Cristóbal Suárez Abad
2º ASIR
Seguridad y Alta Disponibilidad

Índice

1. ¿Qué es OpenVPN Access Server? (La Puerta Blindada)

Es la **infraestructura de acceso**.

- **Función:** Es la puerta de entrada a nuestra red desde un acceso remoto. Se encarga de construir el túnel seguro desde lugar donde se encuentra el usuario hasta la red.
- **En modo "Solo":** Si solo usas OpenVPN AS, este tendrá un listado con los usuario que pueden acceder.
    - *El problema:* Si tienes 5 entradas a tu red diferentes (VPN, Wi-Fi, Switch, Router), tienes que tener una copia de la lista de usuario en cada entrada. Si alguien deja de estar permitido o se agrega, tienes que manualmente cambiarlo en varios lugares

2. ¿Qué es RADIUS?

Es el **protocolo de "El que decide"**. RADIUS no es la base de datos en sí, es el **intermediario**.

- **Función:** Es un estándar que permite que diferentes entradas a la red(VPN, Wi-Fi, etc.) le pregunten a una central si alguien puede pasar.
- **Cómo funciona:** RADIUS tiene acceso a la "Base de Datos Maestra" (puede ser un fichero de texto, SQL, o Active Directory). Cuando alguien intenta entrar, RADIUS consulta esa base de datos y solo responde: **ACCESS-ACCEPT** (Déjale pasar) o **ACCESS-REJECT** (Largo de aquí).

3. ¿Qué aportan TRABAJANDO JUNTOS?

Cuando integras OpenVPN AS con RADIUS, consigues la arquitectura profesional con un único servidor de autenticación.

Aquí está el valor real de la unión:

A. Centralización (No te vuelvas loco)

- **Sin RADIUS:** Tienes que crear el usuario "Juan" en la VPN, "Juan" en el Wi-Fi y "Juan" en el servidor de correo. Si Juan cambia su contraseña, tiene que cambiarla en 3 sitios.
- **Con RADIUS:** Creas a "Juan" **una sola vez** en tu servidor central. OpenVPN (la pasarela) no sabe quién es Juan, simplemente le pasa las credenciales a RADIUS. Si RADIUS dice que son buenas, OpenVPN le deja pasar.
    - *Beneficio:* Gestión de usuarios en un solo punto.

B. Seguridad y Despido Rápido

- Si despides a un empleado o un alumno deja el centro, solo lo borras (o deshabilitas) en el servidor central (RADIUS/Base de datos).

- Automáticamente, **OpenVPN deja de permitirle el acceso** porque cuando pregunte a RADIUS, este le dirá "No".
- Si no tuvieras esto, tendrías que acordarte de entrar en la VPN y borrarlo manualmente.

C. Independencia (Escalabilidad)

- Hoy usas OpenVPN. Mañana compras un firewall Fortinet o pones Wi-Fi corporativo.
- Como ya tienes el servidor RADIUS montado, solo tienes que decirle al Wi-Fi: "Pregúntale a ese servidor RADIUS". No tienes que volver a crear los 500 usuarios en el nuevo aparato.

Actividad

Vamos a simular la integración usando **Docker Compose**. Levantaremos dos contenedores:

1. **`freeradius`**: Hará de Servidor de Autenticación.
2. **`openvpn-as`**: Hará de Pasarela VPN (usamos la versión Access Server porque trae interfaz web y facilita la integración en tiempo récord).

Aquí tienes la práctica lista para copiar y pegar ("Lab in a Box").

