Мультифактор. Обзор технологии.

Защитите свой бизнес с Мультифактором

О компании ActiveCloud

IaaS BaaS SaaS PaaS

Поставляем облачные решения для размещения корпоративных систем, приложений и сайтов, услуги по аудиту и миграции в облако, информационной безопасности, проектированию и техническому сопровождению облачных решений.

- 20+ лет на рынке
- CAGR 35%
- Собственная команда R&D
- Геораспределенные ЦОД Tier III в РФ и РБ
- SLA 99,95%
- RTO <15 минут
- Техподдержка 24/7 с выделенным номером
- Собственная платформа автоматического предоставления облачных сервисов, работающая круглосуточно
- 30000+ пользователей наших сервисов
- Тестовый период

Что такое Мультифактор?

Это сервис многофакторной аутентификации и контроля доступа для всех ваших удаленных подключений (RDP, VPN, VDI, SSH).

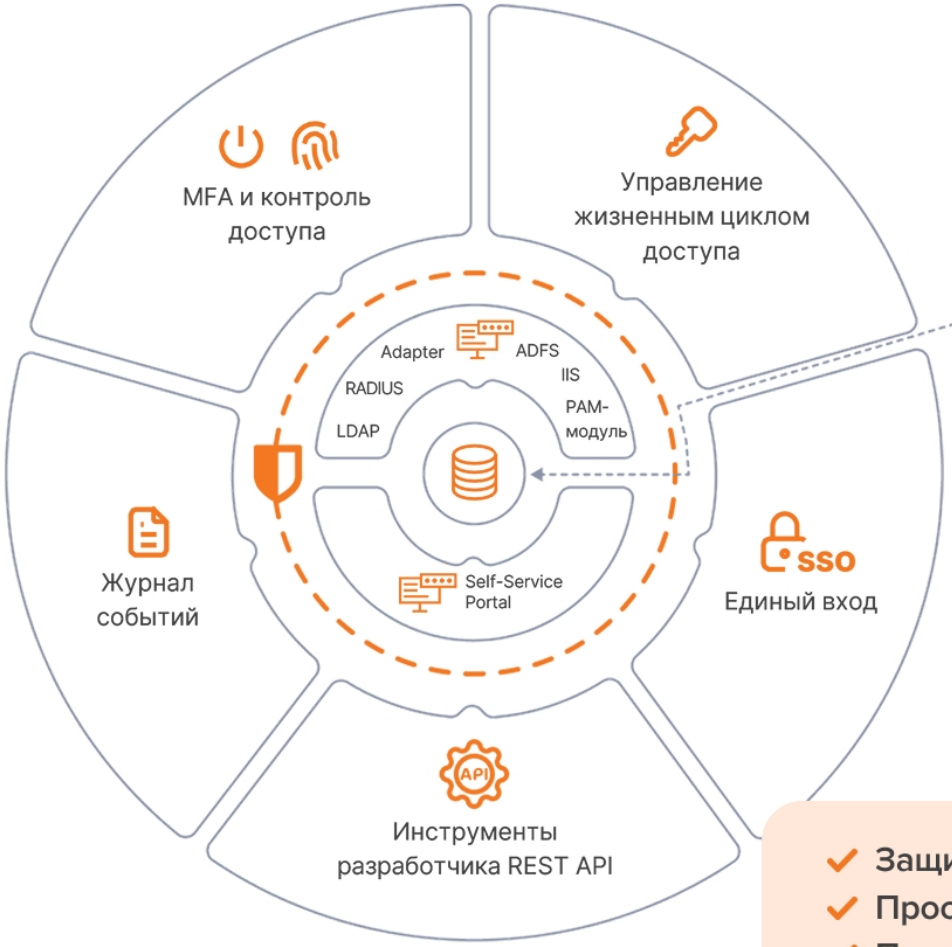
Почему он необходим вашему бизнесу?

