

# Acreditamiento WPA2 / Enterprise con FreeRadius

<b>Herramientas utilizadas:</b>	<b>1</b>
<b>Guía paso a paso:</b>	<b>2</b>
Instalación del paquete "FreeRadius"	2
Verificamos que se nos ha creado una CA	3
Configuración de las interfaces de nuestro servidor FreeRadius	4
Damos de alta todos los AP's (Access Points)	5
Añadir usuarios a nuestro servidor FreeRadius	6
Configurar los AP's	7
Configurar la autenticación WPA2 / Enterprise	12
(TEST) Prueba de autenticación	15
<b>Links Opcionales:</b>	<b>18</b>

## Herramientas utilizadas:

- 1 Access Point (Unifi AC-PRO)



- Software controlador para (Unifi AC-PRO)
  - En mi caso he utilizado la versión de Windows.

**Descarga**



- Instancia de PfSense instalada y configurada.



- Paquete disponible de FreeRadius en el repositorio de PfSense.



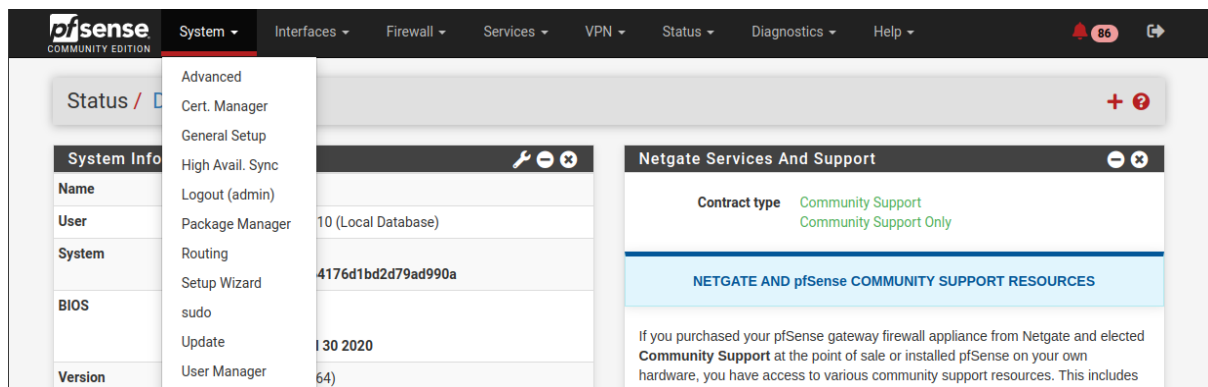
## Guía paso a paso:

### Instalación del paquete “FreeRadius”

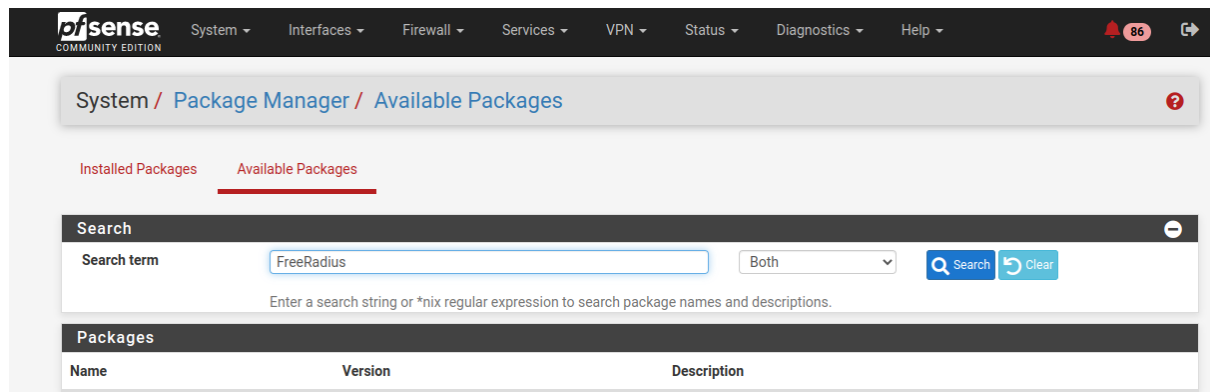
Lo primero que debemos realizar es instalar el paquete necesario para realizar la configuración.

