

**Рутокен Логон для Linux.
Версия 1.0.5.
Примечания к выпуску
(Release Notes)**



Название продукта: Рутокен Логон для Linux

Версия продукта: 1.0.5

Дата релиза: 27 марта 2026 г.

Статус продукта: коммерческий релиз

- [Назначение продукта](#)
- [Что нового?](#)
 - [Новые возможности](#)
 - [Доработанная функциональность](#)
 - [Исправления ошибок](#)
 - [Совместимость с предыдущими версиями](#)
- [Поддерживаемые устройства](#)
- [Поддерживаемые программные аутентификаторы](#)
- [Поддерживаемые платформы](#)
- [Поддерживаемые ОС](#)
- [Поддерживаемые графические окружения](#)
- [Поддерживаемые контроллеры домена](#)
- [Поддерживаемые сценарии работы](#)
- [Реализованные функции](#)
 - [Развертывание](#)
 - [Настройка](#)
 - [Получение информации о настройках и работе продукта](#)
 - [Дополнительные функции](#)
- [Эксплуатация](#)
- [Ограничения](#)
- [Известные проблемы](#)
- [Интерфейс продукта](#)

Назначение продукта

Рутокен Логон для Linux (далее по тексту - **rtlogon**) - это программный комплекс, предназначенный для настройки, управления и использования двухфакторной аутентификации (2ФА) пользователей при входе в операционную систему (ОС) семейства Linux.

Первым фактором аутентификации является владение пользователем ключевым носителем, который подключается к ПК. Вторым фактором - знание пользователем PIN-кода, после предъявления которого предоставляется доступ к секрету, хранящемуся на ключевом носителе.

В качестве секрета может использоваться:

- сертификат;
- сложный пароль .

rtlogon поддерживает следующие типы аутентификации:

- по количеству используемых факторов:
 - 2ФА: первый фактор - владение токеном, второй фактор - знание PIN-кода;
 - 1ФА: знание пароля учетной записи (настраивается вне **rtlogon**).
- по типу УЗ, для которой настраивается аутентификация:
 - локальная;
 - доменная.

rtlogon позволяет задать следующие политики входа в ОС для локальной 2ФА:

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

При доменной 2ФА способ входа в ОС настраивается на стороне контроллера домена.

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

Что нового?

- Добавлена поддержка:
 - устройств:
 - Рутокен ЭЦП 3.0 Touch;
 - Рутокен ОТР.
 - программных аутентификаторов:
 - Яндекс ID (ранее – Яндекс Ключ).
 - ОС:
 - РОСА Хром 12.4.
 - контроллеров домена:
 - ROSA Dynamic Directory 4.13.0 и новее.
- Доработана поддержка:
 - ОС:
 - Альт 11.0 и новее;
 - контроллеров домена:
 - РЕД АДМ 2.0.1 и новее.
- Реализована поддержка темной темы для интерфейса;
- Исправлены ошибки.

> Новые возможности

- При аутентификации пользователя в домены FreeIPA, Dynamic Directory и ALD Pro по простому паролю теперь присутствует возможность использования ОТР в качестве второго фактора.
Поддерживаемые аппаратные и программные решения:
 - Рутокен ОТР;
 - Яндекс ID.
- Реализована поддержка устройств Рутокен ЭЦП 3.0 Touch.
В процессе аутентификации пользователю выводится сообщение о необходимости прикоснуться к токену для подтверждения физического присутствия у ПК.
- Добавлена поддержка ОС РОСА «Хром» 12.4.
- Добавлена поддержка контроллера домена ROSA Dynamic Directory 4.13.0 и новее.
- Реализована поддержка темной темы на экранах входа и блокировки rtlogin.