Preparación del entorno

Crea una carpeta llamada `practica-vpn-radius` y dentro creen un fichero llamado `docker-compose.yml`.

```
PS D:\> cd D:\2°_ASIR\Seguridad\'Tema 04'\'Actividad 3 - OpenVPN Radius'\practica-vpn-radius
PS D:\2°_ASIR\Seguridad\Tema 04\Actividad 3 - OpenVPN Radius\practica-vpn-radius> dir


    Directorio: D:\2°_ASIR\Seguridad\Tema 04\Actividad 3 - OpenVPN Radius\practica-vpn-radius


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        12/12/2025     11:45           1126 docker-compose.yml
```

1. El fichero `docker-compose.yml`

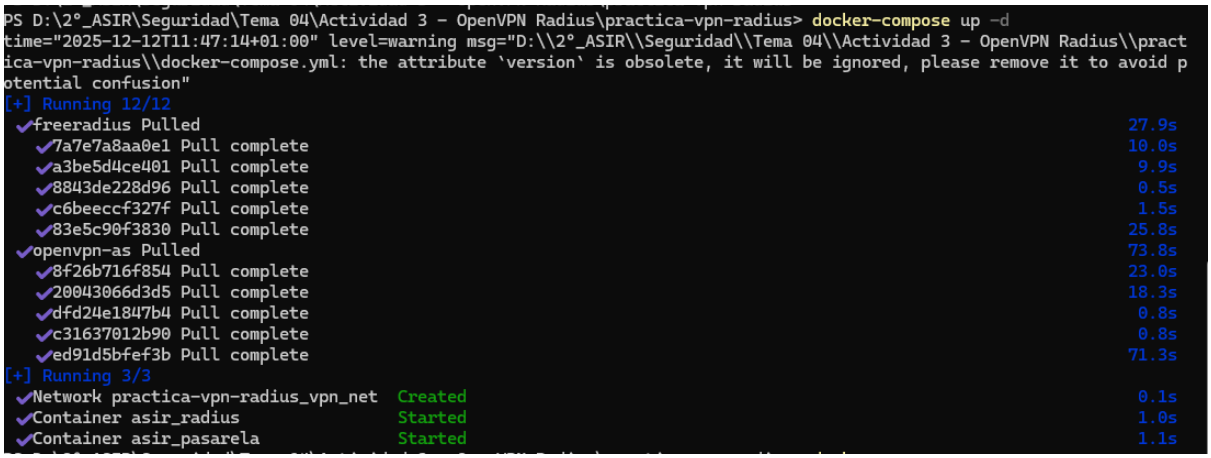
Este fichero define una red privada estática (para que sepamos las IPs de antemano) y los dos servidores.

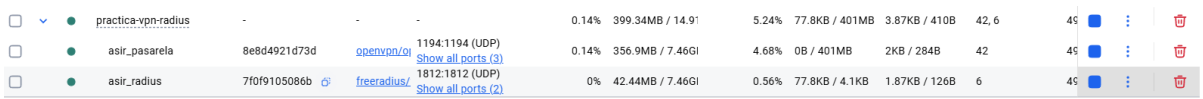
YAML
```
version: "3"

services:
  # --- Servidor RADIUS ---
  freeradius:
    image: freeradius/freeradius-server:latest
    container_name: asir_radius
    restart: unless-stopped
    ports:
      - "1812:1812/udp" # Puerto de autenticación
      - "1813:1813/udp" # Puerto de accounting
    networks:
      vpn_net:
        ipv4_address: 10.5.0.5 # Le damos IP fija para no fallar en la config

  # --- Pasarela VPN (OpenVPN Access Server) ---
  openvpn-as:
    image: openvpn/openvpn-as:latest
    container_name: asir_pasarela
    cap_add:
      - NET_ADMIN # Necesario para crear interfaces de red VPN
    environment:
      - PUID=1000
      - PGID=1000
      - TZ=Europe/Madrid
    ports:
      - "943:943"     # Web Admin UI
      - "9443:9443"   # Web Client UI (TCP)
      - "1194:1194/udp" # Tunel VPN (UDP)
    volumes:
      - ./config:/config
    restart: unless-stopped
    networks:
      vpn_net:
        ipv4_address: 10.5.0.6

# Definimos una red propia para controlar las IPs
networks:
  vpn_net:
    driver: bridge
    ipam:
```

```
config:
  - subnet: 10.5.0.0/24
```

