

Tài liệu hướng dẫn tích hợp xác thực không mật khẩu các ứng dụng với VinCSS FIDO2[®] Cloud

Ngày: 28/01/2021

Mã số: CSS-IP-PUB-UAG-210128-011

Phiên bản: 1.1

Phân loại tài liệu: Tài liệu công bố

Thực hiện: TT. Sản phẩm, VinCSS

Đầu mối liên lạc:

Email:

Điện thoại:

CÔNG TY TNHH DỊCH VỤ AN NINH MẠNG VINCSS

Số 7 Đường Bằng Lăng 1, Khu đô thị sinh thái Vinhomes Riverside, Phường Việt Hưng, Quận Long Biên, Thành phố Hà Nội.

THEO DÕI PHIÊN BẢN

Phiên bản	Ngày	Người thực hiện	Vị trí	Liên hệ	Ghi chú
1.0	06/07/2020		TT. Sản phẩm, VinCSS		Khởi tạo tài liệu
1.1	28/01/2021		TT. Sản phẩm, VinCSS		Cập nhật và hiệu chỉnh



MỤC LỤC

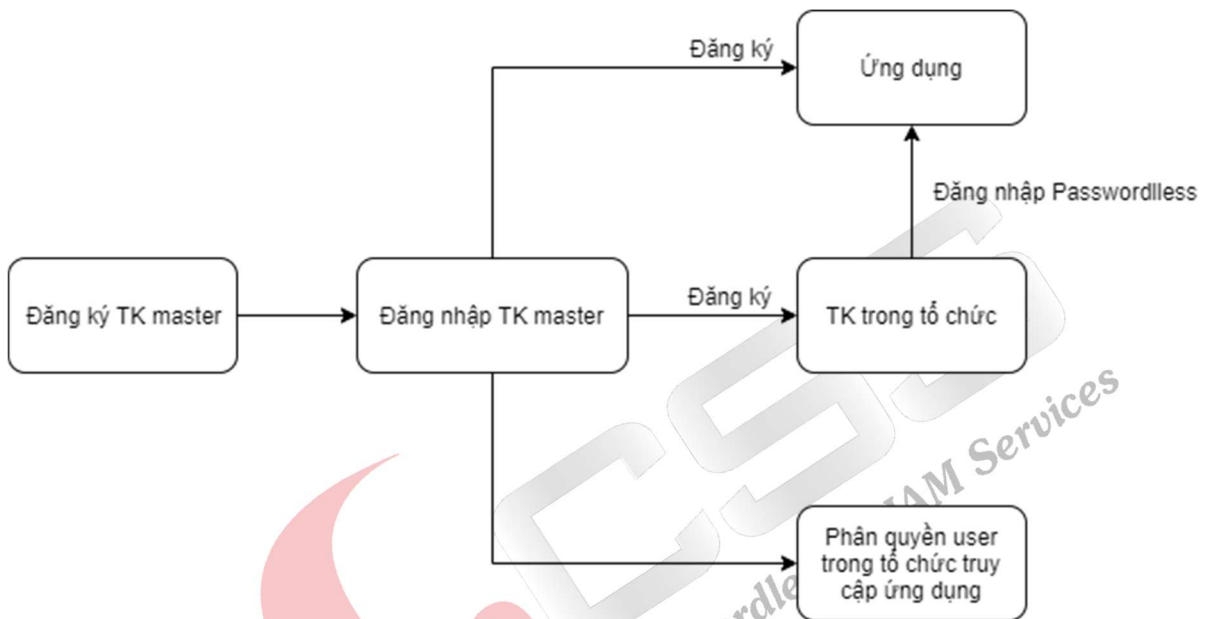
THEO DÕI PHIÊN BẢN.....	2
MỤC LỤC.....	3
1. GIỚI THIỆU HỆ THỐNG VinCSS FIDO2® CLOUD	4
2. CÁC THÔNG SỐ.....	4
2.1. Luồng tích hợp.....	4
2.2. Luồng xác thực khi tích hợp FIDO2 Cloud	5
3. HƯỚNG DẪN TÍCH HỢP.....	5
3.1. Tích hợp Wordpress với VinCSS FIDO2® Cloud.....	5
3.1.1. Add OAuth2 Plugin – MiniOrange.....	5
3.1.2. Cài đặt Plugin	6
3.1.3. Đăng nhập vào hệ thống	7
3.2. Tích hợp Joomla với VinCSS FIDO2® Cloud.....	11
3.2.1. Add OAuth2 Plugin - MiniOrange	11
3.2.2. Cài đặt Plugin	12
3.2.3. Đăng nhập vào hệ thống	13
3.3. Cấu hình OpenVPN (pfSense) với VinCSS FIDO2® Cloud.....	13
3.3.1. Tạo Certificate Authority.....	13
3.3.2. Tạo OpenVPN Server Certificate	14
3.3.3. Tạo VPN Server.....	16
3.3.4. Chỉnh sửa thông số VPN Server để hoạt động với FIDO2	19
3.3.5. Chỉnh sửa thông số Export profile	20
3.3.6. Tạo tài khoản cho người dùng VPN	21
3.3.7. Xuất profile cho người sử dụng.....	22

1. GIỚI THIỆU HỆ THỐNG VinCSS FIDO2® CLOUD

Dịch vụ VinCSS FIDO2® Cloud hướng đến phục vụ các đối tượng doanh nghiệp vừa và nhỏ (SMB) có thể nhanh chóng sử dụng nền tảng dịch vụ xác thực sẵn có của VinCSS để triển khai tích hợp xác thực không mật khẩu một cách nhanh nhất trong khi không phải đầu tư về hạ tầng hệ thống dịch vụ.

Doanh nghiệp đăng ký tài khoản dịch vụ và tự quản trị, tích hợp các ứng dụng, khoá bảo mật nội bộ thông qua giao diện web tại <https://fido2cloud.vincss.net>

Các bước triển khai sử dụng dịch vụ VinCSS FIDO2® Cloud được mô tả như sau:



- Tài khoản Master: có quyền cao nhất, đại diện cho tổ chức, có quyền khai báo ứng dụng với hệ thống FIDO2 Cloud, hỗ trợ tạo người dùng trong tổ chức, đăng ký khóa bảo mật FIDO2 cho người dùng và phân quyền cho người dùng trong tổ chức truy cập vào các ứng dụng đã tích hợp với hệ thống FIDO2 Cloud.
- Người dùng trong tổ chức: được tạo ra bởi tài khoản master, các tài khoản này được đăng ký khóa bảo mật FIDO2 và sử dụng để xác thực không mật khẩu đăng nhập vào các ứng dụng đã tích hợp với hệ thống FIDO2 Cloud.

2. CÁC THÔNG SỐ

2.1. Luồng tích hợp

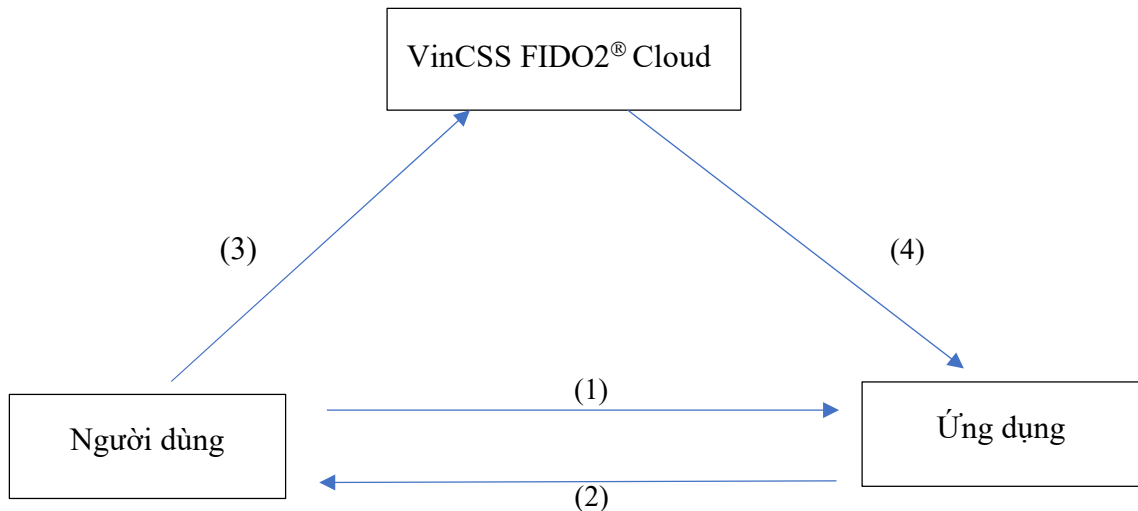
Hệ thống FIDO2 Cloud cung cấp dịch vụ xác thực không mật khẩu, được tích hợp theo chuẩn OAuth2 cho ứng dụng. Các ứng dụng sẽ sử dụng giao thức OAuth2 để xác thực qua hệ thống VinCSS FIDO2® Cloud

Các thông số khi tích hợp:

- **Authorize Endpoint:** <https://fido2cloud.vincss.net/authorize>
- **Access Token Endpoint:** <https://fido2cloud.vincss.net/token>
- **Get User Info Endpoint:** <https://fido2cloud.vincss.net/profile>
- **Client Identifier (Client ID):** chuỗi ký tự được sử dụng để định danh ứng dụng.
- **Client Secret:** chuỗi ký tự bí mật dùng để xác thực ứng dụng với Authorization Server.

