РУТОКЕН

Рутокен Логон для Linux. Версия 1.0.0. Примечания к выпуску (Release Notes)

© 2025 Компания «Актив»

Название продукта: Рутокен Логон для Linux

Версия продукта: 1.0.0

Дата релиза: 5 ноября 2025 г.

Статус продукта: первый коммерческий релиз

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 учётной 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.

Поддерживаемые устройства

- Рутокен Lite;
- устройства Рутокен ЭЦП 2.0;
- устройства Рутокен ЭЦП 3.0;
- JaCarta ГОСТ;
- JaCarta PKI/ГОСТ.

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

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;
- ОС Альт 11;
- РЕД ОС 7.3;
- РЕД ОС 8.

Поддерживаемые графические окружения

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

> *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;
- РЕД АДМ 2.0.

Поддерживаемые сценарии работы

- Доменная аутентификация:
  - по сложному паролю на ключевом носителе;
  - по сертификату на ключевом носителе.
- Локальная аутентификация:
  - по сложному паролю на ключевом носителе;
  - по сертификату (ГОСТ и RSA) на ключевом носителе.

Реализованные функции

Развёртывание, настройка и управление

Развёртывание

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

- установка;
- обновление;
- удаление.

Также предусмотрены вспомогательные скрипты для массового развёртывания 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 локальной 2ФА;
- логирование событий в продукте, в том числе попыток аутентификации пользователя;
- экспорт конфигурационных файлов, лог-файлов и файлов с параметрами 2ФА.

Дополнительные возможности

- кеширование входа в доменные учетные записи;
- автоматическая блокировка сессии пользователя при извлечении ключевого носителя или после периода бездействия;
- ввод ПК в домены (ALDPro, 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 своё устройство к ПК, выбрать учётную запись и ввести PIN-код устройства.

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

Продукт позволяет настроить политику ОС при отключении устройства от ПК:

- вызов экрана блокировки;

> *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 учётной 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).

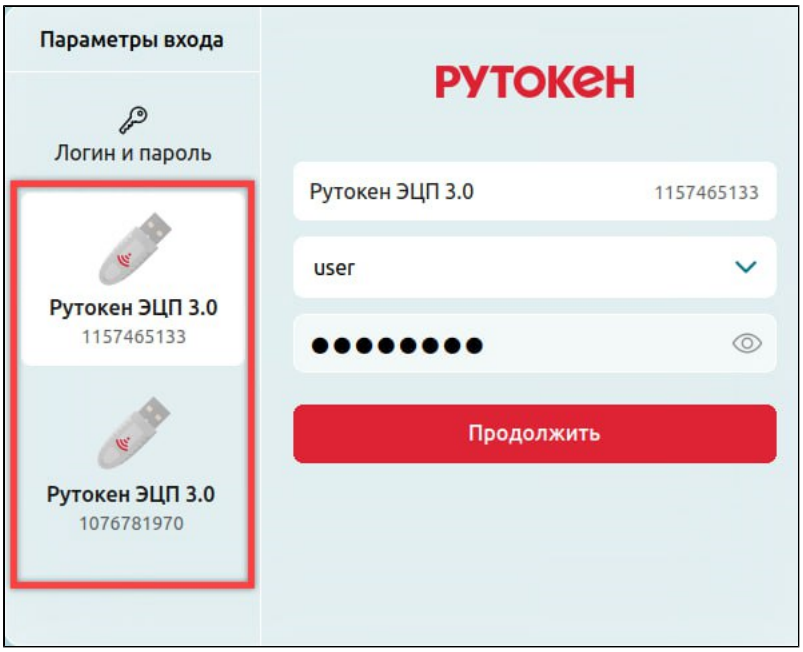
Все возможности продукта подробно описаны в Руководстве администратора и Руководстве пользователя.