Una vez creado, ejecutado levantar los contenedores:

```
docker-compose up -d
```



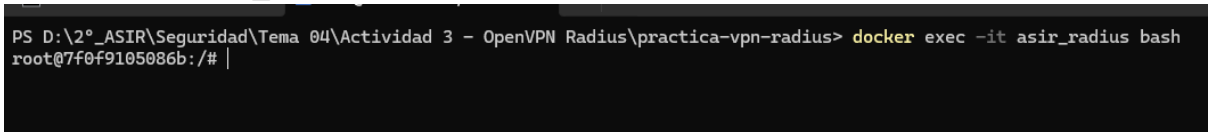


Fase 1: Configurar el Servidor RADIUS

Como estamos en Docker, usaremos `docker exec` para "entrar" en el servidor y configurarlo.

1. Entrar en el contenedor RADIUS:

Bash
docker exec -it asir_radius /bin/bash



2. Autorizar a la Pasarela (Cliente): Tenemos que decirle a RADIUS que acepte peticiones desde la IP de OpenVPN (`10.5.0.6`). *(Dentro del contenedor, pegamos esto en la terminal)*:

Bash
Añadimos el cliente al final del fichero clients.conf
cat >> /etc/raddb/clients.conf <<EOF

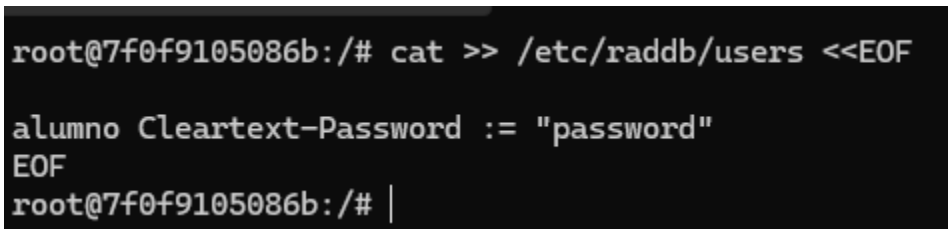
client openvpn-pasarela {
ipaddr = 10.5.0.6
secret = secretoASIR
}
EOF

Comprobamos: cat /etc/raddb/clients.conf

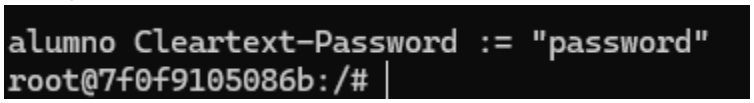
3. Crear un Usuario de prueba: Creamos el usuario `alumno` con contraseña `password`.

Bash
Añadimos el usuario al fichero users
cat >> /etc/raddb/users <<EOF

alumno Cleartext-Password := "password"
EOF



Comprobamos: cat /etc/raddb/users



4. Recargar configuración y salir: Como FreeRADIUS corre como proceso principal, lo ideal es salir y reiniciar el contenedor desde fuera.

Bash
exit
docker restart asir_radius

```
PS D:\2°_ASIR\Seguridad\Tema 04\Actividad 3 - OpenVPN Radius\practica-vpn-radius> docker restart asir_radius
asir_radius
PS D:\2°_ASIR\Seguridad\Tema 04\Actividad 3 - OpenVPN Radius\practica-vpn-radius>
```

5. Comprobación rápida: Podemos probar si RADIUS funciona desde nuestra propia máquina (si tenemos `radtest` instalado) o desde el mismo contenedor:

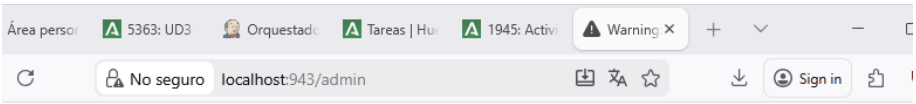
Bash
docker exec -it asir_radius radtest alumno password localhost 0 testing123
Debe responder: Access-Accept

