РУТОКЕН

Рутокен Логон для Linux. Версия 1.0.5. Руководство пользователя

Общая информация

Настоящее руководство описывает взаимодействие с программой **Рутокен Логон для Linux** (далее по тексту — **Рутокен Логон**):

- вход и выход из учетной записи, для которой настроена аутентификация с помощью Рутокен Логона;
- изменение PIN-кода токена;
- просмотр настроек Рутокен Логона;
- настройка графического интерфейса системы.

Термины, определения и аббревиатуры

ОС — операционная система.

ПК — персональный компьютер.

УЗ — учетная запись.

Локальная/доменная запись на токене — информация об УЗ, хранящаяся на токене. Настраивается при помощи Рутокен Логона.

Двухфакторная аутентификация (2ФА) — тип аутентификации, для которой требуется предъявить два фактора. В Рутокен Логоне в качестве этих факторов используются фактор владения (USB-токен или смарт-карта) и фактор знания (PIN-код от устройства).

Однофакторная аутентификация (1ФА) — тип аутентификации, для которой требуется предъявить один фактор. В Рутокен Логоне в качестве этого фактора используется пароль от УЗ, заданный в ОС для выбранной УЗ.

Сложный пароль — пароль, хранящийся на токене. Используется для 2ФА.

Ключевая пара — набор из открытого и закрытого ключей электронной подписи, однозначно привязанных друг к другу. Используется для 2ФА пользователя при входе в ОС.

Сертификат — электронный документ, который подтверждает связь электронной подписи с ее владельцем.

Среда рабочего стола — набор компонентов, использующих общий графический интерфейс, с помощью которых происходит взаимодействие с ОС.

Права суперпользователя (root-права) — права на неограниченное управление системой. Для выполнения команд с правами суперпользователя необходим специальный пароль, который устанавливает администратор системы при настройке ОС.

OTP (One Time Password) — одноразовый пароль, который используется для усиления аутентификации по паролю.

PIN-код токена — набор символов, который используется для входа в ОС с использованием 2ФА.

PIN-код Администратора — набор символов, который используется для администрирования токена. В Рутокен Логоне PIN-код Администратора понадобится для разблокировки PIN-кода токена, если он был заблокирован после нескольких неудачных попыток входа.

О программе

Рутокен Логон — программное решение для настройки двухфакторной аутентификации (2ФА) в Linux. В качестве первого фактора используется подключенный к ПК токен, настроенный администратором, в качестве второго — хранящийся на токене объект, для доступа к которому необходимо ввести верный PIN-код токена.

Таким объектом может быть:

- ключевая пара;
- сложный пароль.

Тип объекта выбирает администратор при настройке 2ФА.

Условия применения

Поддерживаемые устройства

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

Поддерживаемые программные аутентификаторы

Яндекс ID.

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.
- ОС Альт 8 СП, релиз 10;
- ОС Альт 8.4 СП;
- ОС Альт 10 и новее;
- ОС Альт 11 и новее;
- РЕД ОС 7.3;
- РЕД ОС 8;
- РОСА Хром 12.4.

Вход в систему

Для каждой УЗ может быть настроен один из следующих способов входа:

- по токену — для входа нужно подключить токен и ввести его PIN-код;
- по паролю — для входа используется пароль, заданный в ОС для выбранной УЗ;
- по паролю и OTP — для входа используется пароль, заданный в ОС для выбранной УЗ, и одноразовый пароль (OTP), который генерируется на устройстве Рутокен OTP или в приложении Яндекс ID. Этот способ входа может быть настроен только для доменных пользователей.

> Политику входа в ОС настраивает администратор.

Также в процессе установки Рутокен Логона администратор выбирает, какой интерфейс будет использоваться для входа — системный или интерфейс Рутокен Логона. В зависимости от этого инструкции будут различаться.

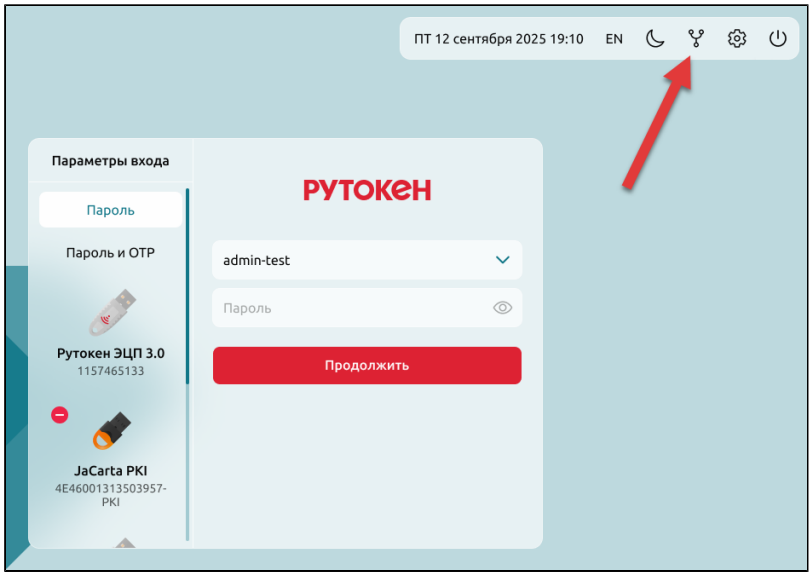
Выбор сети

В этом разделе описывается выбор сети в интерфейсе Рутокен Логона.
Расположение и внешний вид меню выбора сети в системном интерфейсе зависят от настроек графического интерфейса ОС.

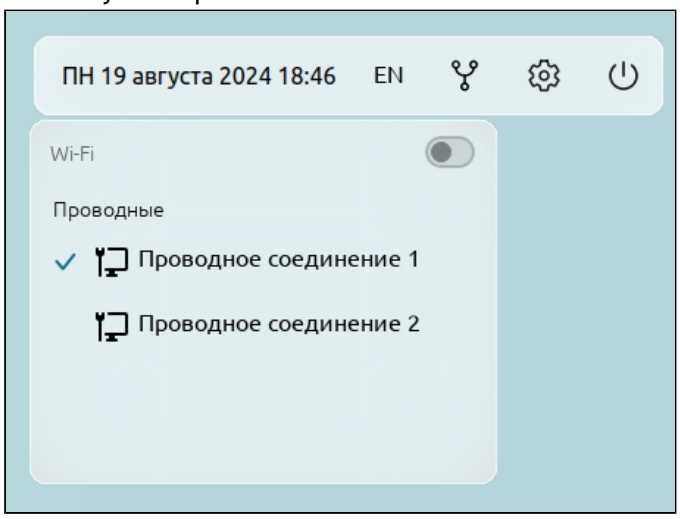
Подключение к сети необходимо для аутентификации в доменную УЗ.

Перед тем, как войти в доменную УЗ, нужно подключиться к сети. Для этого:

1. На панели инструментов нажмите  .



2. В раскрывающемся списке выберите сеть. Если нужно подключиться к беспроводной сети, используйте переключатель **Wi-Fi**.

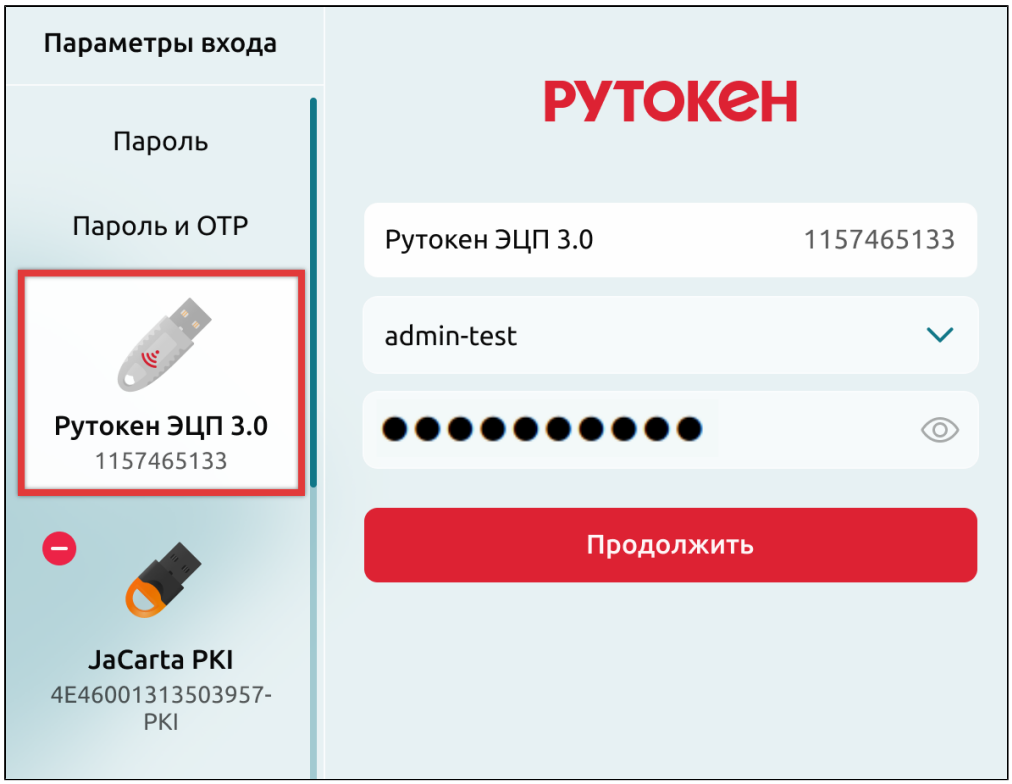


Аутентификация по токену

Через интерфейс Рутокен Логона

Перед началом работы получите от администратора токен, подготовленный для работы с УЗ.

1. Подключите токен к ПК.
2. В списке **Параметры входа** выберите подключенный токен.



3. В раскрывающемся списке **Логин** выберите логин УЗ.
4. Введите PIN-код.
5. Нажмите **Продолжить**.
   Если используется устройство Рутокен ЭЦП 3.0 Touch, прикоснитесь к токену, когда индикатор на нем начнет мигать.

Если все шаги выполнены успешно, произойдет вход в ОС.

Ошибки входа

> ⚠ Для устранения этих ошибок могут понадобиться PIN-код Администратора токена или права суперпользователя. Если у вас их нет, обратитесь за помощью к администратору.

Ошибка	Ситуация	Причина	Варианты решения
Нет библиотек PKCS. Подключенные устройства не будут отображаться	На экране входа в систему не отображается нужный токен	Не установлены необходимые библиотеки	Обратитесь к администратору для установки недостающих библиотек: ■ *librtpkcs11ecp.so* версии 2.14.1 и новее – для устройств Рутокен; ■ *libjcPKCS11-2.so* версии 2.8.0 и новее – для устройств JaCarta. Установка библиотеки *libjcPKCS11-2.so* описана в руководстве администратора. Библиотека *librtpkcs11ecp.so* устанавливается в составе библиотеки PKSC #11
Неверный PIN-код. PIN-код заблокирован	После ввода PIN-кода для аутентификации	Превышен лимит неудачных попыток ввода PIN-кода в Рутокен Логоне или другом сервисе	Если известен PIN-код Администратора токена: 1. Отключите токен от ПК и подключите снова. 2. Нажмите **Разблокировать**. 3. Введите PIN-код Администратора. 4. Укажите новый PIN-код токена
Вход в систему недоступен: PIN-код заблокирован	После выбора токена в списке устройств		Если PIN-код Администратора токена заблокирован, обратитесь к администратору для форматирования устройства и повторной настройки 2ФА
На токене нет сертификата для данного пользователя	После попытки аутентификации	Сертификат, для которого в ОС настроена 2ФА, и сертификат, который записан на токен, не совпадают	1. Убедитесь, что для входа используется тот же токен, который использовался для настройки 2ФА.

Ошибка	Ситуация	Причина	Варианты решения
Срок действия сертификата выбранного пользователя истек	После выбора УЗ на токене	Истек срок действия сертификата, для которого настроена 2ФА	2. Если токен верный, обратитесь к администратору для повторной настройки 2ФА
Нет учетных записей	После выбора токена в списке устройств	На токене нет УЗ, для которых настроена 2ФА	
Сертификат еще не вступил в действие	После выбора УЗ на токене	Дата начала действия сертификата еще не наступила	Убедитесь, что на ПК установлены верные дата и время
Перегенерация сложного пароля заняла больше времени, чем ожидалось	После ввода данных УЗ или PIN-кода токена	После того, как истек срок действия сложного пароля на токене, генерация нового пароля заняла слишком много времени	Попробуйте войти в УЗ еще раз. Если операция снова займет слишком много времени, обратитесь к администратору
Сложный пароль не перегенерирован		После того, как истек срок действия сложного пароля на токене, не получилось сгенерировать новый пароль	
Аутентификация заняла больше времени, чем ожидалось		Проверка данных УЗ заняла слишком много времени. Это могло произойти из-за программного сбоя или неисправности токена	

Предупреждения

⚠ Предупреждения не препятствуют входу в систему, но могут перерасти в ошибку, если не устранить причину.

Предупреждение	Ситуация	Причина	Варианты решения
Срок действия сертификата выбранного пользователя истекает	После ввода данных УЗ или PIN-кода токена	Срок действия сертификата скоро подойдет к концу, после этого его невозможно будет использовать для входа в УЗ	Обратитесь к администратору для выпуска нового сертификата и повторной настройки 2ФА

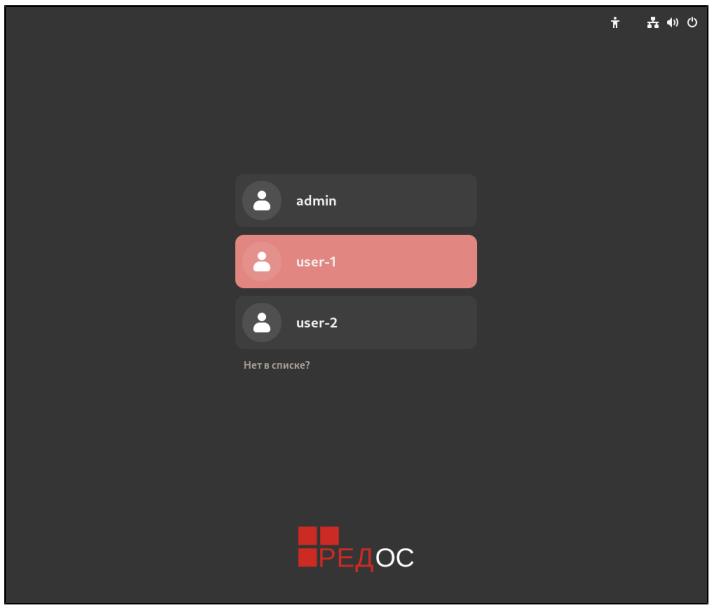
Через системный интерфейс

> В инструкциях ниже приведены скриншоты интерфейсов по умолчанию. В зависимости от настроек графического интерфейса ОС, внешний вид экрана входа и расположение элементов интерфейса на нем могут отличаться.