1. **Блокировка злоумышленников**
   Даже если пароль украден, доступ останется под контролем.
2. **Безопасность данных и защита процессов**
   Защитите конфиденциальную информацию компании и клиентов, обезопасив входы, смены паролей и восстановление доступа.
3. **Обнаружение несанкционированного доступа**
   Отслеживайте подозрительную активность, включая попытки входа от бывших сотрудников.
4. **Повышение лояльности пользователей**
   Обеспечьте безопасную и удобную работу для ваших сотрудников.
5. **Контроль доступа**
   Узнайте, кто, когда и откуда подключается к вашей сети.
6. **Удобство и безопасность**
   Подключайтесь к рабочему месту по отпечатку пальца прямо с вашего ноутбука.

Сотрудники

Партнёры

Клиенты



Провайдер учётных записей

- MultiDirectory – служба каталогов от МУЛЬТИФАКТОР
- Active Directory
- Linux Astra Directory
- NPS
- Samba 4
- Freeipa

- ✓ Защита входа
- ✓ Простая интеграция
- ✓ Покрытие всей инфраструктуры

Защищаемые ИТ-системы

VPN-шлюзы

- UserGate
- C-Терра
- КриптоПро NGate
- Континент 4
- Ideco UTM
- Рубикон
- CheckPoint
- Cisco
- FortiGate
- Mikrotik
- OpenVPN

Linux

- SSH
- SUDO
- OpenVPN
- PAM
- и др.

Windows

- Windows Logon
- VPN
- RD Gateway
- NPS
- и др.

SIEM-системы

Multifactor совместим с SIEM-системами благодаря поддержке стандартных протоколов.

Облака, виртуализация, веб

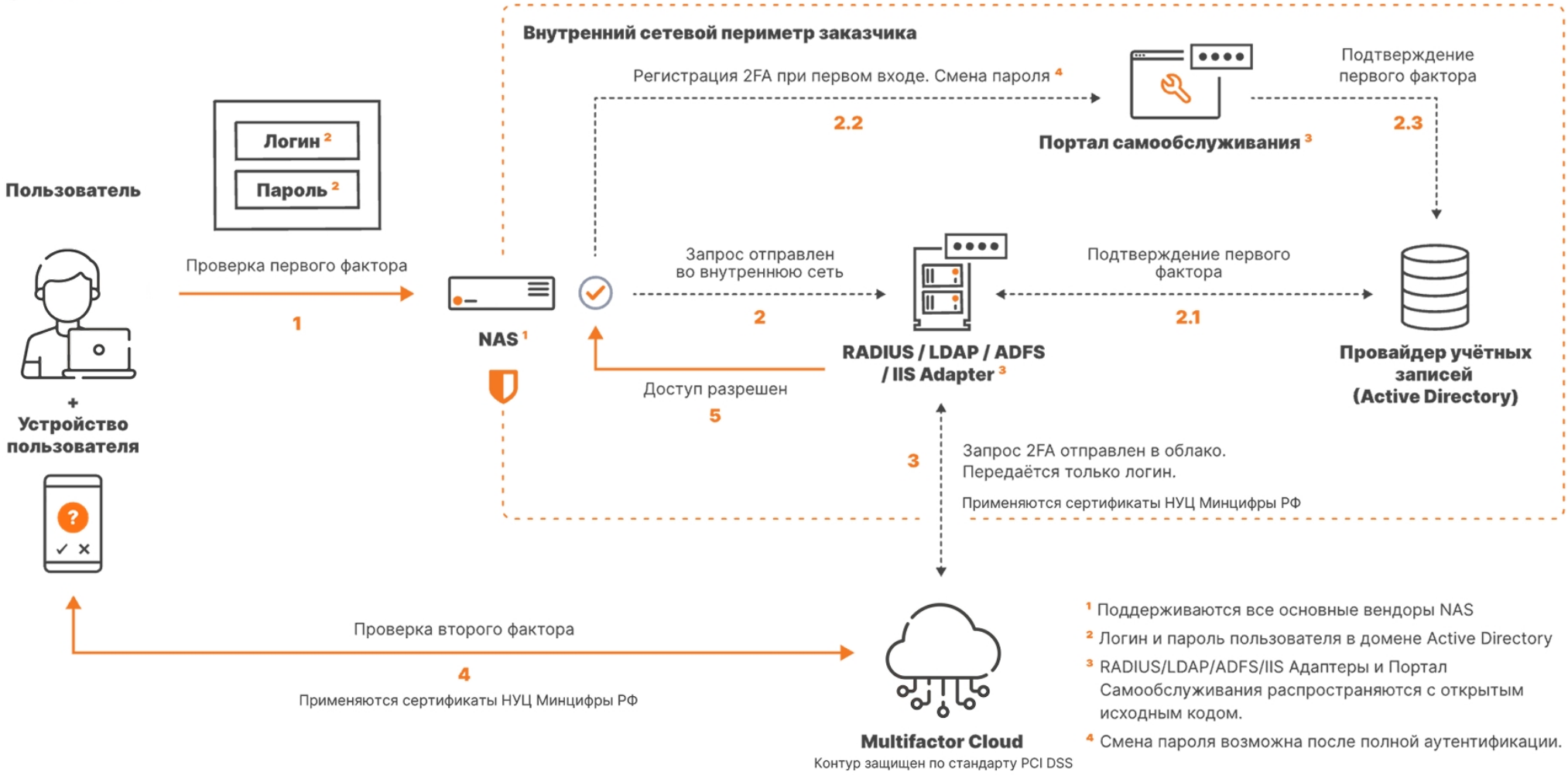
- SAML
- OIDC
- OAuth-приложения
- Outlook Web Access (OWA)
- Huawei Cloud
- Яндекс.Облако
- VMware
- Веб-сайты
- Мобильные приложения

