Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

2FA для Windows и RDP на MultiOTP: наша методология внедрения

Бесплатный TOTP-сервер с интеграцией в Active Directory через LDAP и Credential Provider

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Пароль остаётся единственным рубежом на входе в Windows и RDP: он утекает через фишинг, кейлоггеры, слитые базы и стикеры на мониторах. Для компаний до 50 рабочих мест это прямой путь к захвату домена и терминального сервера. Мы закрываем вход вторым фактором — одноразовым TOTP-кодом с телефона, без покупки лицензий и без выноса аутентификации в облако.

Почему это важно бизнесу

- Один скомпрометированный пароль администратора = полный контроль над доменом и всеми данными
- RDP-порт наружу — цель №1 для брутфорса и вымогателей-шифровальщиков
- Утечка учётки бухгалтера открывает 1С, банк-клиент и персональные данные
- Штрафы по 152-ФЗ и простой бизнеса после инцидента дороже любого внедрения 2FA
- TOTP работает офлайн — защита не зависит от внешних сервисов и SMS-шлюзов

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

5.10.2.2

Версия Credential Provider, которую ставим (PHP 8.5.4 embedded)

GitHub multiOTP

RFC 6238

Стандарт TOTP; HOTP по RFC 4226 — открытые алгоритмы

RFC 6238 и 4226

30 сек

Ширина временного окна TOTP; жёсткий NTP на DC обязателен

RFC 6238

1812/UDP

RADIUS-порт для VPN, Wi-Fi и RD Gateway

наш стандарт

8112/8113

HTTP/HTTPS порты сервера MultiOTP для Credential Provider

GitHub multiOTP

2 группы AD

2FAUsers и No2FA — область охвата и аварийный обход

наш стандарт

РЕАЛИЗАЦИЯ 1 ИЗ 2

Разворачиваем сервер MultiOTP с привязкой к AD

Что настраиваем

Юрфирма, единственный DC Windows Server 2019, вход в 1С и файловый ресурс по доменным учёткам

Как мы это делаем

1. Заводим группы 2FAUsers и No2FA и сервисный аккаунт svc_multiotp с правами только на чтение LDAP
2. Ставим MultiOTP на отдельную VM (не на DC), задаём ldap-domain-controllers, base-dn, in-group и without2fa-in-group
3. Прогоняем multiotp -ldap-users-sync с -debug, сверяем 'users updated'
4. Ставим x86 Visual C++ 2015-2022 Redistributable — иначе веб-интерфейс отдаёт 502
5. Меняем дефолт admin/1234, включаем HTTPS 8113, задаём server-secret

РЕЗУЛЬТАТ

Пользователи из 2FAUsers синхронизируются из AD автоматически, секрет привязывается к учётке при первом сканировании QR. Сервер вынесен с контроллера домена — падение MultiOTP не тянет за собой DC, а бэкап папок users и config уходит в наш регламент.

КЛЮЧЕВОЙ НЮАНС

Сервер MultiOTP всегда отдельно от DC и всегда с резервной копией базы токенов — иначе потеря VM = массовый перевыпуск QR для всех сотрудников.

РЕАЛИЗАЦИЯ 2 ИЗ 2

Ставим Credential Provider и раздаём его через GPO

Что настраиваем

Торговая компания, 40 рабочих мест плюс терминальный сервер с RDP наружу

Как мы это делаем

1. Тестируем MSI multiOTPCredentialProvider-x64 на одной машине: задаём адрес сервера и MULTIOTP_SECRET
2. Проверяем откат: msiexec /x в безопасном режиме на случай неудачи
3. Готовим MST-трансформ в Orca, кладём MSI на \\fileserver\share, назначаем через GPO Software Installation
4. На терминальнике ставим cpus_logon=1 (только RDP), консольный вход админа оставляем без 2FA
5. multiOTPCacheEnabled=0 для строгого режима, оставляем аварийного админа в No2FA

РЕЗУЛЬТАТ

Поле OTP появляется на экране входа всех машин после перезагрузки, установка идёт молча через GPO. На терминальном сервере вторым фактором закрыт именно RDP, а локальная консоль остаётся доступной инженеру при сбое сервера MultiOTP.

КЛЮЧЕВОЙ НЮАНС

cpus_logon на терминальниках ставим в режим RDP-only: при недоступности OTP-сервера нельзя отрезать себе консольный вход для восстановления.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Ставят только x64 VC++ Runtime**
  MultiOTP зависит от 32-битных библиотек: без x86 Redistributable веб отдаёт 502, установка падает с VCRUNTIME140.dll. Ставим обе.

- ✕ **Сервер MultiOTP прямо на DC**
  Совмещение с контроллером домена связывает отказоустойчивость: падение или перегрузка сервиса задевает вход в весь домен.

- ✕ **Нет аварийного обхода**
  Без учётки в No2FA и без строгого NTP недоступность сервера при выключенном кэше блокирует вход всем сотрудникам сразу.