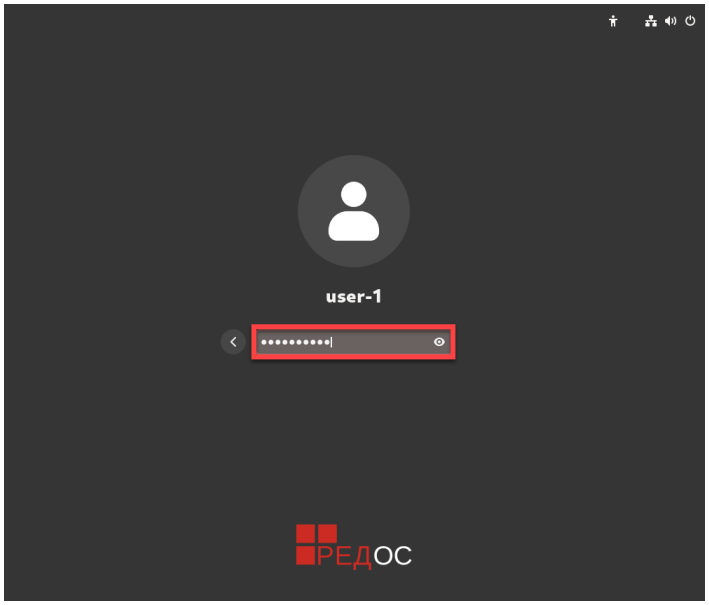
> Перед началом работы получите от администратора токен, подготовленный для работы с УЗ.

В РЕД ОС

1. Подключите токен к ПК.
2. Выберите УЗ.



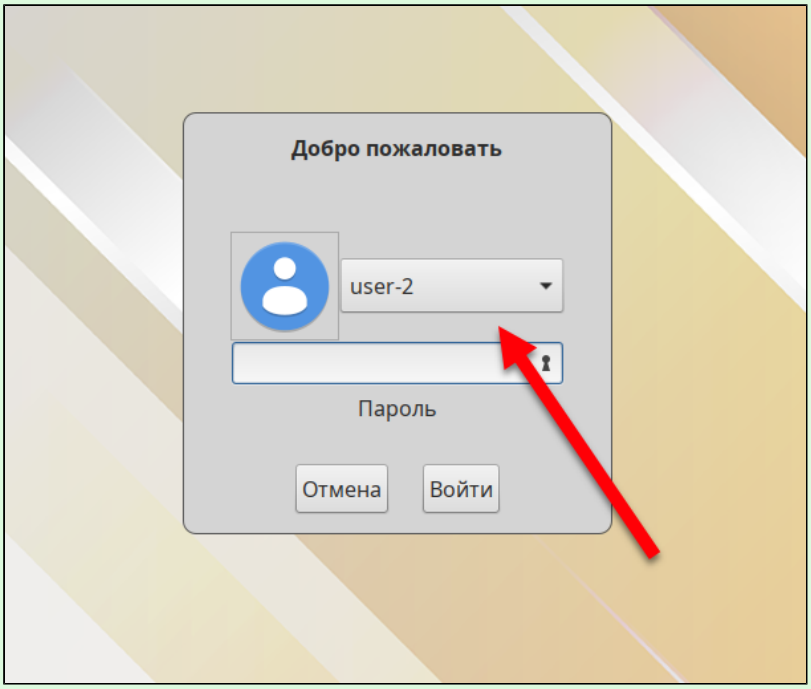
3. В поле **PIN-code** введите PIN-код токена.



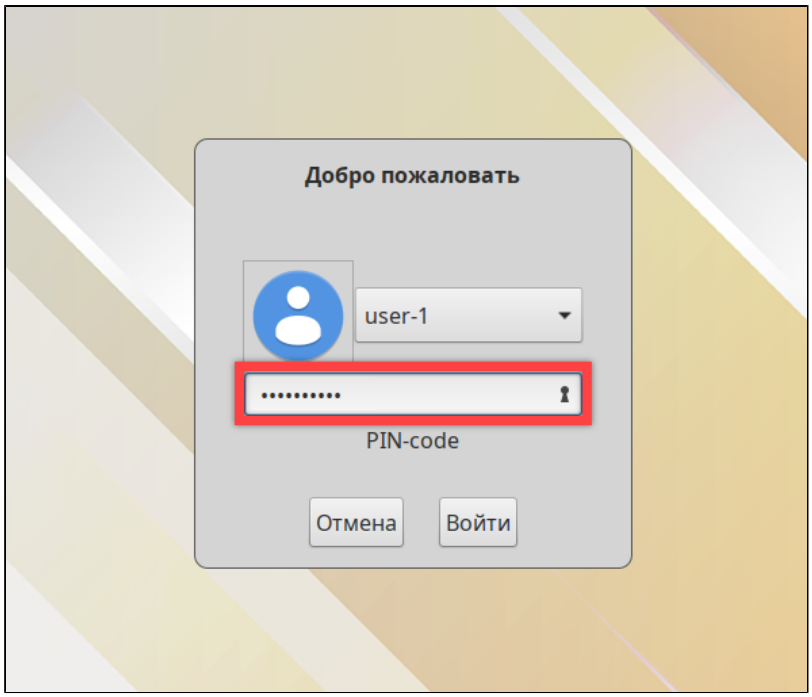
4. Нажмите **Enter**. Если используется устройство Рутокен ЭЦП 3.0 Touch, прикоснитесь к токену, когда индикатор на нем начнет мигать.
   Если логин и PIN-код указаны верно, произойдет вход в ОС.

В ОС Альт

Если на ПК настроено несколько УЗ, чтобы переключиться между ними, нажмите на логин УЗ, которая выбрана на экране входа в систему, и в раскрывающемся списке выберите другую УЗ.



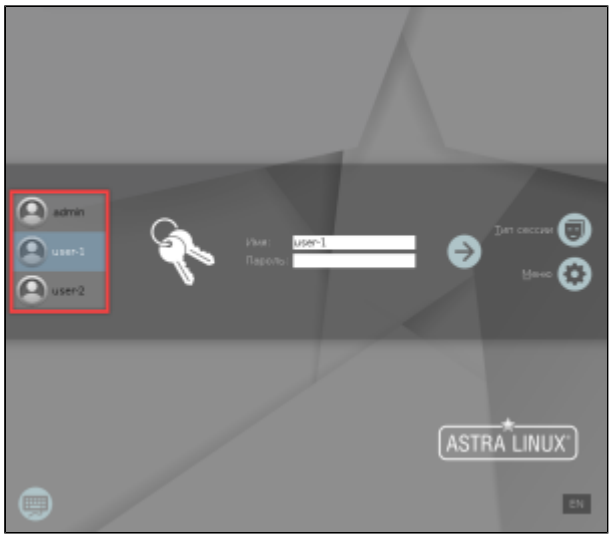
1. Подключите токен к ПК.
2. В поле **PIN-code** введите PIN-код токена.



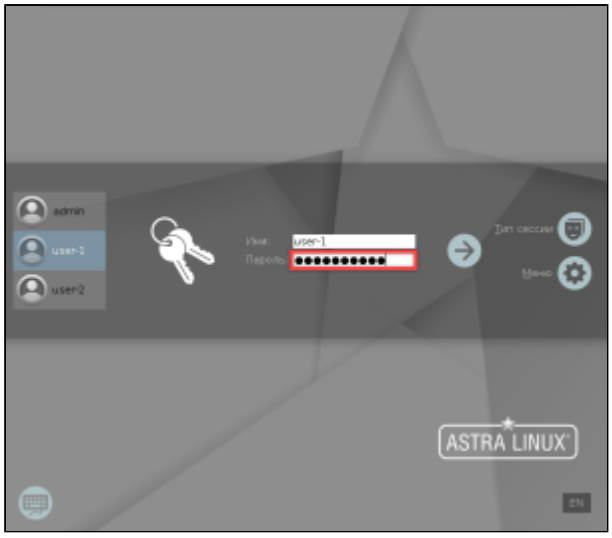
3. Нажмите **Войти**. Если используется устройство Рутокен ЭЦП 3.0 Touch, прикоснитесь к токену, когда индикатор на нем начнет мигать.
   Если логин и PIN-код указаны верно, произойдет вход в ОС.

В Astra Linux

1. Подключите токен к ПК.
2. В списке слева выберите УЗ.



3. В поле **Пароль** введите PIN-код токена.



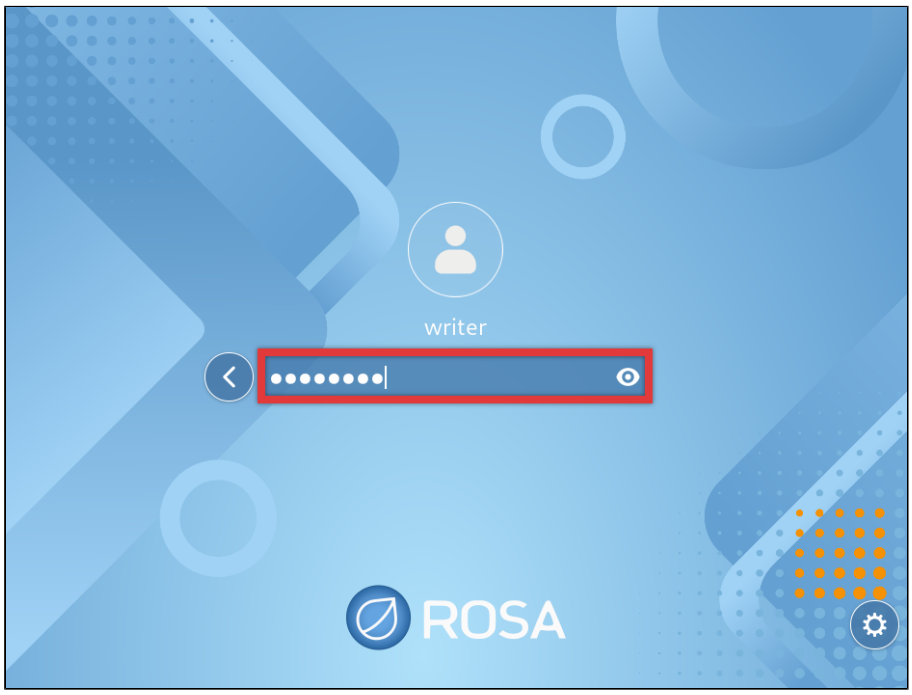
4. Нажмите **Enter**.

> ⚠ Если используется устройство Рутокен ЭЦП 3.0 Touch, прикоснитесь к токену после того, как индикатор на нем начнет часто мигать.
> Если токен слишком долго не получит подтверждение входа, процесс входа прервется и его нужно будет начать заново.

Если логин и PIN-код указаны верно, произойдет вход в ОС.

В ОС РОСА

1. Подключите токен к ПК.
2. Выберите УЗ.
3. В поле **PIN-code** введите PIN-код токена.

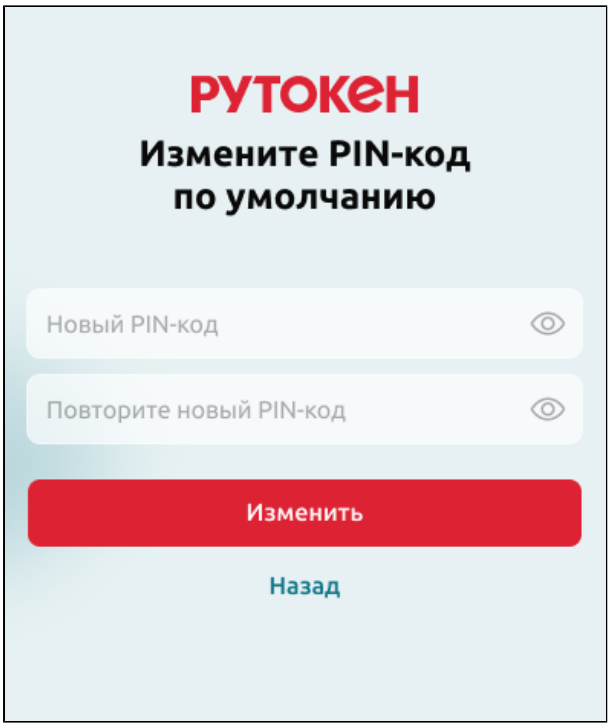


4. Нажмите **Enter**. Если используется устройство Рутокен ЭЦП 3.0 Touch, прикоснитесь к токену, когда индикатор на нем начнет мигать.
   Если логин и PIN-код указаны верно, произойдет вход в ОС.

Смена PIN-кода по умолчанию

Если для 2ФА используется токен, на котором установлен PIN-код по умолчанию, Рутокен Логон попросит его изменить.

Чтобы сделать это, дважды введите новый PIN-код в открывшемся окне и нажмите **Изменить**.



Ошибки смены PIN-кода

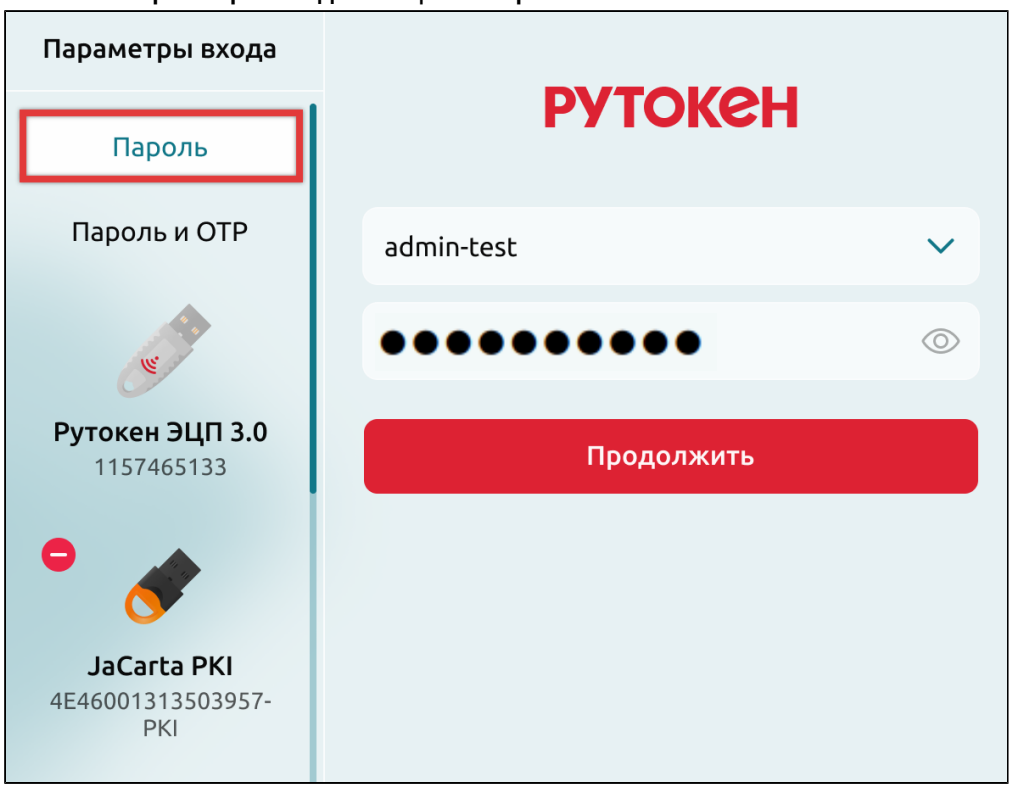
Ошибка	Причина	Варианты решения
Не удалось сменить PIN-код	На токене установлена политика смены PIN-кода, при которой изменить его может только администратор	Для устранения этой ошибки понадобятся права суперпользователя или PIN-код Администратора. Если у вас нет таких прав, обратитесь к администратору. - Отформатируйте ключевой носитель, чтобы изменить политику смены PIN-кода, и заново настройте 2ФА. - Измените PIN-код с помощью PIN-кода Администратора
Новый PIN-код не соответствует политике PIN-кодов	Выбранный PIN-код не соответствует политикам качества, заданным для этого токена	Выберите другой PIN-код

Ошибка	Причина	Варианты решения
Новый и старый PIN-код совпадают	Рутокен Логон не позволяет задать PIN-код, который совпадает с PIN-кодом по умолчанию	Не используйте PIN-код по умолчанию
Ошибка актуальна для устройств линейки **Рутокен ЭЦП 3.0**. Этот PIN-код уже использовался	Аппаратные политики качества для этого токена не позволяют выбрать использованный ранее PIN-код. В зависимости от настроек политик качества, в истории сохраняется до 10 последних PIN-кодов	Выберите другой PIN-код. Он должен отличаться от PIN-кодов, которые задавались для этого токена ранее, и от PIN-кода по умолчанию
Смена PIN-кода заняла больше времени, чем ожидалось. Пожалуйста, повторите попытку	Смена PIN-кода заняла слишком много времени. Это могло произойти из-за программного сбоя или неисправности токена	Попробуйте сменить PIN-код еще раз. Если смена PIN-кода снова займет слишком много времени, обратитесь к администратору

Аутентификация по паролю

Через интерфейс Рутокен Логона

1. В списке **Параметры входа** выберите **Пароль**.