> Доработанная функциональность

- Доработана поддержка ОС Альт 11.0 и новее.
- Доработана поддержка контроллера домена Ред АДМ 2.0.1 и новее.
- Доработана выгрузка сообщений `rtlogon` в `syslog`.
Теперь сообщения всех компонентов `rtlogon` записываются не только в журнал `rtlogon`, но и в `syslog`.
- Улучшена защита от случайного изменения или удаления файлов конфигурации `rtlogon`.
- Список сетей на экране входа `rtlogon` больше не скрывается в случае, если в `polkit` настроен запрет на изменение их состояния.
При попытке выполнения запрещенных действий (например, подключение или отключение сети), пользователь получит сообщение о том, что `polkit` запрещает выполнять данное действие.
- Добавлен вывод информации об отсутствии проводного или беспроводного соединения в интерфейсе `rtlogon`.
- Другие доработки интерфейса `rtlogon`.

> Исправления ошибок

- Исправлены проблемы конфигурирования `rtlogon` с экранами входа и блокировки `rtlogon` в среде Astra 4.7.6, Baikal (ARM64).
- Исправлена проблема, из-за которой в результате использования команд `reconfigure` и `unconfigure` мог повредиться файл-конфигурации `lightdm.conf`.
- Исправлена проблема доменной аутентификации по сертификату на ОС Astra 1.8 с системным экраном входа, если на токене присутствуют 2 ключевых пары и 2 сертификата, но при этом только у одного из них присутствует запись в `publicAuthdesc`.
- Исправлена ошибка, из-за которой могло запрашиваться выполнение конфигурирования `rtlogon` при смене PIN-кода в командно-строчном интерфейсе `rtlogon` для команды `change-pin`.
- Исправлена ошибка, из-за которой могло запрашиваться выполнение конфигурирования `rtlogon` в командно-строчном интерфейсе `rtlogon` для команды `create-cert`.
- Исправлена ошибка, из-за которой могли возникать проблемы при переключении клавиатуры на русскую раскладку для локального пользователя после конфигурирования `rtlogon`.
- Исправлен вывод ошибки при локальном входе с учетной записью по простому паролю с политикой "только по сертификату".
- Исправлен вывод ошибки при попытке настройки 2ФА для заблокированного пользователя.
- Исправлена ошибка, из-за которой в сообщениях журнала `rtlogon.log` для экрана блокировки в среде `lightdm` могло выводиться некорректное имя сервиса.
- Исправлена ошибка в команде `change-pin`, при которой во время запроса нового PIN-кода вызов `ctrl+D` (EOF) приводил к рекурсивному выводу в терминал.
- Исправлен вывод ошибки в лог команды `change-pin` в связи с длиной, не удовлетворяющей политике токена;.
- Исправлена ошибка отсутствия на экране входа `rtlogon` запроса смены пароля в доменах Active Directory и Samba после удаления доменной УЗ по сложному паролю.


> Совместимость с предыдущими версиями

Обеспечена поддержка перехода с версии `rtlogon 1.0.0`.

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

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.

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

Поддерживаемые программные аутентификаторы

- Яндекс ID (прежнее название – Яндекс Ключ).

Поддерживаемые платформы


- x86_64;
- 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 .
- ОС Альт 8 СП, релиз 10;
- ОС Альт 8.4 СП;
- ОС Альт 10.0 и новее;
- ОС Альт 11.0 и новее;
- РЕД ОС 7.3;
- РЕД ОС 8;
- РОСА Хром 12.4.

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.

 *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 4.19.9;
- ROSA Dynamic Directory 4.13.0 и новее;
- РЕД АДМ 2.0.1 и новее.

Поддерживаемые сценарии работы

- Доменная аутентификация:
 - по сложному паролю на ключевом носителе;
 - по сертификату на ключевом носителе;
 - по логину, паролю УЗ и одноразовому паролю (One-Time Password - OTP).
- Локальная аутентификация:
 - по сложному паролю на ключевом носителе;
 - по сертификату (ГОСТ и RSA) на ключевом носителе.