Ограничения на версию

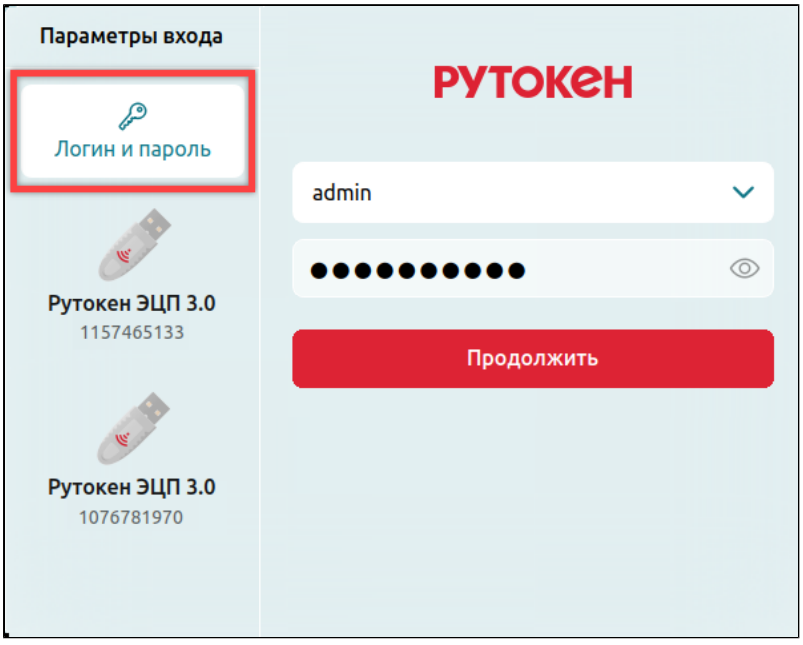
- На ОС Astra 1.8 требуется использовать системные экраны входа и блокировки ОС.
- Графическое окружение GNOME не поддерживается для экранов приветствия и блокировки rtlogon. Для работы с GNOME необходимо использовать системный экран GDM.
- Для снятия блокировки PIN-кода токена JaCarta ГОСТ, необходимо использовать ПК "Единый Клиент JaCarta".

Интерфейс продукта

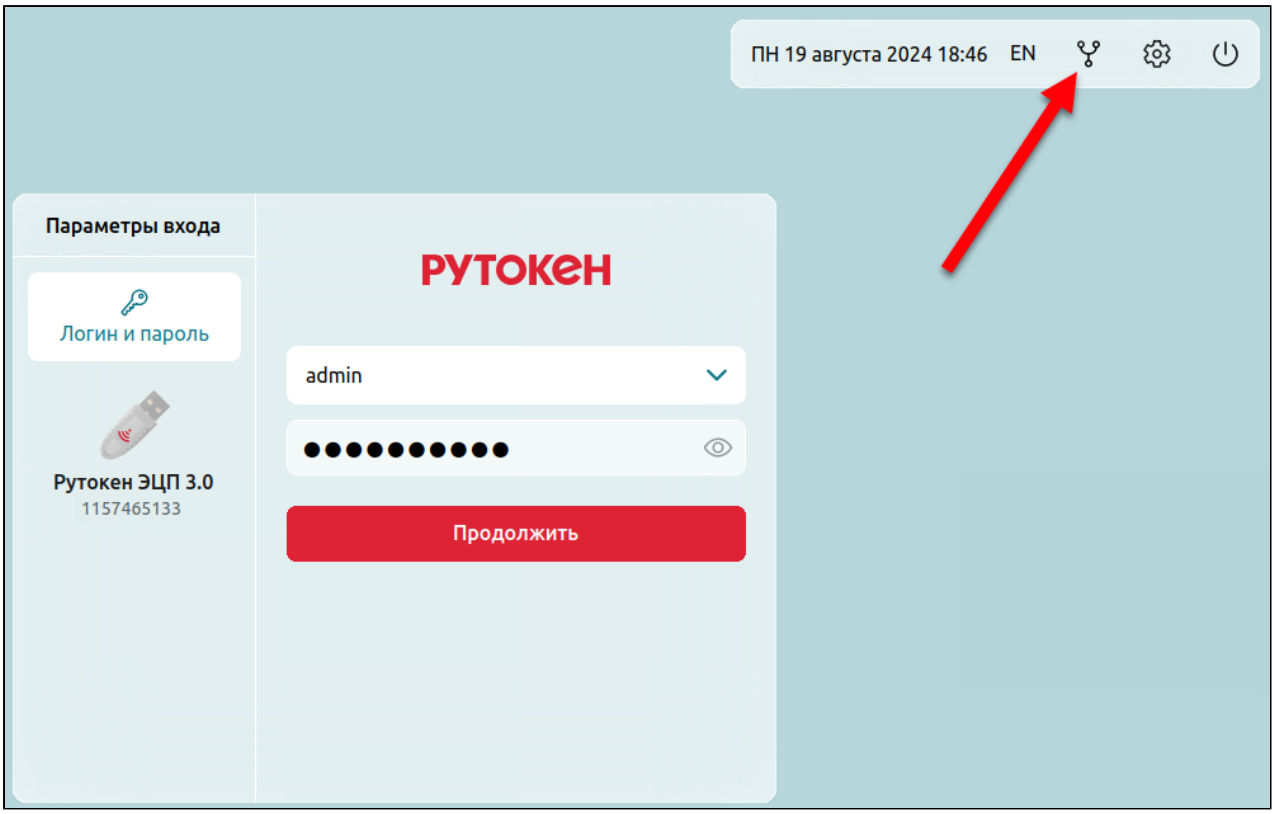
Двухфакторная аутентификация (2ФА) при входе в ОС через экран входа rtlogon

