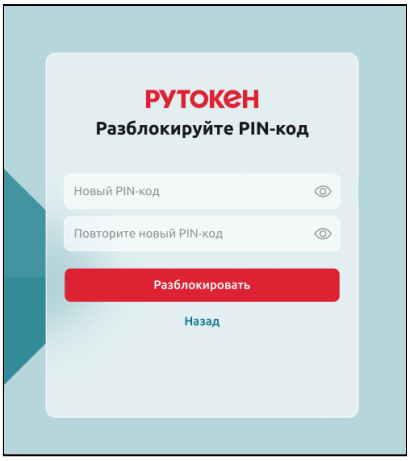
1. Введите PIN-код Администратора токена в поле **PIN-код Администратора**.
2. Нажмите **Продолжить**.



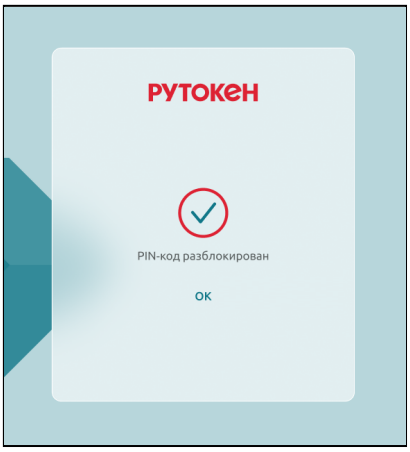
3. Введите новый PIN-код в поле **Новый PIN-код**.

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. Продублируйте новый PIN-код в поле **Повторите новый PIN-код**.
5. Нажмите **Разблокировать**.



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



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

Запрос информации о конфигурации rtlogon и параметрах локальной МФА

rtlogon поддерживает вывод в терминале данных о своей конфигурации и настроенной МФА.

Для получения данных:

1. Если необходимо вывести данные о МФА, хранящейся на токене, подключите токен к компьютеру.
2. Введите в терминале команду:

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

Command parameter

Параметр	Описание	Значение по умолчанию	Наличие параметра в команде	Условие применения

`-v`
или
`--verbose`
	Вывод расширенного набора данных	-	Опционально	Необходимо получить расширенный набор данных

Выводимые данные делятся на:

- стандартный набор;
- расширенный набор.

Стандартный набор данных содержит:

- информацию о библиотеках:
  - Rutoken pkcs11 (librtpkcs11ecp);
  - JaCarta pkcs11 (libjcPKCS11-2);
  - для работы с биометрией (FAPI, FSSM, BioLib).
- конфигурация rtlogon, включая адрес сервера лицензирования и тип используемой лицензии ;
- информацию об УЗ с настроенной локальной МФА;
- информацию о подключенных к компьютеру токенах.

Расширенный набор данных более подробно описывает стандартный набор.

