Двухфакторная аутентификация на Windows Server 2019

С момента написания прошлой заметки Двухфакторная аутентификация на Windows Server 2012 процедуру установки и настройки упростили, теперь все можно делать быстрее и проще.

Открывать RDP для всего мира довольно чревато - какая-нибудь зараза вполне может подобрать пароль. С другой стороны, использовать VPN тоже далеко не всегда удобно или возможно по разным причинам.

Одно из решений - двухфакторная аутентификация.

Мне нравится multiOTP - это крайне мощная штука, много чего умеет - Windows, Hyper-V, VMWare, RADIUS и совместима практически со всем.

> **Настройки времени**
>
> Время на сервере и вашем устройстве (телефон, компьютер) должно совпадать, иначе ключи будут генерироваться неверно!

> **Внимание**
>
> При установке необходимо все сделать аккуратно и внимательно, в противном случае придется подключаться локально консолью или загружаться в безопасный режим!

Установка multiOTP

Примечание: продукт очень быстро допиливают, в более новых версиях процедура установки может немного различаться

- Качаем и устанавливаем VisualC++ (x86 и x64) с сайта Microsoft: https://aka.ms/vs/16/release/vc_redist.x64.exe и https://aka.ms/vs/16/release/vc_redist.x86.exe
- Загружаем multiOTP с сайта https://github.com/multiOTP/multiOTPCredentialProvider/releases (есть еще полная версия тут: https://download.multiotp.net/ но в нее понапихано много лишнего)
- Устанавливаем, заполняем следующим образом поля настроек:
  - Первый экран
    - **multiOTP Login Title**: приветственная фраза которая будет написана на экране входа в систему
    - **URL of your multiOTP server(s), separated by semi-colons**: удаляем все, поле должно быть пустым
    - **No remote server, local multiOTP only**: - включено
    - **Secret shared with your multiOTP server(s)**: удаляем все, поле должно быть пустым

- Второй экран
  - **OTP authentication mandarity for remote desktop only** - выбрано, т.к. требуется проверка только для подключений по RDP
  - **Enable cache support on this machine if authorized by the server(s)** - включено
- Третий экран: Next → Install

На этом установка закончена. На это этапе желательно НЕ ПЕРЕЗАГРУЖАТЬ сервер, требуется добавить хотя бы одного пользователя с административными правами.

Далее добавляем ВСЕХ пользователей, которым нужен доступ по RDP по описанной выше процедуре. Если пользователь присутствует в системе но не добавлен в multiOTP - он не сможет удаленно подключиться. При настройке **OTP authentication mandarity for remote desktop only** пользователи могут входит в систему локально с консоли.

Управление пользователями

При добавлении пользователя создается персональный файл настроек (в моем случае это C:\Program Files (x86)\multiOTP\users\) с расширением db, представляющий обычный текстовый файл в формате «ключ/значение». Если пользователь многократно неверно вводит пароль и ключ авторизации, то блокируется не windows-пользователь, а именно аккаунт multiOTP (параметр locked). Вручную его можно разблокировать изменив locked=1 на locked=0

Добавление пользователей

- Создаем в системе нового пользователя (или будем использовать уже существующего)
- Открываем консоль, переходим в папку с multiOTP (в моем случае это C:\Program Files (x86)\multiOTP)
- Создаем секрет для этого пользователя:

```
multiotp.exe -fastcreatenopin ИМЯ_ПОЛЬЗОВАТЕЛЯ
```

- Создаем QR-файл для добавления в аутентификатор:

```
multiotp.exe -qrcode ИМЯ_ПОЛЬЗОВАТЕЛЯ QR_ИМЯ_ПОЛЬЗОВАТЕЛЯ.png
```

- Открываем аутентификатор (например Google Authenticator) и сканируем полученный QR-код

Отключение/блокировка пользователей и включение обратно

```
multiotp -[des]activate user
```

```
multiotp -[un]lock user
```

Удаление пользователя

```
multiotp -delete user
```

```
multiotp -user-info user
```

Устанавливаем аутентификатор

Для генерации OTP-паролей необходимо установить аутентификатор - это может быть плагин для браузера (Google Chrome: Authenticator) или отдельное приложение на Android (приложение «Google Authenticator») или iOS.

Запускаем аутентикатор, создаем новый аккаунт: нажимаем «Добавить», выбраем QR-код, сканируем полученный код

Тестирование

Тестируем вход под добавленными пользователями, все должно быть Ок.

> Примечание: если компьютер не в домене, указывайте имя пользователя в формате SERVER\Username

Удаление multiOTP

Отключить multiOTP можно удалением программы через Панель управления или импортировав файл реестра:
https://download.multiotp.net/credential-provider/multiOTPCredentialProvider-unregister.reg

Если потеряли возможность войти в систему - необходимо войти локально под пользователем (как вариант - в безопасном режиме).

Замена логотипа

Для логотипа используется файл loginLogo.bmp в папке с multiOTP (в моем случае это C:\Program Files (x86)\multiOTP)

Разрешение: 128x128, формат bmp

2019, windows server, OTP, multiotp, two-factor authentication, двухфакторная аутентификация, двухфакторная авторизация, MultiOTP