Có thể hiểu **Client ID** là *username*, **Client Secret** là *password* của Ứng dụng đối với FIDO2 Cloud.

2.2. Luồng xác thực khi tích hợp FIDO2 Cloud



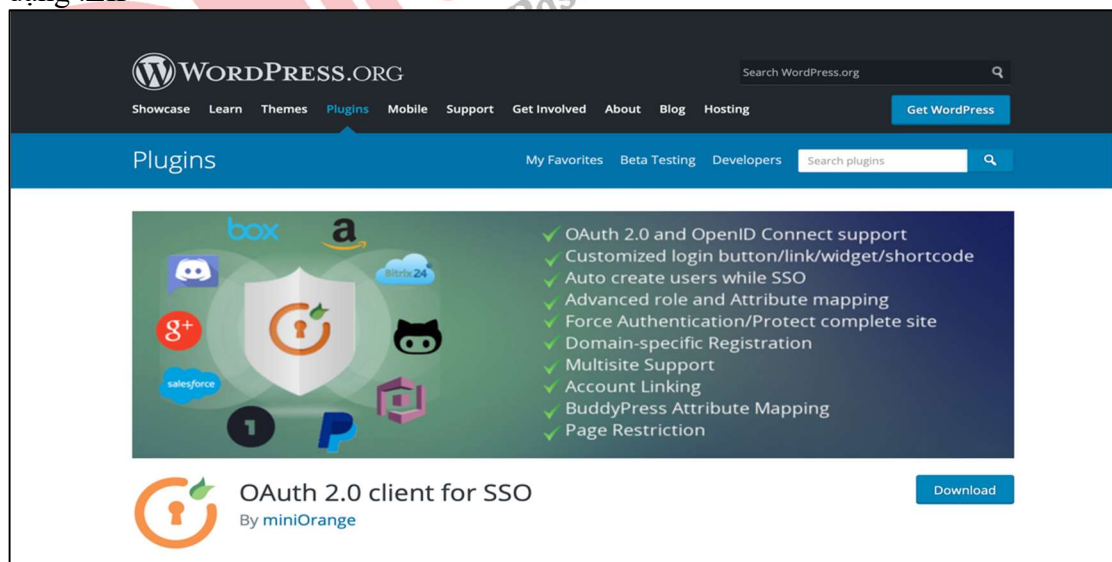
- (1) Người dùng truy cập đến ứng dụng, chọn đăng nhập không mật khẩu (xác thực qua dịch vụ VinCSS FIDO2® Cloud)
- (2) Ứng dụng chuyển hướng Người dùng đến trang xác thực VinCSS FIDO2® Cloud
- (3) Người dùng thực hiện xác thực không mật khẩu với khóa bảo mật đăng ký
- (4) VinCSS FIDO2® Cloud sẽ xác thực thông tin đăng nhập và chuyển hướng người dùng về ứng dụng với kết quả xác thực

3. HƯỚNG DẪN TÍCH HỢP

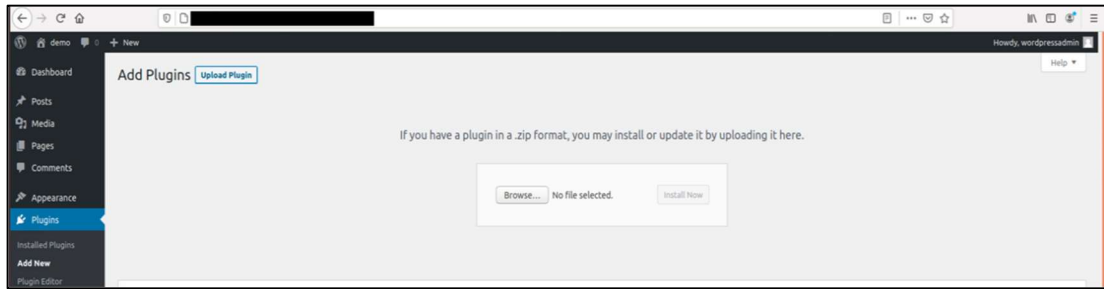
3.1. Tích hợp Wordpress với VinCSS FIDO2® Cloud

3.1.1. Add OAuth2 Plugin – MiniOrange

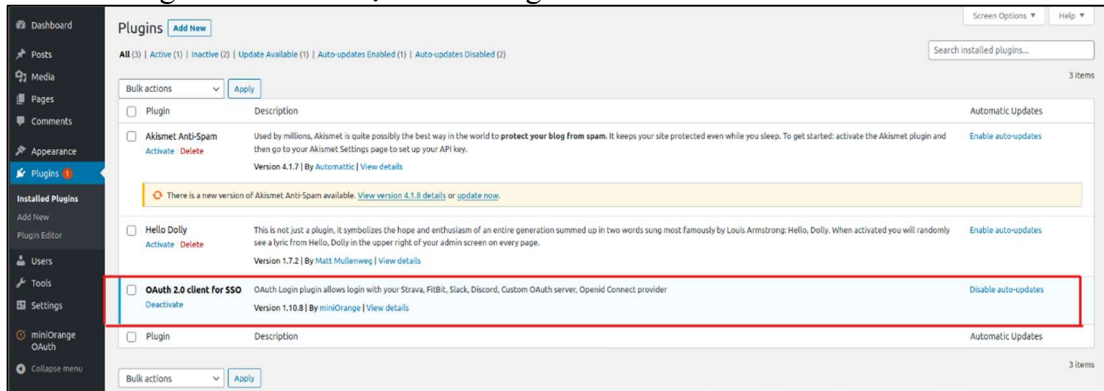
- Truy cập Website <https://wordpress.org/plugins/oauth-client/> và tải về Plugin theo định dạng .ZIP



- Trên trang quản trị, chọn **Plugin > Add New**
- Chọn **Upload Plugin > Browse** và upload file plugin đã tải về theo định dạng .Zip. Chọn **Install Now** để tiến hành cài đặt Plugin



- OAuth2 Plugin sau khi cài đặt thành công



3.1.2. Cài đặt Plugin

- Khai báo thông tin xác thực, tại cột bên trái chọn **MiniOrange OAuth** > **Configure OAuth**

Configure OAuthCustomizationsSign In SettingsReportsFrequently Asked Questions [FAQ]Account SetupAdd-ons

Update Application : test

*Application:

test

Redirect / Callback URL

Display App Name:

[STANDARD]

*Client ID:

*Client Secret:

.....

Scope:

*Authorize Endpoint:

<https://fido2cloud.vincss.net/authorize>

*Access Token Endpoint:

<https://fido2cloud.vincss.net/token>

*Get User Info Endpoint:

<https://fido2cloud.vincss.net/profile>

☐ (Check if does not require Authorization Header)

Save settings

Test Configuration

Attribute Mapping

Do Test Configuration above to get configuration for attribute mapping.

*Email attribute:

user_name

*First Name Attribute:

user_name

Last Name Attribute:

LastName Attribute Name

Username Attribute:

Username Attribute Name

Group Attribute Name:

Group Attribute Name

Display Name:

FirstName

Save settings

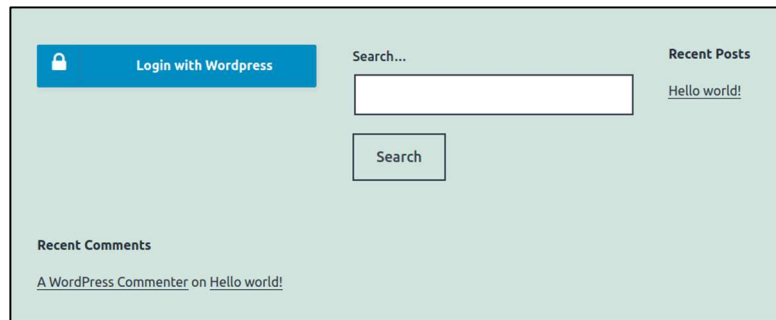
Các thông tin cần khai báo bao gồm:

- Client ID: giá trị Client ID khi đăng ký ứng dụng trên VinCSS FIDO2® Cloud
- Client Secret: giá trị Client Secret khi đăng ký ứng dụng trên VinCSS FIDO2® Cloud
- Scope: email
- Authorize Endpoint: <https://fido2cloud.vincss.net/authorize>
- Access Token Endpoint: <https://fido2cloud.vincss.net/token>
- Get User Info Endpoint: <https://fido2cloud.vincss.net/profile>

Chọn **Save settings** lưu lại các thông tin đã khai báo.

