Руководство пользователя

Получение доступа к ресурсам выполняется при помощи специальной оболочки для Indeed PAM Core, консоли пользователя. Доступна по следующему URL:

- **Windows:** https://pam.domain.local/pam/uc
- **Linux:** https://pam.domain.local/uc

Обучение аутентификатора

Для работы с консолью пользователя необходимо обучить аутентификатор. Выполните вход в консоль, если пользователь не имеет аутентификатора, то он будет перенаправлен на IDP для его регистрации:

Зарегистрировать аутентификатор

Для использования двухфакторной аутентификации выполните слудеющие шаги:

1. Скачайте приложение для двухфакторной аутентификации OTP, например Microsoft Authenticator для Android и iOS или Google Authenticator для Android и iOS.

2. Отсканируйте QR код который появится ниже или введите этот ключ `ewah pqo4 snlg gq4j ksgl fpib lx24 nryy` в ваше приложение для двухфакторной аутентификации.

3. После сканирования QR или ввода ключа сверху, ваше приложение для двухфакторной аутентификации покажет вам уникальный код. Укажите этот код в поле ниже.

Введите код

Code

Зарегистрировать

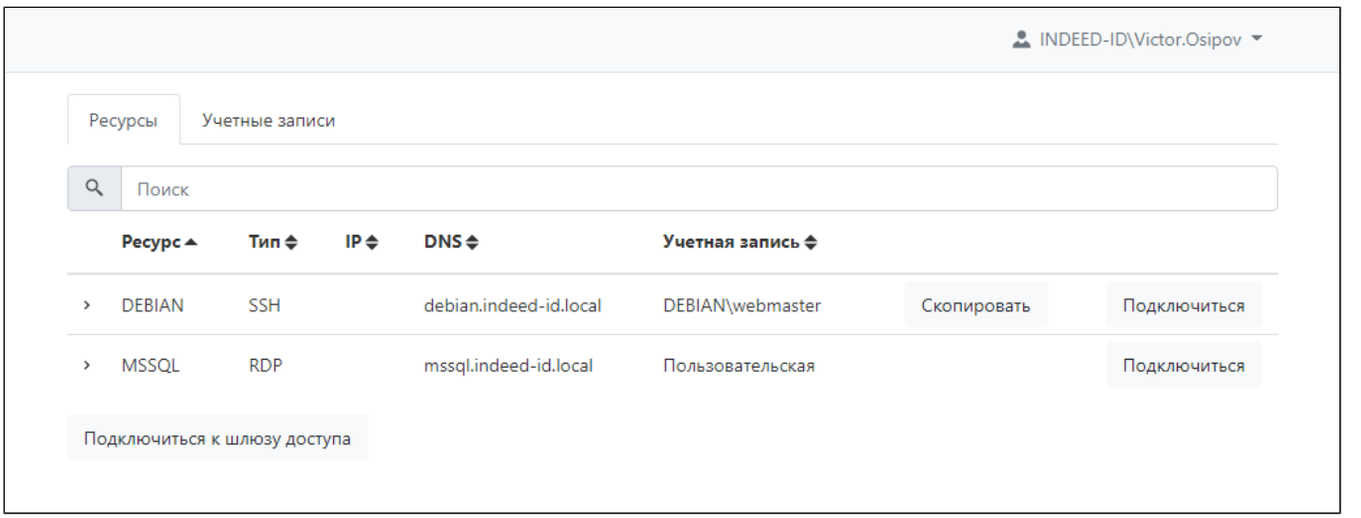
После успешной регистрации вы будете перенаправлены в консоль пользователя.

При превышении попыток неправильного ввода OTP-кода пользователь блокируется на 15 минут.

Для срочного разблокирования Администратору PAM необходимо сбросить аутентификатор заблокированному пользователю.

