

# Configuración VPN

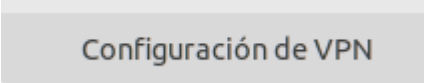
Instrucciones acerca de la configuración de la conexión VPN a las máquinas de PAM launcher (10.114.27.154) y break glass (10.114.27.220) de Cooperativa Andalucía

- [Configuración VPN](#)

# Configuración VPN

Los pasos para configurar la VPN son los siguientes:

- Acceder al **cliente nativo de VPN para Ubuntu:**



Configuración de VPN

- Hacer clic en el "+" para añadir una nueva conexión VPN y seleccionar la opción "**Cliente VPN multi-protocolo (openconnect)**":



- Configurar los campos según se observa en las capturas siguientes:

Cancelar

VPN «COOP. ANDALUCIA»

Aplicar

Detalles

Identidad

IPv4

IPv6

Nombre

### <b>General</b>

Protocolo VPN

VPN SSL Fortinet

Pasarela

vpn.andalucia.fin.ec:10

Certificado CA

(Ninguno)

Proxy

Permitir el escaneo de seguridad troyano (CSD)

Script envolvente de troyano (CSD)

SO declarado

### Certificado de autenticación

Certificado del usuario

(Ninguno)

Clave privada

(Ninguno)

Usar FSID para la frase de paso de la clave

Evitar que el usuario acepte certificados no válidos manualmente

### Testigo software de autenticación

Modo del testigo

Desactivado

Cadena del testigo

Cancelar **VPN «COOP. ANDALUCIA»** Aplicar

Detalles Identidad **IPv4** IPv6

**Método IPv4**

Automático (DHCP)  Sólo enlace local

Manual  Desactivar

Compartida con otros equipos

**DNS** Automático

Direcciones IP separadas por comas

**Rutas** Automático

Dirección	Máscara de red	Puerta de enlace	Métrica	
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	

Usar esta conexión sólo para los recursos en su red

- Guardamos los cambios.
- Previo al test, debemos contactar con [seguridades@andalucia.fin.ec](mailto:seguridades@andalucia.fin.ec) con el objetivo de que nos faciliten nuestro **usuario y contraseña** personales o, en su defecto, servirnos de las cuentas que se han almacenado en el password vault.
- Levantamos la conexión:

Connect to VPN "COOP. ANDALUCIA" ×

VPN host: vpn.andalucia.fin.ec:10443 ✓ Connect

Username: dcompany

Password: .....

Save passwords Cancel Login

> Log Close

- Aparentemente se nos mostrará un mensaje de error, que no es tal. Simplemente falta añadir el **2FA** asociado a nuestro correo electrónico, que recibiremos por esa vía a los pocos segundos:

^ No leídos

---

☆ > DoNotReply AuthCode:

- Añadimos el código y hacemos clic en Login:

Connect to VPN "COOP. ANDALUCIA" ×

VPN host: vpn.andalucia.fin.ec:10443 ✓ Connect

Code: .....

Save passwords Cancel Login

> Log Close

- A partir de ese instante, estaremos conectados a la VPN:



- Realizamos la prueba de conexión **ssh** a la máquina que alberga el break glass (10.114.27.220) sirviéndonos del usuario **root**, cuya contraseña hallaremos en el password vault:

```
lcompany@pw05y1n5:~$ ssh root@10.114.27.220
The authenticity of host '10.114.27.220 (10.114.27.220)' can't be established.
ED25519 key fingerprint is SHA256:ZGK+AWPE7jYue9jkoCPxig0o0LVz6oa0G7Z7qokfPc.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.114.27.220' (ED25519) to the list of known hosts.
root@10.114.27.220's password:
Last login: Tue Jul 29 03:23:57 2025 from 10.212.134.100
root@breakglass:~# docker ps
CONTAINER ID   IMAGE                                COMMAND                  CREATED        STATUS        PORTS                    NAMES
7a3abbf1fe27  eu.gcr.io/soffid-cloud/breakglass:1.0.6  "/bin/sh -c /opt/sof..." About an hour ago  Up About an hour  0.0.0.0:8080->8080/tcp, [::]:8080->8080/tcp, 8443/tcp  root-brea
root@breakglass:~#
```