3.1.3. Đăng nhập vào hệ thống

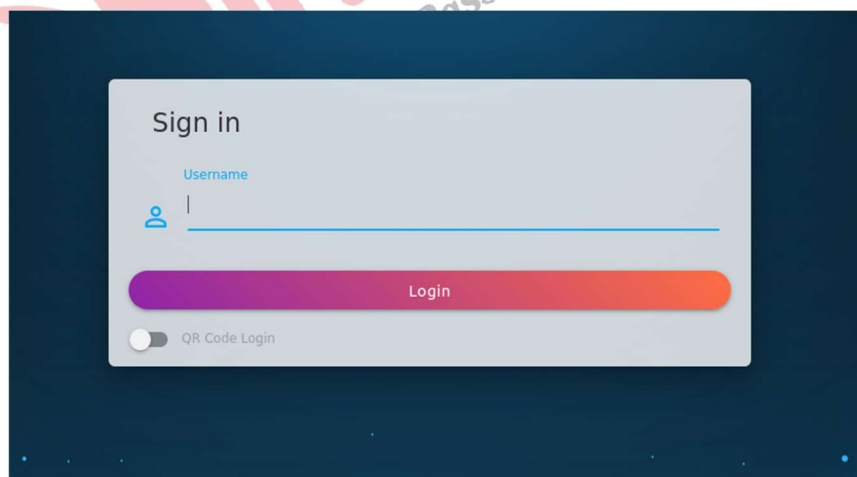
- Trên trang đăng nhập, chọn **Login with Wordpress**



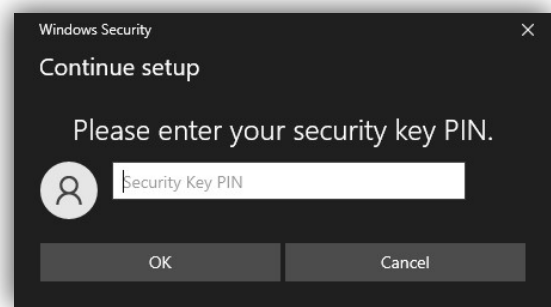
- Đăng nhập xác thực với user đã đăng ký

Nếu chọn Login với VinCSS FIDO2® Touch 1 (không tích chọn QR Code Login), thực hiện các bước tiếp theo như sau để xác thực với khóa bảo mật FIDO2 vật lý:

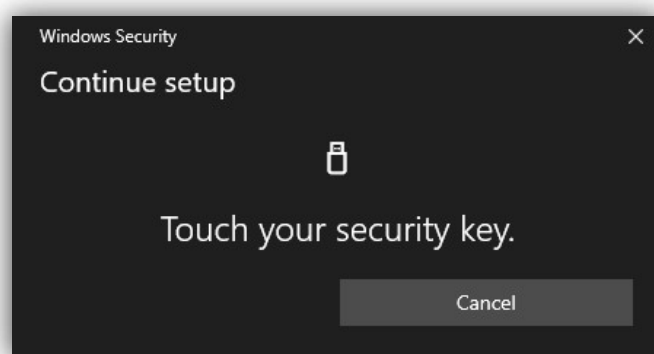
- Bỏ chọn QR Code Login để đăng nhập bằng khóa xác thực VinCSS FIDO2® Touch 1, sau đó nhấn Login.



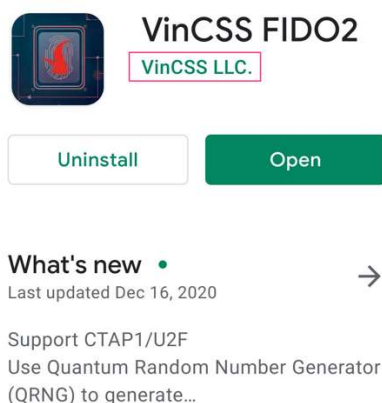
- Kết nối khóa xác thực VinCSS FIDO2® Touch 1 vào máy, sau đó điền mã PIN và nhấn OK



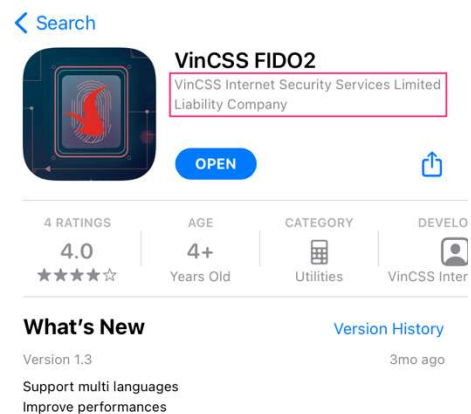
- Chạm vào logo màu vàng trên khóa xác thực



Nếu chọn **QR Code Login**, thực hiện các bước tiếp theo như sau để đăng ký khóa bảo mật FIDO2 trên ứng dụng điện thoại VinCSS FIDO2:

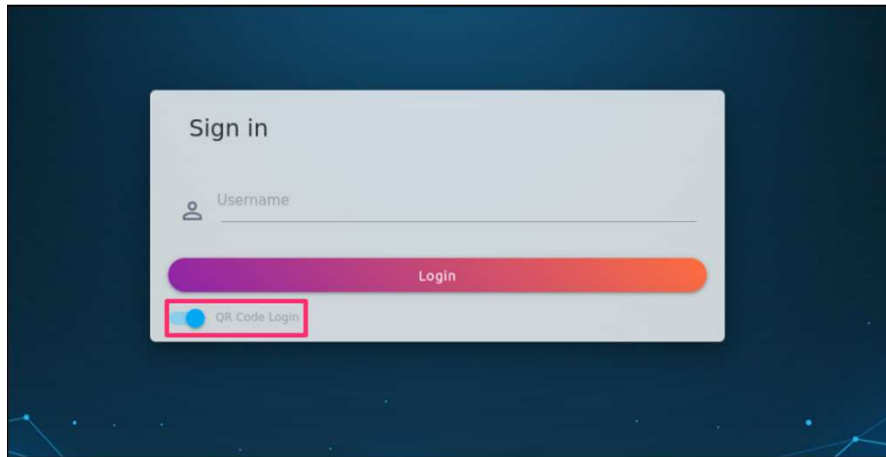


Phần mềm VinCSS FIDO2 trên Play Store

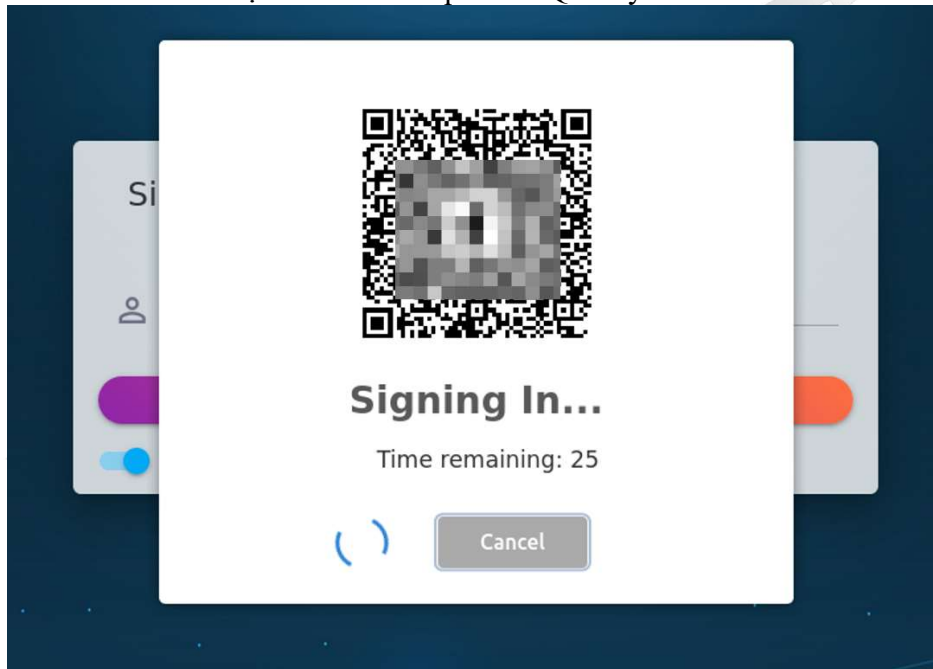


Phần mềm VinCSS FIDO2 trên App Store

Lưu ý: Để sử dụng tính năng quét mã QR bằng ứng dụng VinCSS FIDO2, điện thoại phải bật tính năng mở khóa bằng vân tay (đối với hệ điều hành Android, iOS) và tính năng mở khóa bằng khuôn mặt FaceID (đối với hệ điều hành iOS).



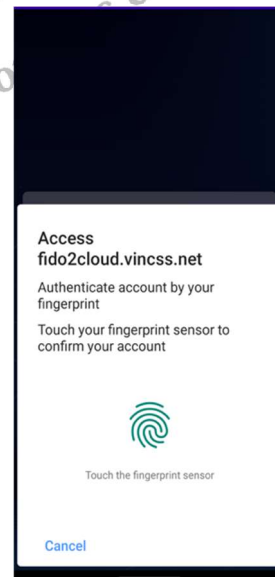
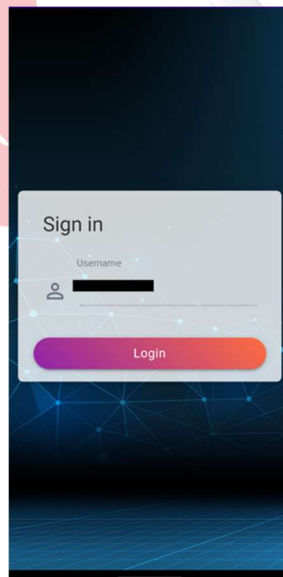
- Màn hình hiển thị mã QR. Mã QR này có hiệu lực trong 40 giây. Sau khoảng thời gian này, nếu chưa kịp thao tác đăng ký, người dùng cần nhấn lại “OK” để hệ thống tạo một mã QR mới. Sử dụng ứng dụng VinCSS FIDO2 trên điện thoại chạy hệ điều hành iOS hoặc Android để quét mã QR này.



