

Simple2FA

Краткое руководство пользователя
программного обеспечения

Simple2FA

ООО «ОРБСОФТ»

Москва

2026

Введение

Данное руководство предназначено для пользователей программы ЭВМ «Simple2FA».

Руководство содержит информацию о добавлении пользователей, ресурсов и провайдеров аутентификации в Simple2FA. Так же, в руководстве описаны процессы настройки групп пользователей и анализа попыток авторизаций.

Оглавление

1. Область применения	3
2. Возможности.....	3
3. Установка компонентов во внутреннем контуре.....	3
4. Программно-аппаратное обеспечение рабочих мест.....	3
5. Вход в Simple2FA.....	4
6. Подключение к облаку Simple2FA.....	4
7. Добавление ресурса	5
8. Добавление провайдера аутентификации.....	7
9. Создание группы пользователей	8
10. Создание пользователей	9
10.1. Импорт пользователей	9
10.2. Ручное добавление пользователя.....	10
10.3. Синхронизация с каталогом	11
11. Попытки авторизации	12
12. Настройка двухфакторной аутентификации для пользователей	13
13. Информация о разработчике	15

1. Область применения

Программа для ЭВМ «Simple2FA» (далее – Simple2FA) предназначена для двухфакторной аутентификации (2FA), обеспечивающей дополнительную защиту доступа пользователей к корпоративным системам.

Система позволяет подтверждать доступ к информационным ресурсам вторым фактором аутентификации в мобильном приложении или с помощью одноразового кода. Так же, разграничивает доступ на основе ролей и выполняет журналирование событий.

2. Возможности

В Simple2FA пользователь имеет возможность:

- создавать пользователей;
- настраивать группы пользователей;
- настраивать провайдеры первого фактора;
- настраивать ресурсы;
- просматривать информации о состоянии лицензий;
- просматривать попытки авторизации пользователей.

3. Установка компонентов во внутреннем контуре

Настоящий раздел описывает порядок установки и первичной настройки компонентов Simple2FA, развёртываемых во внутреннем контуре организации.

Процесс интеграции ресурсов описан в документации на сайте Simple2FA в разделе «Настройка ресурсов»: <https://simple2fa.ru/manual/>

В поставку могут входить следующие компоненты:

- Локальный инстанс Simple2FA — локальный сервер аутентификации и управления интеграциями.
- PAM-адаптер Simple2FA — модуль MFA для SSH/SUDO на Linux через PAM.
- ADFS-адаптер Simple2FA — компонент MFA для Microsoft ADFS.
- IIS-адаптер Simple2FA — компонент MFA для веб-приложений на IIS/OWA.

Инструкцию к установке см. в файлах **README** в поставляемых дистрибутивах.

4. Программно-аппаратное обеспечение рабочих мест

Работа администратора системы Simple2FA осуществляется через веб-интерфейс, предоставляемый компонентом Local Instance, установленным в контуре информационной системы заказчика. Доступ к интерфейсу выполняется по

внутреннему сетевому адресу (домен или IP-адрес задаётся при установке Local Instance). Рекомендуемые параметры рабочего места администратора:

- Устройство с ОС MS Windows 7, 8, 8.1, 10 и выше, Mac OS X 10.9 и выше, Linux (Astra Linux 1.7 и выше, Debian 11 и выше)
- Процессор с тактовой частотой не менее 1.6 ГГц и поддержкой SSE2. Свободное дисковое пространство на компьютере не менее 2 Гб.
- Оперативная память — не менее 2 Гб.
- Свободное место на диске — не менее 1 Гб.
- Интернет-браузеры с поддержкой шифрования по ГОСТ: Internet Explorer не ниже версии 11.0, Chrome GOST, Яндекс.Браузер.
- Доступ по 443/TCP к внутреннему адресу, на котором развёрнут интерфейс Simple2FA Local Instance.

5. Вход в Simple2FA

Чтобы зайти в Simple2FA Local Instance:

1. Убедитесь, что есть соединение с Интернетом.
2. Войдите по адресу, на котором развёрнут интерфейс Simple2FA Local Instance.
3. Введите логин и пароль. Нажмите «Войти».