Lo encontraremos en la siguiente ruta una vez nos situemos en el panel de control de PfSense:

**System → Package Manager**



Una vez nos situamos en el manejador de paquetes de PfSense debemos buscar en “**Available Packages**” la instancia necesaria de **FreeRadius**.



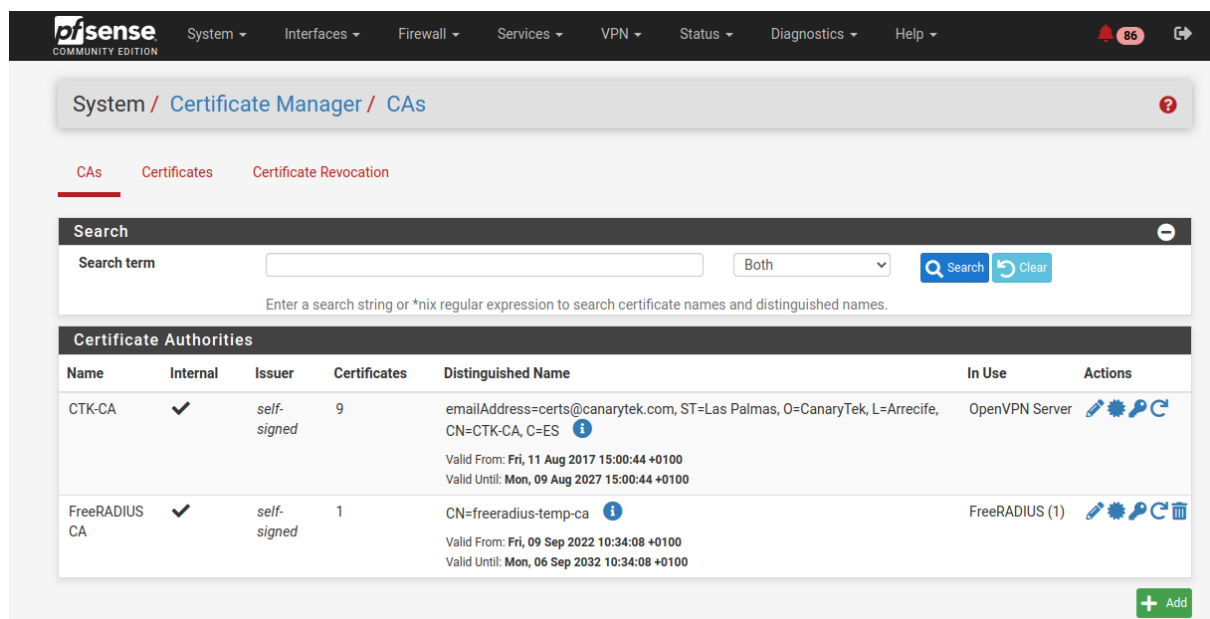
**\*\*En mi caso no aparece puesto que ya lo tenemos instalado.\*\***

## Verificamos que se nos ha creado una CA





Una vez hemos instalado nuestro paquete **FreeRadius** podemos ver como se nos ha creado automáticamente una autoridad gestora de certificados con el nombre de **FreeRadius CA** y un certificado para la autenticación llamado **FreeRadius Server Certificate**.


Lo podemos comprobar si nos situamos en la siguiente ruta:

**System → Cert Manager → CA's**



## System → Cert Manager → Certificates

FreeRADIUS Server Certificate	FreeRADIUS CA	CN=freeradius-temp-server 	FreeRADIUS (1)   
Server Certificate		Valid From: <b>Fri, 09 Sep 2022 10:34:09 +0100</b>	
CA: <b>No</b>		Valid Until: <b>Mon, 06 Sep 2032 10:34:09 +0100</b>	
Server: <b>Yes</b>			

 Add/Sign

## Configuración de las interfaces de nuestro servidor FreeRadius


Una vez realizada la instalación podemos continuar con la configuración de nuestras interfaces por la que un usuario al acceder al Wifi va a poder autenticarse con nuestro servidor.