2. В раскрывающемся списке **Логин** выберите УЗ.

> Если УЗ не отображается в раскрывающемся списке для выбора логина, для нее настроен вход только с помощью 2ФА.

3. Введите пароль, заданный в ОС для выбранной УЗ.
4. Нажмите **Продолжить**.

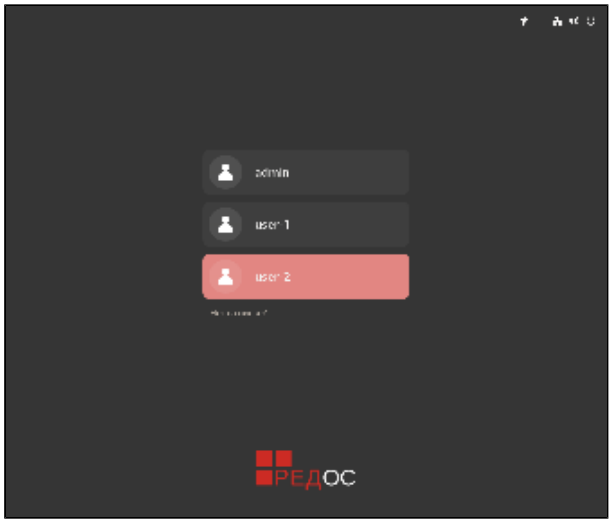
Если логин и пароль указаны верно и пароль действителен, произойдет вход в ОС.
Если логин и пароль указаны верно, но срок действия пароля истек, отобразится окно смены пароля. Придумайте новый пароль, чтобы войти в ОС.

Через системный интерфейс

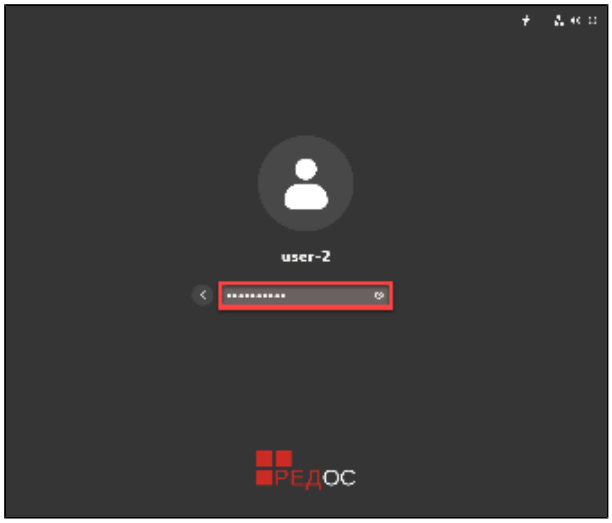
> В инструкциях ниже в качестве примеров используются стандартные интерфейсы указанных ОС. В зависимости от настроек графического интерфейса ОС, внешний вид экрана входа и расположение элементов интерфейса на нем могут отличаться.

В РЕД ОС

1. Выберите УЗ.



2. В поле **Пароль** введите пароль, заданный в ОС для выбранной УЗ.

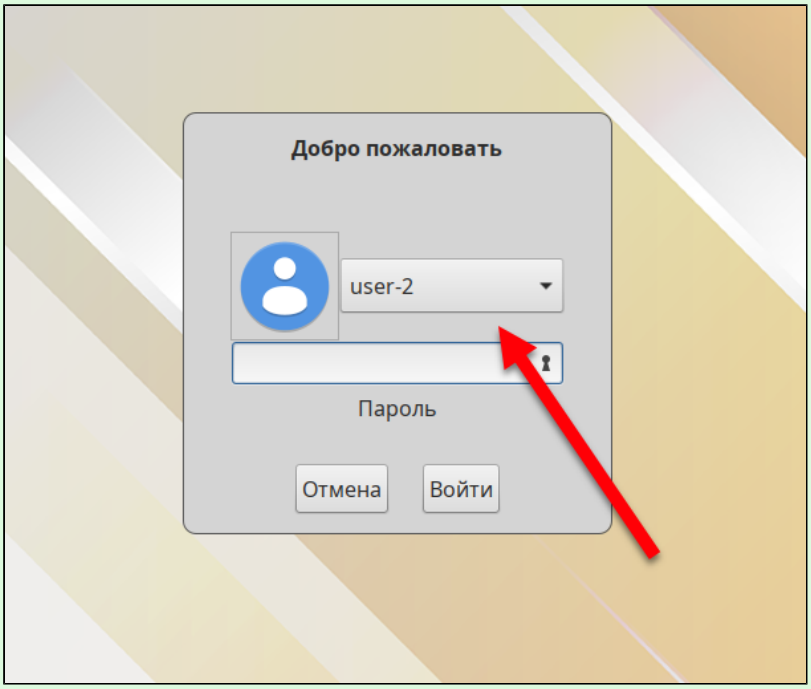


3. Нажмите **Enter**.

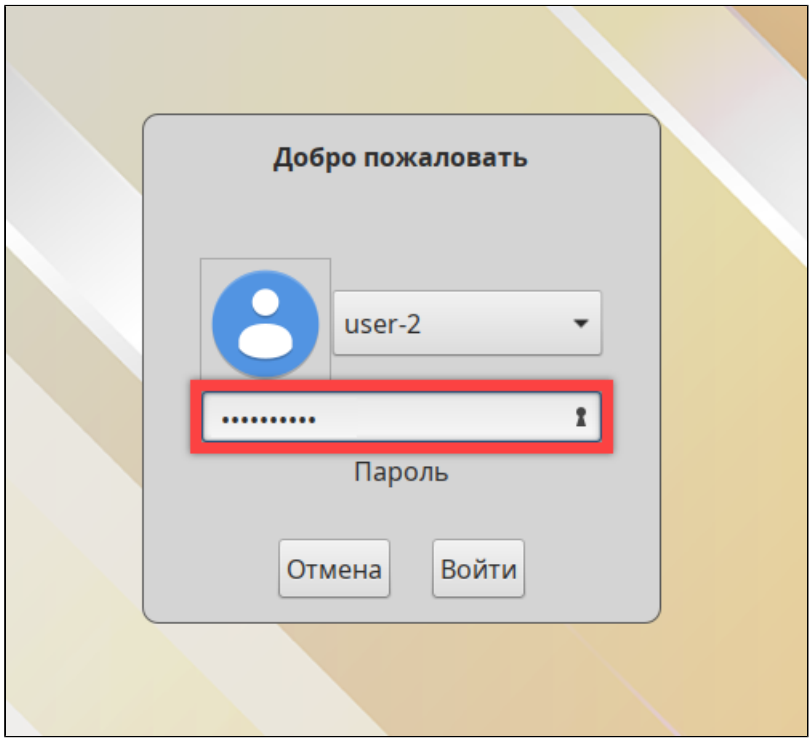
Если логин и пароль указаны верно и пароль действителен, произойдет вход в ОС.
Если логин и пароль указаны верно, но срок действия пароля истек, отобразится окно смены пароля. Придумайте новый пароль, чтобы войти в ОС.

В ОС Альт

Если на ПК настроено несколько УЗ, чтобы переключиться между ними, нажмите на логин УЗ, которая выбрана на экране входа в систему, и в раскрывающемся списке выберите другую УЗ.



1. В поле **Пароль** введите пароль, заданный в ОС для выбранной УЗ.

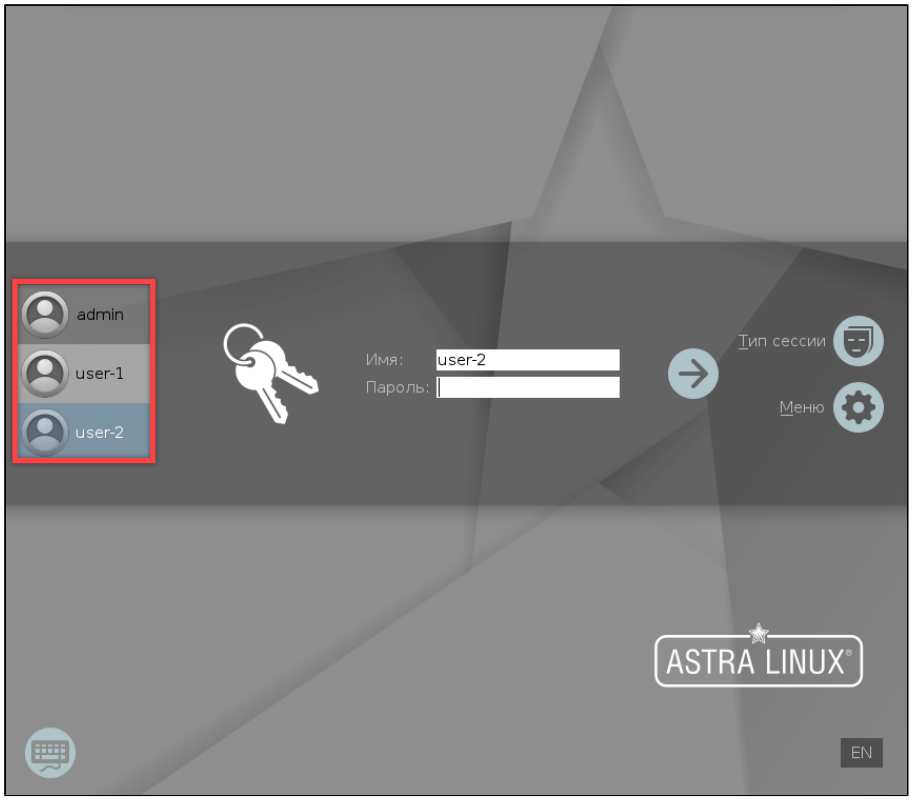


2. Нажмите **Войти**.

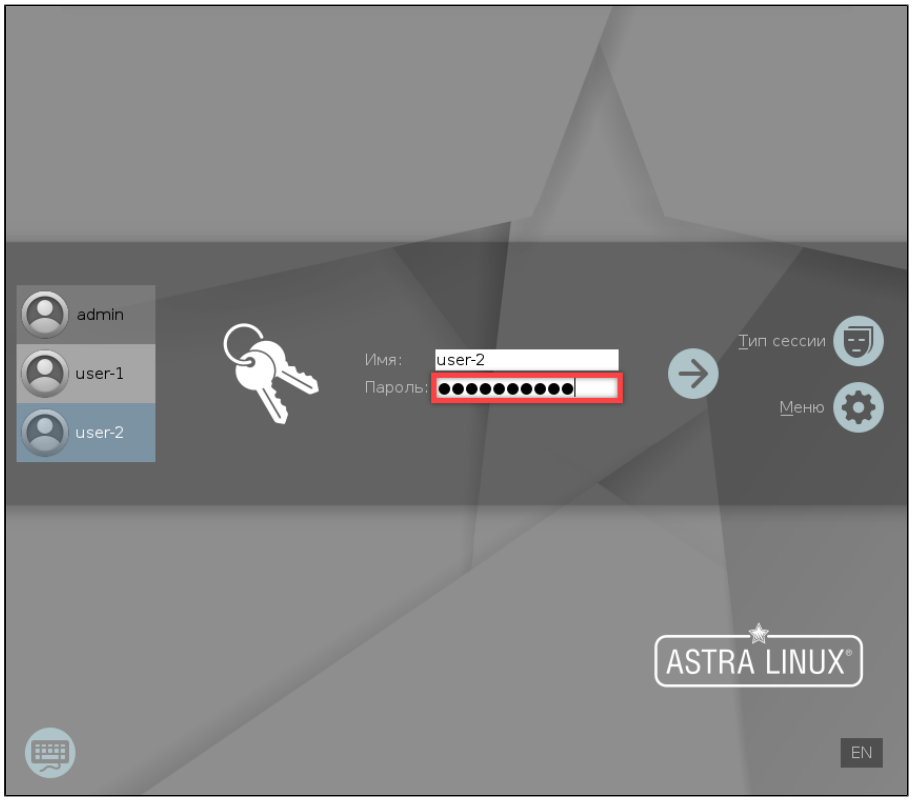
Если логин и пароль указаны верно и пароль действителен, произойдет вход в ОС.
Если логин и пароль указаны верно, но срок действия пароля истек, отобразится окно смены пароля. Придумайте новый пароль, чтобы войти в ОС.

В Astra Linux

1. В списке слева выберите УЗ.



2. В поле **Пароль** введите пароль, заданный в ОС для выбранной УЗ.

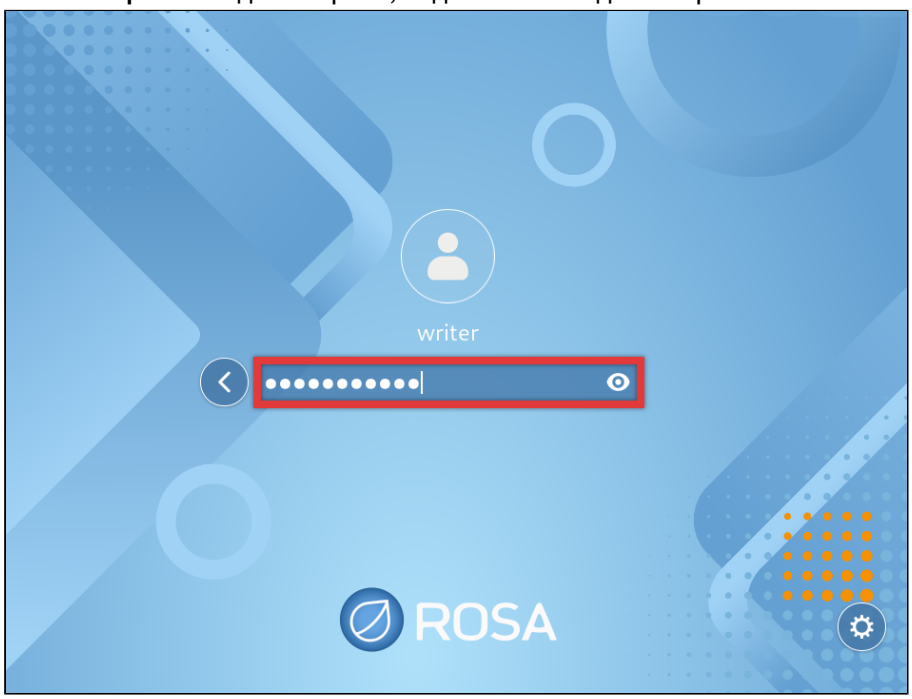


3. Нажмите **Enter**.