Пример:

```
//Standard information
rtlogon-cli info
PKCS#11 libraries info:
Rutoken pkcs11 library:
Cryptoki interface version: 2.40
Cryptoki library version: 2.18
Manufacturer: Aktiv Co.
Library description: Rutoken ECP PKCS #11 library

JaCarta pkcs11 library:
Not found (valid library must be version no lower than 2.8).

Rutoken biometric libraries info:
Version: 1.0.0

Rtlogon configuration:
Host id: 934-469-671-765

Local users with configured rtlogon 2FA:
Record #0
User: bio-test
Token id: 1160607021
Object id: 86a583b9ef13c18b
Auth type: certificate
Login policy: certificate only auth

Tokens info:
Token #0 (id: 0986078429)
Record #0
User: kek
Host id: 992-600-966-077
Auth type: strong password
Disconnection type: lock

Record #1
User: kek
Domain: rtkn.test
Auth type: certificate
Disconnection type: lock
```

```
//Extended information
rtlogon-cli info -v

PKCS#11 libraries info:
Rutoken pkcs11 library:
Cryptoki interface version: 2.40
Cryptoki library version: 2.18
Manufacturer: Aktiv Co.
Library description: Rutoken ECP PKCS #11 library

JaCarta pkcs11 library:
Not found (valid library must be version no lower than 2.8).

Rutoken biometric libraries info:
Version: 1.0.0

Rtlogon configuration:
Host id: 934-469-671-765
System gui: false
Domain type: none
License server: 172.16.112.16
Additional license features: Biometric authentication

Local users with configured rtlogon 2FA:
Record #0
User: bio-test
Token id: 1160607021
Object id: 86a583b9ef13c18b
Auth type: certificate
Login policy: certificate only auth
User's certificate:
Validity starts: 2026-07-02 12:08:33
Validity ends: 2027-07-02 12:08:33
Subject: CN=Petrova C=BB O=Pulse ST=Lilovaja L=Saratov
Issuer: CN=Petrova C=BB O=Pulse ST=Lilovaja L=Saratov
Cert body:
-----BEGIN CERTIFICATE-----
MIIDGDCCAgICAQAwCwYJKoZIhvcNAQELMFQxEDAOBgNVBAMMB1BldHJvdmExCzAJ
BgNVBAYTAkJCMQ4wDAYDVQQKDAVQdWxzZTERMA8GA1UECAwITGlsb3ZhamExEDAO
BgNVBAcMB1NhcmF0b3YwHhcNMjYwNzAyMDkwODMzWhcNMjcwNzAyMDkwODMzWjBU
MRAwDgYDVQQDDAdQZXRyb3ZhMQswCQYDVQQGEwJCQjEOMAwGA1UECgwFUHVsc2Ux
ETAPBgNVBAgMCExpbG92YWphMRAwDgYDVQQHDAdTYXJhdG92MIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0DOxM8zQzdfd2RhtLbG5ij6zV0QtePC4VNbb
MMrozUDJiYEK2U3/+iPHZvGQeG/BApyTsuMXmkhZkIurTOzoc4ZS3or8LUqKyQvJ
YdCcnk4w8Qt1OUtcQt/rOHUfRz0iZecZfRRKtolg5wEflZMMO2JjC39VKa3GZscK
vNvTCQqUhXdYD9GUYV7pCyEQT5Hq1tvMbemfsmMVAELPrWBy87aEbUyheIXwAaoF
ZxG/p3BpUDVmebVXFGOIjDaRz1B4RFn1sXL4P/hwaPogUMMEgI2GhH75N1wyMFcT
nIiqKfiKtD5ccz/KKCgOFdyx0pe5ndR5jyScTDTRMGOPeOu7JwIDAQABMAsGCSqG
SIb3DQEBCwOCAQEAn1hatwHxepN9tNE2oWhMnkbbQLURalqwcR9+Q1gHiDXyDOl1
```

```
oZ9RsLLG1T7GI0mt4WvsJ8nAkywYpT33tV/DIRso6Q2VqADdAXXsaAn1yJv4b6k+
u+OmE4l3ltazErkiIDYpuF34SuRkEwhxsYGxxMLKRpBhbHvjSi1ULjjHDpVN61LD
UKKOsEdrNAvEdc1UomXsoPXXMwB7uLTkeYR2Ti26QrBeNZRd3DxF5JdF1i5timm5
/ezGGZeLT7/KEo0VQcNPZejkUir81cBP01wcR6IkSe8zVSExOZKf8H0g6DELznS6
WL+sZAOx1nDwfT+6M6N8gFcAobYmTO8uhkOK5Q==
-----END CERTIFICATE-----

Tokens info:
Token #0 (id: 0986078429)
Record #0
User: kek
Host id: 992-600-966-077
Auth type: strong password
Disconnection type: lock
Object id: 2a2abd17e6335dcc

Record #1
User: kek
Domain: rtkn.test
Auth type: certificate
Disconnection type: lock
User's certificate:
Label: e1c22ddcc13a0a70
Object id: e1c22ddcc13a0a70
Validity starts: 2025-07-01 15:47:47
Validity ends: 2027-07-02 15:47:47
Subject: O=RTKN.TEST CN=kek
Issuer: O=RTKN.TEST CN=Certificate Authority
Cert body:
-----BEGIN CERTIFICATE-----
MIIEezCCAuOgAwIBAgIDARmgMA0GCSqGSIb3DQEBCwUAMDQxEjAQBgNVBAoMCVJU
S04uVEVTVDEeMBwGA1UEAwwVQ2VydGlmaWNhdGUgQXV0aG9yaXR5MB4XDTI1MDcw
MTEyNDc0N1oXDTI3MDcwMjEyNDc0N1owIjESMBAGA1UECgwJUlRLTi5URVNUMQww
CgYDVQQDDANrZWswggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDQkxZF
OnaeuAaLOaOubxEMBzaqw+iAHG5Zw5wtIOcwG7rAscZmo4oVEkAhzbrRyzWkzHM7
4dytlQLoD5gwnH/hoB9PPuoi/s01khvnGZC5eIMB3GG7NtVMxuPK0fPQ5A0wbAbJ
HAwOYDyCn6j0KgcI1J+xOcZWNLjlEQcrcf5HVxeywu+758IzooJ8MMLVlckvc6xW
9DqIoNF8Rf1OY4VybVqVvpIjNouQN15dJDxlrYzfPM9caILNrRInMZrSZzH+BZ6V
ho2wD+02uGxqAQPILGZ0al39oLm8GtSoMnNqKQ4CRHIOmj8yY9NTNEAAVmIbFA5U
s2SXFc067raOVrb/AgMBAAGjggEmMIIBIjAfBgNVHSMEGDAWgBRqIkQC+S530N/K
rgppGxafi95YSDA7BggrBgEFBQcBAQQvMC0wKwYIKwYBBQUHMAGGH2h0dHA6Ly9p
cGEtY2EucnRrbi50ZXN0L2NhL29jc3AwDgYDVR0PAQH/BAQDAgTwMB0GA1UdJQQW
MBQGCCsGAQUFBwMBBggrBgEFBQcDAjB0BgNVHR8EbTBrMGmgMaAvhi1odHRwOi8v
aXBhLWNhLnJ0a24udGVzdC9pcGEvY3JsL01hc3RlckNSTC5iaW6iNKQyMDAxDjAM
BgNVBAoMBWlwYWNhMR4wHAYDVQQDDBVDZXJ0aWZpY2F0ZSBBdXRob3JpdHkwHQYD
VR0OBBYEFMveJEKuO5IQRYWg00BP7ZQNbh27MA0GCSqGSIb3DQEBCwUAA4IBgQC0
MTnhyu9E/010QvIMMm4sZn2Xx7LlbZjIj2XEoVUHYIBSYcdV5EfM4Ypzy3HFKnjO
UfLJjLbyhBHA5gGODfJexjTuh/EZ00xMkyHkRYZbn2MLlFZWQsTnHM6r0fuhP6/t
ZgBbgOXAQrQDb7ZJNZ39Q7nboFC6mc6rvTrFuSR56sZpTvkg57EQ02aMyZgTDZV2
2cp9QhSyU6UblK4DTQo5MU4RJ3wo2/gins/m4wrRmUe2NuYZwBG6Ud6gWt6gnE5o
```

```
LosVsXSfAlw7p8GphyelBH4UWIT+CkpCwk4nJElJCkk4hHaYFTZ1JL3QYuIhXFtR
PD9a0rr8jD3re1lF4EN1nFijxEl+K3C9KwEoIQhj7JYDSbr3FjEa+kU98yLJO3zY
3qjnvUnEM0pQoroq+5NgoWJu93bt2eN8DCFCrkZOjp2d/07EFTbv4NdoJy2FX21b
4FkYFu4P31JlCdE4iyetgsF51qtSXHLtYlAa10V4EwgVuGcT2AGcp2E+fywlyGc=
-----END CERTIFICATE-----
```

Логирование работы rtlogon

Запись сообщений о событиях rtlogon в лог-файлы выполняют следующие сервисы:

- rtlogon_log,
- syslog.

rtlogon_log

Сервис rtlogon_log записывает сообщения в лог-файл */var/log/ rtlogon.log*, который имеет следующие характеристики:

- максимальный размер файла — 5 Мб;
- количество файлов для обеспечения ротации — 5.