VDI

- VMware Horizon
- Citrix
- Remote Desktop

Другое ПО

- СКДПУ АйТи-Бастион
- 1С-Bitrix24
- Точки доступа Wi-Fi
- Все Desktop-приложения



[1] Поддерживаются все основные вендоры NAS

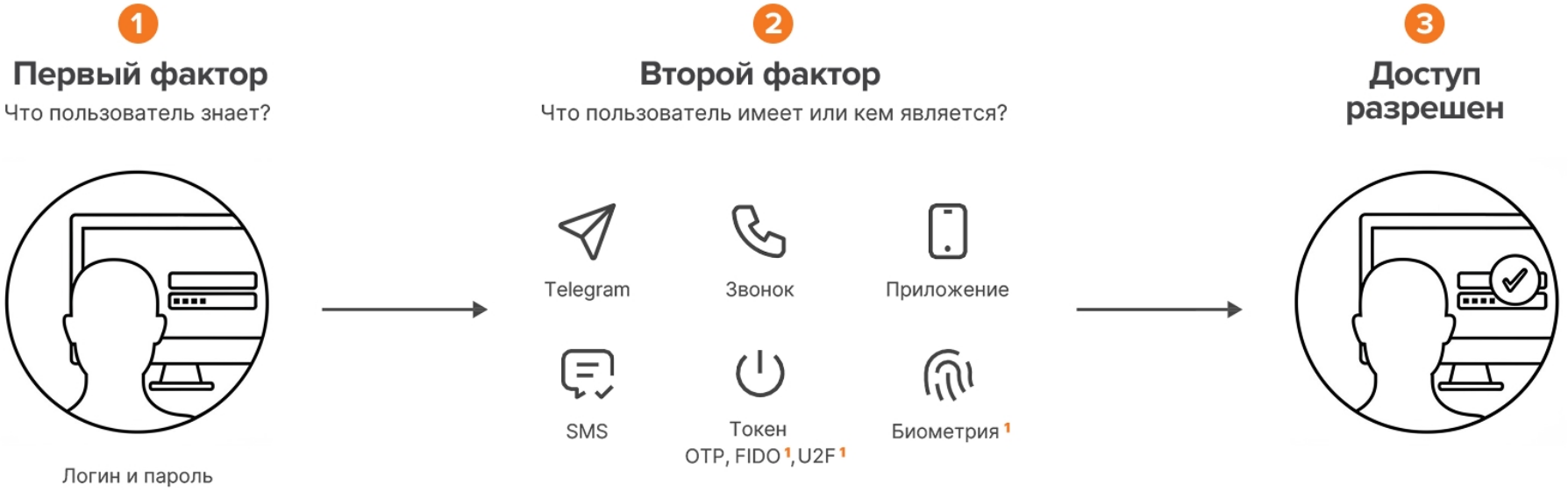
[2] Логин и пароль пользователя в домене Active Directory