Para configurar nuestro servidor Radius debemos ir a **Services → FreeRadius → Interfaces**

Crearemos en nuestro caso una para la “**Autenticación**”:

Añadiremos una nueva interfaz con los siguientes parámetros:

**General Configuration**

<u>Interface IP Address</u>	<input type="text" value="*"/>
Enter the IP address (e.g. 192.168.100.1) of the listening interface. If you choose * then it means all interfaces. (Default: *)	
<u>Port</u>	<input type="text" value="1812"/>
Enter the port number of the listening interface. Different interface types need different ports. Click Info for details. 	
<u>Interface Type</u>	<div>Authentication</div>
Enter the type of the listening interface. (Default: Authentication)	
<u>IP Version</u>	<div>IPv4</div>
Enter the IP version of the listening interface. (Default: IPv4)	
<u>Description</u>	<input type="text" value="Authentication Port"/>
Optionally enter a description here for your reference.	

 Save

Añadiremos una segunda interfaz de tipo “Accounting” con los siguientes parámetros:

**General Configuration**


**Interface IP Address**

\*

Enter the IP address (e.g. 192.168.100.1) of the listening interface. If you choose \* then it means all interfaces. (Default: \*)

**Port**

1813

Enter the port number of the listening interface. Different interface types need different ports. Click Info for details. 

**Interface Type**

Accounting

Enter the type of the listening interface. (Default: Authentication)

**IP Version**


IPv4

Enter the IP version of the listening interface. (Default: IPv4)

**Description**

Account Port

Optionally enter a description here for your reference.

 Save

Listo por ahora deberían verse dos interfaces en nuestro dashboard tal que así:

Interface IP Address	Port	Interface Type	IP Version	Description	
*	1812	auth	ipaddr	Authentication Port	 
*	1813	acct	ipaddr	Account Port	 
					 Add

 Save

## Damos de alta todos los AP's (Access Points)

Para dar de alta nuestros puntos de acceso debemos ir a la siguiente ruta:

**Services → FreeRadius → Nas / Clients**

Cabe destacar que si tenemos algún controlador en nuestra red por ejemplo un Ruckus también debemos incluirlo.

Añadiremos uno configurando los siguientes parámetros:

**General Configuration**

**Client IP Address**

192.168.20.0/24

Enter the IP address or network of the RADIUS client(s) in CIDR notation. This is the IP of the NAS (switch, access point, firewall, router, etc.).

**Client IP Version**

IPv4

**Client Shortname**

FreeRadius\_Test

Enter a short name for the client. This is generally the hostname of the NAS.

**Client Shared Secret**

\*\*\*\*\*

Enter the shared secret of the RADIUS client here. This is the shared secret (password) which the NAS (switch, accesspoint, etc.) needs to communicate with the RADIUS server. FreeRADIUS is limited to 31 characters for the shared secret.  
**Warning:** Single quotes in shared secret must be escaped with a backslash ( \ ' ). Backslash must be escaped by using two backslashes ( \\ ).








**Client IP Address:** IP del punto de acceso que queremos registrar o también podemos usar notación CIDR.


**Client IP Version:** IPv4 por defecto

**Client Shortname:** Nombre que le pondremos a nuestra instancia para identificarla. Es recomendable que se le ponga un nombre que haga referencia al AP que estamos añadiendo.

**Client Shared Secret:** Clave secreta que compartirá nuestro servidor FreeRadius y nuestro AP para poder autenticarse el uno con el otro.

Después de añadir los distintos AP que se encuentran en el establecimiento nos quedaría una tabla así:

Client IP Address	Client IP Version	Client Shortname	Client Protocol	Client Type	Require Message Authenticator	Max Connections	Description
192.168.20.0/24	ipaddr		udp	other	no	16	 
	ipaddr	FreeRadius_Ruckus_Controller	udp	other	no	16	 
192.168.20.210	ipaddr	TestRadiusAP-PRO	udp	other	no	16	 
<div> Add</div>							

 Save

## Añadir usuarios a nuestro servidor FreeRadius

Para poder añadir usuarios en nuestro servidor debemos seguir la siguiente ruta:

## Services → FreeRadius → Users

Una vez allí solo tenemos que añadir nuevos usuarios usando los siguientes parámetros por defecto:

General Configuration	
<b>Username</b>	<input type="text"/> <small>Enter the username. Whitespace is allowed. Note: May only contain a-z, A-Z, 0-9, underscore, period and hyphen when using OTP.</small>
<b>Password</b>	<input type="password"/> <small>Enter the password for this username. Leave empty if you want to use custom options (such as OTP) instead of username/password.</small>
<b>Password Encryption</b>	<div>Cleartext-Password ▾</div> <small>Select the password encryption for this user. If the (pre-hashed) options are used, the password should already be hashed by the expected hash function. Note that not all authentication protocols are compatible with all types of hashed passwords. Default: Cleartext-Password</small>

Una vez configurado nuestro servidor Radius debemos ir a cada punto de acceso para configurar la autenticación **WPA2 / Enterprise** y dar de alta nuestro servidor Radius.

## Configurar los AP's

En nuestro caso se realizaron pruebas con Ruckus pero me resultó bastante lioso y tuve varios errores.

Luego probé con el UniFi AC-PRO y la configuración fue bastante sencilla la verdad.

Tenemos que configurar cada Access Point uno a uno.

En este tutorial vamos a realizar la configuración con el UniFi AC-PRO.

Para configurar inicialmente este dispositivo vamos a tener que conectarlo a un cable de red POE y conectarnos también con un cable ethernet.

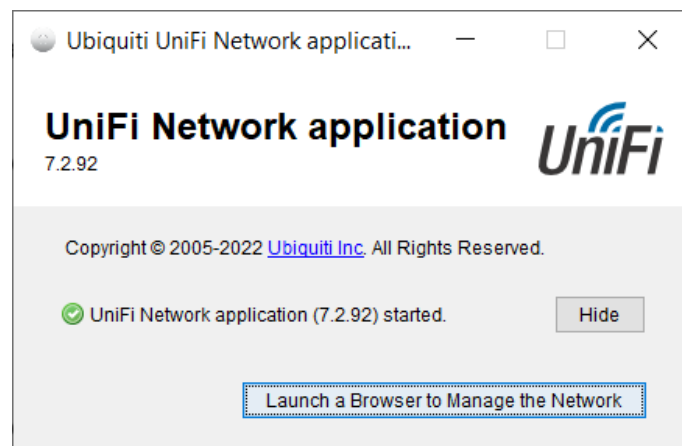
Si conectamos nuestro AP a la red directamente este obtendrá una dirección por DHCP.

Debemos tener instalada el controlador de UniFi, el cual voy a dejar los links de las versiones de Windows y Ubuntu para que no tengáis que buscarlos arriba:

UniFi Network Application 7.2.92 for Windows [Link](#)

UniFi Network Application 7.2.92 for Debian/Ubuntu [Link](#)

Una vez instalada la aplicación y estando conectados al Access Point abriremos la aplicación.



Se nos iniciará una interfaz web dónde podemos configurar el punto de acceso.



The image shows the UniFi login interface. At the top center is the UniFi logo with the version number 7.2.92 below it. Below the logo are two input fields: 'Username' and 'Password'. Under the password field is a checkbox labeled 'Remember me' with an information icon to its right. A blue 'SIGN IN' button is positioned below these elements. At the bottom center, there is a link for 'FORGOT PASSWORD?'.