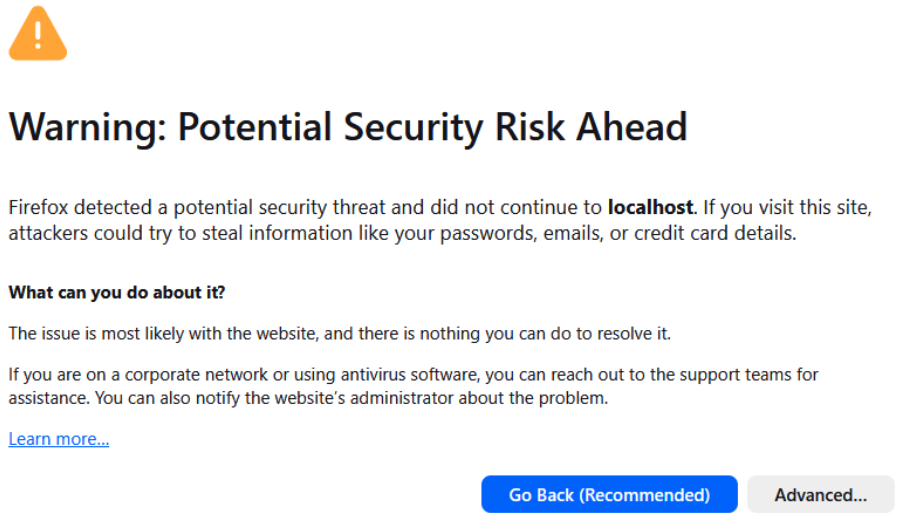
```
PS D:\2°_ASIR\Seguridad\Tema 04\Actividad 3 - OpenVPN Radius\practica-vpn-radius> docker exec -it asir_radius radtest al
umno password localhost 0 testing123
Sent Access-Request Id 50 from 0.0.0.0:33205 to 127.0.0.1:1812 length 76
        User-Name = "alumno"
        User-Password = "password"
        NAS-IP-Address = 10.5.0.5
        NAS-Port = 0
        Message-Authenticator = 0x00
        Cleartext-Password = "password"
Received Access-Accept Id 50 from 127.0.0.1:1812 to 127.0.0.1:33205 length 38
        Message-Authenticator = 0xeabb3622cefc51ac14dc0825a33f8844
PS D:\2°_ASIR\Seguridad\Tema 04\Actividad 3 - OpenVPN Radius\practica-vpn-radius>
```

Fase 2: Configurar la Pasarela OpenVPN

Ahora integramos la pasarela vía web.

1. **Acceder a la administración:**
    - Abrir navegador: `https://localhost:943/admin` (Aceptar advertencia de certificado SSL).

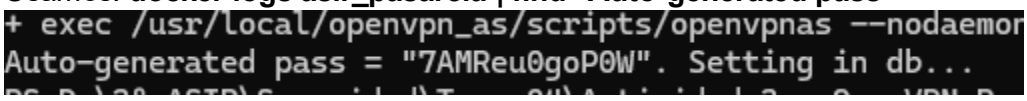




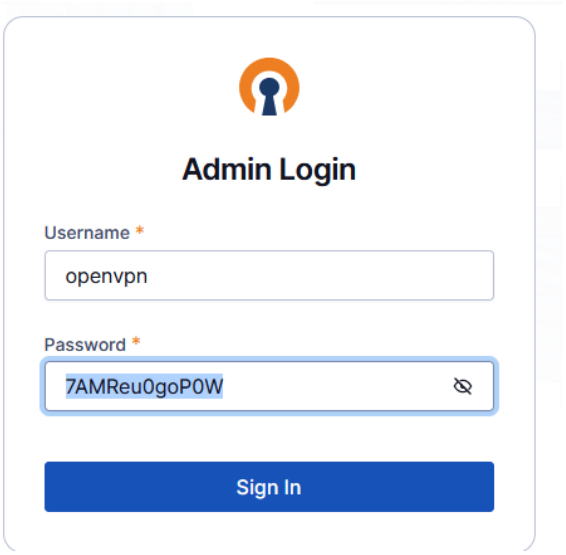
    - **Usuario:** openvpn

Contraseña: Mirar los logs para ver la contraseña temporal que genera el contenedor la primera vez, buscar “Auto-generated pass”.