Если логин и пароль указаны верно и пароль действителен, произойдет вход в ОС.
Если логин и пароль указаны верно, но срок действия пароля истек, отобразится окно смены пароля. Придумайте новый пароль, чтобы войти в ОС.

В ОС РОСА

1. Подключите токен к ПК.
2. Выберите УЗ.
3. В поле **Пароль** введите пароль, заданный в ОС для выбранной УЗ.



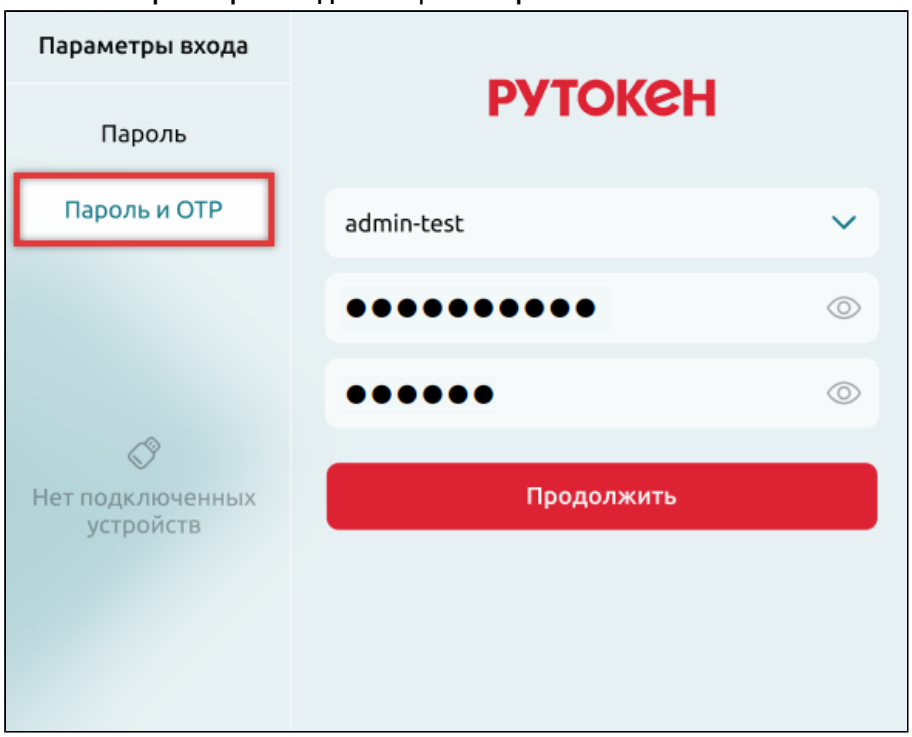
4. Нажмите **Enter**.

Если логин и пароль указаны верно и пароль действителен, произойдет вход в ОС.
Если логин и пароль указаны верно, но срок действия пароля истек, отобразится окно смены пароля. Придумайте новый пароль, чтобы войти в ОС.

Аутентификация по паролю и OTP

Через интерфейс Рутокен Логона

1. В списке **Параметры входа** выберите **Пароль и OTP**.



2. В раскрывающемся списке **Логин** выберите УЗ.
3. В поле **Пароль** ведите пароль, заданный в ОС для выбранной УЗ.
4. В поле **OTP** введите OTP, сгенерированный на устройстве Рутокен OTP или в приложении Яндекс ID.
5. Нажмите **Продолжить**.

Если логин и пароль указаны верно и пароль действителен, произойдет вход в ОС.
Если логин и пароль указаны верно, но срок действия пароля истек, отобразится окно смены пароля. Придумайте новый пароль, чтобы войти в ОС.

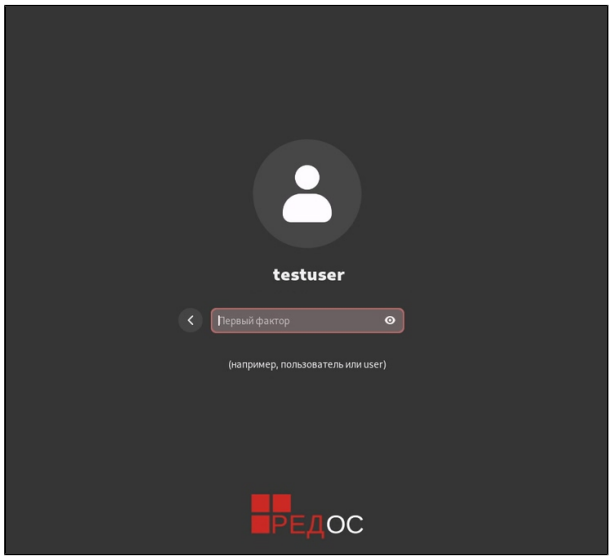
⚠ Смену пароля необходимо подтвердить с помощью OTP. Перед изменением пароля дождитесь генерации нового OTP.

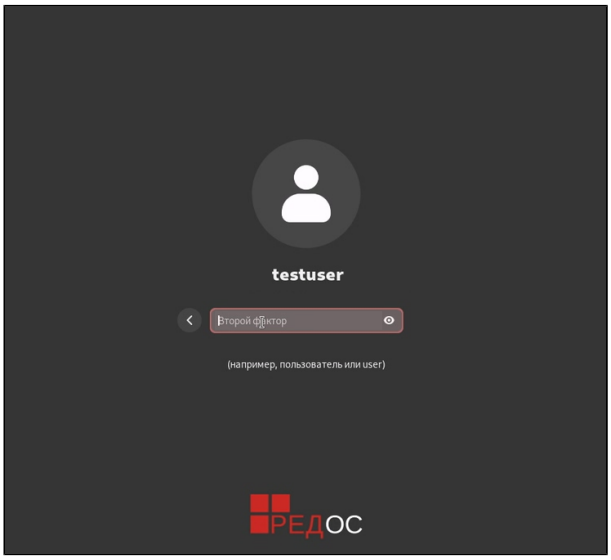
Через системный интерфейс

> В инструкциях ниже приведены скриншоты интерфейсов по умолчанию. В зависимости от настроек графического интерфейса ОС, внешний вид экрана входа и расположение элементов интерфейса на нем могут отличаться.

В РЕД ОС

1. В поле **Пароль** введите пароль, заданный в ОС для выбранной УЗ.
2. В поле **Первый фактор** введите пароль, заданный в ОС для выбранной УЗ, и нажмите **Enter**.
3. В поле **Второй фактор** введите OTP, сгенерированный на устройстве Рутокен OTP или в приложении Яндекс ID.

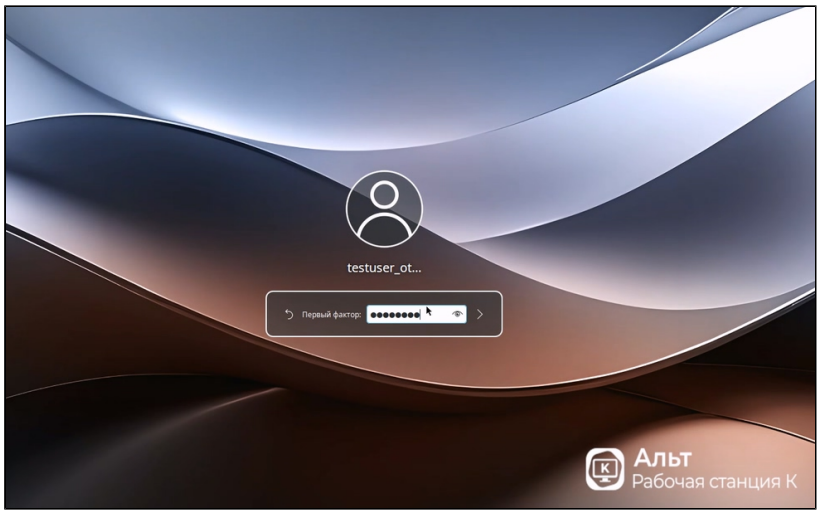


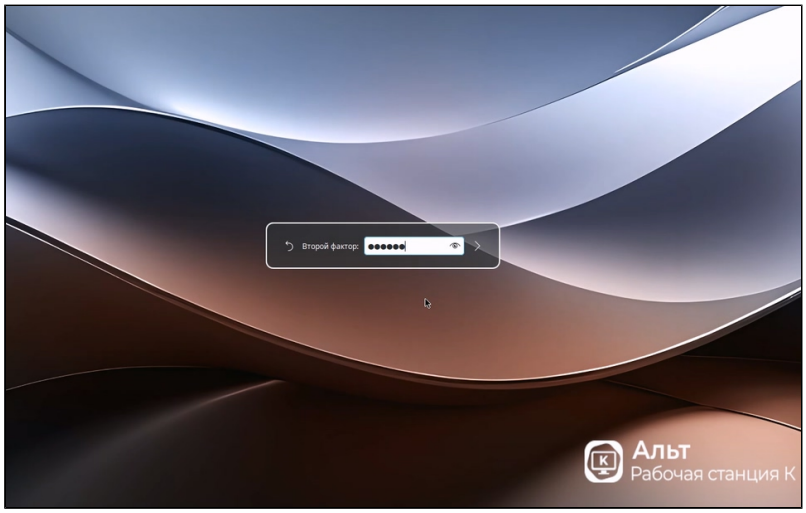


4. Нажмите **Enter**. Если логин, пароль и OTP указаны верно, произойдет вход в ОС.

В ОС Альт

1. Выберите нужную УЗ.
2. В поле **Первый фактор** введите пароль, заданный в ОС для выбранной УЗ, и нажмите **Enter**.
3. В поле **Второй фактор** введите OTP, сгенерированный на устройстве Рутокен OTP или в приложении Яндекс ID.

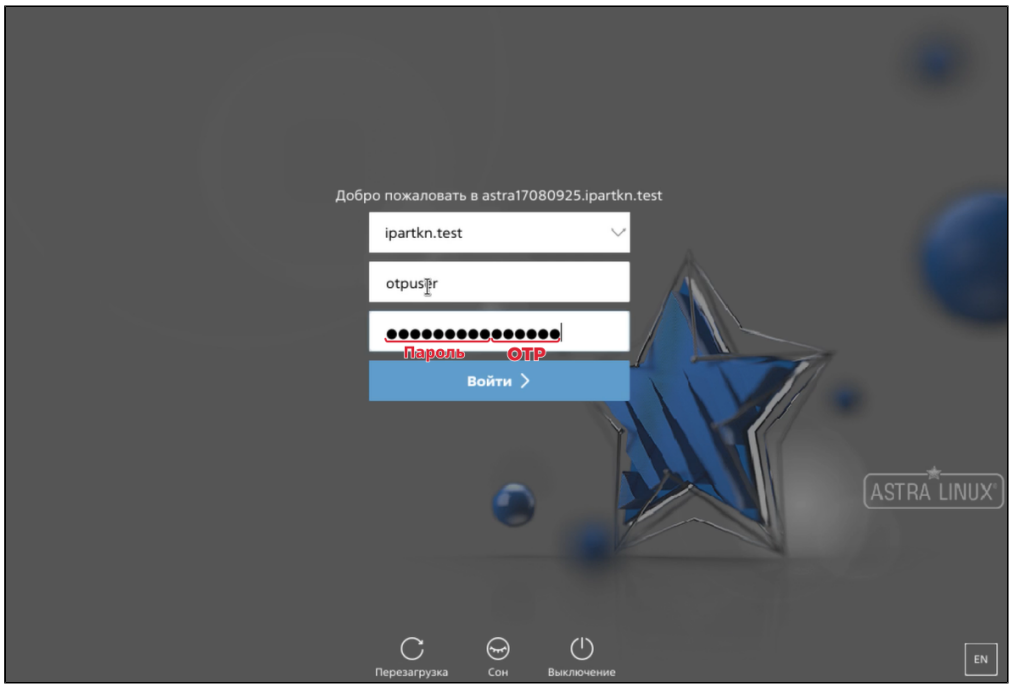




4. Нажмите **Enter**. Если логин, пароль и OTP указаны верно, произойдет вход в ОС.

В Astra Linux

1. Выберите домен, в котором находится нужная УЗ.
2. В поле **Имя пользователя** введите логин УЗ.
3. В поле **Пароль** введите пароль, заданный в ОС для выбранной УЗ.
4. В это же поле сразу после пароля введите OTP, сгенерированный на устройстве Рутокен OTP или в приложении Яндекс ID.



5. Нажмите **Войти**. Если логин, пароль и OTP указаны верно, произойдет вход в ОС.

В ОС РОСА

1. В поле **Пароль** введите пароль, заданный в ОС для выбранной УЗ.
2. В поле **Первый фактор** введите пароль, заданный в ОС для выбранной УЗ, и нажмите **Enter**.
3. В поле **Второй фактор** введите OTP, сгенерированный на устройстве Рутокен OTP или в приложении Яндекс ID.

4. Нажмите **Enter**. Если логин, пароль и OTP указаны верно, произойдет вход в ОС.

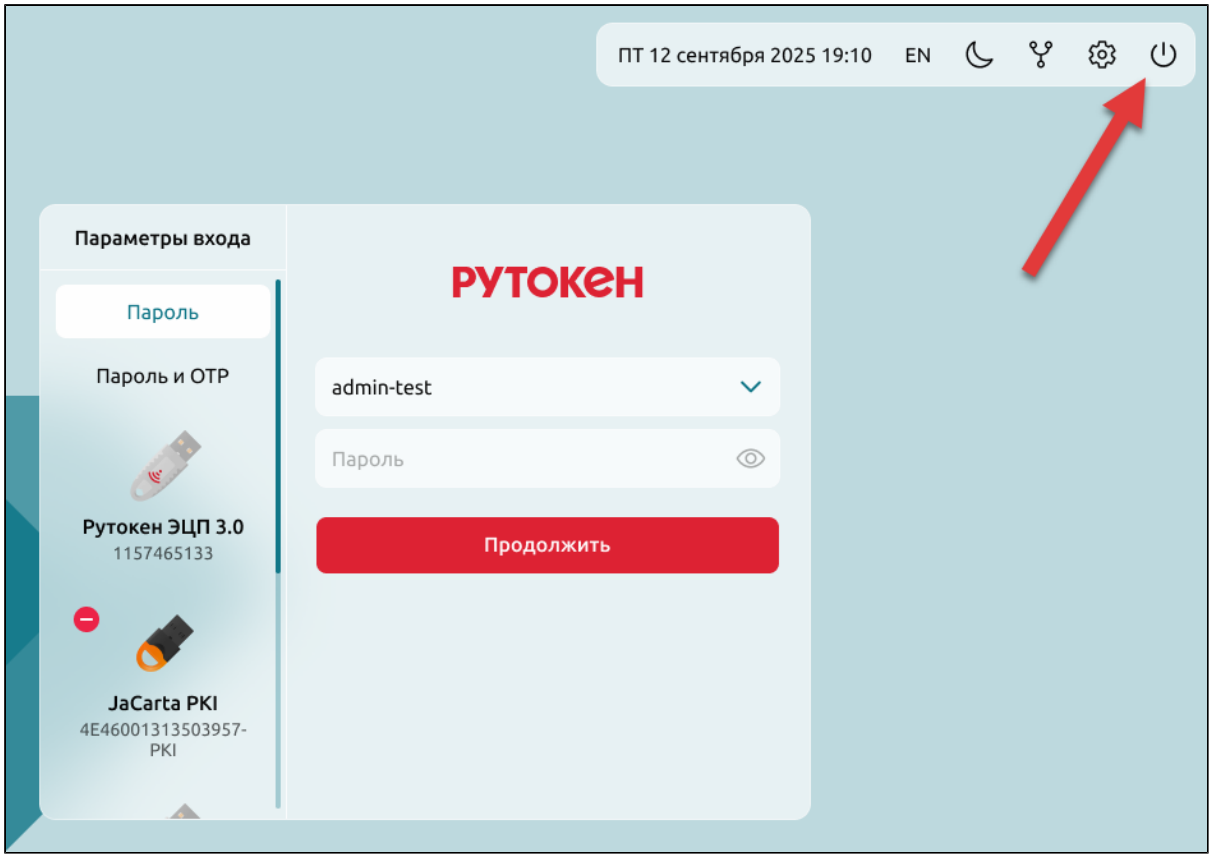
Выключение и перезагрузка ПК

Перед тем, как выключать ПК, убедитесь, что закончены все рабочие процессы и сохранены изменения в файлах. Если на ПК есть активные пользовательские сессии, перезагрузка и выключение в меню на экране входа завершат их без сохранения файлов.