Реализованные функции

> Развертывание

При помощи командно-строчного интерфейса обеспечено выполнение следующих процедур развертывания `rtlogon`:

- установка;
- обновление;
- удаление.

Также предусмотрены вспомогательные скрипты для массового развертывания `rtlogon` на ПК пользователей.

> Настройка

- конфигурирование, реконфигурирование и отключение настроек ОС для работы с 2ФА;
- настройка учетной записи пользователя для работы с 2ФА;
- отключение 2ФА для учетной записи пользователя.

> Получение информации о настройках и работе продукта

- вывод в консоль подробной информации о конфигурации `rtlogon` и параметрах настроенной локальной 2ФА;
- логирование событий в продукте, в том числе попыток аутентификации пользователя;
- экспорт конфигурационных файлов, лог-файлов и файлов с параметрами настроенной 2ФА.

> Дополнительные функции

- кеширование входа в доменные учетные записи;
- автоматическая блокировка сессии пользователя при извлечении ключевого носителя или после периода бездействия;
- ввод ПК в домены (ALD Pro, AD, FreeIPA или Samba DC) при помощи вспомогательных скриптов;
- средство генерации запросов на получение сертификата, выпуск самоподписанного сертификата;
- проверка сертификатов пользователей на статус "отозванный" с использованием списков отзыва сертификатов **CRL** или протокола **OCSP**;
- интерактивное изменение пароля для локальной учетной записи при удалении настроенной аутентификации по сложному паролю;
- блокировка входа по логину-паролю (только для локальной учетной записи);
- смена PIN-кода ключевого носителя (по необходимости).

Эксплуатация

Для успешного входа в ОС пользователь должен подключить свое устройство к ПК, выбрать учетную запись и ввести PIN-код устройства.

Пользователь проходит аутентификацию в домене или ОС на основе данных, размещенных в защищенной памяти устройства: сложного пароля или ключевой пары.

Продукт позволяет настроить политику ОС при отключении устройства от ПК:

- вызов экрана блокировки;

i В этом случае для возобновления доступа пользователю необходимо снова подключить устройство к ПК и ввести PIN-код токена.

- продолжение активной пользовательской сессии.

Помимо совместимости rtlogon с системными экранами входа и блокировки ОС, в продукте также предусмотрены собственные экраны входа и блокировки ОС, обеспечивающие следующие возможности:

- выбор подключенного ключевого носителя;
- отображение присутствия/отсутствия учетной записи на ключевом носителе;
- обеспечение возможности введения PIN-кода пользователя и входа в учетную запись;
- обеспечение возможности входа с помощью простого пароля (1ФА), если это разрешено политикой входа;
- управление питанием ПК (выключение/перезагрузка);
- управление сетевыми подключениями (проводные и Wi-Fi);
- выбор графической оболочки ОС;
- интерактивная смена PIN-кода пользователя в случае обнаружения PIN-кода по-умолчанию;
- разблокировка пользовательского PIN-кода администратором в случае его блокировки;
- смена пользователя (с завершением/без завершения активной сессии);
- использование темной темы для экранов входа и блокировки.

i Все возможности продукта подробно описаны в Руководстве администратора и Руководстве пользователя.

Ограничения

- На ОС Astra 1.8 требуется использовать системные экраны входа и блокировки ОС.
- Графическое окружение GNOME не поддерживается для экранов приветствия и блокировки `rtlogin`. Для работы с GNOME необходимо использовать системный экран GDM.
- Для снятия блокировки PIN-кода токена JaCarta ГОСТ, необходимо использовать ПК "Единый Клиент JaCarta".
- Если при настроенной на контроллере домена политике входа только по сертификату, выполнить вход в доменную учетную запись по логину и паролю, то возникает ошибка: "Неверный логин или пароль" вместо ожидаемого "Вход возможен только по сертификату".