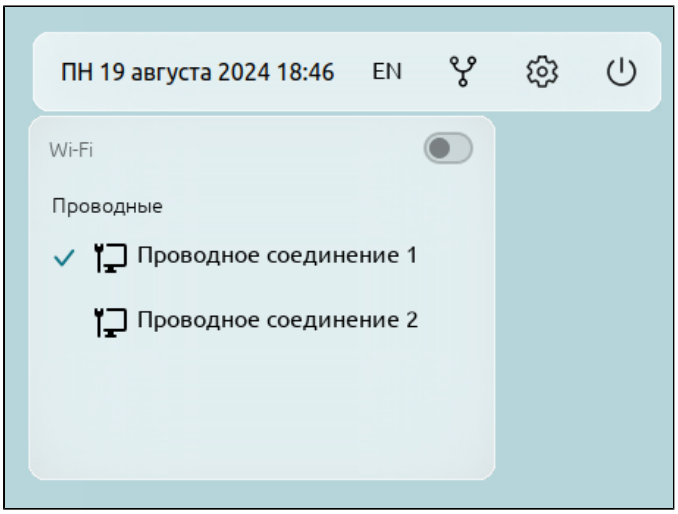


Однофакторная аутентификация (1ФА) при входе в ОС

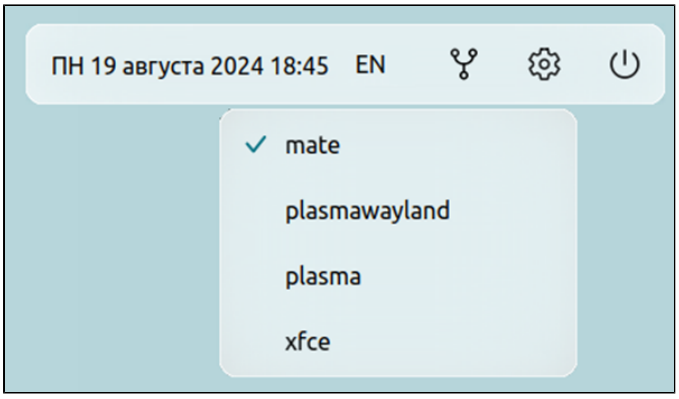


Инструмент управления сетевыми подключениями