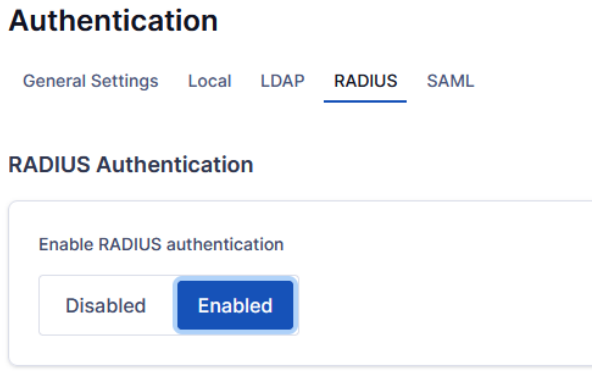
Usamos: **docker logs asir_pasarela | find "Auto-generated pass"**



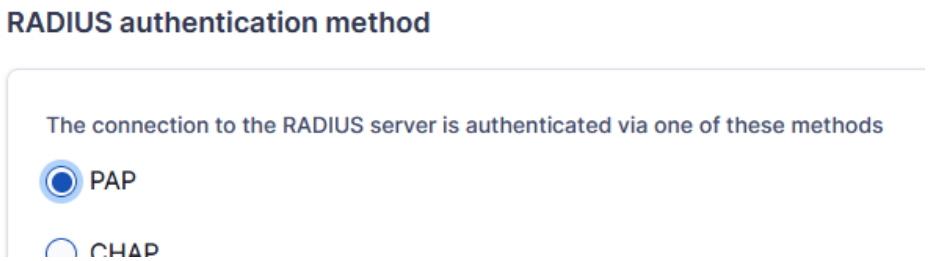
Pass: **7AMReu0goP0W**


Admin Login
Username *
openvpn
Password *
7AMReu0goP0W
Sign In

2. **Configurar RADIUS:**
    - Ir al menú **Authentication > RADIUS**.
    - Click en **"Enable RADIUS Authentication"**.

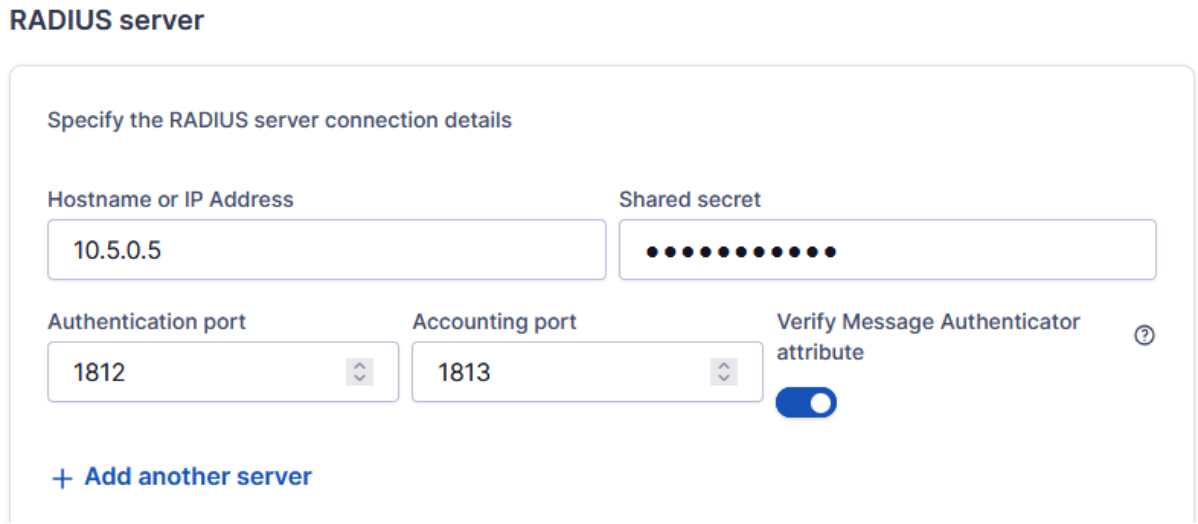


    - **PAP/CHAP:** Dejar en PAP o Auto.