Известные проблемы

- После удаления локальной учетной записи из ОС, токен отображается как доступный для входа, но выполнить вход по нему невозможно.
- Удаление и добавление языков ввода не отражается на экранах входа и блокировки.

Интерфейс продукта

Двухфакторная аутентификация (2ФА) при входе в ОС через экран входа rtlogin

Параметры входа

Логин и пароль

Рутокен ЭЦП 3.0
1157465133

Рутокен ЭЦП 3.0
1076781970

РУТОКЕН

Рутокен ЭЦП 3.0 1157465133

user

●●●●●●●●●●

Продолжить

Однофакторная аутентификация (1ФА) при входе в ОС

Параметры входа

Логин и пароль

Рутокен ЭЦП 3.0
1157465133

Рутокен ЭЦП 3.0
1076781970

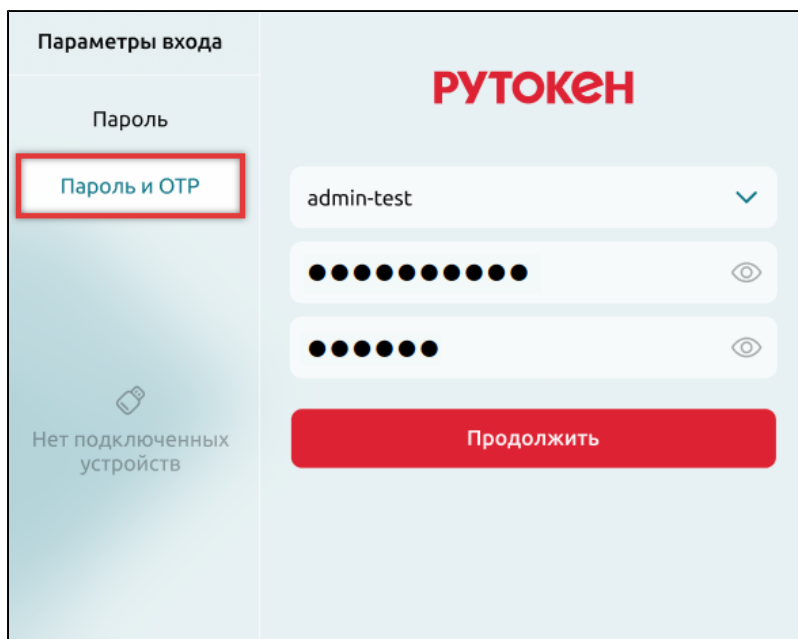
РУТОКЕН

admin

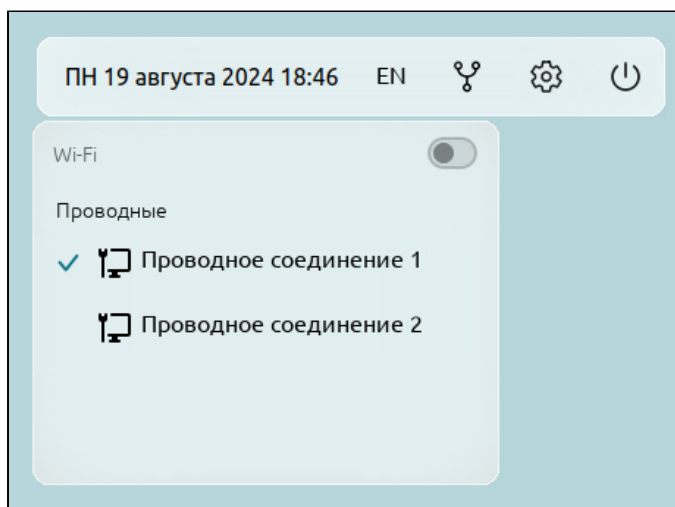
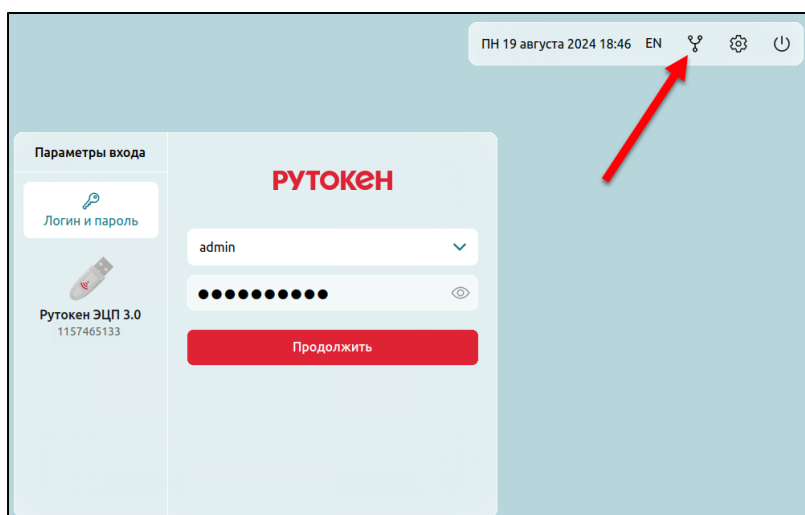
●●●●●●●●●●