[3] RADIUS/LDAP/ADFS/IIS Адаптеры и Портал Самообслуживания распространяются с открытым исходным кодом.

[4] Смена пароля возможна после полной аутентификации.

Мультифакторная аутентификация

Пользователи могут подтвердить свою личность тем, что они знают (основной метод аутентификации, как правило, логин и пароль); тем, что у них есть (например, аппаратный или программный токен); тем, кем они являются (биометрия). Последние два — возможные способы проверки второго фактора.



1 FIDO, U2F токены и биометрия недоступны в конфигурации с межсетевыми экранами NAS (Checkpoint, Cisco, Mikrotik и др.) и VDI.

Методы

В таблице представлены 6 основных методов проверки второго фактора, поддерживаемых Мультифактором, в зависимости от сценария использования.

	VPN и VDI	Linux инфраструктура	Windows инфраструктура	Облачные приложения (SAML)	API (Web)
Мобильное приложение Multifactor	✓	✓	✓	✓	✓
Telegram-бот Multifactor	✓	✓	✓	✓	✓
SMS или звонок	✓	✓	✓	✓	✓
OTP токены (аппаратные, и программные)	✓	✓	✓	✓	✓
U2F/FIDO токены				✓	✓
Биометрия				✓	✓

Портал самообслуживания

Позволяет пользователям Active Directory и других LDAP-каталогов самостоятельно настраивать и подтверждать второй фактор доступа, менять пароль после полной аутентификации. Поддерживает управление устройствами Exchange ActiveSync. Компонент с открытым исходным кодом для Windows и Linux.

Самостоятельный онбординг пользователей

Самостоятельная конфигурация 2FA

Самостоятельное восстановление паролей пользователями[1]

Решение проблем с доступом без участия IT-поддержки

Базовые требования:

- 1 ядро CPU
- 2Gb RAM
- Windows Server 2012 и выше

1 При условии прохождения предварительной аутентификации в мобильном приложении Multifactor.

Управление облачными приложениями в компании

С ростом компании увеличивается количество различных приложений, пользователей и устройств, распределённых по разным географическим локациям. IT и команды безопасности должны обеспечить доступ к приложениям для защиты корпоративных данных, одновременно упрощая этот доступ для сотрудников, чтобы поддерживать их продуктивность.

- Облачные приложения
- Собственные приложения
- Мобильный клиент Outlook
- OWA
- Windows-среда
- SAML 2.0 приложения
- Интеграция с Keycloak
- Веб - приложения
- Linux-среда

Проблемы управления

1 Затраты на поддержку

Мультипликация учетных данных в облачных сервисах и системах идентификации.

Неэффективный процесс онбординга и офбординга пользователей, требующий дополнительных ресурсов от сотрудников.

2 Продуктивность сотрудников

Запоминание паролей, их учет и соответствие множеству паролей и политик.

Необходимость использования сторонних инструментов (например, аппаратных токенов, VPN), что снижает эффективность сотрудников.

3 Угрозы безопасности

Неотозванные доступы сотрудников.

Проблемы с безопасностью учетных данных и подключений.