Ротацию данных обеспечивает внешняя утилита — **logrotate**.

В лог-файл записываются данные о следующих событиях безопасности:

- успешная/неуспешная аутентификация пользователя;
- перегенерация сложного пароля;
- изменение PIN-кода по умолчанию;
- события запуска скриптов проверок компьютера:
  - запуск и результат выполнения скрипта;
  - невозможность диагностики в связи с отсутствием скриптов проверок на компьютере;
  - невозможность использования скрипта в связи с тем, что он не удовлетворяет требованиям к скриптам.

Запись сообщений о событиях rtlogon в лог-файл включена по умолчанию.

Для доступа к лог-файлу необходимы права администратора.

syslog

rtlogon поддерживает запись сообщений в syslog. Запись выполняет PAM-модуль rtlogon — pam_rtlogon.

Установка и настройка сервиса syslog на компьютере пользователя выполняется администратором.

Для выгрузки сообщений syslog в SIEM-систему рекомендуется воспользоваться стандартным коннектором сообщений syslog.

Если в SIEM-системе отсутствует коннектор для syslog, можно выгрузить сообщения в файл и разработать собственный коннектор для приема сообщений из файла.

Пример настройки записи сообщений в формате JSON.

```
destination d_rtlogon_file {
file("xxx"
template("{\"@timestamp\": \"$ISODATE\", \"facility\": \"$FACILITY\",
\"priority\": \"$PRIORITY\", \"level\": \"$LEVEL\", \"host\": \"$HOST\",
\"program\": \"$PROGRAM\", \"message\": \"$MSG\"}\n"));
};
log {
source(s_src);
filter(xxx);
destination(d_rtlogon_file);
};
```

Экспорт конфигурационных файлов, лог-файлов и файла с параметрами локальной МФА

1. Введите в терминале команду:

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

2. При запросе введите пароль администратора.

Command parameter

Параметр	Описание	Значение по умолчанию	Наличие параметра в команде

`-o arg`
или
`--output arg`
	Путь к выгружаемому архиву (содержит имя архива).
	Имя выгружаемого архива определяет администратор.
	Доступные расширения архива:
	• tar.gz,
	• tar.bz2,
	• tar.xz,
	• zip
		-	Обязательно

Пример.

```
sudo rtlogon-cli collect-log -o test_log.tar.gz
```

Выгруженный архив содержит следующие файлы:

- *state_info.txt* – со следующей информацией:
  - параметры конфигурации rtlogon;
  - данные об установленных библиотеках:
    - PKCS#11;
    - для работы с биометрией.
  - записи о настроенной локальной МФА;
  - записи о МФА, хранящиеся на токене;
  - сведения о подключенных к компьютеру токенах;
  - описание публичных объектов на токенах (объекты данных, сертификаты, публичные ключи);
  - сведения о корневом сертификате и промежуточных сертификатах УЦ, составляющих цепочку доверия.
- *os_info.txt* – файл с информацией о ядре ОС;
- *installed_deb_packages.txt* или *installed_rpm_packages.txt* – файл с информацией об установленном пакете;
- *journalctl.log* – системный журнал, содержащий записи за последние 30 дней;
- лог-файлы:
  - */var/log/audit/audit.log* – журнал аудита системных событий;
  - */var/log/auth.log* или */var/log/secure* – лог-файл pam-модулей и pam-приложений;
  - */var/log/fly-dm.log* – лог-файл модуля fly-dm (для ОС Astra Linux);
  - */var/log/rtlogon.log* – лог-файл rtlogon;
  - */var/log/messages* – системный лог-файл;
  - */var/log/syslog* – системный лог-файл;
  - */var/log/lightdm* – лог-файл LightDM (для ОС РЕД ОС, ОС Альт);
  - */var/log/sssd/* – лог-файлы служб SSSD.
- */etc/rtlogon/rtlogon.conf* – конфигурационный файл rtlogon;
- */etc/rtlogon/localAuthDesc* – файл, содержащий данные об УЗ с настроенной локальной 2ФА;
- */etc/pki* – корневые сертификаты;
- 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/sssd/* – 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.

- CRL-файлы.

Приложение 1. Ошибки

Ошибки, выводимые в GUI

Ошибка на английском языке	Ошибка на русском языке
Administrator PIN-code is blocked	PIN-код Администратора заблокирован
An unknown error has occurred	Произошла неизвестная ошибка
Auth object on token and in local config mismatch	Способ аутентификации в системе, указанный на токене и на компьютере, не совпадают
Auth type on token and in local config mismatch	Тип аутентификации в системе, указанный на токене и на компьютере, не совпадают