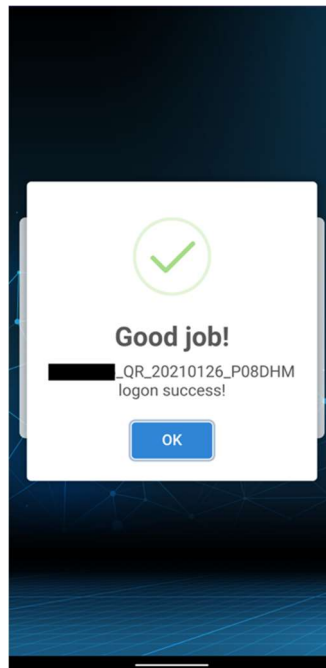
- Trên điện thoại tiến hành mở ứng dụng VinCSS FIDO2, nhấn chọn “Scan QR code” và tiến hành quét mã QR.



- Màn hình điện thoại hiển thị thông tin xác nhận khoá. Nhấn vào chọn “Login”, sau đó quét vân tay (đối với điện thoại chạy hệ điều hành Android) hoặc quét FaceID (đối với điện thoại chạy hệ điều hành iOS) để xác nhận.



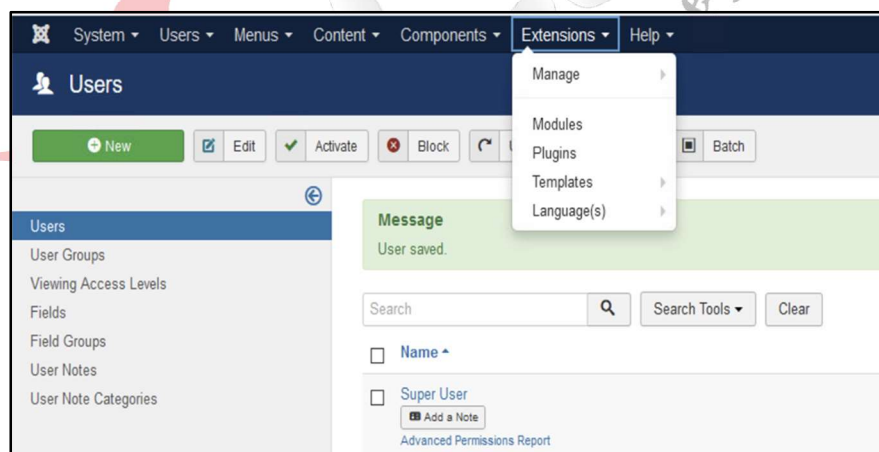
- Trên màn hình hiển thị thông tin Login thành công



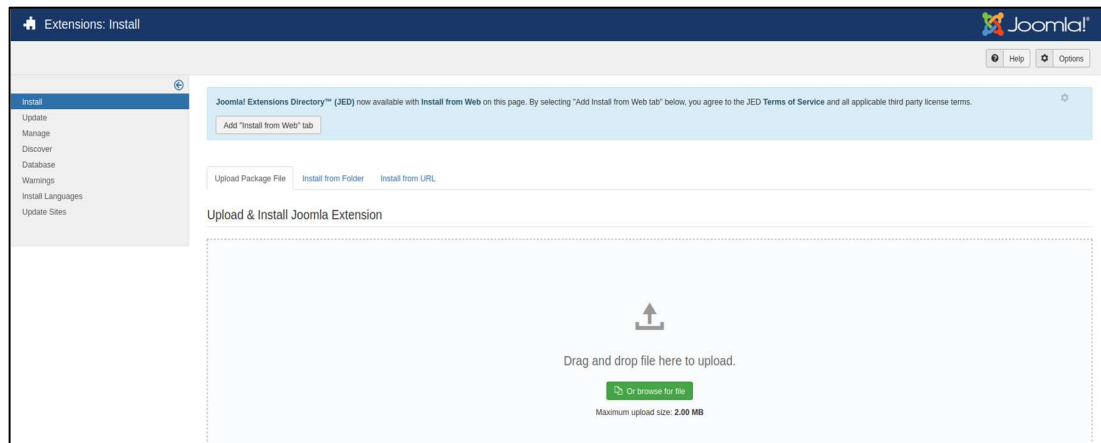
3.2. Tích hợp Joomla với VinCSS FIDO2® Cloud

3.2.1. Add OAuth2 Plugin - MiniOrange

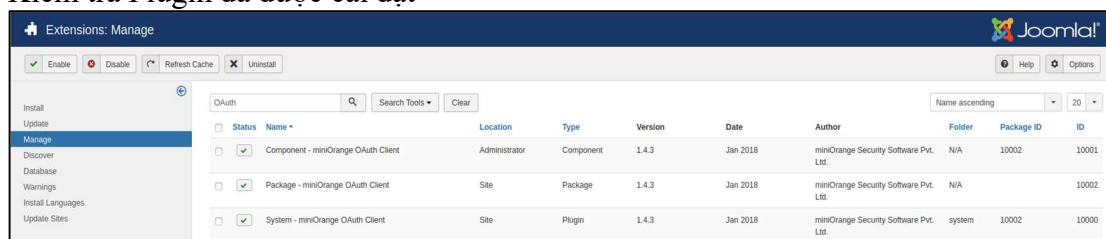
- Truy cập Website <https://extensions.joomla.org/extension/miniorange-oauth-client/> và tải về Plugin theo định dạng .ZIP.
- Trên trang quản trị, để add plugin, chọn **Extensions > Manage > Install**



- Chọn **Upload Package File** và upload file plugin đã tải về theo định dạng Zip.

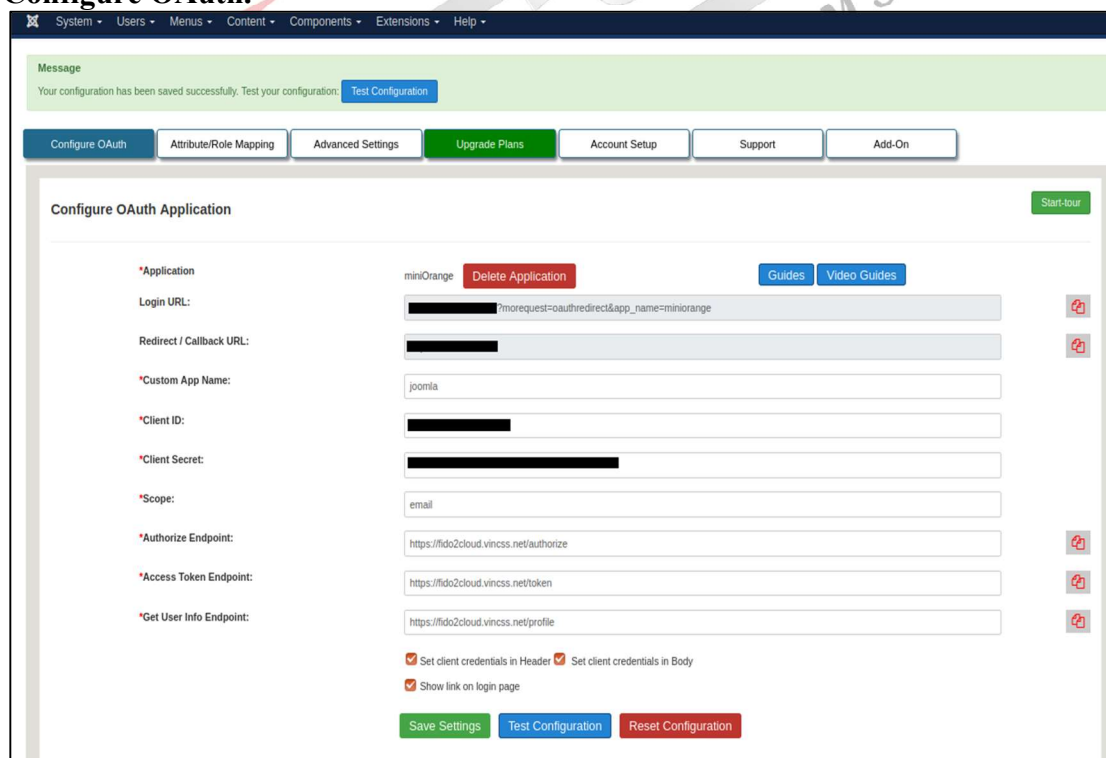


- Kiểm tra Plugin đã được cài đặt



3.2.2. Cài đặt Plugin

- Khai báo thông tin xác thực, chọn **Components** > **MiniOrange OAuth Client** > **Configure OAuth**.