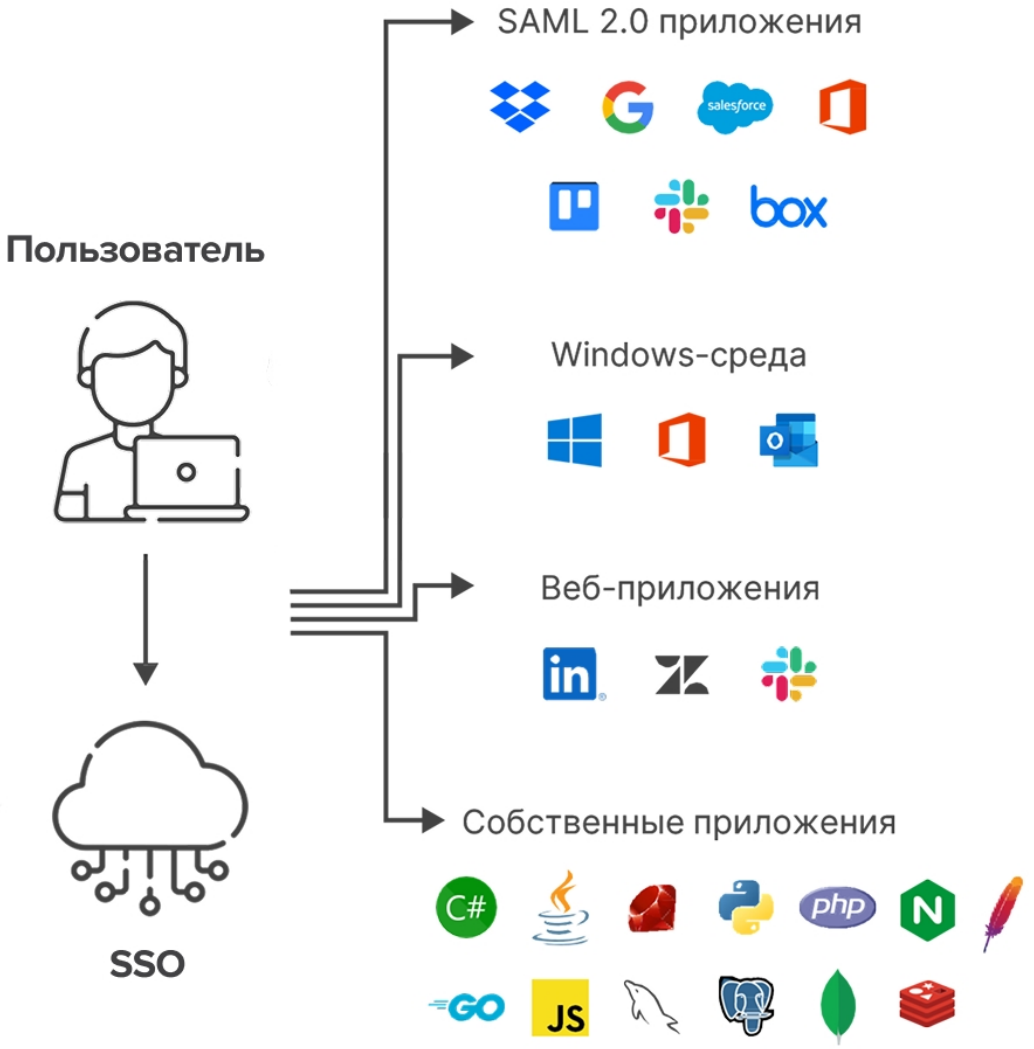
Единый вход SSO

Удобный и безопасный доступ к корпоративным приложениям с поддержкой второго фактора аутентификации.

1. **Снижение затрат**
   Единый провайдер учетных записей упрощает управление пользователями, предоставляя доступы согласно должностям.
2. **Улучшенный пользовательский опыт**
   Не нужно запоминать множество паролей – смена пароля во всех сервисах всего в пару кликов.
3. **Повышенная безопасность**
   Второй фактор аутентификации во всех системах, независимо от их возможностей.
4. **Гибкие парольные политики**
   Парольные требования определяет провайдер учетных записей, а не сторонние системы.
5. **Рост продуктивности**
   Простое управление доступами и кадровыми изменениями в организации.
6. **Быстрая интеграция**
   Подключение новых приложений к инфраструктуре компании занимает меньше времени.