The image shows the login interface of Simple2FA. At the top, the text "Simple2FA" is displayed in a large, blue, sans-serif font. Below this is a horizontal blue bar. Underneath the bar, there are two input fields. The first is labeled "Имя пользователя:" in a small, grey font. The second is labeled "Пароль:" in a small, grey font. Below the password field is a blue button with the word "ВОЙТИ" in white, uppercase letters.

6. Подключение к облаку Simple2FA

Для подключения к облачному инстансу Simple2FA необходимо установить API ключ в глобальных настройках:

1. На панели слева выберите раздел «Глобальные настройки».

НАСТРОЙКИ	
Глобальные Настройки	
Группы пользователей	+ Добавить
Провайдеры аутентификации	+ Добавить
Ресурсы	+ Добавить

- В поле «API Key» укажите API ключ для подключения к облаку Simple2FA. Ключ выдается специалистами Simple2FA после обращения и регистрации организации.

Глобальные настройки

☐ Отключить 2FA

Если настройка включена, то второй фактор не будет запрашиваться вообще

☐ Отключить 2FA при
неудачном подключении
к облаку

Если настройка включена, то второй фактор не будет запрашиваться, если подключение к облаку не удалось

API ключ:

КЛЮЧ

API ключ для подключения к облаку Simple2FA

Последняя
синхронизация:

16 мая 2026 г. 4:05

Сохранить

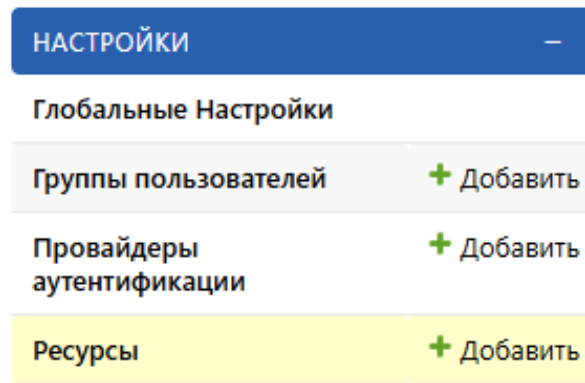
Сбросить кеш логинов

- Сохраните изменения.

7. Добавление ресурса

Для настройки взаимодействия Simple2FA с ресурсами организации:

- На панели слева выберите раздел «Ресурсы».



2. Нажмите кнопку «Добавить» в правой верхней части экрана.
3. Укажите необходимые данные:
 - Название ресурса – краткое обозначение ресурса;
 - Описание ресурса;
 - Флаг «Проверять первый фактор» – необходимость проверки первого фактора (логин и пароль) при аутентификации пользователя;
 - Флаг «Отправить ссылку на почту при подключении без настроенного 2FA» – если включен, то при попытке входа пользователя без настроенного 2FA на его почту будет отправлена ссылка на мастер настройки;
 - Протокол, по которому ресурс будет взаимодействовать с Simple2FA;
 - Порт, который будет слушать Simple2FA;
 - Флаг «Автоматическое создание пользователей» – Если настройка включена, то при первом входе пользователя после проверки первого фактора он будет автоматически создан, если не существует;
 - Группа по умолчанию - группа, которая будет назначена автоматически созданным пользователям;
 - Флаг «Использовать кеширование сессий» – если настройка включена, то после успешной авторизации у пользователя не будет запрашиваться второй фактор в течение указанного времени;
 - Длительность кэша (минуты).

Добавить ресурс

Название: Описание:

☒ Проверять первый фактор

☐ Отправить ссылку на почту при подключении без настроенного 2FA

Если включено, при попытке входа пользователя без настроенного 2FA на его почту будет отправлена ссылка на мастер настройки

Протокол: Port:

Порт, который будет слушать сервер. Для HTTP нужно указать 443, для RADIUS от 1812 до 1814. Несколько RADIUS ресурсов могут использовать один порт (различаются по NAS-Identifier)

NAS ID: RADIUS Secret:

ID NAS, на котором будет работать ресурс в случае использования RADIUS RADIUS secret, который будет использоваться в случае использования RADIUS

☐ Автоматическое создание пользователей

Если настройка включена, то при проверке пользователя через API он будет автоматически создан, если не существует

Группа пользователей по умолчанию:    

Группа, которая будет назначена автоматически созданным пользователям

☒ Использовать кеширование сессий

Если настройка включена, то после успешной авторизации у пользователя не будет запрашиваться второй фактор в течение указанного времени

Длительность кеша (минуты):