Authentication failed. Contact the Administrator	Вход в систему недоступен. Обратитесь к администратору. Это общая выводимая на экран ошибка для следующих ошибок в лог-файлах: • на токене не найден закрытый ключ (no private key found on token); • проверка ключевой пары не пройдена (challenge request didn't pass); • на токене не найден сложный пароль (no strong password object found on token); • неподдерживаемый тип ключа (unsupported key type); • атрибут сертификата CKA_LABEL пуст или содержит неверное значение (certificate's CKA_LABEL attribute is empty or contains invalid characters); • метка токена пуста или содержит неверное значение (token label is empty or contains invalid characters); • ошибки pam_sss ([pam_sss errors]); • неизвестная ошибка pam_sss (an unknown pam sss error has occurred); • на токене обнаружено несколько закрытых ключей с одинаковым CKA_ID (multiple private keys with the same CKA_ID found on token); • на токене обнаружено несколько сложных паролей с одинаковым CKA_ID (multiple strong password objects with the same CKA_ID found on token); • неизвестный пользователь (user is unknown); • ошибка инициализации проверки EVP_Digest (EVP_DigestVerifyInit failed). Также общая ошибка может возникать в следующих случаях: • сертификат пользователя отозван; • целостность данных CRL-файла нарушена; • CRL-файл отсутствует по пути, указанному в настройках; • срок действия CRL-файла истек, и параметр soft_crl не включен в конфигурационный файл sssd.conf; • возникли ошибки в цепочке доверия CRL-файла;

Ошибка на английском языке	Ошибка на русском языке
	• сервер OCSP недоступен, и параметр soft_ocsp не включен в конфигурационный файл sssd.conf
Authentication took longer than expected and was terminated. Please try again	Аутентификация заняла больше времени, чем ожидалось. Пожалуйста, повторите попытку
Authentication with a token is required to access this account	Войти в данную учетную запись можно только при помощи токена
Bad login policy provided	Указана неверная политика входа в систему
Bad user name	Плохое имя пользователя
Biometric authentication failed	Ошибка входа по биометрии
Biometric authentication has not been unblocked	Вход по биометрии не разблокирован
Biometric authentication is blocked	Вход по биометрии заблокирован
Biometric authentication is unavailable	Аутентификация по биометрии недоступна
Can't login as admin	Не удалось войти под администратором
Can't open /etc/passwd	Не удалось открыть /etc/passwd
Can't set strong password for user in system	Не удалось установить сложный пароль для пользователя в системе
Can't unblock	Разблокировка для этой модели токена недоступна
Certificate is not yet valid	Сертификат еще не вступил в действие
Connect the fingerprint scanner and try again	Подключите сканер отпечатков и повторите попытку
Connection failed, please try again	Установить соединение не удалось. Повторите попытку
Couldn't change PIN-code	Не удалось сменить PIN-код
Couldn't parse the account records on the token	Не удалось считать УЗ на токене
Couldn't parse the local account records on the PC	Не удалось считать локальные УЗ на компьютере
Current user certificate has expired	Срок действия сертификата выбранного пользователя истек
Diagnostic tools aren't available	Инструменты для диагностики недоступны
error BIO_write	Ошибка записи биометрии
Fingerprint scan failed. Please try again	Не удалось считать отпечаток. Пожалуйста, повторите попытку
Fingerprint scan has timed out	Время ожидания отпечатка пальца истекло
Incorrect Administrator PIN-code	Неверный PIN-код Администратора

Ошибка на английском языке	Ошибка на русском языке
Incorrect Administrator PIN-code. Attempts left:	Неверный PIN-код Администратора. Осталось попыток:
Incorrect fingerprint. Attempts left:	Неверный отпечаток. Осталось попыток:
Incorrect login or password	Неверный логин или пароль
Incorrect PIN-code	Неверный PIN-код
Incorrect PIN-code. Attempts left: ...	Неверный PIN-код. Осталось попыток: ...
Login policy provided with non-cert auth type	Невозможно войти в УЗ по сложному паролю при политике 'вход только по сертификату'
Multiple certificates with the same CKA_ID found on token	На токене обнаружено несколько сертификатов с одинаковым CKA_ID
Multiple copies of the same domain account record detected. Make sure there are no duplicate domain account records on connected tokens	Обнаружено несколько копий одной и той же записи доменной УЗ. Убедитесь, что в подключенных токенах нет повторяющихся записей доменной УЗ
Mutually exclusive flags PAM_PRELIM_CHECK and PAM_UPDATE_AUTHTOK are set	Внутренняя ошибка PAM
Network change isn't available	Невозможно изменить сетевое соединение
Network control is restricted by OS policies	Управление сетевыми подключениями запрещено политиками ОС
Network manager isn't available	Утилита Network manager недоступна
New and old PIN-code are same	Новый и старый PIN-код совпадают
New PIN-code can't be empty	Поле для PIN-кода не заполнено
New PIN-code doesn't comply with PIN-code policy	Новый PIN-код не соответствует политике качества PIN-кодов
New PIN-code doesn't comply with PIN-code policy: PIN-code must contain at least ... characters	Новый PIN-код не соответствует политике качества PIN-кодов: PIN-код должен содержать не менее ... символов
New PIN-code has invalid length	Неверная длина нового PIN-кода
New PIN-code is default	Новый PIN-код совпадает с PIN-кодом по умолчанию
No accounts found on token	На токене не найдены УЗ
No certificate body found on token	Отсутствует сертификат на токене
No CKA_ID attribute	Отсутствует атрибут CKA_ID
No connected devices found	Нет подключенных устройств
No connections available	Нет доступных подключений
No matching certificate found on token	На токене не найден соответствующий сертификат
No PKCS libraries found. Authentication with a token isn't available	Нет библиотек PKCS. Аутентификация по токену недоступна
No PKCS libraries found. Connected devices won't be shown	Нет библиотек PKCS. Подключенные устройства не будут отображаться