Получение доступа к ресурсу

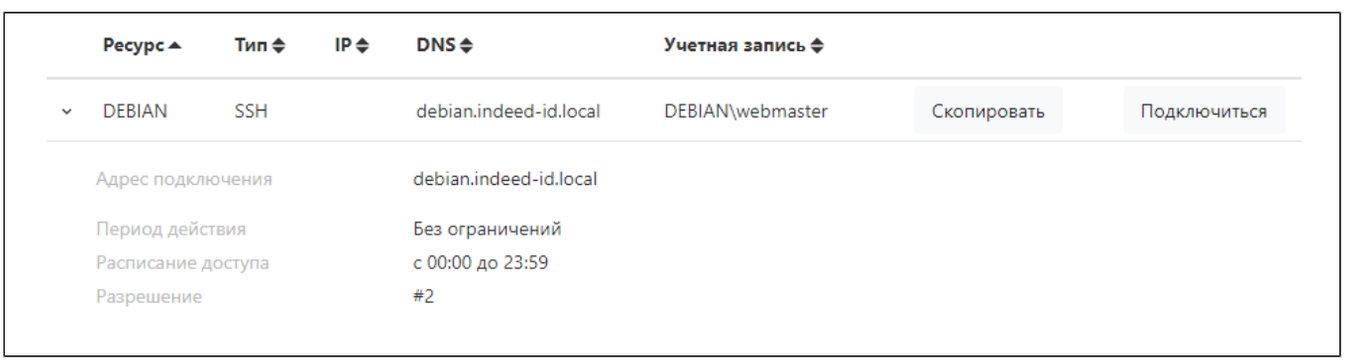
В консоли отображаются разрешения на доступ к ресурсам. Для каждого разрешения указан ресурс, тип подключения, адрес подключения и учётная запись, от имени которой будет открыта сессия. По каждому столбцу доступна сортировка. При вводе символов в поле для поиска совпадения будут выводиться по всем столбцам.



Доступ к ресурсам осуществляется при помощи RDP-файлов. Для загрузки файла необходимо нажать **Подключиться** справа от нужного разрешения или нажать **Подключиться к шлюзу доступа**. Скачанные RDP-файлы могут быть сохранены и использованы для дальнейших подключений к ресурсам через PAM пока разрешение активно.

RDP-файл **шлюза доступа** PAM можно использовать для подключения к ресурсам независимо от доступных разрешений: каждый раз при подключении к шлюзу будет отображаться актуальный список ресурсов.

В деталях разрешений отображаются период действия, расписание доступа и идентификатор разрешения (порядковый номер разрешения в Разделе разрешений в консоли управления).



Прямое подключение к ресурсу

- Нажмите **Подключиться** справа от нужного разрешения.
- Запустите RDP-файл для доступа к ресурсу.
- Выполните аутентификацию и следуйте этапам настройки подключения.

Подключение к шлюзу доступа

- Нажмите **Подключиться к шлюзу доступа**.
- Запустите RDP-файл для доступа к ресурсу.
- Выполните аутентификацию и следуйте этапам настройки подключения.

Подключение к SSH Proxy

Для подключения к шлюзу SSH Proxy можно воспользоваться любым SSH клиентом.

- Запустите SSH-клиент.
- Укажите адрес SSH Proxy и выполните подключение.
- Пройдите аутентификацию.
- Выберите ресурс для подключения.

Подключение по SSH напрямую

В консоли пользователя напротив SSH-ресурса нажмите кнопку **Скопировать**. При этом в буфер обмена скопируется SSH-команда для подключения к данному ресурсу.

Шаблон команды для подключения напрямую к ресурсу через ssh-клиент:

```
ssh [user-name]#[resource]#[account-name]#[reason]@[proxy-address]
```

где:

- **user-name** - имя пользователя
- **resource** - IP адрес/DNS имя конечного ресурса
- **account-name** - имя привилегированной учетной записи
- **reason** - текст причины подключения
- **proxy-address** - IP адрес/DNS SSH Proxy

Данную команду можно вводить в SSH-клиенте и вручную, опуская любой параметр кроме адреса сервера SSH Proxy. Если какой-то из параметров не указан, то SSH Proxy дополнительно запросит необходимую информацию. Если причина содержит пробелы, то её следует указывать в кавычках.