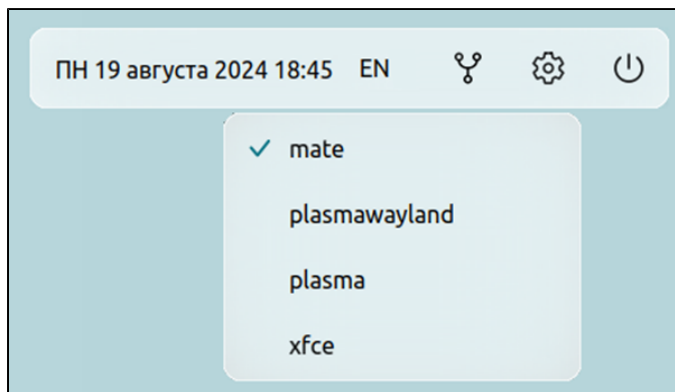
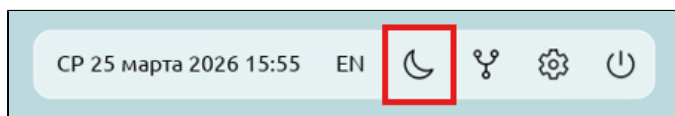
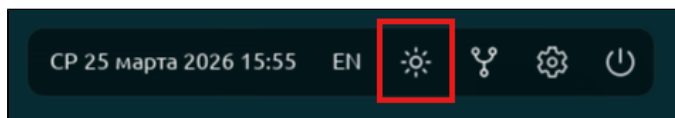
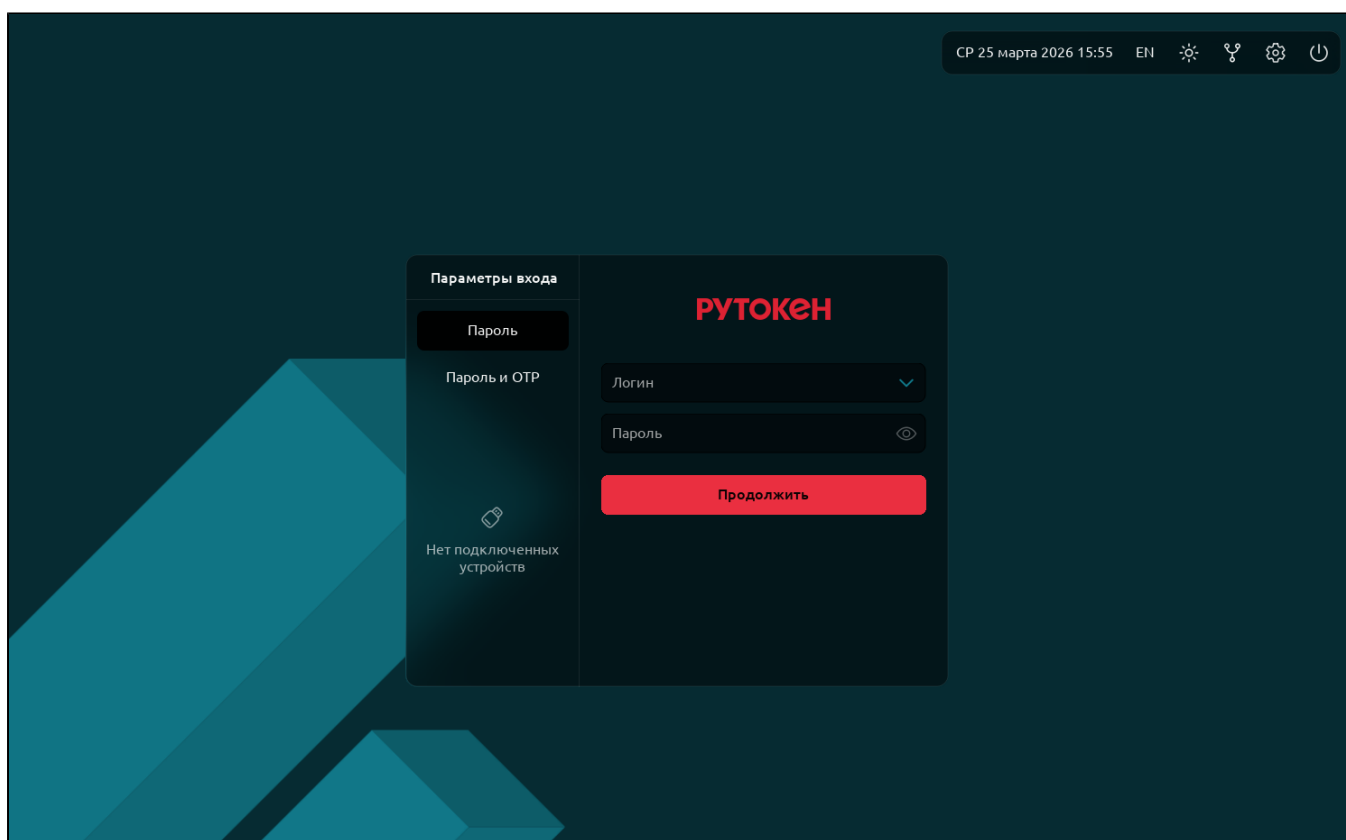
Продолжить