Các thông tin cần khai báo bao gồm:

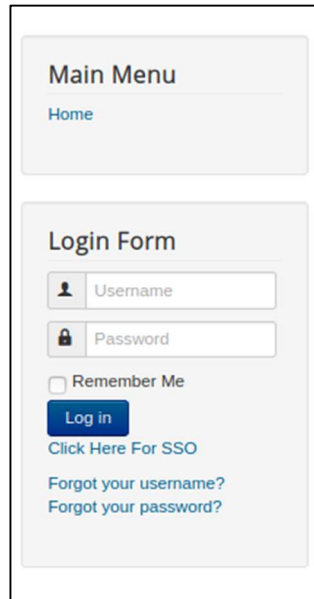
- Client ID: giá trị Client ID khi đăng ký ứng dụng trên VinCSS FIDO2® Cloud
- Client Secret: giá trị Client Secret khi đăng ký ứng dụng trên VinCSS FIDO2® Cloud
- Scope: email
- Authorize Endpoint: <https://fido2cloud.vincss.net/authorize>

- Access Token Endpoint: <https://fido2cloud.vincss.net/token>
- Get User Info Endpoint: <https://fido2cloud.vincss.net/profile>
- Chọn **Show link on login page**, hiển thị link đăng nhập sử dụng xác thực với VinCSS FIDO2® Cloud

Chọn **Save Setting** lưu lại các thông tin đã khai báo

3.2.3. Đăng nhập vào hệ thống

- Trên trang đăng nhập, chọn **Click Here For SSO**

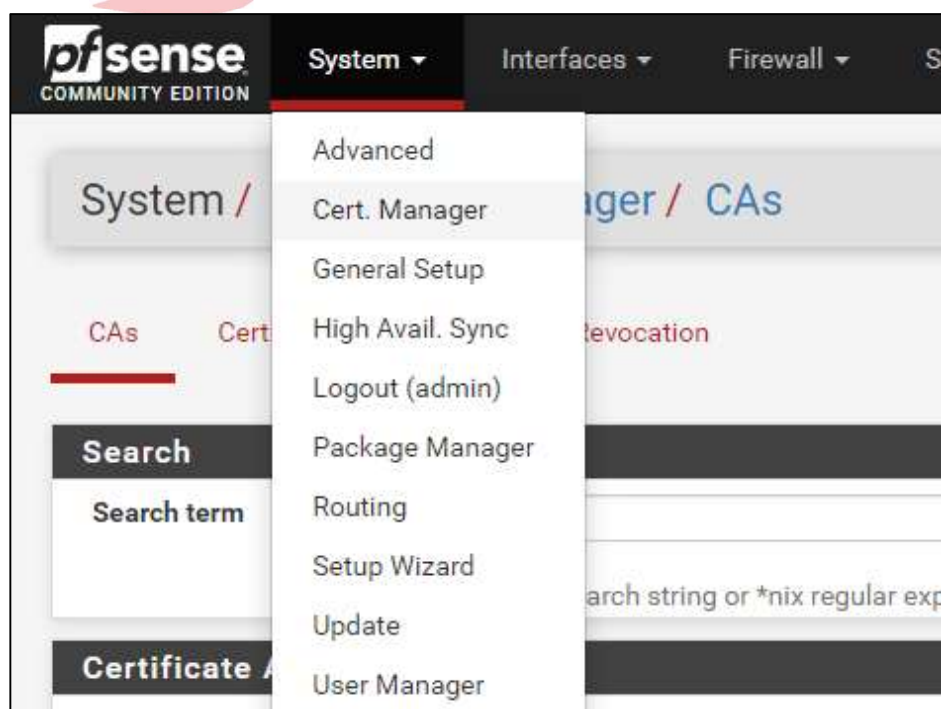


- Đăng nhập với User đã đăng ký (tham chiếu mục 3.1.3)

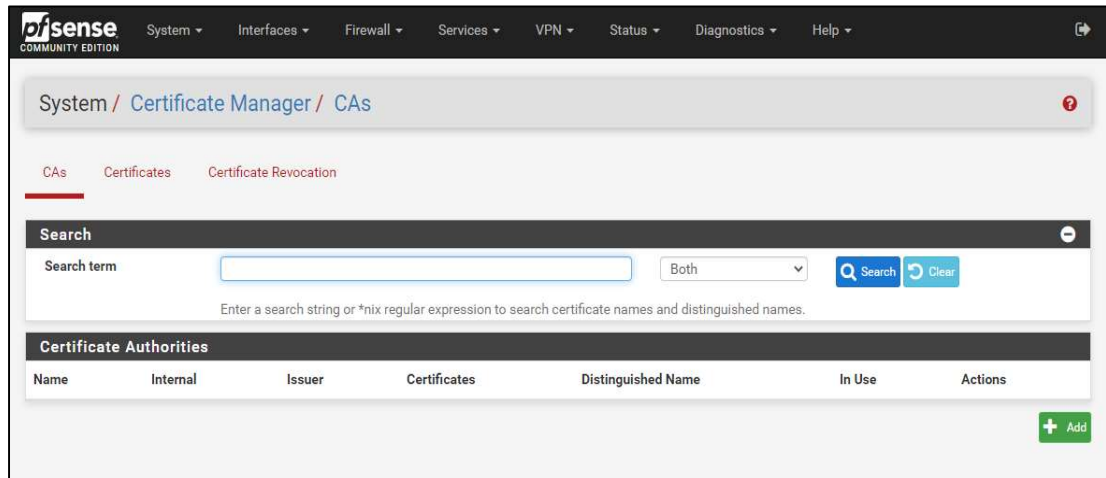
3.3. Cấu hình OpenVPN (pfSense) với VinCSS FIDO2® Cloud

3.3.1. Tạo Certificate Authority

- Nhấn **System > Cert. Manager**

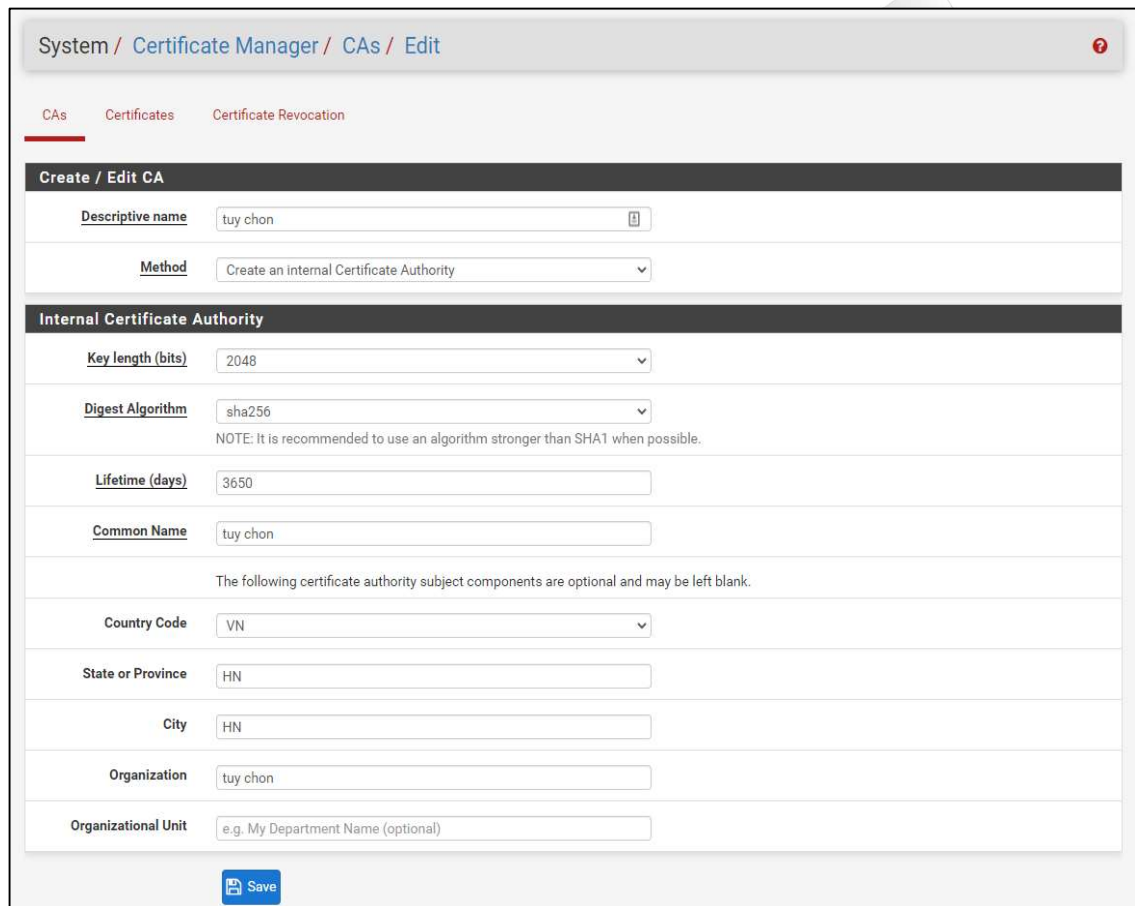


- Tại **System / Certificate Manager / CAs**, nhấn **Add**



The screenshot shows the Pfsense web interface for the Certificate Manager. The breadcrumb trail is "System / Certificate Manager / CAs". There are tabs for "CAs", "Certificates", and "Certificate Revocation". A search bar is present with a "Search" button and a "Clear" button. Below the search bar is a table titled "Certificate Authorities" with columns: Name, Internal, Issuer, Certificates, Distinguished Name, In Use, and Actions. An "Add" button is located at the bottom right of the table.

- Điền các thông tin như hình, sau đó nhấn **Save**.



The screenshot shows the Pfsense web interface for the Certificate Manager, specifically the "Edit" page for a Certificate Authority. The breadcrumb trail is "System / Certificate Manager / CAs / Edit". There are tabs for "CAs", "Certificates", and "Certificate Revocation". The "Create / Edit CA" section contains a "Descriptive name" field (placeholder: "tuy chọn") and a "Method" dropdown menu (selected: "Create an internal Certificate Authority"). Below this is the "Internal Certificate Authority" section with various configuration options: "Key length (bits)" (2048), "Digest Algorithm" (sha256), "Lifetime (days)" (3650), "Common Name" (placeholder: "tuy chọn"), "Country Code" (VN), "State or Province" (HN), "City" (HN), "Organization" (placeholder: "tuy chọn"), and "Organizational Unit" (placeholder: "e.g. My Department Name (optional)"). A "Save" button is located at the bottom.