Единый вход SSO

Удобный и безопасный доступ к корпоративным приложениям с поддержкой второго фактора аутентификации.



Компоненты On-Premise

Портал самообслуживания

- Самостоятельная регистрация 2-ого фактора аутентификации в Multifactor Cloud.
- Смена пароля в корпоративном Active Directory с проверкой пароля и подтверждением 2-ым фактором в Multifactor Cloud.
- Компонент с открытым исходным кодом для Windows и Linux.

Требования для Windows:

- ✓ 1 ядро CPU ✓ 2Gb RAM
- ✓ Windows Server 2012 и выше

Для Linux:

- ✓ 1 Linux-сервер, протестирован на Debian 11

RADIUS, LDAP, ADFS, IIS Адаптеры

- Обработка запросов на аутентификацию в Check Point VPN, RDP и Citrix по стандартным протоколам.
- Проверка первого фактора (логин и пароль) в корпоративном домене.
- Проверка второго фактора в Multifactor Cloud.
- Компоненты с открытым исходным кодом для Windows и Linux.

Требования для Windows:

- ✓ 4 ядра CPU ✓ 4Gb RAM
- ✓ Windows Server 2012 и выше

Для Linux:

- ✓ 1 CPU ✓ 2Gb RAM ✓ 8Gb HDD

Облако Multifactor

Безопасное размещение в ДЦ DataLine, Selectel и LinxCloud

- Двухфакторная аутентификация – подтверждение и подпись запросов пользователей.
- Личный кабинет IT-службы для управления и контроля доступа.
- Журнал событий для мониторинга активности.
- API и инструменты разработчика для интеграции.

SLA

- ✓ Аптайм 99.99%
- ✓ Тех. поддержка

multifactor.ru

Режимы 2FA

Автоматический

Регистрация СМС в качестве второго фактора доступа (синхронизация телефонных номеров с Active Directory).

- Пользовательский опыт
- Простота интеграции
- Скорость подключения

Вручную

Администраторы вручную добавляют или импортируют пользователей и рассылают регистрационные ссылки на email.

- Пользовательский опыт
- Простота интеграции
- Скорость подключения

Режим самообслуживания

1. **Диалог с пользователем**

   Настройка второго фактора в режиме диалога в VPN/VDI клиенте или в API/SAML интерфейсе Мультифактор при первом подключении.

   - Пользовательский опыт
   - Простота интеграции
   - Скорость подключения

2. **Портал самообслуживания**

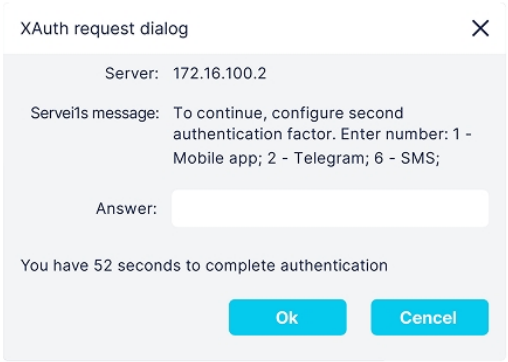
   В этом сценарии необходимо подготовить и разослать пользователям инструкцию.

   - Пользовательский опыт
   - Простота интеграции
   - Скорость подключения

Регистрация в режиме диалога с пользователем

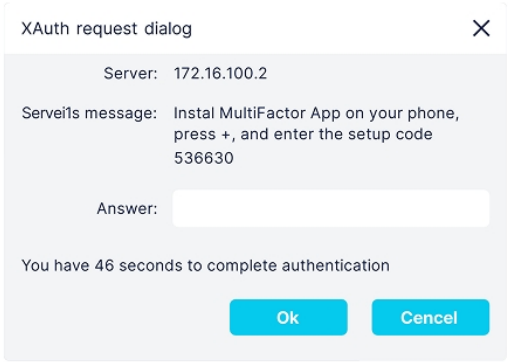
1 Выбор фактора

Пользователь выбирает удобный ему способ двухфакторной аутентификации из преднастроенного списка[1], вводя необходимую цифру.