UniFi®  
7.2.92

Username

Password

☐ Remember me ⓘ

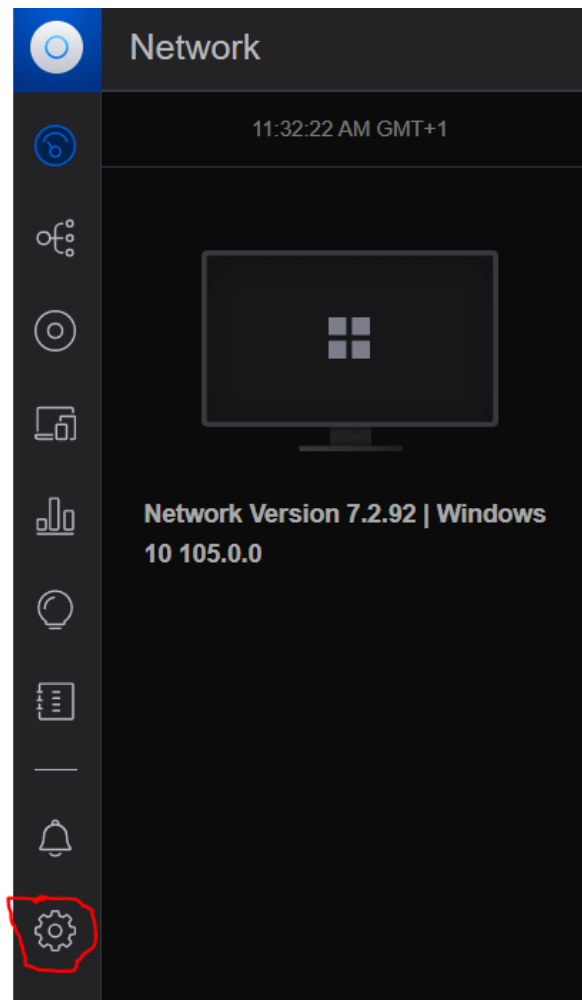
SIGN IN

FORGOT PASSWORD?

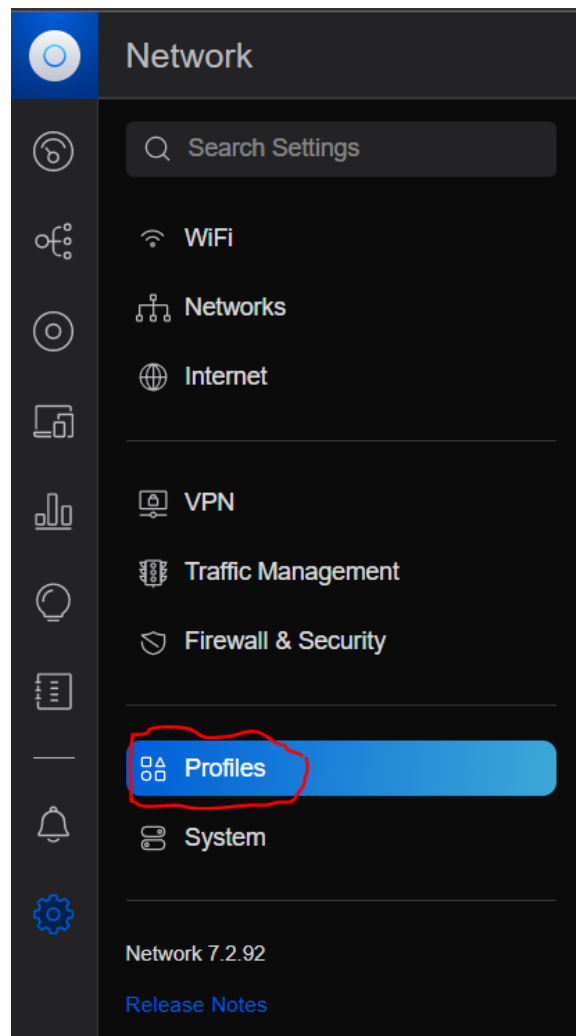
Se nos abrirá una pestaña en la que tendremos que autenticarnos con nuestra cuenta de UniFi. Si no posees una puedes registrarte accediendo a través de este [link](#).

Una vez hemos iniciado sesión con nuestra cuenta debemos configurar nuestro servidor radius.

Para ello accederemos a la configuración del punto de acceso tal y como se muestra en la siguiente imagen:



Para ello debemos darle de alta en los perfiles de nuestro AP:



En esta pestaña encontraremos un apartado dedicado a los perfiles del servidor radius:

RADIUS		
NAME ^	AUTH SERVERS	ACCOUNTING SERVERS
Default		
RadiusAuth	192.168.20.1 : 1...	192.168.20.1 : 1813
RadiusPFSENSE	192.168.20.1 : 1...	192.168.20.1 : 1813
+ Create New RADIUS Profile		

Crearemos un perfil nuevo. Configurando los siguientes parámetros:

The screenshot shows a configuration page with a dark theme. At the top, there is a 'Name' label followed by a dark input field. Below this is a section titled 'RADIUS Assigned VLAN Support'. It contains two rows: 'Wired Networks' with an information icon and an 'Enable' checkbox, and 'Wireless Networks' with an information icon and an 'Enable' checkbox. The next section is 'RADIUS Settings', which is separated by a horizontal line. It contains four rows: 1. 'Authentication Servers' with an 'IP Address' label, a text input containing '1812', a 'Shared Secret' label, and a '+ Add' button. 2. 'Enable Accounting' with an 'Enable' checkbox. 3. 'RADIUS Accounting Servers' with an 'IP Address' label, a text input containing '1813', a 'Shared Secret' label, and a '+ Add' button. 4. 'Enable Interim Update' with an 'Enable' checkbox and a numeric input containing '3600'.