2ФА по паролю и OTP при входе в ОС

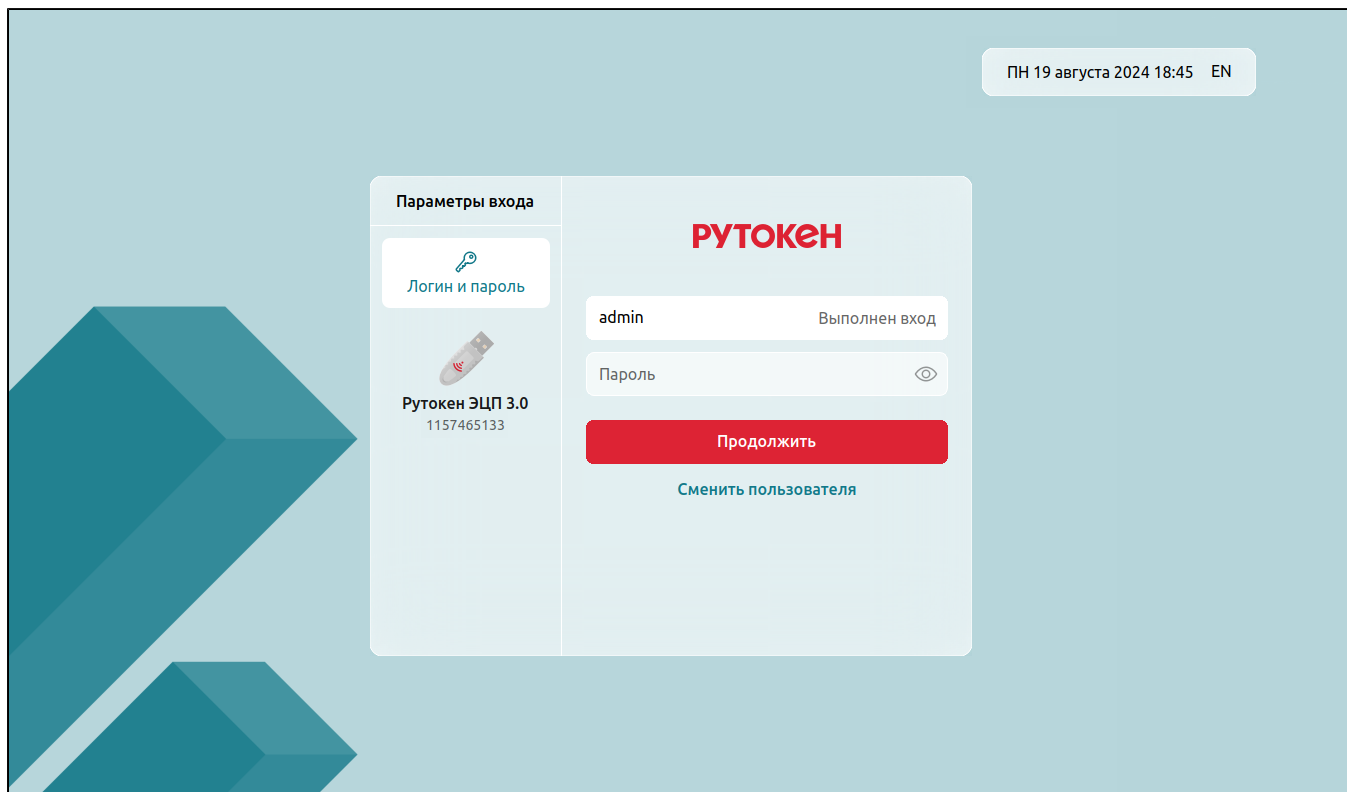


Инструмент управления сетевыми подключениями

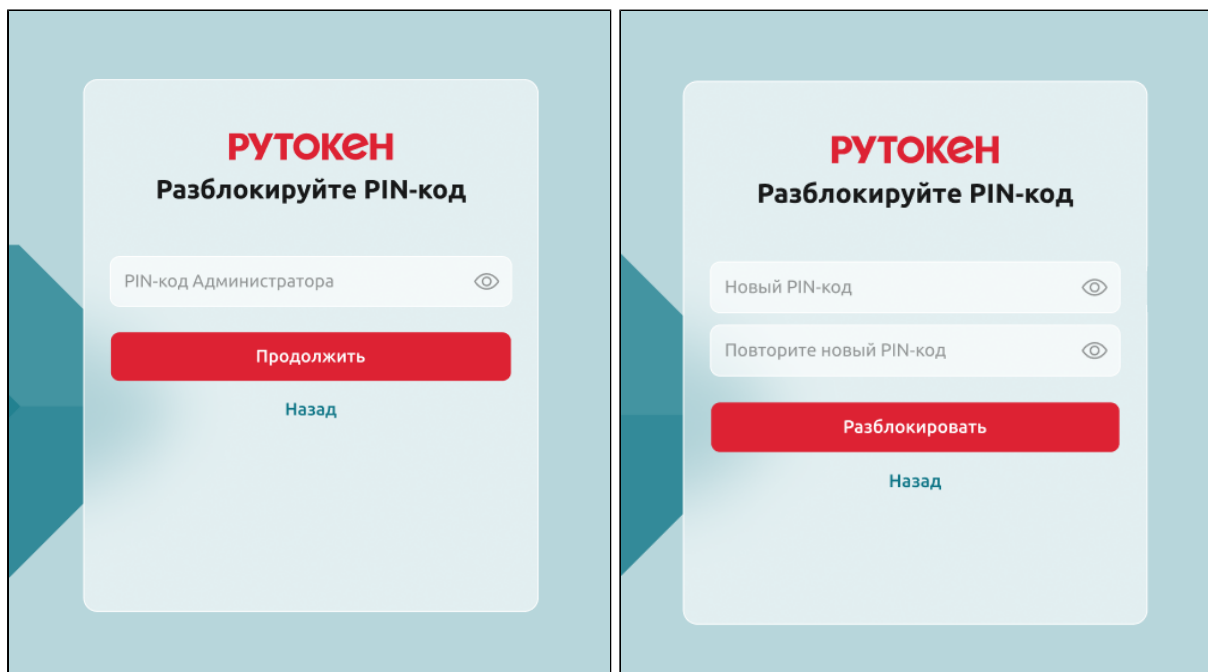


Смена среды рабочего стола*Переключение на темную тему**Переключение на светлую тему**1ФА при входе в ОС. Выбрана темная тема интерфейса rtlogon*

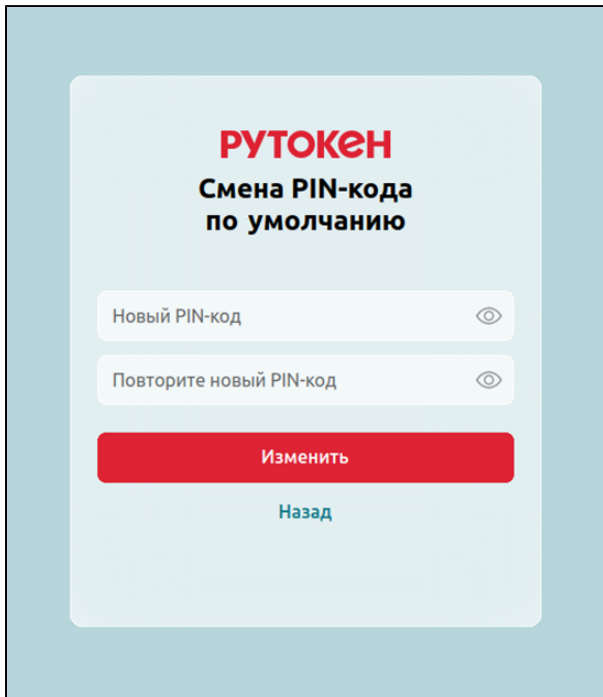
Экран блокировки сессии



Разблокировка пользовательского PIN-кода



Окно для смены PIN-кода по умолчанию



РУТОКЕН
Смена PIN-кода по умолчанию

Новый PIN-код

Повторите новый PIN-код

Изменить

[Назад](#)

Командно-строчный интерфейс

```
Файл  Правка  Вид  Поиск  Терминал  Помощь
[admin@localhost ~]$ rtlogon-cli
Usage:
  rtlogon-cli <command> [options]

Supported commands:
  configure
    Setting up a system to work with tokens using two-factor authentication
  reconfigure
    Edit the system's two-factor authentication settings
  unconfigure
    Return the system to original state. Disable two-factor authentication
  setup-auth
    Setting up two-factor authentication for users
  create-cert
    Create a self-signed certificate or certificate signing request
  unsetup-auth
    Disable two-factor authentication for users
  change-pin
    Changing the PIN-code on the token
  collect-log
    Collecting system logs and configuration files
  info
    Show application configuration and account records on the PC and tokens

General options:
  --version
    Show current version string of rtlogon
  -h [ --help ]
    Show help message. Use '<command> -h' to show help message for specific command.
```