Ошибка на английском языке	Ошибка на русском языке
No tokens found	Не найдены токены
Not logged in	Пользователь не авторизован
Operation took longer than expected and was terminated. Please try again	Операция заняла больше времени, чем ожидалось. Пожалуйста, повторите попытку
OTP field is empty	Поле для OTP не заполнено
Parallel sessions not supported	Не поддерживается несколько сессий
Passwords don't match	Пароли не совпадают
Password field doesn't filled	Поле для пароля не заполнено
PIN-code can only be changed by the Administrator	PIN-код может изменить только администратор
PIN-code change has been aborted	Смена PIN-кода была прервана
PIN-code change took longer than expected and was terminated. Please try again	Смена PIN-кода заняла больше времени, чем ожидалось. Пожалуйста, повторите попытку
PIN-code field doesn't filled	Поле для PIN-кода не заполнено
PIN-code has not been unblocked	PIN-код не разблокирован
PIN-code is blocked	PIN-код заблокирован
PIN-code is blocked. Contact the Administrator to unblock it	PIN-код заблокирован. Для разблокировки обратитесь к Администратору
PIN-code length must be between ... and ... characters	Длина PIN-кода должна находиться в пределах допустимого диапазона: от ... до ... включительно
PIN-code must contain at least one digit	PIN-код должен содержать хотя бы одну цифру
PIN-code must contain at least one lowercase letter	PIN-код должен содержать хотя бы одну строчную букву
PIN-code must contain at least one special character	PIN-код должен содержать хотя бы один специальный символ
PIN-code must contain at least one uppercase letter	PIN-код должен содержать хотя бы одну заглавную букву
PIN-code must not consist of only repeating characters	PIN-код не может состоять из повторяющегося символа
PIN-code must not match the default PIN-code	PIN-код не может совпадать с PIN-кодом по умолчанию
PIN-code must not match the previous PIN-code	PIN-код не может совпадать с предыдущим PIN-кодом
PIN-code on token was corrupted	PIN-код токена поврежден
PIN-code too weak	PIN-код слишком простой
PIN-codes don't match	Введенные PIN-коды не совпадают
Policy "Require PIN-code change" is set	Выставлена политика "Require PIN-code change"

Ошибка на английском языке	Ошибка на русском языке
PublicAuthDesc object is ambiguous. There is more than one instance of this object on token	На токене найдено несколько УЗ
Strong password is corrupted	Сложный пароль поврежден
Strong password regeneration failed	Сложный пароль не перегенерирован
Strong password regeneration took longer than expected and was terminated. Please try again	Перегенерация сложного пароля заняла больше времени, чем ожидалось. Пожалуйста, повторите попытку
The domain user's password has expired. Change your password	Срок действия пароля доменного пользователя истек. Измените пароль
This PIN-code has already been used	Этот PIN-код уже использовался (PIN-код содержится в истории PIN-кодов)
To unblock, please contact the administrator	Для разблокировки обратитесь к администратору
Token device error	Внутренняя ошибка токена
Token general error	Ошибка токена
Token has not been unblocked	Токен не разблокирован
Token not present	Токен отсутствует
Token not recognized	Токен не распознан
Token removed	Токен удален с компьютера
Too many sessions already open	Превышен лимит открытых сессий
Too many simultaneously logged users	Превышен лимит авторизованных пользователей
Unable to convert the specified crl	Не удается преобразовать указанный crl
Unknown auth type	Неизвестный тип аутентификации
X509 cert parse failure	Ошибка анализа сертификата X509

Ошибки, выводимые в терминале

Ошибка	Описание ошибки
Account(s) with two-factor authentication was(were) found:	Были найдены учетные записи с настроенной 2ФА
An unknown error has occurred	Произошла неизвестная ошибка
Application couldn't be configured. Join PC to a domain first	Не удалось сконфигурировать rtlogon. Добавьте компьютер в домен
Application has already been configured. To change the configuration, run the reconfigure command	ОС уже настроена для работы с МФА. Чтобы изменить настройки используйте команду `rtlogon-cli reconfigure`
Application hasn't been configured yet	ОС не была настроена для работы с МФА
Application hasn't been configured yet. Run the configure command first	ОС не была настроена для работы с МФА. Сначала выполните команду `rtlogon-cli configure`

Ошибка	Описание ошибки
Application isn't configured for domain operations	ОС не настроена для работы с доменной МФА
Application isn't configured for domain operations. Use the option --domain to specify the domain type	ОС не настроена для работы с доменной МФА. Используйте параметр `--domain`, чтобы задать тип домена
Application parameters have not been changed. Application was not reconfigured	Параметры rtlogon не изменились. ОС не была рекон-фигурирована для работы с МФА
Archive extension is required	Необходимо указать расширение для архива
At least one of the ... or ... options should be specified	Должен быть указан один из обязательных параметров
Bad auth type provided:	Указан неверный тип аутентификации
Biometric authentication failed	Проблема аутентификации по биометрии
Biometric authentication is blocked	Вход по биометрии заблокирован
Biometric authentication is unavailable	Аутентификация по биометрии недоступна
Biometric data on the token is missing. Contact the Administrator	Биометрические данные на токене отсутствуют. Обратитесь к администратору
CA certificates file corrupted. Try run: rtlogon-cli reconfigure	Файл сертификатов УЦ поврежден. Попробуйте выполнить команду `rtlogon-cli reconfigure`
Cannot get authselect profile	Не удается получить профиль authselect
Cannot get passwd info	Не удается получить информацию о пароле доступа
Can't change password for domain user	Не удается изменить пароль для доменного пользова-теля
Can't collect object information	Невозможно собрать информацию об объекте
Can't complete collection of token info	Не удается завершить сбор информации о токенах
Can't complete collection of OS info	Не удается завершить сбор информации об ОС
Can't complete collection of PKCS#11 libraries info	Не удается завершить сбор информации о библиотеках PKCS#11
Can't configure password expiration	Не удается задать срок истечения действия пароля
Can't convert DER to x509 structure	Не удается преобразовать DER в структуру x509
Can't create hash	Не удается вычислить хеш
Can't create new cipher context	Не удается создать новый контекст шифрования
Can't create temp dir to collect rtlogon logs	Не удается создать временную директорию для сбора лог-файлов rtlogon
Can't decrypt data	Не удается расшифровать данные
Can't determine domain name	Не удается определить имя домена при настройке аутентификации
Can't determine kdc hostname	Не удается определить имя КД при настройке аутен-тификации
Can't enable lightdm greeter	Не удается включить экран приветствия LightDM