3.3.2. Tạo OpenVPN Server Certificate

- Nhấn vào tab **Certificates**. Tại **System / Certificate Manager / Certificates**, nhấn **Add/Sign**

System / Certificate Manager / Certificates

CA's Certificates Certificate Revocation

Search

Search term Both

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificates

Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (5f03274c3d8dc) Server Certificate CA: No Server: Yes	self- signed	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense- 5f03274c3d8dc Valid From: Mon, 06 Jul 2020 13:29:48 +0000 Valid Until: Sun, 08 Aug 2021 13:29:48 +0000	webConfigurator	

- Điền các thông tin như hình, sau đó nhấn **Save**.

System / Certificate Manager / Certificates / Edit

CA's Certificates Certificate Revocation

Add/Sign a New Certificate

Method Create an Internal Certificate

Descriptive name

Internal Certificate

Certificate authority

Key length

Digest Algorithm
NOTE: It is recommended to use an algorithm stronger than SHA1 when possible.

Lifetime (days)

Common Name

The following certificate subject components are optional and may be left blank.

Country Code

State or Province

City

Organization

Organizational Unit

Certificate Attributes

Attribute Notes The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode.
For Internal Certificates, these attributes are added directly to the certificate as shown.

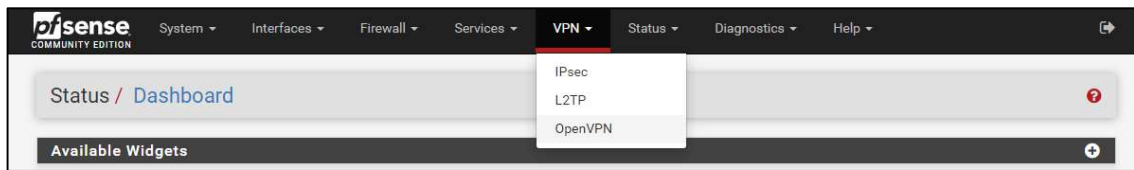
Certificate Type
Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.

Alternative Names
Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate as an Alternative Name. The signing CA may ignore or change these values.

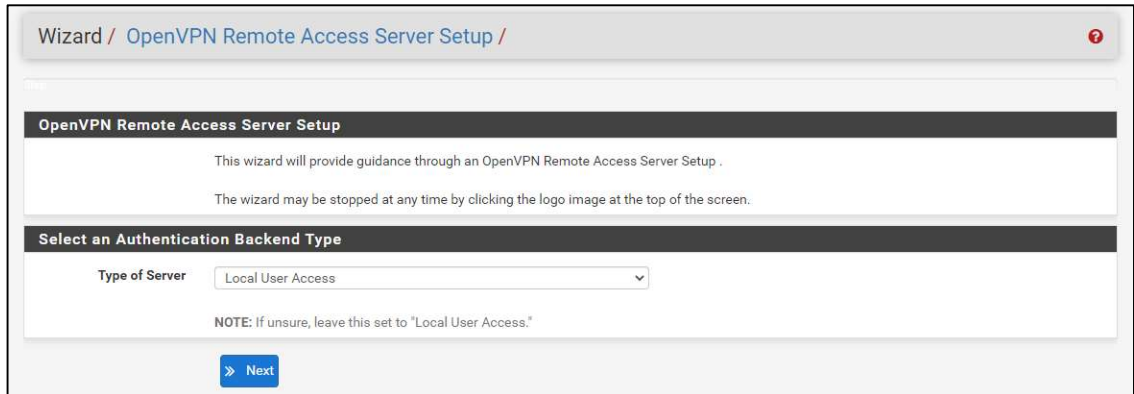
Add

3.3.3. Tạo VPN Server

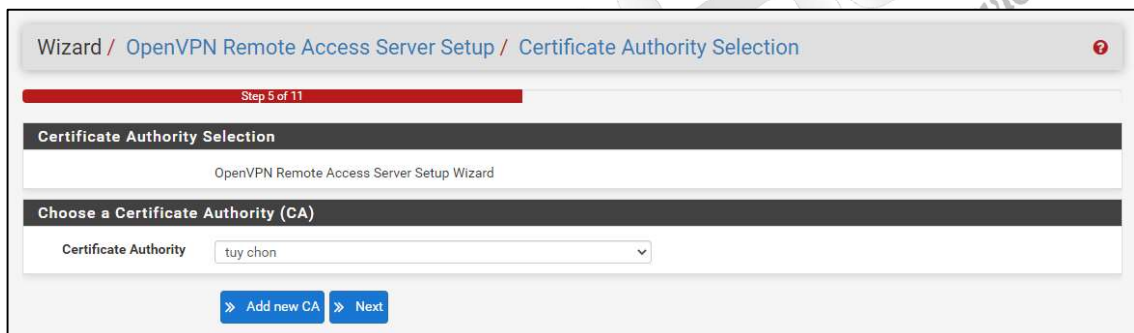
- Truy cập **VPN > OpenVPN**.



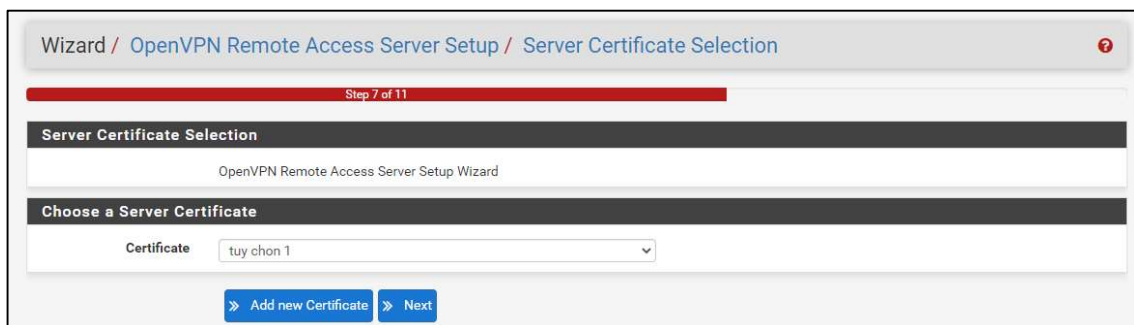
- Tại **OpenVPN**, nhấn vào tab **Wizards**. Chọn như hình, sau đó nhấn **Next**.



- Chọn CA đã tạo ở bước trước, sau đó nhấn **Next**.



- Chọn **OpenVPN Server Certificate** đã tạo ở bước trước, sau đó nhấn **Next**.



- Tại mục **Server Setup**, điền các thông tin như sau, sau đó nhấn **Next**.

General OpenVPN Server Information	
Interface	<div>WAN</div> <div>The interface where OpenVPN will listen for incoming connections (typically WAN.)</div>
Protocol	<div>UDP on IPv4 only</div> <div>Protocol to use for OpenVPN connections. If unsure, leave this set to UDP.</div>
Local Port	<div>Tùy chọn port</div> <div>Local port upon which OpenVPN will listen for connections. The default port is 1194. This can be left at its default unless a different port needs to be used.</div>
Description	<div>Tùy chọn mô tả</div> <div>A name for this OpenVPN instance, for administrative reference. It can be set however desired, but is often used to distinguish the purpose of the service (e.g. "Remote Technical Staff"). It is also used by OpenVPN Client Export to identify this VPN on clients.</div>

Cryptographic Settings	
TLS Authentication	<div><input checked="" type="checkbox"/></div> <div>Enable authentication of TLS packets.</div>
Generate TLS Key	<div><input checked="" type="checkbox"/></div> <div>Automatically generate a shared TLS authentication key.</div>
TLS Shared Key	<div></div> <div>Paste in a shared TLS key if one has already been generated.</div>
DH Parameters Length	<div>2048 bit</div> <div>Length of Diffie-Hellman (DH) key exchange parameters, used for establishing a secure communications channel. The DH parameters are different from key sizes, but as with other such settings, the larger the key, the more security it offers, but larger keys take considerably more time to generate. As of 2016, 2048 bit is a common and typical selection.</div>
Encryption Algorithm	<div>AES-128-CBC (128 bit key, 128 bit block)</div> <div>The algorithm used to encrypt traffic between endpoints. This setting must match on the client and server side, but is otherwise set however desired. Certain algorithms will perform better on different hardware, depending on the availability of supported VPN accelerator chips.</div>
Auth Digest Algorithm	<div>SHA256 (256-bit)</div> <div>The method used to authenticate traffic between endpoints. This setting must match on the client and server side, but is otherwise set however desired.</div>
Hardware Crypto	<div>No Hardware Crypto Acceleration</div> <div>The hardware cryptographic accelerator to use for this VPN connection, if any.</div>

Tunnel Settings	
Tunnel Network	<div>CIDR cấp cho người dùng VPN</div> <div>This is the virtual network used for private communications between this server and client hosts expressed using CIDR notation (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses will be assigned to connecting clients.</div>
Redirect Gateway	<div><input type="checkbox"/> Cho phép toàn bộ network traffic người dùng đi qua VPN</div> <div>Force all client generated traffic through the tunnel.</div>
Local Network	<div>Khái báo các CIDR để VPN có thể remote</div> <div>This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.</div>
Concurrent Connections	<div></div> <div>số user được sử dụng VPN tại cùng một thời điểm</div> <div>Specify the maximum number of clients allowed to concurrently connect to this server.</div>
Compression	<div>Omit Preference (Use OpenVPN Default)</div> <div>Compress tunnel packets using the LZO algorithm. Adaptive compression will dynamically disable compression for a period of time if OpenVPN detects that the data in the packets is not being compressed efficiently.</div>
Type-of-Service	<div><input type="checkbox"/></div> <div>Set the TOS IP header value of tunnel packets to match the encapsulated packet's TOS value.</div>
Inter-Client Communication	<div><input type="checkbox"/></div> <div>Allow communication between clients connected to this server.</div>
Duplicate Connections	<div><input type="checkbox"/></div> <div>Allow multiple concurrent connections from clients using the same Common Name. NOTE: This is not generally recommended, but may be needed for some scenarios.</div>

Client Settings

Dynamic IP ☒

Allow connected clients to retain their connections if their IP address changes.