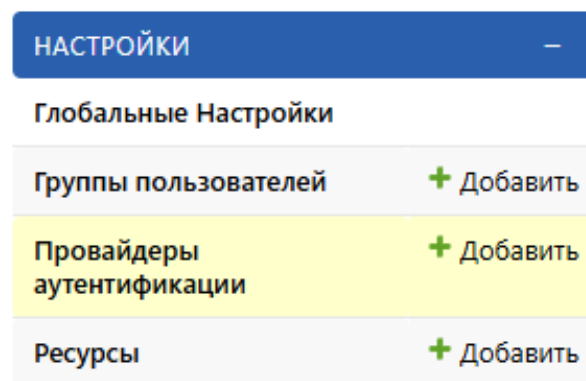
4. Сохраните изменения.

API ключ, NAS ID и RADIUS Secret генерируются автоматически.

8. Добавление провайдера аутентификации

Для настройки взаимодействия Simple2FA со службой каталогов организации:

1. На панели слева выберите раздел «Провайдеры аутентификации».



2. Нажмите кнопку «Добавить» в правой верхней части экрана.

3. Укажите необходимые данные:

- Название ресурса – краткое обозначение провайдера аутентификации;
- Провайдер аутентификации – тип провайдера аутентификации;
- Флаг «Активен» – активность провайдера аутентификации;

Далее, в зависимости от выбранного типа провайдера аутентификации, необходимо заполнить соответствующие данные для интеграции с Simple2FA.

Название:

☒ Активен

Провайдер аутентификации: LDAP ▾
Ваш провайдер аутентификации

LDAP

☒ Использовать TLS при подключении к LDAP

URL для подключения к LDAP:
Должен иметь вид: ldap://127.0.0.1:389/

Строка домена LDAP:
Строка поиска пользователя в LDAP, к примеру - dc=simple2fa,dc=test,dc=ru

Строка фильтрации LDAP:
Строка фильтрации LDAP, замените имя пользователя на {login}. Чаще всего это (&(objectClass=user)(sAMAccountName={login}))

Строка сервисного аккаунта LDAP:
Строка авторизации сервисного аккаунта LDAP, к примеру - cn=Administrator,cn=Users,dc=simple2fa,dc=test,dc=ru

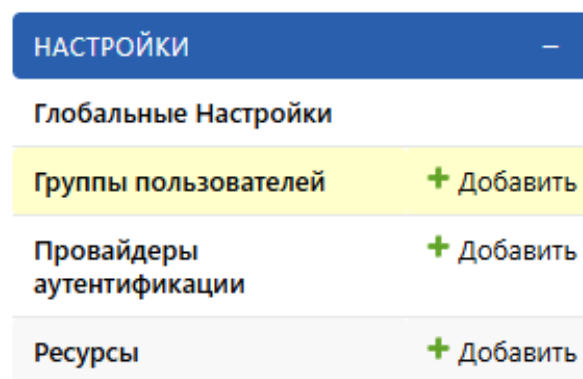
Пароль сервисного аккаунта LDAP:

4. Сохраните изменения.

9. Создание группы пользователей

Для создания группы пользователей с целью настройки групповой политики доступа:

1. На панели слева выберите раздел «Группы пользователей».



2. Нажмите кнопку «Добавить» в правой верхней части экрана.

3. Укажите необходимые данные:

- Название – краткое обозначение группы пользователей;
- Флаг «Отключить второй фактор» – отключение необходимости проверки второго фактора;
- Провайдер аутентификации – провайдер аутентификации, через который необходимо проверять первый фактор для данной группы пользователей;
- Доступные вторые факторы – доступные способы подтверждения второго фактора;

- Обязательные способы для настройки - пользователь не сможет завершить настройку, пока не подключит все указанные способы.
- Флаг «Отключить второй фактор» – при включении пользователи данной группы будут иметь доступ ко всем ресурсам;
- Доступ к ресурсам – доступен при отключении флага «Отключить второй фактор». Необходимо для выбора конкретных ресурсов, которые будут доступны для пользователей данной группы.

Изменить группу пользователей

Default group

Название: ☐ Отключить второй фактор

Провайдер аутентификации:   

Доступные вторые факторы: ☒ telegram ☒ push ☒ otp

Обязательные способы для настройки: ☐ telegram ☐ push ☐ otp

Пользователь не сможет завершить настройку, пока не подключит все указанные способы. Можно выбрать только из доступных вторых факторов.