Ошибка	Описание ошибки
Can't encrypt string	Не удается зашифровать строку
Can't find cipher	Не удается найти шифр (код)
Can't find rtlogon configuration file. Try run: rtlogon-cli configure	Не удается найти конфигурационный файл rtlogon. Попробуйте выполнить команду `rtlogon-cli configure`
Can't find p11_child	Не удается найти p11_child
Can't find pkinit plugin. Try to install 'krb5-pkinit' package	Не удается найти плагин pkinit. Попробуйте установить пакет " krb5 - pkinit "
Can't find record on token to auth user via smart-card	Не удается найти на токене запись для аутентификации пользователя по смарт-карте
Can't get decrypt result	Не удается получить результат расшифрования
Can't get encrypt result	Не удается получить результат шифрования
Can't get hash result	Не удается получить результат хеширования
Can't get info from inserted tokens	Не удается получить информацию от подключенных токенов
Can't get mem from BIO	Не удается получить сообщение из BIO
Can't get PEM from X509	Не удается получить PEM из X509
Can't get PEM from X509_REQ	Не удается получить PEM из X509_REQ
Can't get pubkey from EVP_PKEY	Не удается получить открытый ключ из EVP_PKEY
Can't get pubkey value	Не удается получить значение открытого ключа
Can't get rtengine	Не удается получить rtengine
Can't init decrypt context	Не удается инициализировать контекст расшифрования
Can't init encrypt context	Не удается инициализировать контекст шифрования
Can't init hash context	Не удается инициализировать хеш-контекст
Can't init openssl	Не удается инициализировать OpenSSL
Can't init rtengine	Не удается инициализировать rtengine
Can't load rtengine	Не удается загрузить rtengine
Can't open file to read:	Не удается открыть файл для чтения
Can't open file to write:	Не удается открыть файл для записи
Can't read certificate	Не удается прочитать сертификат
Can't restart sssd: You have to restart it manually. Or just restart your PC	Не удается перезапустить sssd. Необходимо перезапустить его вручную или перезагрузить компьютер
Can't retrieve env vars	Не удается получить переменные env

Ошибка	Описание ошибки
Can't use argument --passwd: authentication via strong password isn't available for root and users with access to sudo. Use authentication setup with arguments --cert and --login-policy certandpass	Невозможна аутентификация администратора по сложному паролю
Certificates must be in PEM format. Try run: rtlogon-cli reconfigure	Сертификаты должны быть в формате PEM. Попробуйте выполнить команду `rtlogon-cli reconfigure`
Configurator failed with error:	Настройка не выполнена. Возникла ошибка:
Configurator failed with unknown error	Настройка не выполнена. Возникла неизвестная ошибка
Connect the fingerprint scanner and try again	Подключите сканер отпечатков и повторите попытку
Could not find greeter plugin	Не удалось найти плагин экрана приветствия
Could not find greeter theme	Не удалось найти тему экрана приветствия
Couldn't change password	Не удалось сменить пароль
Couldn't configure the system: missing configuration utilities. Supported pam configuration utilities: pam-auth-update, authselect, control	Не удалось настроить систему: отсутствуют утилиты настройки. Поддерживаемые утилиты настройки pam: pam - auth - update, authselect, control
Couldn't create an rtlogon profile in authselect	Не удалось создать профиль rtlogon в authselect
Couldn't determine Alt version	Не удалось определить версию ОС Альт
Couldn't determine default profile	Не удалось определить профиль по умолчанию
Couldn't determine Redos version	Не удалось определить версию ОС РЕД ОС
Couldn't determine the ldap hostname	Не удалось определить имя хоста ldap
Couldn't enable the rtlogon profile in pam-auth-update	Не удалось включить профиль rtlogon в pam - auth - update
Couldn't find a password section with pam_tcb or pam_unix in pam configs	Не удалось найти раздел паролей с помощью pam_tcb или pam_unix в настройках pam
Couldn't find CA certificates in configuration files. Use the option --ca-cert to provide it manually	Не удалось найти в конфигурации rtlogon файл, содержащий корневой сертификат или сертификаты цепочки доверия УЦ. Добавьте его вручную, используя параметр `--ca-cert arg`
Couldn't find ldap tools. Try to install openldap utils (ldap-utils/openldap-client packages)	Не удалось найти инструменты ldap. Попробуйте установить утилиты openldap (ldap-utils/openldap-client packages)
Couldn't find the pam config with passwords	Не удалось найти конфигурацию pam с паролями
Couldn't find the user in the shadow file	Не удалось найти пользователя в теневом файле
Couldn't get domain administrator rights	Не удалось получить права администратора домена