Topology

Subnet -- One IP address per client in a common subnet

Specifies the method used to supply a virtual adapter IP address to clients when using tun mode on IPv4. Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Android). Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "net30".

DNS Default Domain

localdomain

Provide a default domain name to clients.

DNS Server 1

khai báo DNS server

DNS server IP to provide to connecting clients.

DNS Server 2

khai báo DNS server

DNS server IP to provide to connecting clients.

DNS Server 3

DNS server IP to provide to connecting clients.

DNS Server 4

DNS server IP to provide to connecting clients.

NTP Server

khai báo NTP server

Network Time Protocol server to provide to connecting clients.

NTP Server 2

khai báo NTP server

Network Time Protocol server to provide to connecting clients.

NetBIOS Options ☐

Enable NetBIOS over TCP/IP.
If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.

NetBIOS Node Type

none

Possible options: b-node (broadcasts), p-node (point-to-point name queries to a WINS server), m-node (broadcast then query name server), and h-node (query name server, then broadcast).

NetBIOS Scope ID

A NetBIOS Scope ID provides an extended naming service for NetBIOS over TCP/IP. The NetBIOS scope ID isolates NetBIOS traffic on a single network to only those nodes with the same NetBIOS scope ID.

WINS Server 1

A Windows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern networks.

WINS Server 2

A Windows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern networks.

Next

- Tại mục **Firewall Rule Configuration**, giữ cấu hình mặc định (chọn 2 mục **Firewall Rule** và **OpenVPN rule**), sau đó nhấn **Next**

Wizard / OpenVPN Remote Access Server Setup / Firewall Rule Configuration

Step 10 of 11

Firewall Rule Configuration

OpenVPN Remote Access Server Setup Wizard

Firewall Rule Configuration

Firewall rules control what network traffic is permitted. Rules must be added to allow traffic to the OpenVPN server's IP and port, as well as allowing traffic from connected clients through the tunnel. These rules can be automatically added here, or configured manually after completing the wizard.

Traffic from clients to server

Firewall Rule ☒

Add a rule to permit connections to this OpenVPN server process from clients anywhere on the Internet.

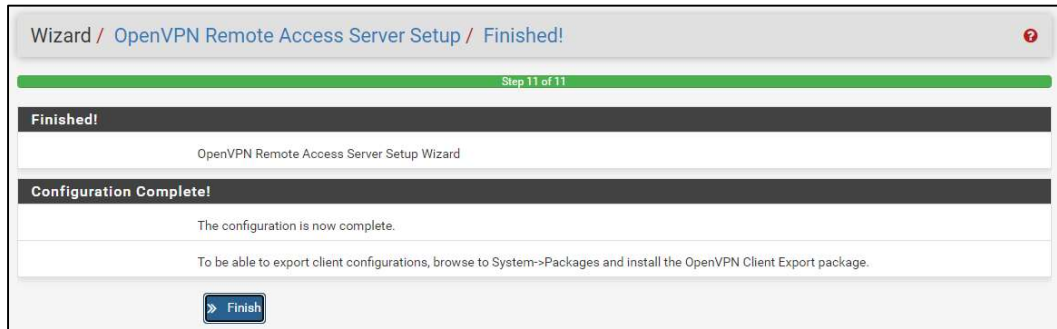
Traffic from clients through VPN

OpenVPN rule ☒

Add a rule to allow all traffic from connected clients to pass inside the VPN tunnel.

Next

- Tạo VPN Server thành công. Nhấn **Finish**.

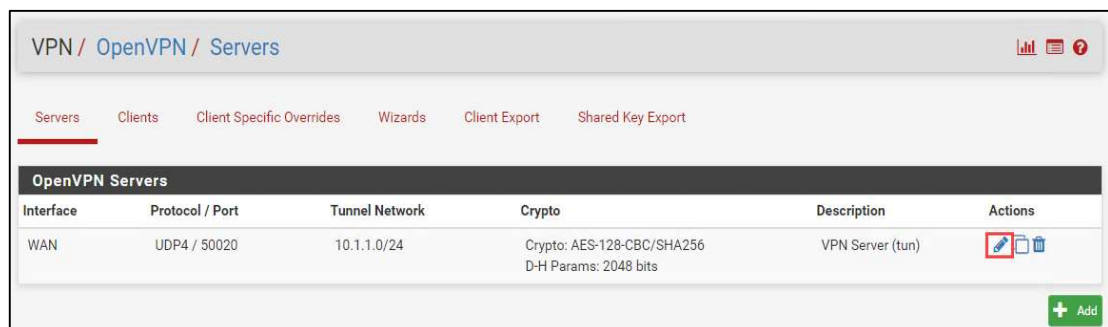


3.3.4. *Chỉnh sửa thông số VPN Server để hoạt động với FIDO2*

- Truy cập SSH vào pfSense và tạo một script có nội dung như sau:

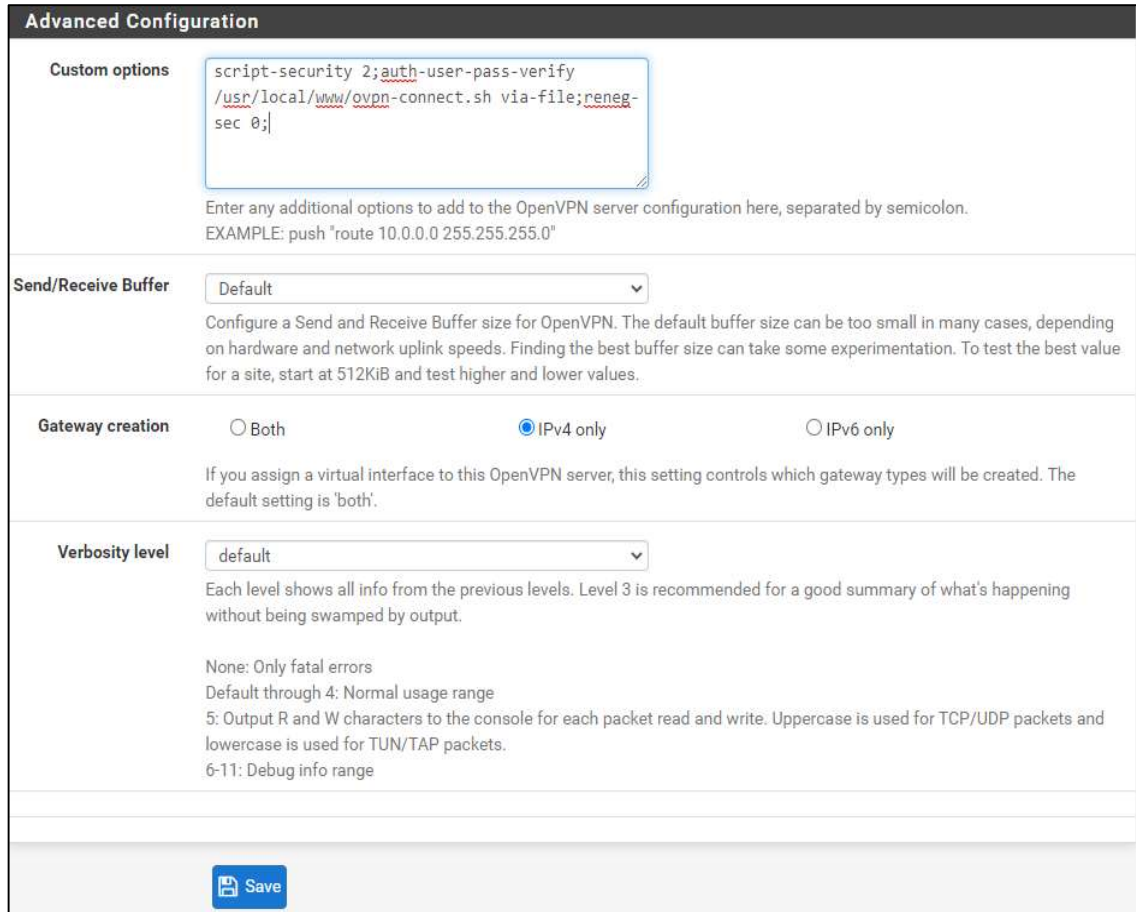
```
#!/bin/sh
username=`head -1 $1`
token=`tail -1 $1`
clientid="..." //điền ClientID đã tạo trên hệ thống VincSS FIDO2® Cloud
if [ "${username}" != "${common_name}" ]; then
    logger -4 -t openvpn "User ${username} not match with profile"
    exit 1
fi
response=$(curl -s --header "Content-Type: application/json" --request POST --data '{"username":"'${username}',"token":"'${token}',"clientid":"'${clientid}'"}' https://fido2cloud.vincss.net/oauth2/check)
if [ "$response" == "success" ]; then
    logger -4 -t openvpn "User '${username}' authenticated succeeded"
    exit 0
else
    logger -4 -t openvpn "User '${username}' authenticated failed"
    exit 1
fi
```

- Lưu file này vào đường dẫn `/usr/local/www/ovpn-connect.sh`
- Truy cập tab **VPN > OpenVPN > Servers**. Nhấn vào logo chỉnh sửa của OpenVPN Server vừa tạo như trong hình.