☐ Все ресурсы
Пользователи этой группы будут иметь доступ ко всем ресурсам

Доступ к ресурсам: 

Поиск

- ☒ ADFS (HTTP)
- ☒ OWA (HTTP)
- ☒ OpenVPN (HTTP)
- ☒ OpenVPN (RADIUS)

Пользователи этой группы будут иметь доступ ко всем или указанным ресурсам

4. Сохраните изменения

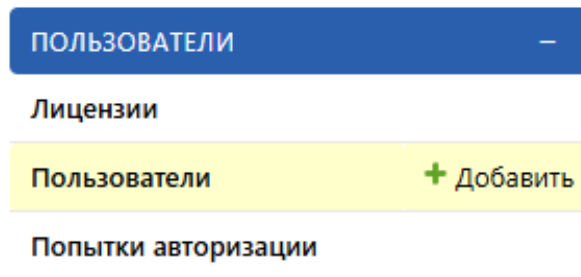
10. Создание пользователей

В Simple2FA можно добавлять пользователей вручную, импортировать их или выполнить автоматическую синхронизацию с каталогом пользователей.

10.1. Импорт пользователей

Чтобы импортировать пользователей в систему:

1. На панели слева выберите раздел «Пользователи».



2. Нажмите кнопку «Импорт» в правой верхней части экрана.
3. Укажите необходимые данные:
 - Файл для импорта – загрузка .csv файла с пользователями. Шаблон файла с заголовками можно скачать на странице.
 - Группа пользователей – группа, к которой будут относиться импортируемые пользователи;
 - Флаг «Отправить ссылку настройки 2FA» – при включении пользователям после создания будет направлена ссылка для настройки двухфакторной аутентификации.

Импорт

Файл загружать в формате CSV (Разделитель: запятая. Кодировка: UTF8) с заголовками: `login`, `email`, `name`

Файл для импорта:

Файл не выбран

Формат:
csv

Шаблон файла импорта:
[Загрузить](#)

Группа пользователей:

Default group ▼

Отправить ссылку
настройки 2FA:



4. Нажмите на кнопку «Отправить».

10.2. Ручное добавление пользователя

1. На странице «Пользователи» нажмите кнопку «Добавить» в правой верхней части экрана.
2. Укажите необходимые данные:
 - Группа пользователей – группа, к которой будет относиться создаваемый пользователь;
 - Логин;
 - Имя;

- Почта.

Группа пользователей: SAMBA_group   

Логин: user.test1

Имя: Иван

Адрес электронной почты: user.test1@mail.ru

3. Нажмите кнопку «Сохранить и продолжить редактирование».

4. Пользователь успешно создан в системе.

user.test1

Пересоздать код OTP

Пересоздать код Telegram

Пересоздать код МП

Логин: user.test1 Имя: Дмитрий

Группа пользователей: SAMBA_group    Адрес электронной почты: user.test1@mail.ru

☒ Активен ☐ Отключить второй фактор
Только для этого пользователя

Провайдер второго фактора: ----- ▾

Групповые политики

Ресурс: OpenVPN (RADIUS)

Провайдер аутентификации: Samba

Доступные провайдеры второго фактора: telegram, mobile, otp

10.3. Синхронизация с каталогом

1. На панели слева выберите раздел «Синхронизация с каталогом».

НАСТРОЙКИ

Глобальные настройки

Тема визарда

Группы пользователей + Добавить

Провайдеры аутентификации + Добавить

Ресурсы + Добавить

Синхронизация с каталогом

2. Нажмите кнопку «Добавить» в правой верхней части экрана.
3. Укажите настройки:
 - Флаг «Включена» – включает синхронизацию;
 - Интервал синхронизации (мин) – период автоматической синхронизации пользователей;
 - Маппинги атрибутов для каталогов, из которых будут считываться данные пользователей;
 - Сопоставление групп каталога.

Синхронизация с каталогом
ИСТОРИЯ

Управление сервисом синхронизации

☐ Включена
Включить сервис синхронизации с каталогом

Настройки сервиса

Интервал синхронизации (мин):
Период автоматической синхронизации пользователей. 0 — только вручную.