**Name:** Nombre que hace referencia a nuestro servidor Radius.

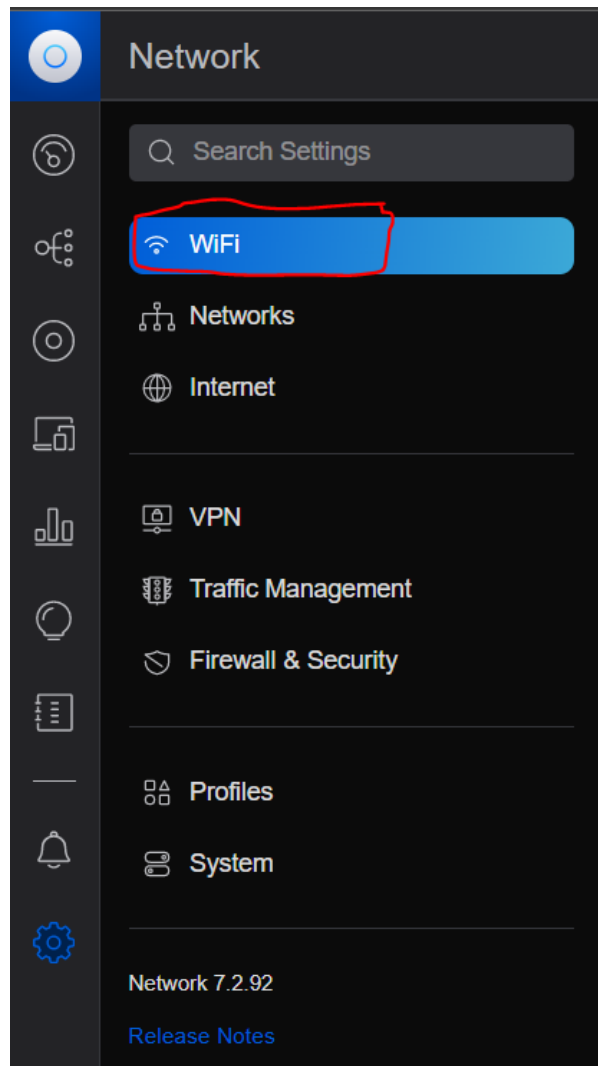
**Radius Assigned VLAN Support:** Esta configuración hace que según con el usuario que nos autenticamos nos asigna una VLAN que deberíamos tener previamente configurada en nuestro controlador. (Nosotros omitimos esta configuración)

**Authentication Servers:** IP del servidor Radius junto con la interfaz a la que hace referencia. Nosotros usaremos las dos que creamos previamente (1812 = “Authentication” y 1813 = “Accounting”). También tenemos que aportar el “*Shared Secret*” que usamos para dar de alta a nuestro AP. Si estos Shared Secrets no coinciden nuestro AP no podrá solicitar la autenticación a nuestro servidor Radius.

## Configurar la autenticación WPA2 / Enterprise

Habilitar la red WiFi creada para que la autenticación sea por WPA2 / Enterprise usando nuestro servidor Radius.

Para ello debemos ir al apartado de configuración de nuestra WiFi:



Seleccionamos nuestra red:

[illegible]

Una vez abierta la configuración de nuestra red debemos acceder a la configuración avanzada:

The screenshot shows the 'Advanced Configuration' section of a network management interface. At the top, there are input fields for 'Name' (TestRadiusAP-PRO) and 'Network' (Default). Below these is a 'Broadcasting APs' section with a table header: NAME, MODEL, IP ADDRESS, and WIFI EXP. The table contains one entry: a checked checkbox, a plus icon, a speech bubble icon, and the text 'All APs (1 APs)'. Below the table is a '+ Create New Group' link. The 'Advanced Configuration' section has two tabs: 'Auto' and 'Manual' (selected). Under the 'Manual' tab, there are settings for 'WiFi Band' (checked for 2.4 GHz and 5 GHz) and 'WiFi Type' (radio buttons for Standard and Guest Hotspot, with Standard selected). At the bottom, there are 'Pause' and 'Remove' buttons.