- Tại mục **Advanced Configuration / Custom options**, điền các tham số như sau, sau đó nhấn **Save**.

```
script-security 2;auth-user-pass-verify /usr/local/www/ovpn-connect.sh via-file;reneg-sec 0;
```



Advanced Configuration

Custom options

```
script-security 2;auth-user-pass-verify /usr/local/www/ovpn-connect.sh via-file;reneg-sec 0;
```

Enter any additional options to add to the OpenVPN server configuration here, separated by semicolon.
EXAMPLE: push "route 10.0.0.0 255.255.255.0"

Send/Receive Buffer Default

Configure a Send and Receive Buffer size for OpenVPN. The default buffer size can be too small in many cases, depending on hardware and network uplink speeds. Finding the best buffer size can take some experimentation. To test the best value for a site, start at 512KiB and test higher and lower values.

Gateway creation ☐ Both ☒ IPv4 only ☐ IPv6 only

If you assign a virtual interface to this OpenVPN server, this setting controls which gateway types will be created. The default setting is 'both'.

Verbosity level default

Each level shows all info from the previous levels. Level 3 is recommended for a good summary of what's happening without being swamped by output.

None: Only fatal errors
Default through 4: Normal usage range
5: Output R and W characters to the console for each packet read and write. Uppercase is used for TCP/UDP packets and lowercase is used for TUN/TAP packets.
6-11: Debug info range

Save

3.3.5. **Chỉnh sửa thông số Export profile**

- Truy cập tab **VPN > OpenVPN > Client Export**
- Tại mục **Advanced > Additional configuration options**, thêm các thông tin sau:

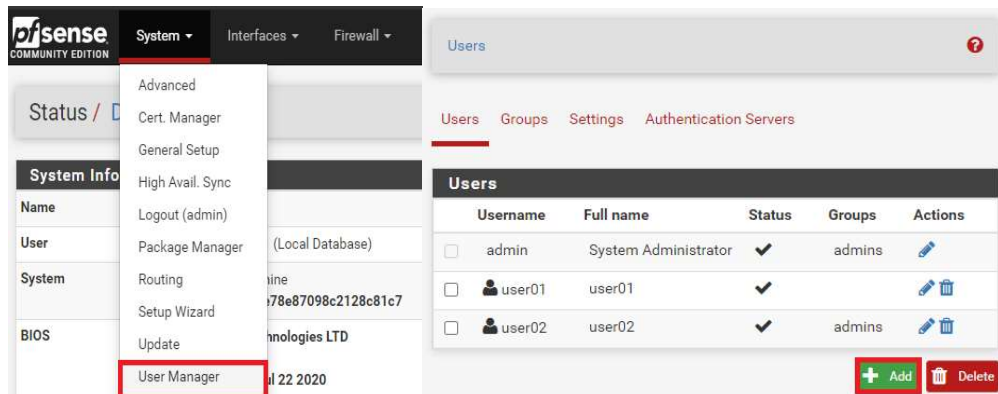
```
auth-user-pass
auth-user-allow-oauth2
client-id .....
client-secret .....
redirect-uri-port ....
oauth2-authorize-endpoint https://fido2cloud.vincss.net/authorize
oauth2-token-endpoint https://fido2cloud.vincss.net/token
oauth2-resource-endpoint https://fido2cloud.vincss.net/profile
reneg-sec 0
```

Trong đó:

- client-id, client-secret: được tạo bởi VinCSS FIDO2® Cloud, chi tiết tham chiếu “Tài liệu vận hành VinCSS FIDO2® Cloud”
- redirect-uri-port: sử dụng port trống bất kỳ
- oauth2-authorize-endpoint: URL của OAuth2 authorize endpoint
- oauth2-token-endpoint: URL của OAuth2 token endpoint
- oauth2-resource-endpoint: URL của OAuth2 resource endpoint

3.3.6. Tạo tài khoản cho người dùng VPN

- Truy cập System > User Manager. Tại tab Users, nhấn Add.



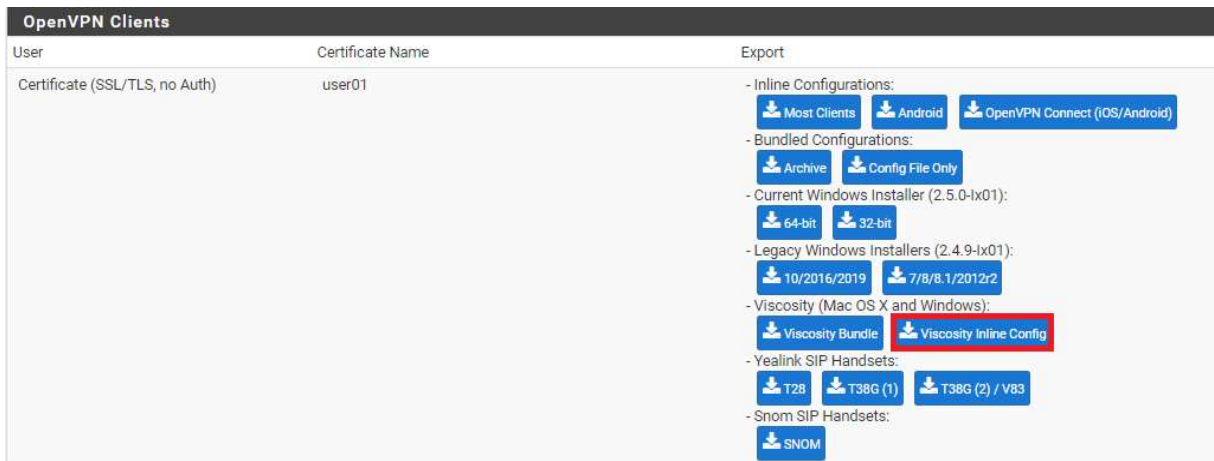
- Điền các thông tin chính như sau:
 - Username: tên tài khoản người dùng, bắt buộc phải trùng với tài khoản trong tổ chức trên hệ thống VinCSS FIDO2 Cloud
 - Password: mật khẩu của tài khoản
 - Full name: tên đầy đủ của người sử dụng
 - Certificate: chọn tại mục “Click to create a user certificate”
 - Descriptive name: giống với Username ở trên
 - Certificate authority: chọn CA đã tạo ở bước trên
- Nhấn Save để tạo tài khoản cho người dùng VPN.

3.3.7. Xuất profile cho người sử dụng

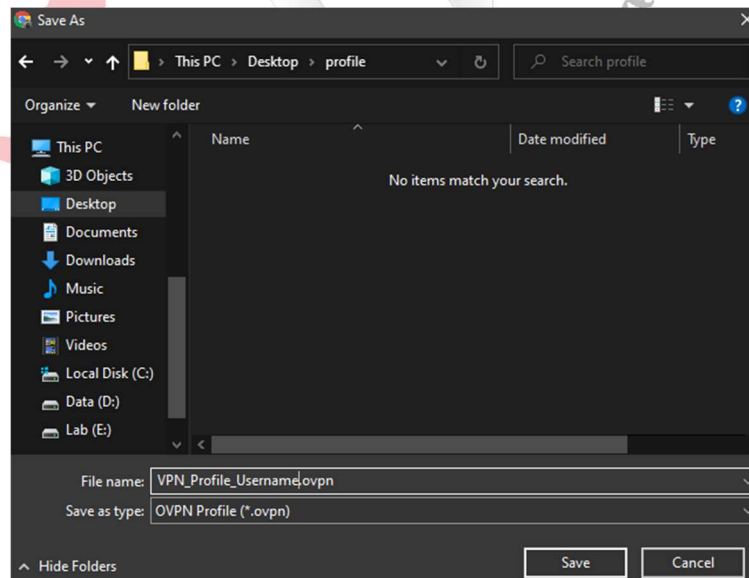
- Truy cập tab VPN > OpenVPN. Sau đó chọn mục Client Export



- Tại mục OpenVPN Clients, chọn người dùng cần xuất VPN profile, sau đó nhấn vào nút “Viscosity Inline Config”



- Chọn nơi lưu file OVPN, sau đó nhấn Save để lưu.



Sau khi Export Profile, sử dụng phần mềm **VinCSS OVPN Client** để kết nối. Chi tiết về cách sử dụng, vui lòng tham chiếu tài liệu “**Hướng dẫn sử dụng phần mềm VinCSS OVPN Client**”

Link download phần mềm VinCSS OVPN Client: <https://github.com/VinCSS-Public-Projects/VinCSS-FIDO2-OVPN-Client>

Link download tài liệu “**Hướng dẫn sử dụng phần mềm VinCSS OVPN Client**”:
<https://github.com/VinCSS-Public-Projects/FIDO2-Public-Documents>