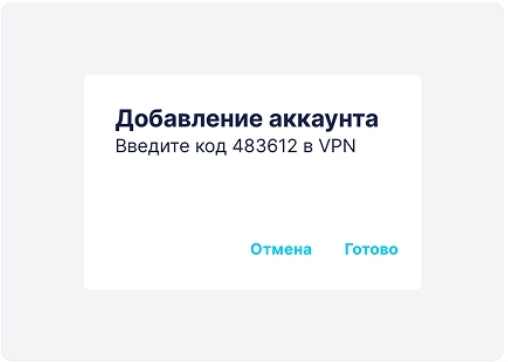
2 Привязка фактора

Клиент сообщает пользователю код, который ему необходимо ввести в приложении или Telegram-боте Multifactor.



3 Подтверждение владения

Пользователь подтверждает владение фактором, вводя код из Telegram, мобильного приложения Multifactor или СМС обратно в клиент.



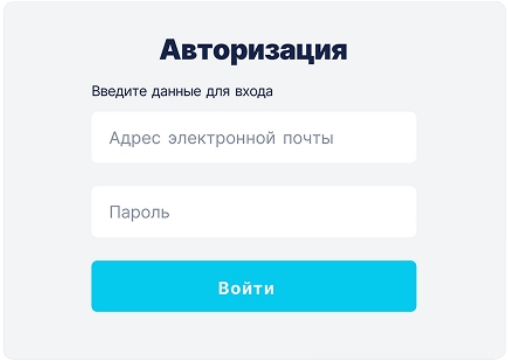
✔ Регистрация второго фактора завершена. Вход дополнительно защищён вторым фактором.

1 Telegram, СМС, Приложение Multifactor в случае защиты VPN и VDI соединений.

Регистрация на портале самообслуживания

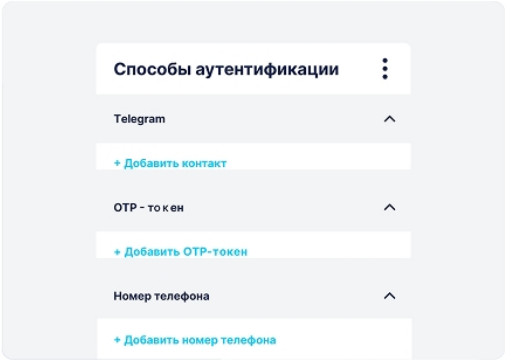
1 Первое подключение

Пользователь проходит аутентификацию на Портале Самообслуживания (учетные данные Active Directory).



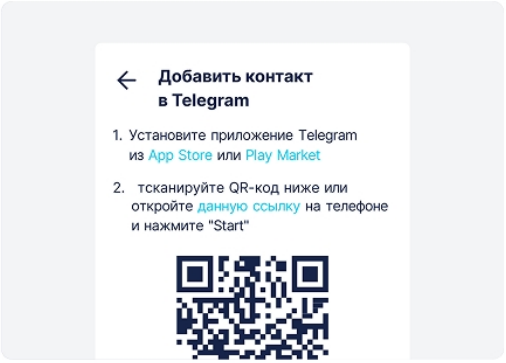
2 Выбор фактора

Пользователь выбирает удобный ему способ двух-факторной аутентификации из преднастроенного списка[1]



3 Подтверждение владения

Пользователь подтверждает владение фактором[2].



✔ Регистрация второго фактора завершена. Вход дополнительно защищён вторым фактором.

1 Telegram, СМС, Звонок, Приложение Multifactor или OTP-токены (аппаратные или программные) в случае защиты VPN и VDI соединений.
2 Скачать приложение Multifactor: App Store, Google Play, RuStore.

Остались вопросы?

ActiveCloud Россия

+7 499 11-006-11
sales@activecloud.ru
activecloud.ru