В Astra Linux для перезагрузки или выключения ПК с активными сессиями понадобится ввести пароль от УЗ, на которых активны сессии.

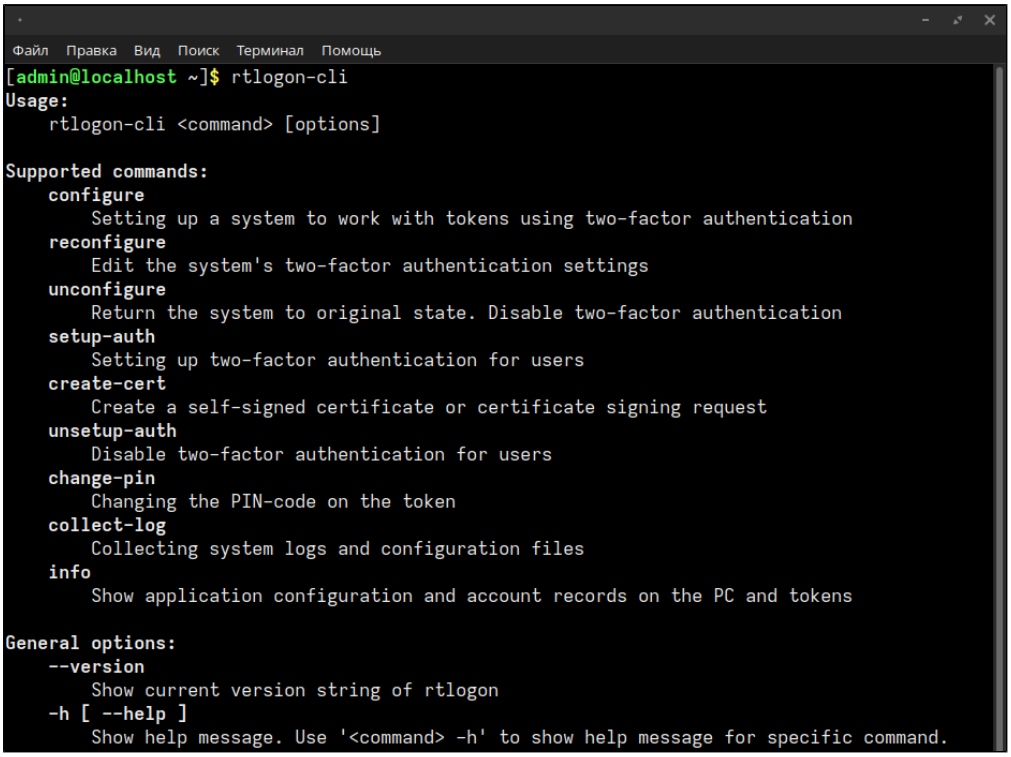
На экране входа можно перезагрузить или выключить ПК, не заходя в систему. Для этого:

1. В правом верхнем углу нажмите ⏻.



2. Выберите нужную опцию.

Консольная утилита



Утилита **rtlogon-cli** по умолчанию доступна в системах, в которых настроен Рутокен Логон. С ее помощью можно изменить PIN-коды подключенных токенов или посмотреть сведения о конфигурации Рутокен Логона и настройках 2ФА.

Для выполнения описанных ниже команд не требуются права суперпользователя.

Смена PIN-кода

Чтобы отменить ввод PIN-кода после активации команды и прервать операцию ручной смены PIN-кода, нажмите **Ctrl+C**.

Подключен один токен

1. Откройте терминал.
2. Введите команду:

```
rtlogon-cli change-pin
```

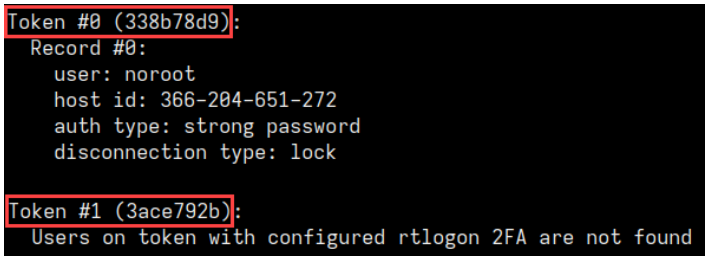
3. Введите текущий PIN-код.
4. Введите дважды новый PIN-код.
5. Нажмите **Enter**.

Подключено несколько токенов

1. Откройте терминал.
2. Введите команду:

```
rtlogon-cli info
```

3. Найдите записи, которые начинаются со слова **Token**. В скобках указан идентификатор (token_id) каждого токена (на иллюстрации: **338b78d9** и **3ace792b**).



4. Введите команду:

```
rtlogon-cli change-pin --token-id token_id
```

Например, команда для смены PIN-кода для второго токена на иллюстрации (Token #1) будет выглядеть так:

```
rtlogon-cli change-pin --token-id 3ace792b
```

5. Введите текущий PIN-код.
6. Введите дважды новый PIN-код.
7. Нажмите **Enter**.

Ошибки смены PIN-кода

Ошибка	Причина	Варианты решения
PIN-codes don't match	Значения нового PIN-кода при первом и втором вводе не совпадают	Убедитесь, что новый PIN-код вводился без ошибок оба раза
More than one token inserted. Option --token-id should be specified	К ПК подключено несколько токенов	Воспользуйтесь инструкцией для смены PIN-кода в случаях, когда к ПК подключено несколько токенов
New PIN-code doesn't comply with PIN-code policy	Вводимый PIN-код не соответствует политикам качества	Выберите другой PIN-код, который соответствует политикам качества
PIN-code can only be changed by the Administrator	PIN-код этого токена может изменить только администратор	Обратитесь к администратору
PIN-code length must be between X and Y characters	Новый PIN-код слишком длинный или слишком короткий	Выберите PIN-код нужной длины
This PIN-code has already been used	Политики качества для этого токена не позволяют выбрать использованный ранее PIN-код. В зависимости от настроек политик качества, в истории сохраняется до 10 последних PIN-кодов	Выберите другой PIN-код. Он должен отличаться от PIN-кодов, которые задавались для этого токена ранее

Просмотр сведений о 2ФА и конфигурации приложения

Утилита **rtlogon-cli** может вывести в окно терминала информацию о конфигурации Рутокен Логона и об УЗ, для которых настроена 2ФА. Эти сведения могут понадобиться администратору для устранения проблем.

В зависимости от того, какая проблема возникла, администратор может попросить прислать ему базовые или подробные сведения.

Базовые сведения

1. Подключите токен к ПК.
2. Откройте терминал.
3. Введите команду:

   ```
   rtlogon-cli info
   ```

4. Нажмите **Enter**.

Пример базовых сведений

PKCS#11 libraries info **(Сведения о библиотеках PKCS#11)**	
Rutoken pkcs11 library	
`Cryptoki interface version: 2.40`	Версия используемого стандарта PKCS#11
`Cryptoki library version: 2.14`	Версия библиотеки PKCS#11
`Manufacturer: Aktiv Co.`	Разработчик библиотеки
`Library description: Rutoken ECP PKCS #11 library`	Описание библиотеки
JaCarta pkcs11 library	
`Not found (valid library must be version no lower than 2.8)`	Информация о библиотеке PKCS#11 для устройств JaCarta. Значение `not found` указывает на то, что библиотека не установлена, или установленная версия библиотеки ниже 2.8
Rtlogon configuration **(Сведения о конфигурации Рутокен Логона)**	
`Host id: 366-204-651-272`	Идентификатор ПК, к которому привязана УЗ

Local users with configured rtlogon 2FA **(Сведения о локальных УЗ)**	
`Record #0`	Номер УЗ на ПК
`User: user-1`	Логин УЗ
`Token id: 338b78d9`	Идентификатор токена, на который записана эта УЗ
`Object id: 37b8d2228e2c5212`	Идентификатор секрета, записанного на токен
`Auth type: certificate`	Тип секрета. Возможные значения: ■ certificate (сертификат); ■ strong password (сложный пароль)
`Login policy: certificate and password auth`	Политика входа. Возможные значения: ■ certificate and password auth (вход по сертификату или паролю); ■ certificate only auth (вход только по сертификату)
Tokens info **(Сведения об УЗ, записанных на токены)**	
Token #0 **(Пример токена, на котором нет настроенных УЗ)**	
`id: 3f2a50b2`	Идентификатор токена
`Users on token with configured rtlogon 2FA are not found`	Уведомление о том, что на токене нет УЗ, настроенных для работы с Рутокен Логоном
Token #1 **(Пример токена с 2ФА по сертификату)**	
`id: 338b78d9`	Идентификатор токена
`Record #0`	Номер УЗ на токене
`User: user-1`	Логин УЗ
`Domain:rtkn.test`	Идентификатор ПК или имя домена, к которому привязана УЗ. Название поля зависит от типа УЗ. Для доменных УЗ используется `Domain`, для локальных — `Host id`
`Auth type: certificate`	Тип секрета. Возможные значения: ■ certificate (сертификат); ■ strong password (сложный пароль)

`Disconnection type: lock`	Поведение системы при отключении токена от ПК. Возможные значения: ■ lock (блокировка); ■ none (ничего — отключение токена не влияет на работу)
Token #2 (Пример токена с 2ФА по сложному паролю)	
`id: 1100841922`	Идентификатор токена
`Record #0`	Номер УЗ на токене
`User: tester`	Логин УЗ
`Host id: 366-204-651-272`	Идентификатор ПК или имя домена, к которому привязана УЗ. Название поля зависит от типа УЗ. Для доменных УЗ используется `Domain`, для локальных — `Host id`
`Auth type: strong password`	Тип секрета. Возможные значения: ■ certificate (сертификат); ■ strong password (сложный пароль)
`Disconnection type: lock`	Поведение системы при отключении токена от ПК. Возможные значения: ■ lock (блокировка); ■ none (ничего — отключение токена не влияет на работу)

Чтобы передать администратору данные из терминала:

1. Выделите текст в терминале.
2. Нажмите на него правой кнопкой мыши.
3. Выберите **Копировать**.
4. Вставьте скопированный текст в письмо или сообщение администратору.

Подробные сведения

1. Подключите токен к ПК.
2. Откройте терминал.
3. Введите команду:

```
rtlogon-cli info --verbose
```

4. Нажмите **Enter**.

Пример подробных сведений

PKCS#11 libraries info **(Сведения о библиотеках PKCS#11)**	
Rutoken pkcs11 library	
`Cryptoki interface version: 2.40`	Версия используемого стандарта PKCS#11
`Cryptoki library version: 2.14`	Версия библиотеки PKCS#11
`Manufacturer: Aktiv Co.`	Разработчик библиотеки
`Library description: Rutoken ECP PKCS #11 library`	Описание библиотеки
JaCarta pkcs11 library	
`Not found (valid library must be version no lower than 2.8)`	Информация о библиотеке PKCS#11 для устройств JaCarta. Значение `not found` указывает на то, что библиотека не установлена, или установленная версия библиотеки ниже 2.8
Rtlogon configuration **(Сведения о конфигурации Рутокен Логона)**	
`Host id: 366-204-651-272`	Идентификатор ПК, к которому привязана УЗ
`System gui: false`	Используемый интерфейс. Возможные значения: - true — для экранов входа и блокировки используется интерфейс системы; - false — для экранов входа и блокировки используется интерфейс Рутокен Логона

`Domain type: samba`	Тип домена, в котором находится УЗ. Возможные значения: ■ ipa; ■ aldpro; ■ ad; ■ samba. Отображается только при 2ФА в домене

`CA certificates chain:`
 	
`Certificate #0`
 	
`Validity starts: 2025-07-01 15:47:47`
`Validity ends: 2027-07-02 15:47:47`
`Subject: O=RTKN.TEST CN=Progress`
`Issuer: O=RTKN.TEST CN=Certificate Authority`
 	
`Cert body:`
`-----BEGIN CERTIFICATE-----`
`...`
`-----END CERTIFICATE-----`
 	
`Certificate #1...`
	Цепочка доверия.
	
	Отображает информацию о каждом сертификате в цепочке между сертификатом пользователя и корневым сертификатом:
	■ `Validity` — срок действия сертификата;
	■ `Subject` — владелец сертификата;
	■ `Issuer` — удостоверяющий центр, выпустивший сертификат;
	■ `Cert body` — содержимое сертификата

Local users with configured rtlogon 2FA (Сведения о локальных УЗ)	
`Record #0`	Номер УЗ на ПК
`User: user-1`	Логин УЗ
`Token id: 338b78d9`	Идентификатор токена, на который записана УЗ
`Object id: 08bad51ff4e66db6`	Идентификатор секрета, записанного на токен
`Auth type: certificate`	Тип секрета. Возможные значения: ■ certificate (сертификат); ■ strong password (сложный пароль)
`Login policy: certificate and password auth`	Политика входа. Возможные значения: ■ certificate and password auth (вход по сертификату или паролю); ■ certificate only auth (вход только по сертификату)
`Validity starts: 2025-07-01 15:47:47` `Validity ends: 2027-07-02 15:47:47`	Срок действия сертификата
`Subject: O=RTKN.TEST CN=Ivanov`	Информация о владельце сертификата

`Issuer: O=RTKN.TEST CN=Progress`	Информация об удостоверяющем центре, который выдал сертификат

`Cert body:`
`-----BEGIN CERTIFICATE-----`
`MIICtDCCAZwCAQAwDQYJKoZIhvcNAQELB...`
`-----END CERTIFICATE-----`
	Содержимое сертификата

Tokens info **(Сведения об УЗ, записанных на токены)**	
Token #0 **(Пример токена, на котором нет настроенных УЗ)**	
`Token id: 3f2a50b2`	Идентификатор токена
`Users on token with configured rtlogon 2FA are not found`	Уведомление о том, что на токене нет УЗ, настроенных для работы с Рутокен Логоном
Token #1 **(Пример токена с 2ФА по сертификату)**	
`id: 338b78d9`	Идентификатор токена
`Record #0`	Номер УЗ на токене
`User: user-1`	Логин УЗ
`Domain:rtkn.test`	Идентификатор ПК или имя домена, к которому привязана УЗ. Название поля зависит от типа УЗ. Для доменных УЗ используется `Domain`, для локальных — `Host id`
`Auth type: certificate`	Тип секрета. Возможные значения: - certificate (сертификат); - strong password (сложный пароль)
`Disconnection type: lock`	Поведение системы при отключении токена от ПК. Возможные значения: - lock (блокировка); - none (ничего — отключение токена не влияет на работу)
`User's certificate:`	Начало раздела с информацией о сертификате пользователя
`Label: 08bad51ff4e66db6`	Метка сертификата
`Object id: 08bad51ff4e66db6`	Идентификатор секрета, записанного на токен