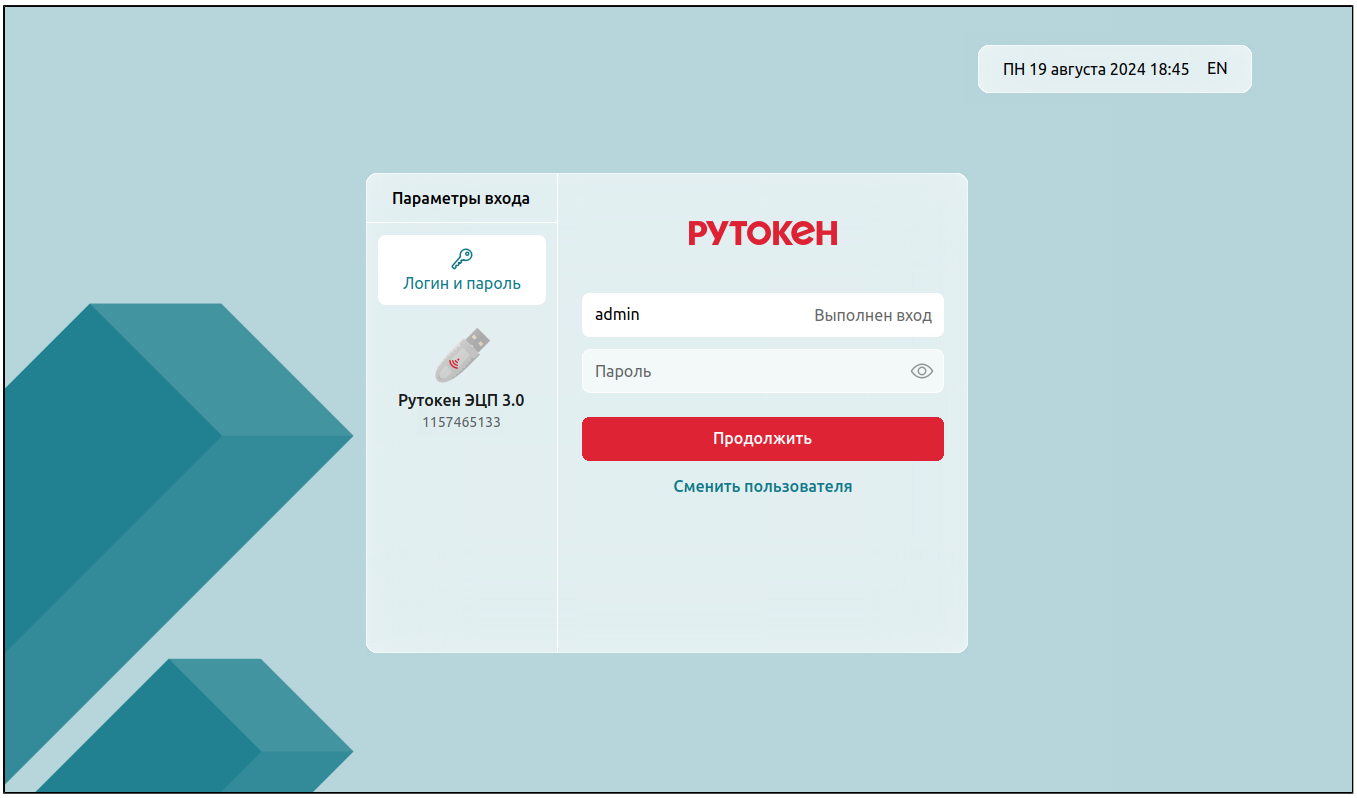




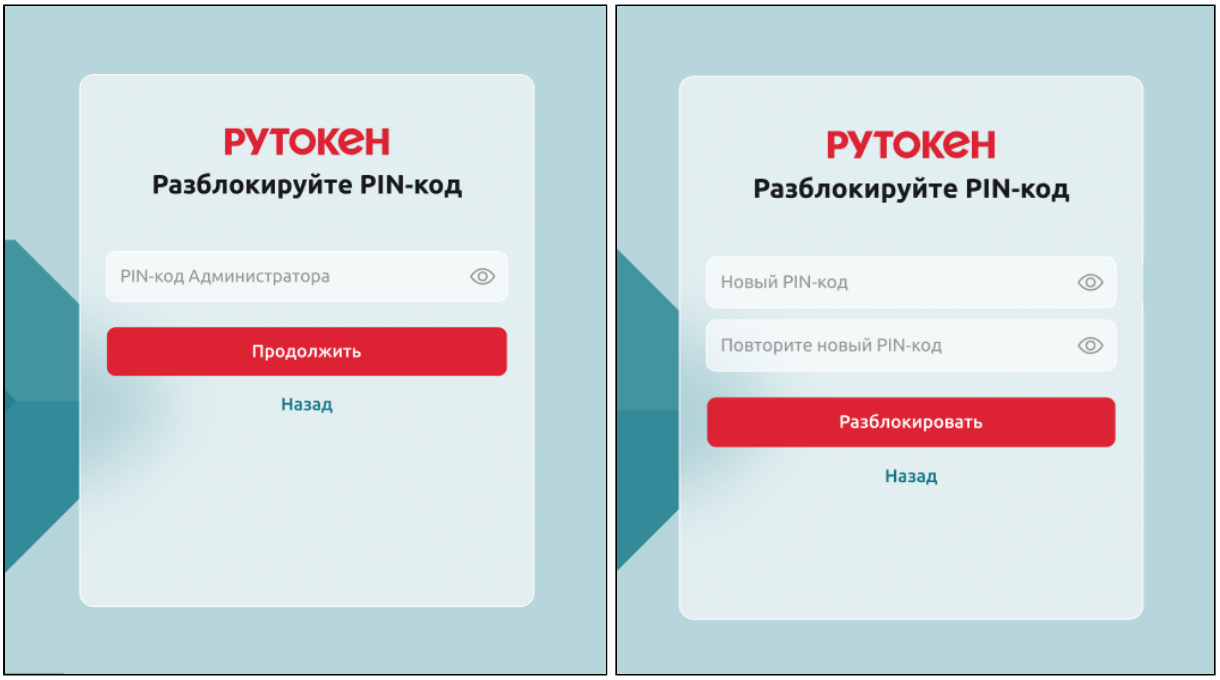
Смена среды рабочего стола



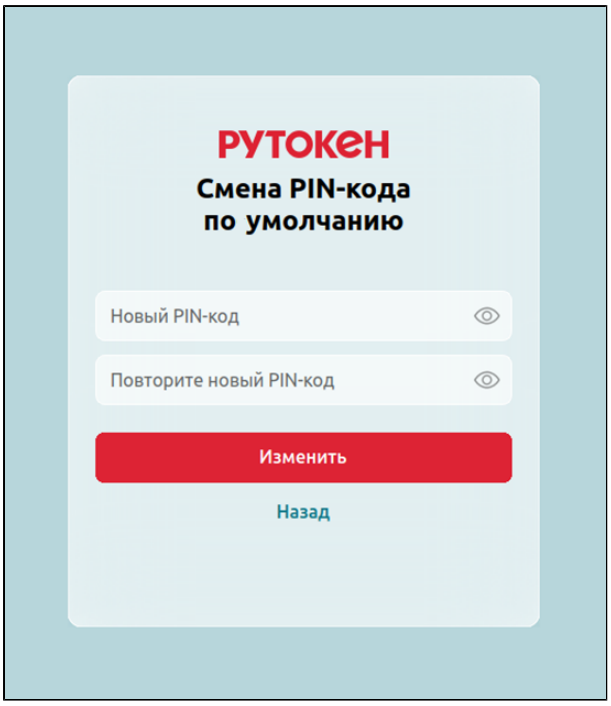
Экран блокировки сессии



Разблокировка пользовательского PIN-кода



Окно для смены PIN-кода по умолчанию



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.
```