После выполнения команды SSH Proxy запросит пароль пользователя и TOTP.

Пример команды:

```
ssh victor.osipov#ubuntu#webmaster#"system configuration"@sshproxy.indeed-id.local
```

Передача файлов по SCP

Для передачи файлов по протоколу SCP используйте встроенную в ОС утилиту SCP. Для Windows подойдут также WinSCP, OpenSSH. Используйте стандартную команду для копирования, но вместо адреса ресурса укажите адрес SSH Proxy:

```
scp -r C:\temp\configs\ victor.osipov@sshproxy.indeed-id.local:/tmp
```

Далее, после успешной аутентификации выберите номер ресурса для передачи файлов.

Для WinSCP нужно создать новое подключение, указать имя пользователя PAM и адрес подключения SSH Proxy. Во время подключения будет выведен список доступных ресурсов, после выбора ресурса в правой панели откроется дерево файловой системы ресурса.

Выполнение команд с привилегией root

Для выполнения команд с привилегией root, аналогично sudo используется команда pamsu. Отличие заключается в том, что аутентификация будет запрашиваться у пользователя PAM, а не привилегированной УЗ от имени которой открыта сессия.

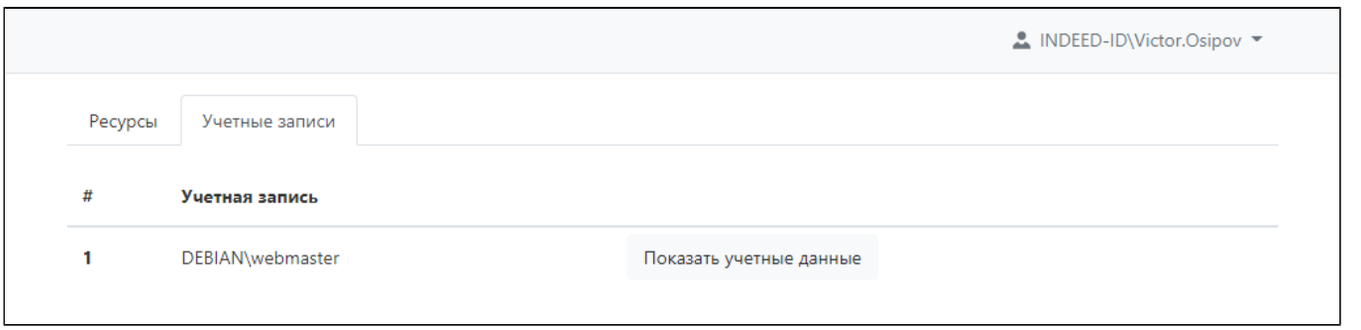
Уточните у администратора PAM на каких ресурсах доступен функционал pamsu.

Пример:

```
[administrator@centos7su ~]$ pamsu ls -la /etc/ssl
Password for indeed-id\victor.osipov:
total 12
drwxr-xr-x. 4 root root 68 Sep 22 19:20 .
drwxr-xr-x. 75 root root 8192 Sep 22 17:49 ..
drwxr-xr-x. 2 root root 123 Sep 22 19:30 CA
lrwxrwxrwx. 1 root root 21 Sep 22 15:51 cert.pem -> /etc/pki/tls/cert.pem
lrwxrwxrwx. 1 root root 16 Nov 23 2020 certs -> ../pki/tls/certs
[administrator@centos7su ~]$
```

Просмотр пароля и SSH-ключа учётной записи

Если пользователь имеет разрешение, в котором включена опция **Разрешить просмотр учётных данных пользователем**, то в разделе **Учётные записи** будут доступны соответствующие данные. Для просмотра нажмите **Показать учётные данные**, введите причину просмотра и подтвердите свои действия.



Завершение сессии

Для завершения сессии завершите сеанс пользователя на ресурсе, либо закройте окно удалённого подключения.