Ошибка	Описание ошибки
Couldn't get the current authselect profile. You might need to set it up first using the 'authselect select <profile>' command	Не удалось получить текущий профиль authselect. Возможно, вам необходимо сперва настроить его с помощью команды `authselect select <profile>`
Couldn't get the current control system-auth profile	Не удалось получить текущий профиль контроля системы аутентфикации
Couldn't get the domain's defaultNamingContext	Не удалось получить имя домена по умолчанию
Couldn't get the user's distinguished name	Не удалось получить исключительное имя пользователя
Couldn't load biometric libraries	Не удалось загрузить библиотеки для работы с биометрией
Couldn't lock the shadow file	Не удалось заблокировать теневой файл
Couldn't mark the user's password as expired	Не удалось пометить пароль пользователя как просроченный
Couldn't modify the rtlogon profile in authselect. Error in	Не удалось изменить профиль rtlogon в authselect. Ошибка в ...
Couldn't open the shadow file for reading	Не удалось открыть теневой файл для чтения
Couldn't open the shadow file for writing	Не удалось открыть теневой файл для записи
Couldn't parse the account records on the token	Не удалось считать УЗ на токене
Couldn't parse the local account records on the PC:	Не удалось считать локальные УЗ на компьютере
Couldn't parse the local account records on the PC. Try run rtlogon-cli reconfigure	Не удалось считать локальные учетные записи на компьютере. Выполните команду `rtlogon-cli reconfigure`
Couldn't parse the rtlogon configuration file	Не удалось считать конфигурационный файл rtlogon
Couldn't read the shadow file	Не удалось прочитать теневой файл
Couldn't read the specified CA certificates	Не удалось прочитать сертификат коревого УЦ или цепочки доверия УЦ
Couldn't remove the rtlogon profile from pam-auth-update	Не удалось удалить профиль rtlogon из pam - auth - update
Couldn't restore the default authselect profile	Не удалось восстановить профиль authselect по умолчанию
Couldn't restore the old authselect profile:	Не удалось восстановить старый профиль authselect:
Couldn't restore the old control system-auth profile	Не удалось восстановить старый профиль контроля системы аутентификации
Couldn't revoke domain administrator rights	Не удалось отозвать права администратора домена
Couldn't select the rtlogon profile in authselect	Не удалось выбрать профиль rtlogon в authselect
Couldn't setup the control system-auth profile	Не удалось настроить профиль контроля системы аутентификации

Ошибка	Описание ошибки
Couldn't update the shadow file	Не удалось обновить теневой файл
Custom GUI isn't supported by the current operating system	Экраны приветствия и блокировки rtlogon не поддерживаются текущей ОС
Custom GUI isn't supported by the current operating system. Use the configure command with the flag `--use-system-gui yes`	Экраны приветствия и блокировки rtlogon не поддерживаются текущей ОС. Используйте в команде настройки ОС для работы с 2ФА параметр `--use-system-gui yes`
error BIO_write	Ошибка записи биометрии
error readPem	Ошибка чтения pem-файла
Failed while setting certificate duration	Произошел сбой при установке срока действия сертификата
Failed to create archive via tar	Не удалось создать tar-архив
Failed to create archive via zip	Не удалось создать zip-архив
Failed to generate a key pair	Не удалось сгенерировать ключевую пару
Failed to get Samba Workgroup	Не удалось получить рабочую группу Samba
Failed to open file:	Не удалось открыть файл:
Failed to read file:	Не удалось считать файл:
Failed to set the user's password	Не удалось установить пароль пользователя
Failed while assigning BIGNUM	Не удалось назначить BIGNUM
Failed while getting BIGNUM	Не удалось получить BIGNUM
Failed while getting RSA size	Не удалось получить размер ключа RSA
Failed while setting DN values	Не удалось задать значения DN
Failed while setting pubkey	Не удалось задать открытый ключ
Failed while signing certificate	Не удалось подписать сертификат
File not found at specified path:	Файл не найден по указанному пути:
Fingerprint scan failed	Не удалось считать отпечаток
Fingerprint scan has timed out	Время ожидания отпечатка пальца истекло
Found conflicting options: ... and ...	Конфликт параметров: ... и ...
Incorrect domain type	Неверный тип домена
Incorrect fingerprint	Неверный отпечаток
Incorrect file provided: ... is a certificate request. Please provide a valid certificate	Указан неверный файл. ... – запрос на сертификат. Укажите действительный сертификат
Incorrect PIN-code	Неверный PIN-код
Incorrect PIN-code. Attempts left: ...	Неверный PIN-код. Осталось попыток: ...
INI file parse error:	Ошибка анализа файла INI:
Invalid --alg argument:	Неверный аргумент у параметра `--alg`:

Ошибка	Описание ошибки
Invalid --disconnect-policy argument:	Неверный аргумент у параметра `--disconnect-policy`:
Invalid --dn argument:	Неверный аргумент у параметра `--dn`:
Invalid --login-policy argument:	Неверный аргумент у параметра `--login-policy`
Invalid path to CA certificates	Неверный путь к файлу сертификата УЦ (сертификатам цепочки доверия УЦ)
Invalid value of ... param: ...	Неверное значение параметра:
Login policy \"certonly\" isn't available for root and users with access to sudo. Use authentication setup with argument --login-policy certandpass	Невозможна аутентификация администратора только по сертификату
More than one token inserted. Option --token-id should be specified. Select one of these token IDs:	К компьютеру подключено несколько токенов. Необходимо задать значение параметру `--token-id`
Multiple certificates with the same CKA_ID found on token	На токене обнаружено несколько сертификатов с одинаковым CKA_ID
New PIN-code doesn't comply with PIN-code policy	Новый PIN-код не соответствует политике качества PIN-кодов
New PIN-code doesn't comply with PIN-code policy: PIN-code must contain at least ... characters	Новый PIN-код не соответствует политике качества PIN-кодов: PIN-код должен содержать не менее ... символов
New PIN-code has invalid length	Неверная длина нового PIN-кода
No biometric libraries found	Нет библиотек для работы с биометрией
No filename was provided for option --output	Не указан файл для параметра `--output`
No 'lightdm' package found. Try configure with the flag --use-system-gui	Не настроен пользовательский экран приветствия. Пакет "lightdm" не найден. Попробуйте настроить экран приветствия с помощью параметра `--use-system-gui yes`
No login policy provided	Не предоставлены политики входа
No matching certificate found on token	На токене не найден соответствующий сертификат
No tokens found	Не найдены токены
Not enough memory on token to complete this operation	На токене недостаточно памяти для выполнения этой операции
Not found (valid library must be version no lower than).	Библиотека не найдена
Operation was canceled	Отключение настроек ОС для работы 2ФА было прервано. Администратор не подтвердил продолжение выполнения команды `rtlogon-cli unconfigure`
Option ... can only be set for local users with authentication via a strong password	Параметр ... может быть задан только для локального пользователя с настроенной 2ФА по сложному паролю