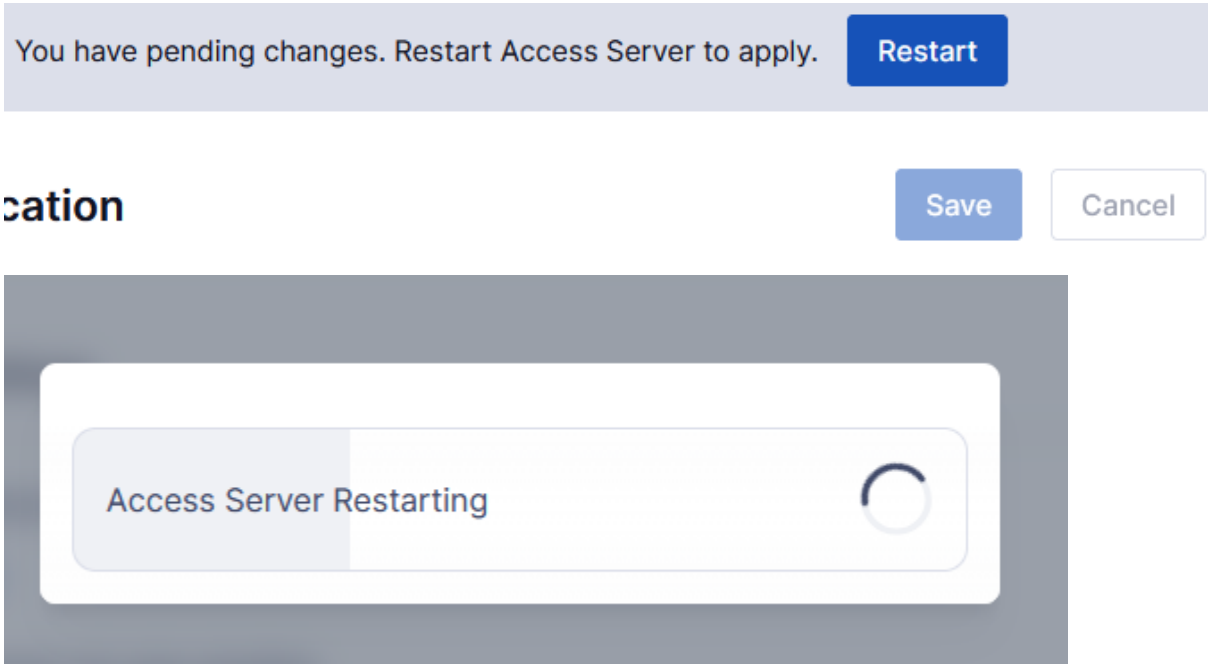


    - **Hostname:** `10.5.0.5` (La IP fija que pusimos en el docker-compose).
    - **Shared Secret:** `secretoASIR` (Lo que pusimos en clients.conf).