Y en el apartado de seguridad debemos seleccionar la autenticación **WPA2 / Enterprise** a la vez que elegimos el perfil Radius que creamos previamente.

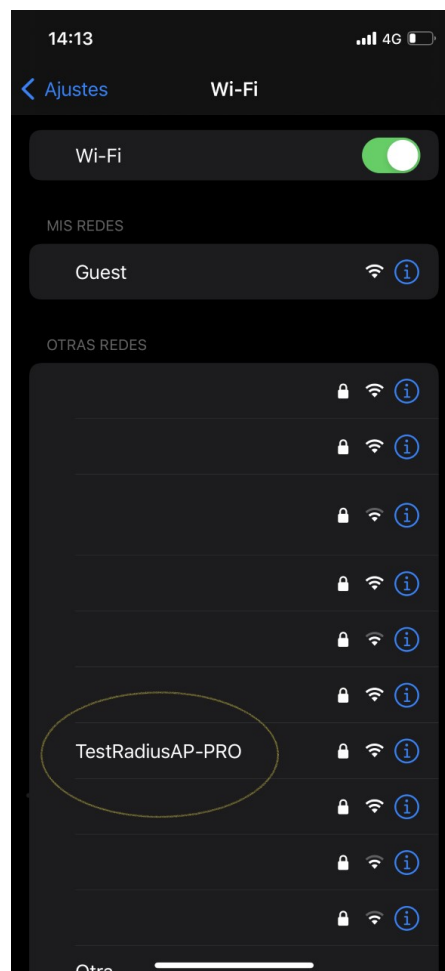
The screenshot shows the 'Security' section of a network management interface. It has a title 'Security' with an information icon. Below the title are several settings: 'Security Protocol' with radio buttons for Open, WPA2, WPA2 Enterprise (selected), WPA2/WPA3, WPA3, and WPA3 Enterprise; 'RADIUS Profile' with a dropdown menu showing 'RadiusAuth'; 'PMF' with radio buttons for Required, Optional, and Disabled (selected); 'Group Rekey Interval' with a checked 'Enable' checkbox and a dropdown menu showing '3600' seconds; and 'Hide WiFi Name' with an unchecked 'Enable' checkbox.

Por ahora ya tendríamos la autenticación WPA2 / Enterprise habilitada, notaremos que nuestro Punto de Acceso se reiniciará durante unos segundos y volverá a levantar nuestra WiFi pero esta vez utilizando las medidas de seguridad que le hemos configurado.

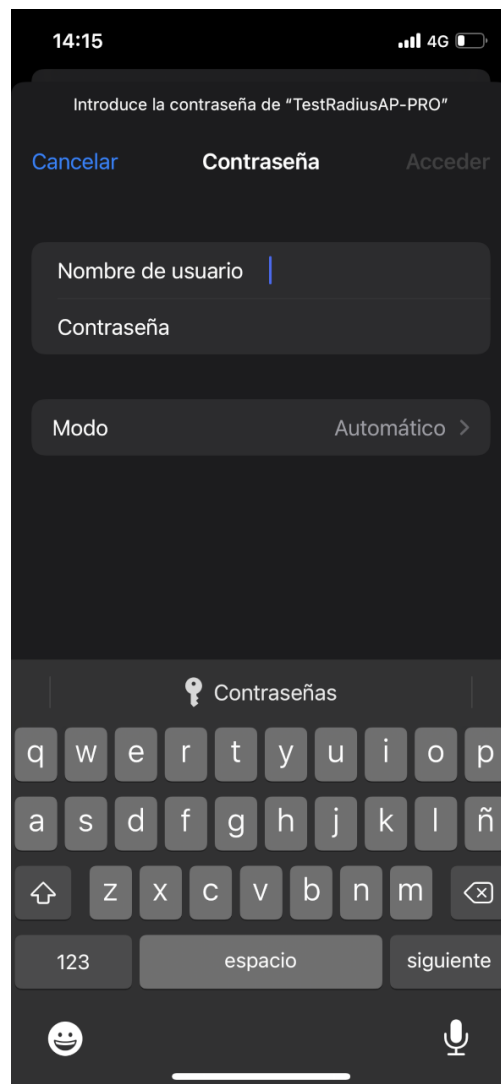
## (TEST) Prueba de autenticación

Para realizar una prueba de autenticación voy a realizarla en un iPhone 12, en el cual me conectaré al punto WiFi que acabamos de crear para verificar que se me instala el certificado y se me conecta adecuadamente.