`Validity starts: 2025-07-01 15:47:47` `Validity ends: 2027-07-02 15:47:47`	Срок действия сертификата
`Subject: O=RTKN.TEST CN=Ivanov`	Информация о владельце сертификата
`Issuer: O=RTKN.TEST CN=Progress`	Информация об удостоверяющем центре, который выдал сертификат

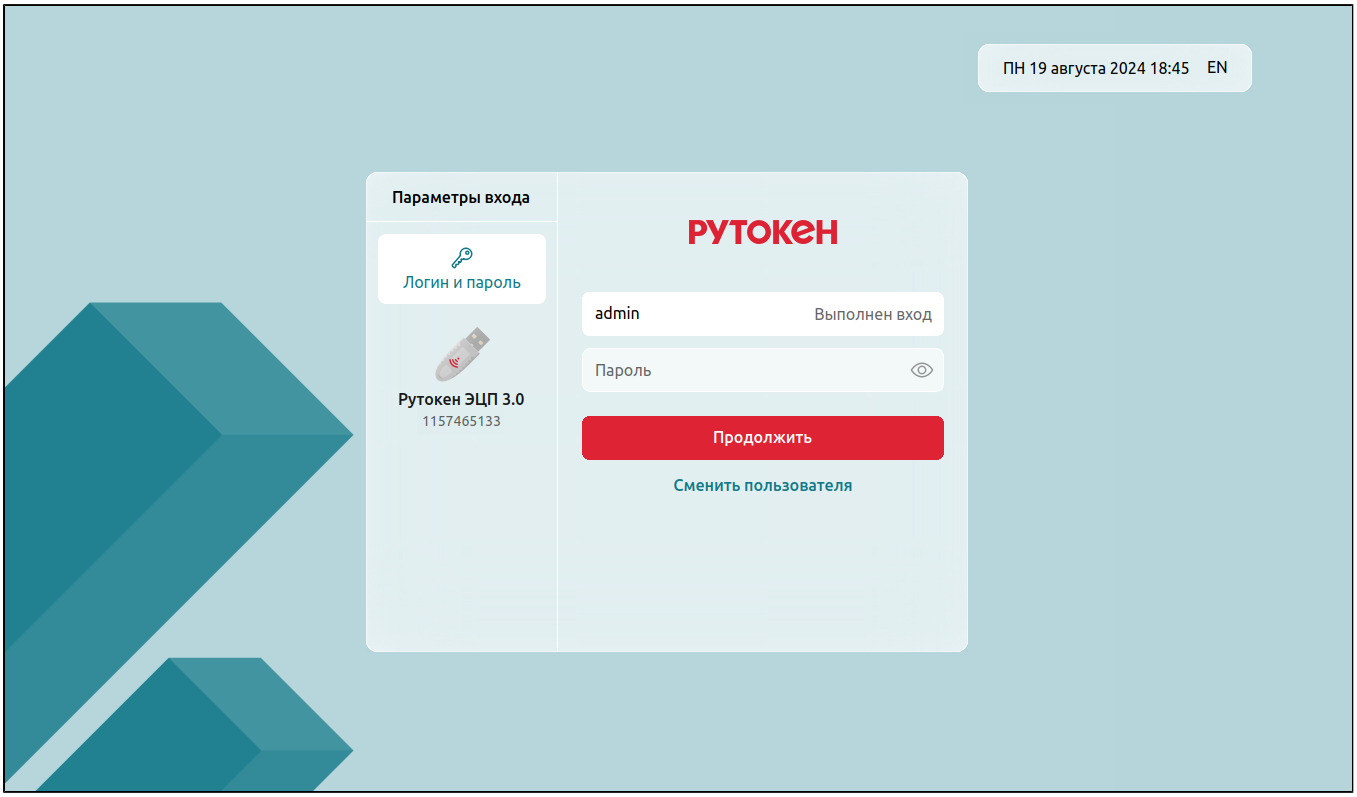
`Cert body:`
`-----BEGIN CERTIFICATE-----`
`MIICtDCCAZwCAQAwDQYJKoZIhvcNAQELB...`
`-----END CERTIFICATE-----`
	Содержимое сертификата

Token #2 **(Пример токена с 2ФА по сложному паролю)**	
`id: 1100841922`	Идентификатор токена
`Record #0`	Номер УЗ на токене
`User: tester`	Логин УЗ
`Host id: 366-204-651-272`	Идентификатор ПК или имя домена, к которому привязана УЗ. Название поля зависит от типа УЗ. Для доменных УЗ используется `Domain`, для локальных — `Host id`
`Auth type: strong password`	Тип секрета. Возможные значения: - certificate (сертификат); - strong password (сложный пароль)
`Disconnection type: none`	Поведение системы при отключении токена от ПК. Возможные значения: - lock (блокировка); - none (ничего — отключение токена не влияет на работу)
`Object id: f5d9a354ae815a0d`	Идентификатор секрета, записанного на токен

Чтобы передать администратору данные из терминала:

1. Выделите текст в терминале.
2. Нажмите на него правой кнопкой мыши.
3. Выберите **Копировать**.
4. Вставьте скопированный текст в письмо или сообщение администратору.

Блокировка сессии



Экран блокировки

Сессия может быть заблокирована вручную или автоматически после периода бездействия или извлечения токена из ПК, если администратор задал этот параметр при настройке Рутокен Логона.

В результате блокировки сессии вместо стандартного экрана входа в систему отобразится экран блокировки. На нем можно вернуться обратно в активную сессию или сменить пользователя.

Автоматическая блокировка

Рутокен Логон автоматически блокирует сессию:

- после периода бездействия, заданного в ОС;
- после извлечения токена, если такой параметр задан администратором.

Ручная блокировка

Вручную заблокировать сессию можно с помощью механизмов конкретной ОС, которые описаны в документации к ней. Наиболее популярные способы:

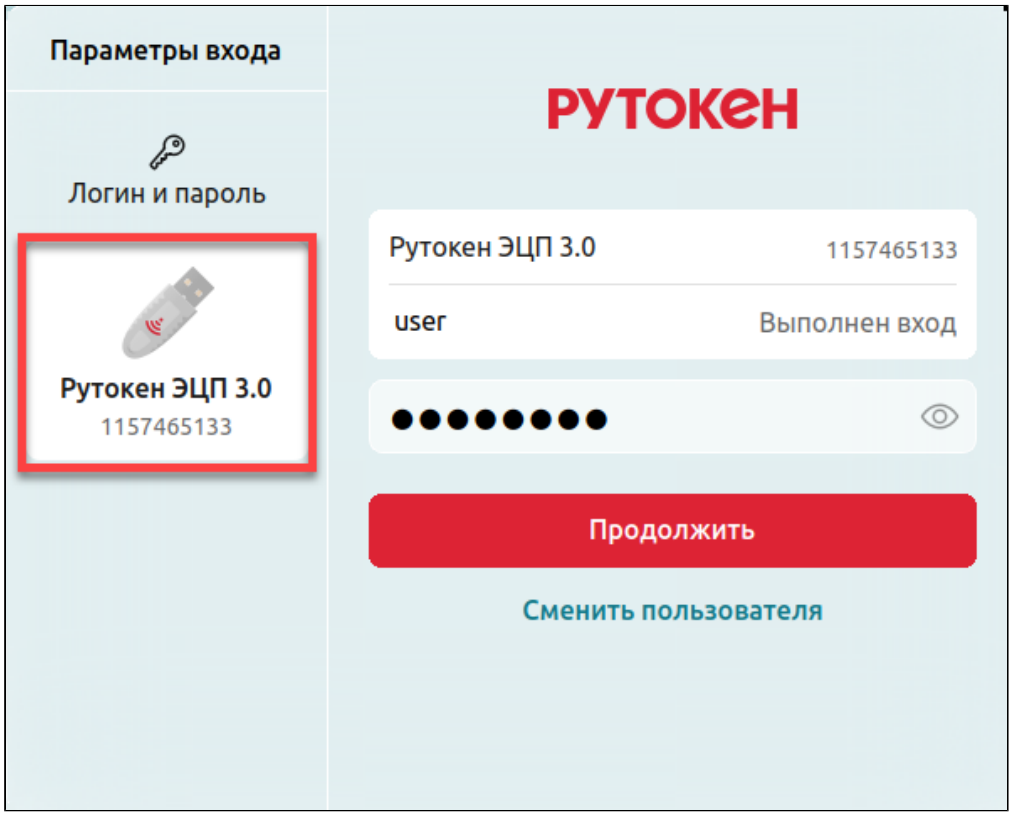
- комбинация клавиш **Ctrl+Alt+L** или **Meta+L (Win + L)**;
- команда `loginctl lock-session` в терминале;
- через главное меню (в Astra Linux это меню Пуск).

Разблокировка сессии

Аутентификация по токену

Через интерфейс Рутокен Логона

1. В разделе **Параметры входа** выберите токен, который использовался для входа в ОС.



2. Введите PIN-код токена.
3. Нажмите **Продолжить**. Если используется устройство Рутокен ЭЦП 3.0 Touch, прикоснитесь к токену, когда индикатор на нем начнет мигать.

Если логин и PIN-код указаны верно, произойдет разблокировка.

Через системный интерфейс

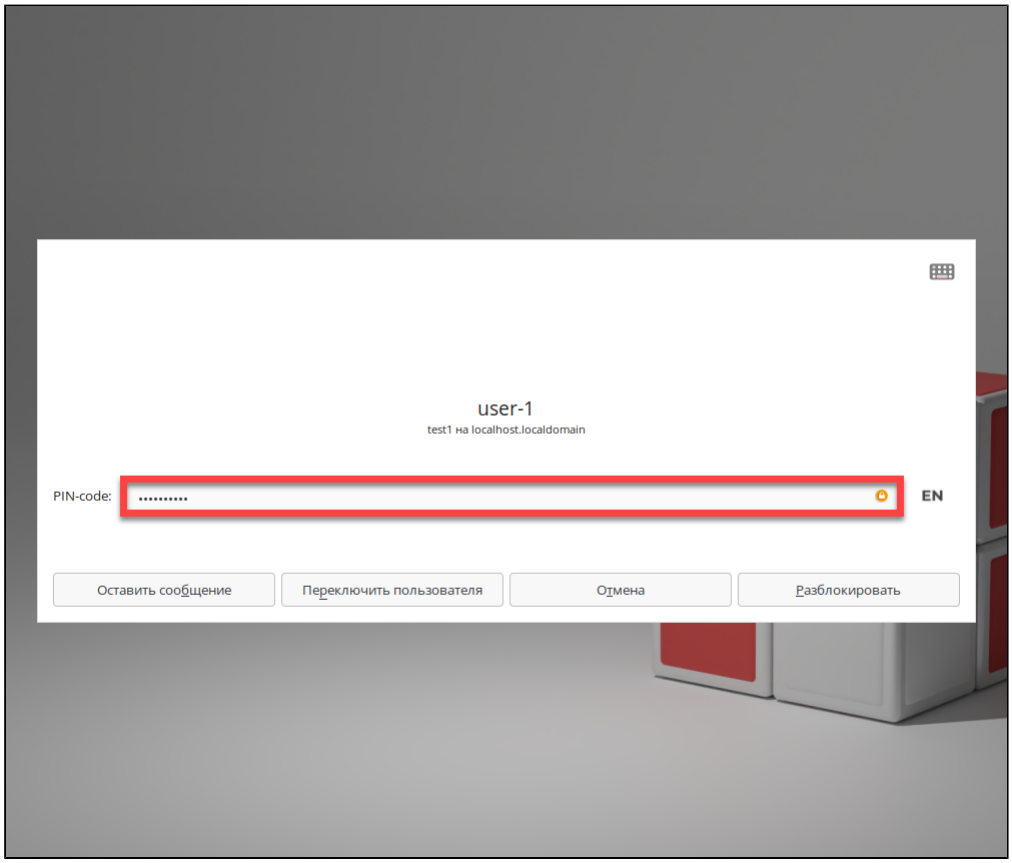
В инструкциях ниже приведены скриншоты интерфейсов по умолчанию. В зависимости от настроек графического интерфейса ОС, внешний вид экрана входа и расположение элементов интерфейса на нем могут отличаться.

При разблокировке сессии через системный интерфейс нет возможности переключиться между способами аутентификации вручную.

Если к ПК подключен токен, системный экран блокировки потребует PIN-код токена. Если к ПК не подключен токен, системный экран блокировки потребует пароль для 1ФА.

В РЕД ОС

1. Подключите токен к ПК.
2. В поле **PIN-code** введите PIN-код токена.

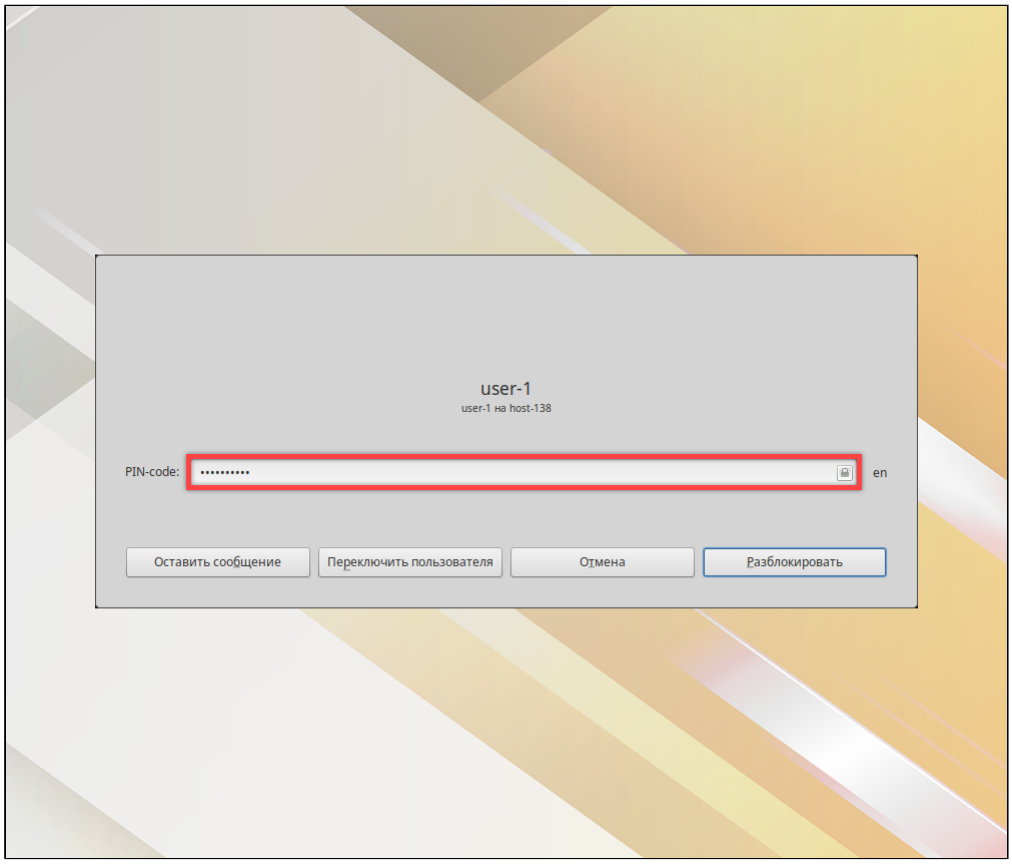


3. Нажмите **Разблокировать**. Если используется устройство Рутокен ЭЦП 3.0 Touch, прикоснитесь к токену, когда индикатор на нем начнет мигать.