- ✕ **Кэш OTP включён на терминалке**
  Кэширование при разрыве сети во время RDP-запроса позволяет проскочить проверку. Для строгого контура multiOTPCacheEnabled=0.

- ✕ **Забывают про рассинхрон времени**
  TOTP-окно 30 сек: расхождение часов сервера и телефона больше минуты отклоняет верный код. NTP на DC жёстко, w32tm /query /status.

- ✕ **Секрет и дефолтный admin/1234**
  Оставленный пароль веб-интерфейса и слабый server-secret обесценивают всю схему. Меняем сразу, HTTPS 8113 вместо 8112.

- ✕ **Развёртывание без пилота**
  Массовый GPO-раскат без теста на одной машине рискует запереть парк. Всегда проверяем откат msiexec /x в Safe Mode.

- ✕ **Нет резервных scratch-кодов**
  Потерянный телефон без backup-кодов = звонок админу и перевыпуск токена. Выдаём аварийные коды при первичной активации.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- 2FA на RDP терминального сервера (cpus_logon=1)
- Группы 2FAUsers и No2FA + сервисный svc_multiotp read-only
- Смена admin/1234 и включение HTTPS 8113
- Бэкап папок users и config в регламент

НОРМАЛЬНО

- Сервер MultiOTP на отдельной VM, не на DC
- Строгий NTP на DC, автовремя на смартфонах
- GPO-раскат Credential Provider с MST-трансформом
- Аварийный админ в No2FA + scratch-коды пользователям

ХОРОШО

- multiOTPCacheEnabled=0 для строгого контура
- RADIUS 1812 для VPN, Wi-Fi и RD Gateway
- Мониторинг multiotp.log в Zabbix/Telegram по ERROR/FAIL
- Резервирование сервера OTP под отказоустойчивость

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Заведены группы 2FAUsers, No2FA и сервисный аккаунт svc_multiotp только на чтение LDAP
- [ ] MultiOTP развёрнут на отдельной VM, LDAP-синхронизация проходит без LDAP bind failed
- [ ] Установлен x86 Visual C++ 2015-2022 Redistributable, веб-интерфейс отвечает без 502
- [ ] Сменён дефолт admin/1234, включён HTTPS 8113, задан стойкий server-secret
- [ ] NTP на DC синхронизирован, на смартфонах включено автоматическое время
- [ ] Credential Provider протестирован на одной машине, проверен откат msiexec /x в Safe Mode
- [ ] GPO с MSI и MST назначен на OU рабочих станций и терминальных серверов
- [ ] На терминальнике выставлен cpus_logon в режим RDP-only, консоль админа доступна
- [ ] Аварийный администратор в группе No2FA, пользователям выданы scratch-коды
- [ ] Бэкап папок users и config автоматизирован, мониторинг multiotp.log настроен

Если хотя бы на два вопроса ответ «нет» или «не знаю» — тема требует внимания.

ЧТО МЫ ДЕЛАЕМ

Как поможет ITFresh

ITFresh — ИТ-аутсорсинг для юридических лиц до 50 рабочих мест в Москве и области. 15+ лет практики, собственная инфраструктура в дата-центре МТС (8 серверов Dell Xeon Platinum).

- Разворачиваем MultiOTP под ключ: сервер, LDAP-интеграция с AD, генерация QR для сотрудников
- Раздаём Credential Provider через GPO на весь парк и терминальные серверы без простоя
- Настраиваем 2FA на RDP наружу и RADIUS для VPN, Wi-Fi и RD Gateway
- Закладываем аварийный обход, scratch-коды и бэкап базы токенов от блокировки входа
- Подключаем мониторинг попыток OTP в Zabbix и Telegram, ведём регламент обновлений

15+
лет в ИТ-поддержке

50
рабочих мест — наш профиль

МТС
дата-центр, Москва

КОНТАКТЫ

Обсудить вашу задачу

Сайт	**itfresh.ru**
Телефон	**+7 903 729-62-41**
Telegram	**@ITfresh_Boss**

Бесплатно посмотрим вашу инфраструктуру по этому чек-листу и скажем, где тонко — без обязательств.

itfresh.ru

ДОКУМЕНТАЦИЯ И НАШ СТЕК

Техническая база

01 multiOTP/multiotp — open source OTP library, GitHub (github.com — 2026)

02 multiOTP/multiOTPCredentialProvider — Releases (github.com — 2026)

03 multiOTPCredentialProvider Wiki — Registry Configuration (github.com — 2026)

04 RFC 6238 TOTP: Time-Based One-Time Password (ietf.org — 2011)

05 RFC 4226 HOTP: HMAC-Based One-Time Password (ietf.org — 2005)

06 multiOTP Wiki — LDAP sync и RADIUS (github.com — 2026)

07 Наш шаблон внедрения 2FA MultiOTP + AD (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.