Seleccionamos nuestro AP:

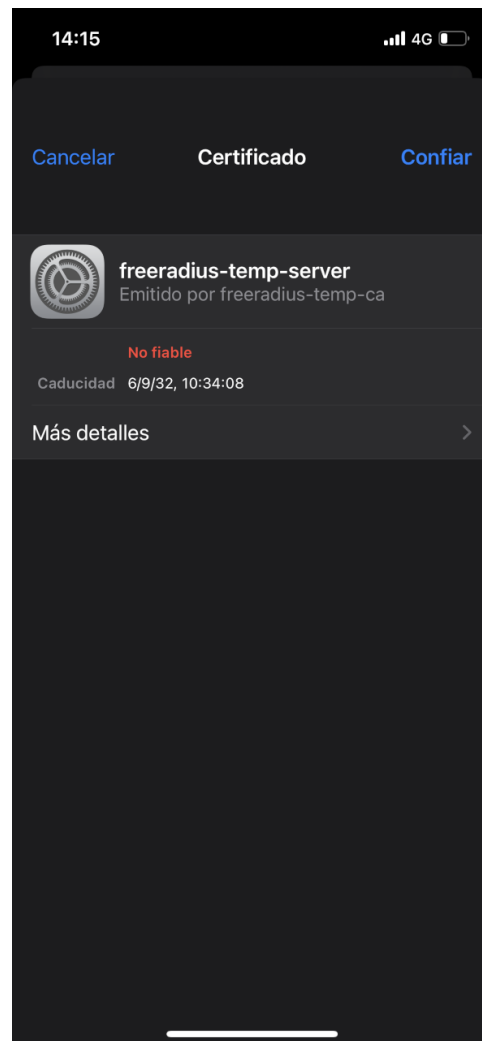


Insertamos nuestras credenciales:

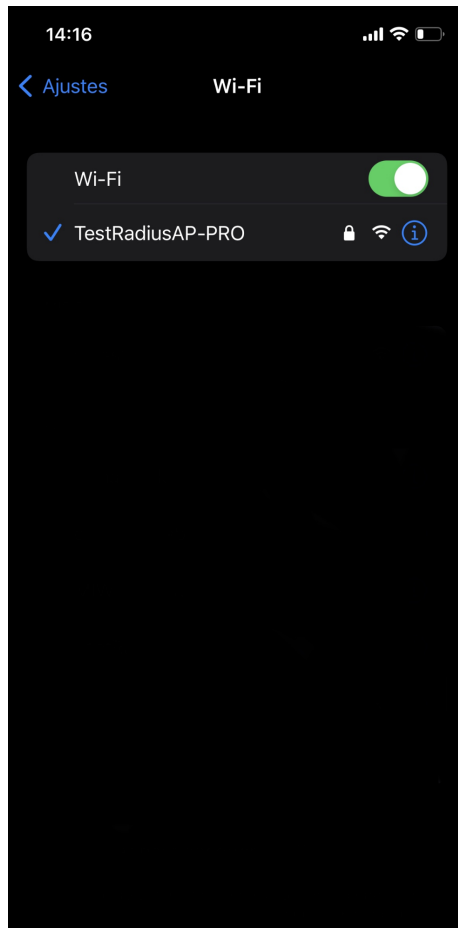


Instalamos el certificado generado por nuestra entidad de confianza:





Comprobamos la conexión:



Hemos verificado que tenemos acceso con nuestras credenciales y que el punto de acceso queda configurado.

## Links Opcionales:

Manual de usuario Access Point (Unifi AP-PRO) [Link](#)

Documentación PFSense [Link](#)