Если логин и PIN-код указаны верно, произойдет разблокировка.

В ОС Альт

1. Подключите токен к ПК.
2. В поле **PIN-code** введите PIN-код токена.



3. Нажмите **Разблокировать**. Если используется устройство Рутокен ЭЦП 3.0 Touch, прикоснитесь к токену, когда индикатор на нем начнет мигать.

Если логин и PIN-код указаны верно, произойдет разблокировка.

В Astra Linux

1. Подключите токен к ПК.
2. В поле **Введите пароль** введите PIN-код токена.

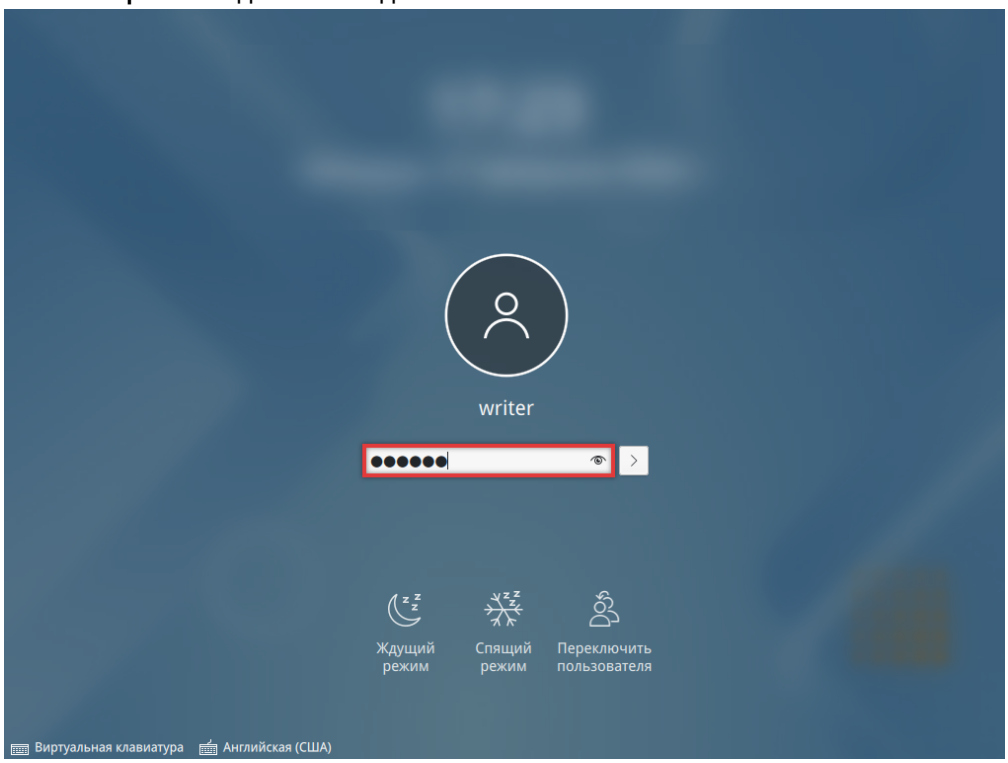
3. Нажмите **Enter**.

> ⚠ Если используется устройство Рутокен ЭЦП 3.0 Touch, прикоснитесь к токену после того, как индикатор на нем начнет часто мигать.
> Если токен слишком долго не получит подтверждение входа, процесс входа прервется и его нужно будет начать заново.

Если логин и PIN-код указаны верно, произойдет разблокировка.

В ОС РОСА

1. Подключите токен к ПК.
2. В поле **Пароль** введите PIN-код токена.



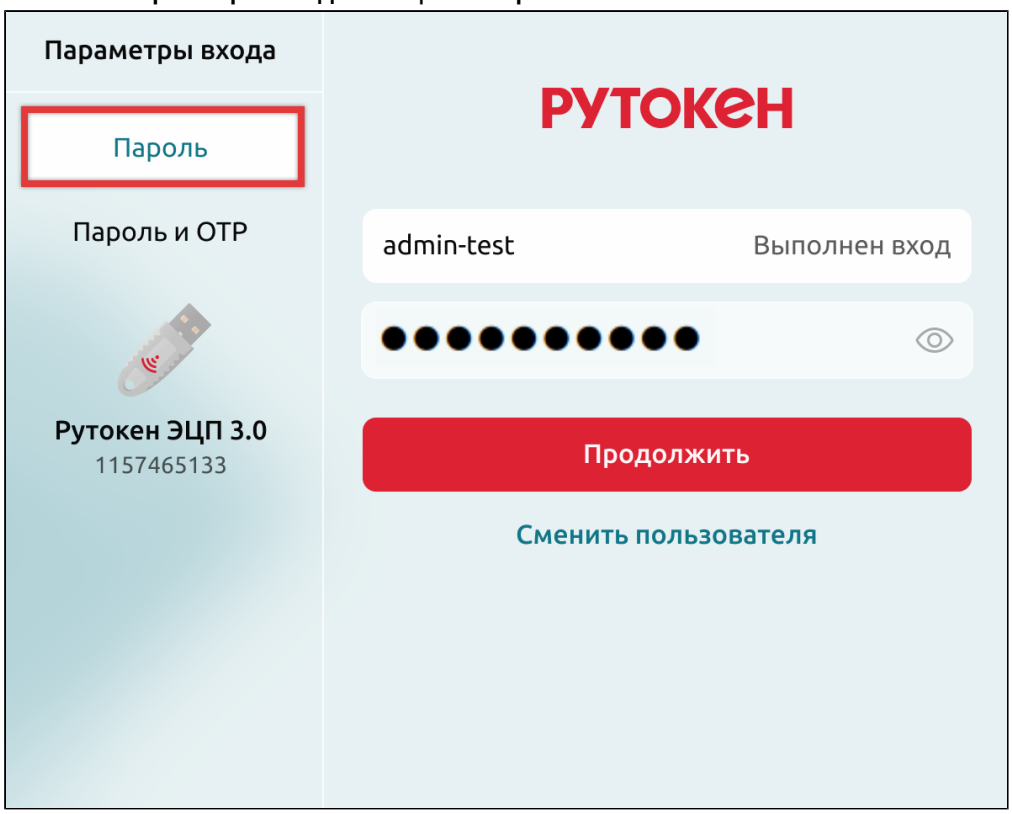
3. Нажмите **Enter**. Если используется устройство Рутокен ЭЦП 3.0 Touch, прикоснитесь к токену, когда индикатор на нем начнет мигать.

Если логин и PIN-код указаны верно, произойдет разблокировка.

Аутентификация по паролю

Через интерфейс Рутокен Логона

1. В списке **Параметры входа** выберите **Пароль**.



2. Введите пароль, заданный в ОС для выбранной УЗ.
3. Нажмите **Продолжить**. Если логин и пароль указаны верно, произойдет разблокировка.

Ошибки разблокировки сессии в интерфейсе Рутокен Логона

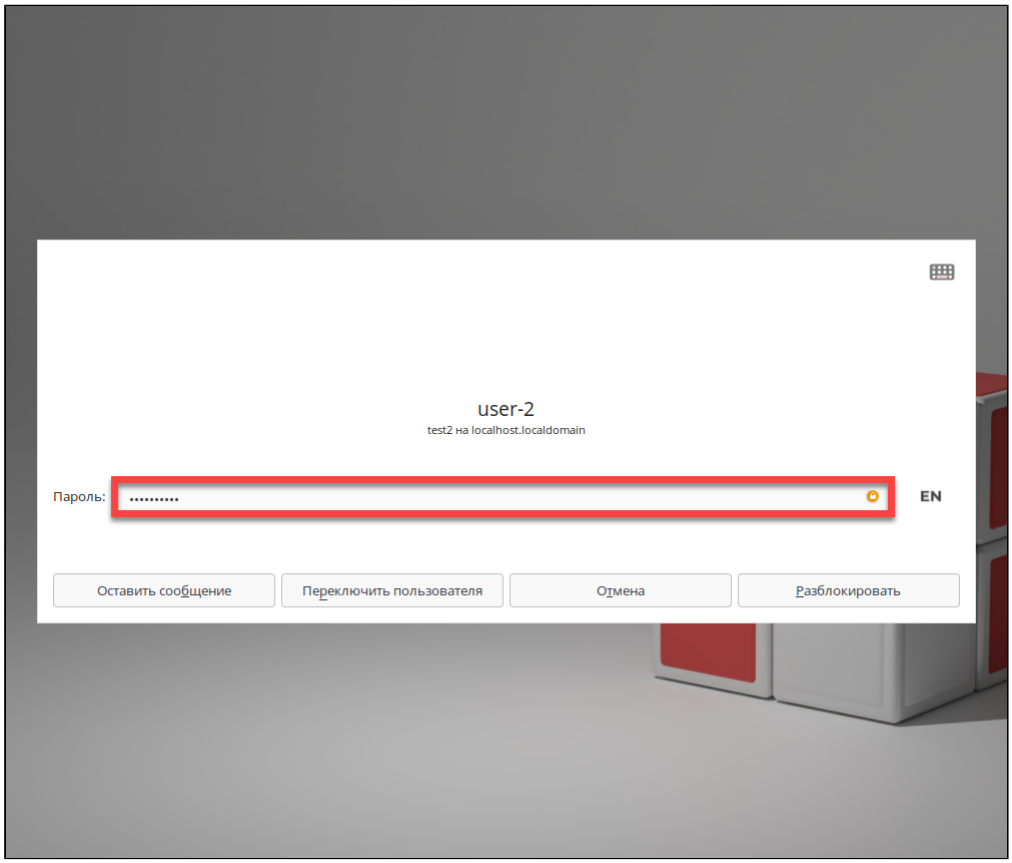
Ошибка	Причина	Варианты решения
Войти в данную учетную запись можно только при помощи токена	Попытка с помощью пароля вернуться в ОС, для которой настроен вход только с помощью 2ФА по сертификату	В разделе **Параметры входа** переключитесь с опции **Логин и пароль** на токен, который использовался для первого входа в ОС
Токен с заданным идентификатором не найден	К ПК не подключен токен, который использовался для входа в ОС	Убедитесь, что токен с данными УЗ подключен к ПК. Если он подключен, но не отображается в списке устройств, переподключите его

Через системный интерфейс

В инструкциях ниже приведены скриншоты интерфейсов по умолчанию. В зависимости от настроек графического интерфейса ОС, внешний вид экрана входа и расположение элементов интерфейса на нем могут отличаться.

В РЕД ОС

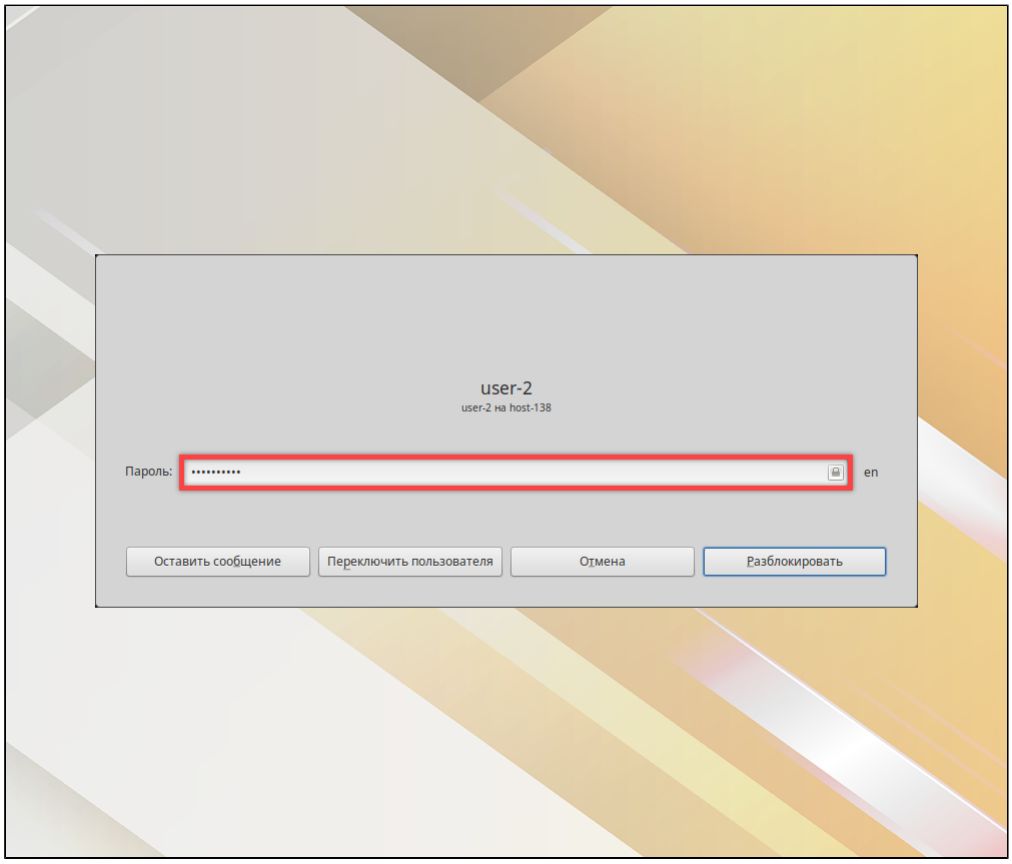
1. В поле **Пароль** введите пароль, заданный в ОС для выбранной УЗ.



2. Нажмите **Разблокировать**. Если логин и пароль указаны верно, произойдет разблокировка.

В ОС Альт

1. В поле **Пароль** введите пароль, заданный в ОС для выбранной УЗ.



2. Нажмите **Разблокировать**. Если логин и пароль указаны верно, произойдет разблокировка.

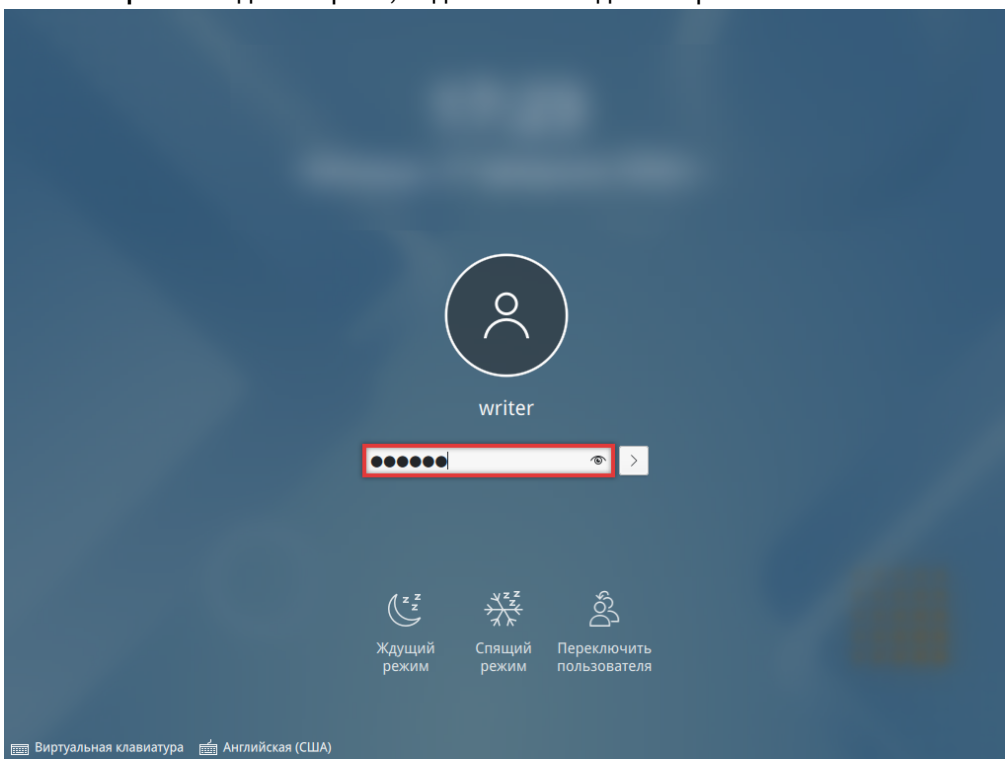
В Astra Linux

1. В поле **Введите пароль** введите пароль, заданный в ОС для выбранной УЗ.