Ошибка	Описание ошибки
Option --dn ... should be specified	При вызове команды `rtlogon-cli create-cert` не был указан параметр `dn`
Option --output should be specified	Должен быть указан параметр `--output`
Option ... should be specified	Пропущен обязательный параметр
PIN-code can only be changed by the Administrator	PIN-код может изменить только администратор
PIN-codes don't match	Введенные PIN-коды не совпадают
PIN-code length must be between ... and ... characters	Длина PIN-кода должна находиться в пределах допустимого диапазона: от ... до ... включительно
PIN-code must contain at least one digit	PIN-код должен содержать хотя бы одну цифру
PIN-code must contain at least one lowercase letter	PIN-код должен содержать хотя бы одну строчную букву
PIN-code must contain at least one special character	PIN-код должен содержать хотя бы один специальный символ
PIN-code must contain at least one uppercase letter	PIN-код должен содержать хотя бы одну заглавную букву
PIN-code must not consist of only repeating characters	PIN-код не может состоять из повторяющегося символа
PIN-code must not match the default PIN-code	PIN-код не может совпадать с PIN-кодом по умолчанию
PIN-code must not match the previous PIN-code	PIN-код не может совпадать с предыдущим PIN-кодом
PIN-code not initialized	PIN-код не инициализирован
PIN-code too weak	PIN-код слишком простой
Policy "Require PIN-code change" is set	Выставлена политика "Require PIN-code change"
Policy "Require PIN-code change" is set. Run: rtlogon-cli change-pin	Выставлена политика "Require PIN-code change". Выполните команду: `rtlogon-cli change-pin`
Read error	Ошибка чтения
Record for user: "..." already exists	Запись для пользователя уже существует
Record not found for user:	Не найдена запись пользователя
Record on token not found for user:	На токене не найдена запись о пользователе:
run as root	Запуск от имени root (администратора)
Shell command failed	Не выполнена команда оболочки
Shell command failed with error:...	Команда оболочки завершилась ошибкой:...
The --days option can only be set with the --self-signed option	Параметр `--days` может быть установлен только с совместно с параметром `--self-signed`
The license validation failed with error: ...	Проверка лицензии завершилась ошибкой: ...
The operation can't be executed. Fix the rtlogon configuration file	Операция не может быть выполнена. Исправьте конфигурационный файл rtlogon

Ошибка	Описание ошибки
The option can only be set for records with the 'cert' auth type	Параметр может быть установлен только для 2ФА по сертификату
The package does not match the environment	Пакет не соответствует окружающей среде
The passwd command failed	Не удалось выполнить команду passwd
The required argument CN for option --dn is missing	При вызове команды `rtlogon-cli create-cert` не был указан аргумент параметра `dn --CN`
The required argument for option ... is missing	Не указан аргумент у параметра...
The token doesn't support biometric authentication	Токен не поддерживает аутентификацию по биометрии
This PIN-code has already been used	Этот PIN-код уже использовался (PIN-код содержится в истории PIN-кодов)
Token doesn't support gost256	Токен не поддерживает криптоалгоритм ГОСТ с длиной ключа 256 байт
Token doesn't support gost512	Токен не поддерживает криптоалгоритм ГОСТ с длиной ключа 512 байт
Token doesn't support RSA	Токен не поддерживает криптоалгоритм RSA
Token is write protected	Токен недоступен для записи
Token with provided token ID was not found	Токен с заданным идентификатором не найден
Too many failed attempts in a row	Слишком много неудачных попыток подряд
Unable to change owner of:	Не удается сменить владельца
Unable to convert Subject to DER	Не удается конвертировать субъект в формат DER
Unable to convert the specified certificate	Не удается конвертировать указанный сертификат
Unable to convert x509 object to DER	Не удается конвертировать объект x509 в формат DER
Unable to get length of asn1 object	Не удается получить длину объекта asn1
Unable to get length of Subject	Не удается получить длину субъекта
Unable to get length of x509 object	Не удается получить длину объекта x509
Unable to stringify asn1 object	Не удается структурировать объект asn1
Unknown control system-auth profile: ...	Неизвестный профиль контроля системы аутентификации
Unknown domain type	Неизвестный тип домена
Unknown option(s)	Неизвестный параметр(ы)
Unknown user type (domain or local) for:	Неизвестный тип пользователя (доменный или локальный)
Unsupported archive extension. Check if the appropriate compression utilities are installed. Supported extensions: ...	Неподдерживаемый тип архива
Unsupported command	Неподдерживаемая команда

Ошибка	Описание ошибки
Unsupported operating system:	Неподдерживаемая ОС Astra Linux
User has expired account	У пользователя истек срок действия УЗ
User not found on host	Пользователь не найден на компьютере
Value for argument --days must be between 1 and 5500, inclusive	Время действия сертификата должно быть в диапазоне от 1 до 5500 дней включительно
Wrong expire value	Неверное значение срока действия
X509_cmp_current_time	Текущее время X509_cmp
X509_cmp_current_time failed	Неверное текущее время X509_cmp
X509 cert parse failure	Ошибка анализа сертификата X509
You can't run lock screen using sudo	Вы не можете запустить экран блокировки с помощью sudo