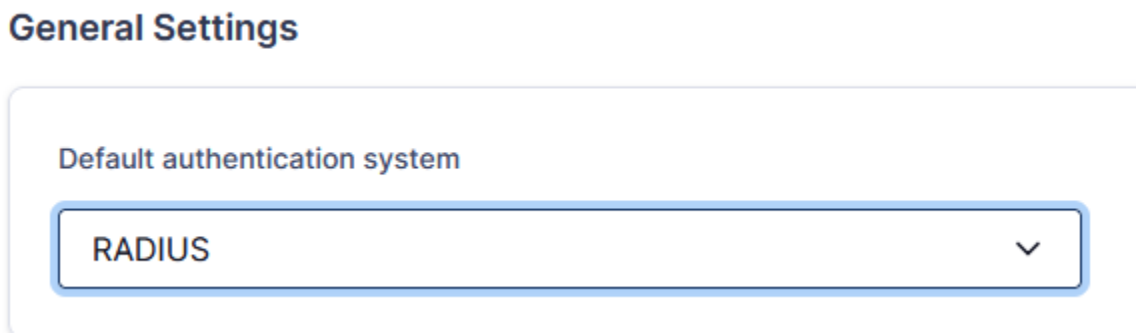
Fíjate que los puertos que se especifican sean los mismo que aparecen en el docker compose.



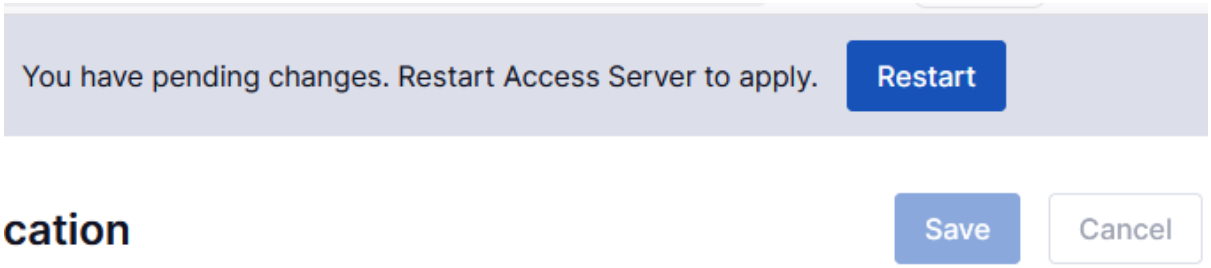
- Click en **"Save"** y luego arriba en **"Restart"**.



3. **Forzar RADIUS para todos**
    - Ve al menú **Authentication > General Settings**
    - Busca la opción que dice **Default Authentication System** (Sistema de autenticación por defecto).
    - Cámbialo de `Local` a **`RADIUS`**.



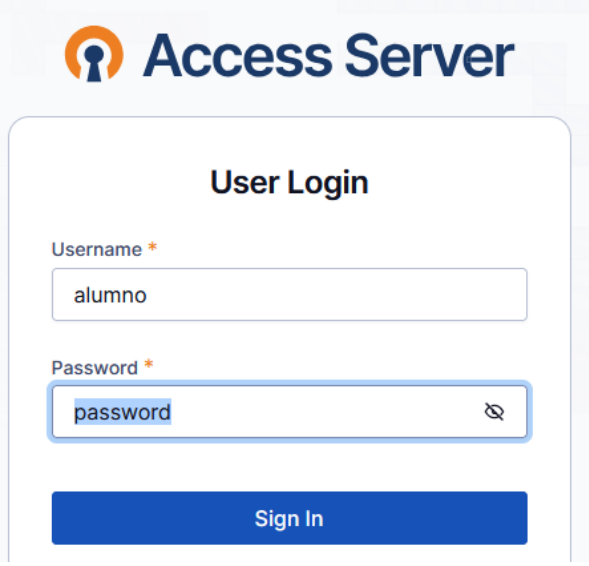
- Haz clic en **Save**
- Haz clic en **Restart** (el botón que aparece arriba).



Fase 3: La Prueba Final y Evaluación

Para evaluar que **realmente** hay integración, haremos la prueba de conexión y miraremos los logs.

1. **Prueba de Usuario:**
    - Ir a `https://localhost:943` (Interfaz de usuario).
    - Intentar entrar con Usuario: `alumno` / Contraseña: `password`.



    - Si entra y muestra la pantalla de "Download Client", **Superado**.