2. Нажмите **Enter**. Если логин и пароль указаны верно, произойдет разблокировка.

В ОС РОСА

1. Подключите токен к ПК.
2. В поле **Пароль** введите пароль, заданный в ОС для выбранной УЗ.

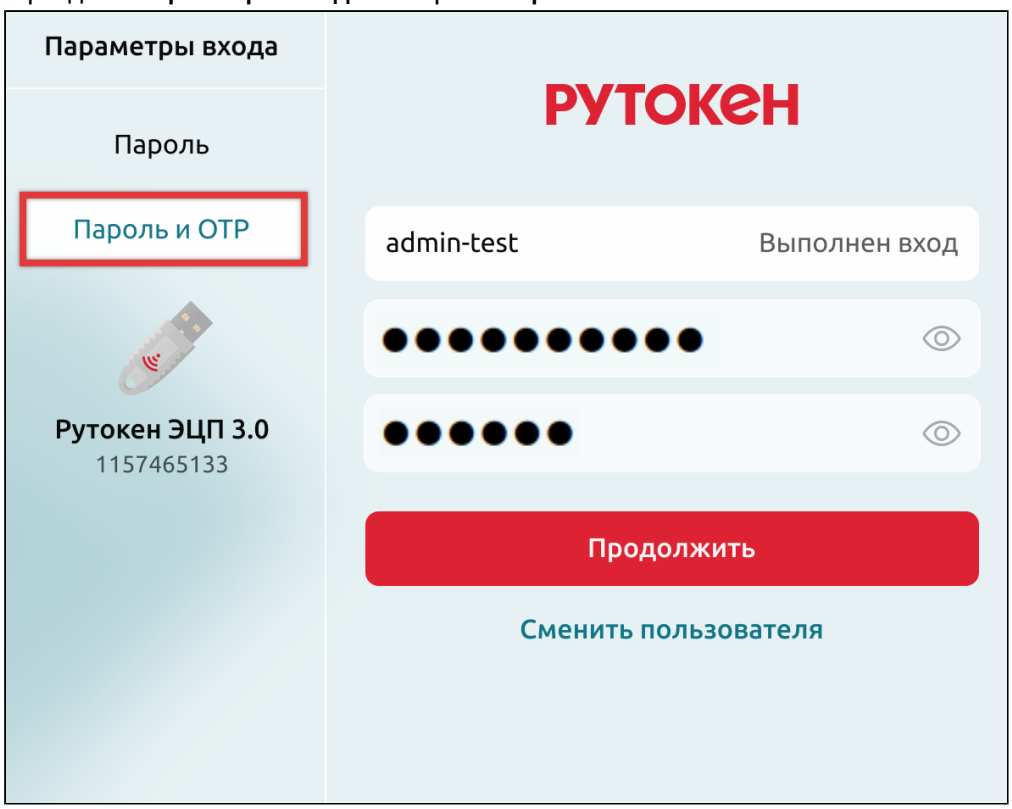


3. Нажмите **Enter**. Если логин и пароль указаны верно, произойдет разблокировка.

Аутентификация по паролю и OTP

Через интерфейс Рутокен Логона

1. В разделе **Параметры входа** выберите **Пароль и OTP**.

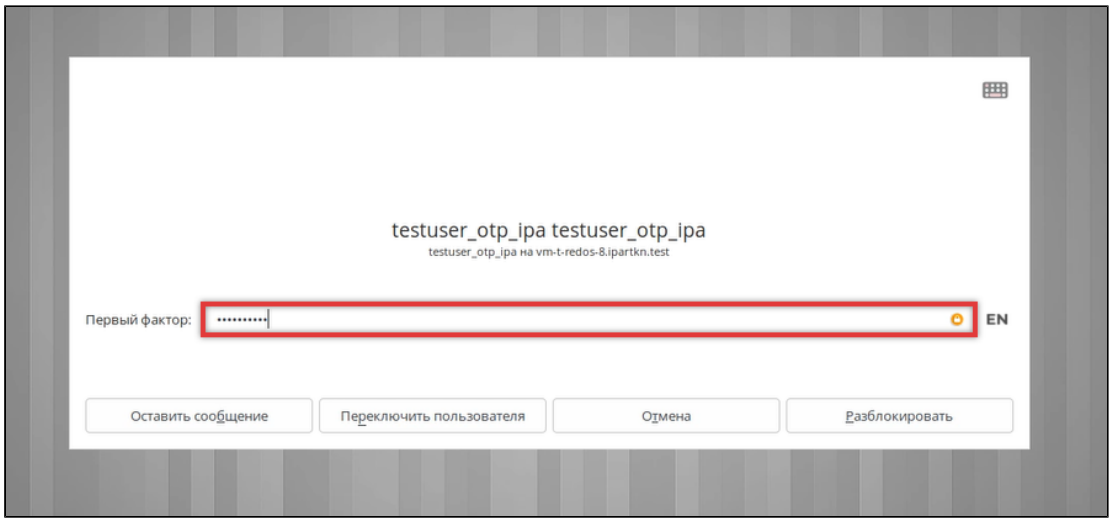


2. В поле **Пароль** введите пароль, заданный в ОС для выбранной УЗ.
3. В поле **OTP** введите OTP.
4. Нажмите **Продолжить**. Если логин, пароль и OTP указаны верно, произойдет разблокировка.

Через системный интерфейс

В РЕД ОС

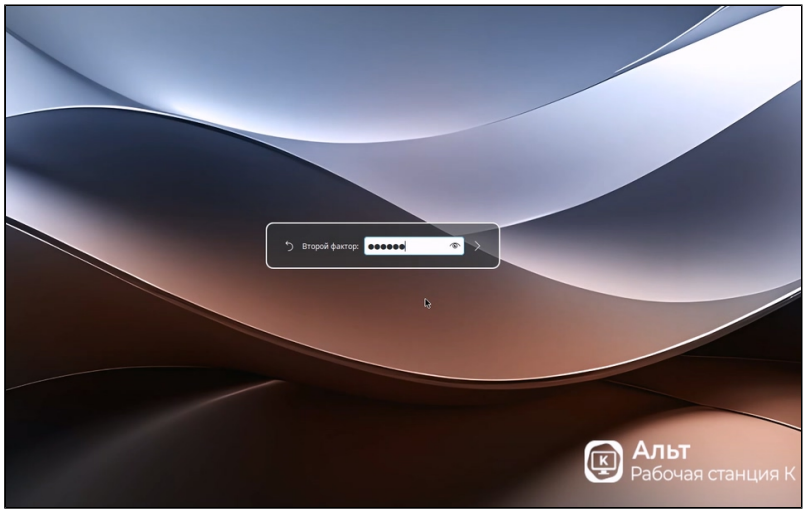
1. В поле **Первый фактор** введите пароль, заданный в ОС для выбранной УЗ, и нажмите **Enter**.
2. В поле **Второй фактор** введите OTP, сгенерированный на устройстве Рутокен OTP или в приложении Яндекс ID.



3. Нажмите **Enter**. Если логин, пароль и OTP указаны верно, произойдет разблокировка.

В ОС Альт

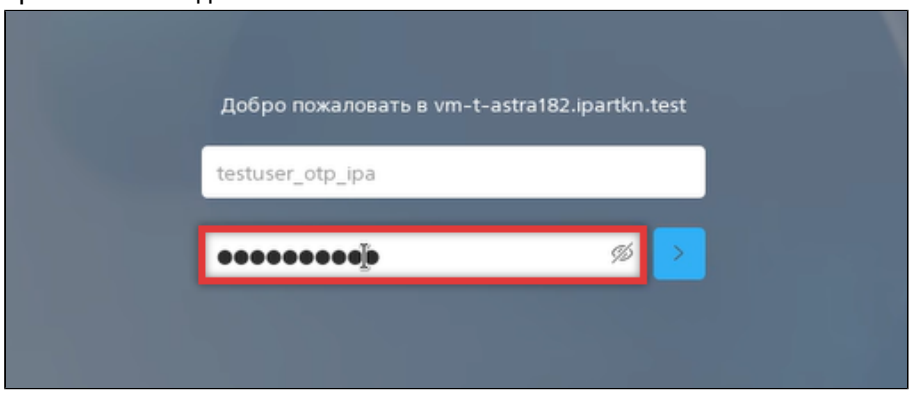
1. В поле **Первый фактор** введите пароль, заданный в ОС для выбранной УЗ, и нажмите **Enter**.
2. В поле **Второй фактор** введите OTP, сгенерированный на устройстве Рутокен OTP или в приложении Яндекс ID.



3. Нажмите **Enter**. Если логин, пароль и OTP указаны верно, произойдет разблокировка.

В Astra Linux

1. В поле **Введите пароль** введите пароль, заданный в ОС для выбранной УЗ.
2. В это же поле сразу после пароля введите OTP, сгенерированный на устройстве Рутокен OTP или в приложении Яндекс ID.



3. Нажмите **Enter**. Если логин, пароль и OTP указаны верно, произойдет разблокировка.

В ОС РОСА

1. В поле **Пароль** введите пароль, заданный в ОС для выбранной УЗ.
2. В поле **Первый фактор** введите пароль, заданный в ОС для выбранной УЗ, и нажмите **Enter**.
3. В поле **Второй фактор** введите OTP, сгенерированный на устройстве Рутокен OTP или в приложении Яндекс ID.

4. Нажмите **Enter**. Если логин, пароль и OTP указаны верно, произойдет вход в ОС.

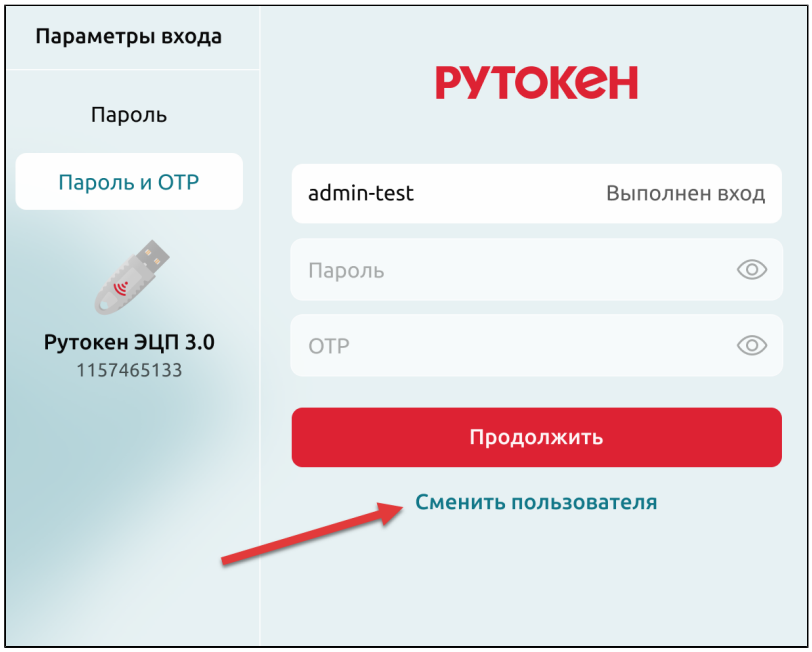
Смена пользователя

Без завершения активной сессии

Смена пользователя в Astra Linux

В Astra Linux сохранение активной сессии при смене пользователя регулируется системными настройками управления сессиями. Изменить их можно в приложении **Панель управления** в разделе **Сессии Fly**.
Для работы с сессиями Рутокен Логон использует настройки ОС. Если сохранение сессии отключено в настройках Astra Linux, при смене пользователя предыдущая сессия завершится, а при следующем входе будет создана новая.

1. Заблокируйте сессию вручную.
2. Нажмите **Сменить пользователя**.



3. Выберите другую УЗ и войдите в нее.

С завершением активной сессии

Перед завершением сессии закончите все рабочие процессы и сохраните файлы.

1. Завершите сессию любым способом. Например, через главное меню (в Astra Linux это меню Пуск).
2. Выберите другую УЗ и войдите в нее.

Дополнительные настройки

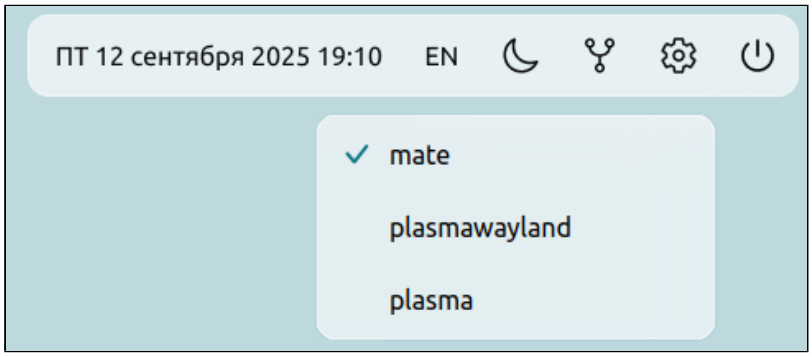
Смена среды рабочего стола

Если на ПК установлены несколько сред рабочего стола, можно переключиться между ними на экране входа в систему.

Если в ОС уже есть активные пользовательские сессии, чтобы сменить среду рабочего стола, нужно их завершить.

Перед завершением сессии закончите все рабочие процессы и сохраните файлы.

1. На панели инструментов в правом верхнем углу нажмите  .
2. Выберите среду.



3. Войдите в ОС с помощью данных УЗ.

Поддерживаемые среды рабочего стола:

- для Astra Linux: Fly;
- для ОС Альт: Mate, KDE;
- для РЕД ОС: Mate, Cinnamon, KDE.

Графическое окружение GNOME не поддерживается для экранов приветствия и блокировки Рутокен Логон.

Изменение темы

Интерфейс Рутокен Логона доступен в двух темах: светлой и темной.

На панели инструментов на экране приветствия или блокировки нажмите:

-  — чтобы переключиться со светлой темы на темную;
-  — чтобы переключиться с темной темы на светлую.

Тема сохраняется после перезагрузки и выключения ПК.

Особенности изменения темы в Astra Linux

Настройки темы экранов входа и блокировки общие во всех ОС, кроме Astra Linux. В Astra Linux тема на экране входа задается отдельно от темы на экране блокировки. Также в Astra Linux настройки темы экрана блокировки индивидуальны для каждого пользователя.