Таймаут запроса к каталогу (сек):

Маппинг атрибутов LDAP

Укажите LDAP-атрибуты, из которых будут считываться данные пользователей. Для почты и групп можно указать несколько атрибутов через точку с запятой.

Атрибут идентификации:

Атрибут имени:

Атрибуты почты:
Укажите один или несколько атрибутов через ";"

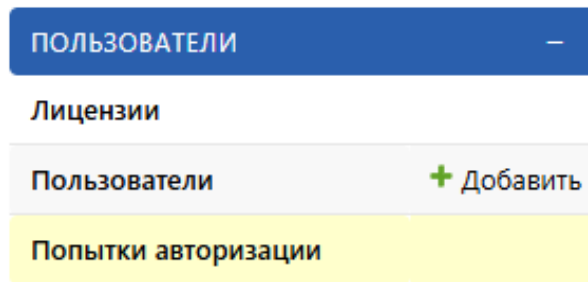
Атрибуты групп LDAP:
Укажите один или несколько атрибутов через ";"

4. Сохраните изменения.
5. Также, есть возможность моментальной синхронизации. Для этого необходимо нажать кнопку «Синхронизировать сейчас».

11. Попытки авторизации

Simple2FA позволяет просматривать все попытки авторизации пользователей. Для просмотра попыток авторизации:

1. На панели слева выберите раздел «Попытки авторизации».



2. Откроется страница со списком попыток авторизации.

Попытки авторизации

Действие: Выполнить Выбрано 0 из 100

☐	ПОЛЬЗОВАТЕЛЬ	ДАТА И ВРЕМЯ	РЕСУРС	СПОСОБ	IP	УСПЕШНО
☐	artyom.s	15 мая 2026 г. 18:44	ADFS	telegram	195.19.224.238	✓
☐	artyom.s	15 мая 2026 г. 18:43	ADFS	-	195.19.224.238	✗
☐	artyom.s	15 мая 2026 г. 18:43	ADFS	telegram	195.19.224.238	✗
☐	artyom.s	15 мая 2026 г. 18:39	ADFS	telegram	195.19.224.238	✗
☐	artyom.s	15 мая 2026 г. 18:38	ADFS	-	195.19.224.238	✗
☐	gorbunov	15 мая 2026 г. 12:41	ADFS	push	194.156.201.115	✓
☐	gorbunov	15 мая 2026 г. 12:41	ADFS	push	194.156.201.115	✗
☐	gorbunov	15 мая 2026 г. 12:40	ADFS	push	194.156.201.115	✗
☐	gorbunov	15 мая 2026 г. 12:39	ADFS	push	194.156.201.115	✓
☐	gorbunov	15 мая 2026 г. 12:38	ADFS	push	194.156.201.115	✗
☐	gorbunov	15 мая 2026 г. 12:37	ADFS	push	194.156.201.115	✓
☐	gorbunov	15 мая 2026 г. 12:32	ADFS	push	194.156.201.115	✓
☐	gorbunov	15 мая 2026 г. 12:22	ADFS	push	194.156.201.115	✓

12. Настройка двухфакторной аутентификации для пользователей

Настройка двухфакторной аутентификации выполняется пользователями самостоятельно через встроенный мастер настройки (Wizard).

При первом входе пользователя в защищаемый ресурс Simple2FA проверяет, настроен ли второй фактор. Если второй фактор ещё не подключён и используемый ресурс поддерживает отображение экрана мастера настройки, пользователь автоматически перенаправляется на Wizard.

В мастере настройки пользователь:

- выбирает способ второго фактора;
- привязывает мобильное устройство;
- завершает активацию двухфакторной аутентификации.

Поддерживаются следующие методы второго фактора:

- Push-уведомления в мобильном приложении;
- TOTP-коды;
- Telegram-бот.

Если ресурс не поддерживает отображение мастера настройки, пользователю может быть направлена ссылка для самостоятельного подключения второго фактора. Ссылка может отправляться:

- вручную администратором со страницы просмотра информации о пользователе;

- автоматически при создании пользователя.

После успешного завершения настройки пользователь может продолжить вход в систему с использованием двухфакторной аутентификации.

13. Информация о разработчике

Программа для ЭВМ «Simple2FA»

ООО «ОРБСОФТ»

Россия, Москва, р-н Троицк, д. Станиславль, 13

Телефон: (495) 150-80-59

E-mail: info@orbsoft.ru