AUTENTICACIÓN MEDIANTE SERVIDOR FREERADIUS

INDUSTRY MANAGEMENT AND AUTOMATION

PHOENIX CONTACT

Tabla de Contenido

Tabla de Ilustraciones

1.Introducción

Para poder usar el sistema de autentificación FreeRADIUS se necesitan tres componentes: el equipo con el **servidor RADIUS**, el **Autentificador** y el **Cliente solicitante**.

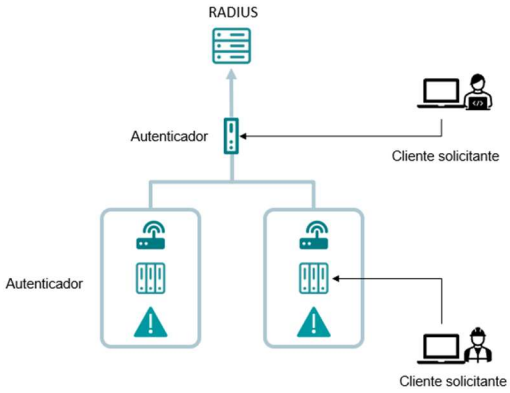

Ilustración 1.1.- Ejemplo de arquitectura con el servidor RADIUS

1.1. Equipo con servidor RADIUS

Almacena y administra la base de datos de los usuarios autorizados y sus respectivas credenciales de acceso (como nombre de usuario y contraseña). Cuando alguien intenta conectarse con el servidor FreeRADIUS verifica si esa persona tiene los permisos necesarios y decide si permite o niega el acceso.

1.2. Autenticador

Actúa como un intermediario entre el cliente y el servidor FreeRADIUS. Generalmente, el autenticador es un equipo de red como un router, switch o un punto de acceso WiFi. Su función consiste en recibir las solicitudes de conexión de los usuarios y enviarlas al servidor FreeRADIUS para que las verifique.

1.3. Cliente solicitante

El usuario final que desea acceder a la red. Puede ser un ordenador, tablet, PLC u otro dispositivo. Este cliente envía sus credenciales (como usuario y contraseña) al autenticador, quien luego las pasará al servidor FreeRADIUS.

2.Ejemplo

Para este ejemplo, los componentes serán:

- **EPC 1502** como **servidor FreeRADIUS** alojado en un Docker container.
- **Fl Switch 2220** como autentificador.
- Ordenador con sistema operativo Windows 11 como cliente solicitante.

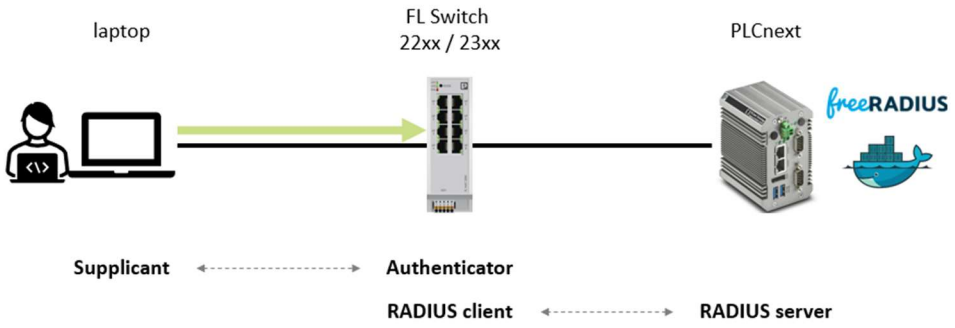

Ilustración 2.1.- Componentes de la arquitectura de ejemplo

2.1. Configuración del EPC 1502

Esta guía detalla los pasos necesarios para implementar un servidor FreeRADIUS en equipos de Phoenix Contact utilizando contenedores Docker y el motor de contenedores BalenaEngine. La arquitectura de cada dispositivo debe verificarse previamente para asegurar la compatibilidad.

2.1.1. Compatibilidad de arquitectura

- IA-64 (Itanium & Itanium2)
- PPC (IBM POWER & PowerPC)
- Sparc
- Sparc64
- x86
- x86_64 (AMD64 & EMT64)

Por tanto, el servidor FreeRADIUS puede ser instalado, por ejemplo, en los equipos **AXC F 3152**, **EPC 1502 y EPC 1522** por tener arquitectura **x86_64**, pero **no** puede ser instalado en los **AXC F 1152** o **AXC F 2152** por tener arquitectura **ARMv7**.

2.1.2. Instalación de BalenaEngine

Para desplegar contenedores en el equipo **EPC 1502**, se debe instalar el motor de contenedores BalenaEngine [1] a través de la PLCnext Store [2].

1. **Descarga de BalenaEngine**:
   a) Acceder a la PLCnext Store y localizar la aplicación **balenaEngine-DockerForIOT-x86**.
   b) Descargar el archivo con extensión .app, compatible con la arquitectura x86 del EPC 1502.
2. **Instalación de BalenaEngine en el equipo EPC 1502**:
   a) Ingresar a la interfaz del EPC 1502 utilizando su dirección IP en un navegador web.

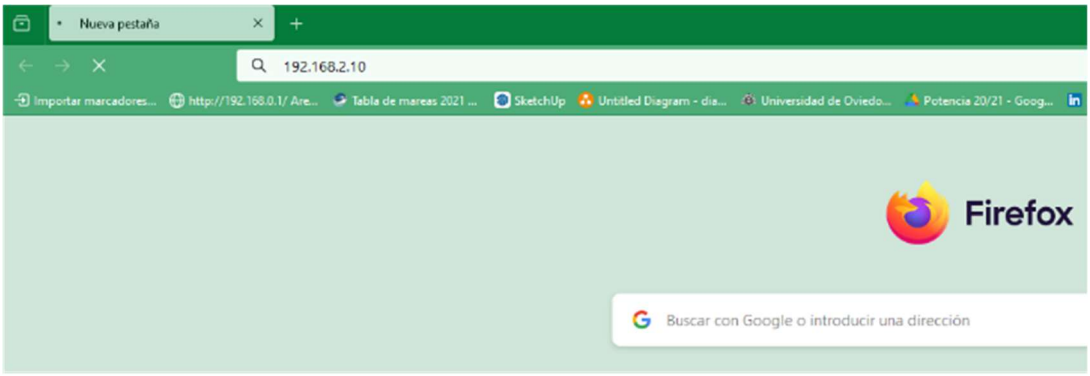

Ilustración 2.2.- Dirección IP del EPC 1502 en el navegador web

   b) Validar credenciales y acceder a **Administration → PLCnext Apps**.

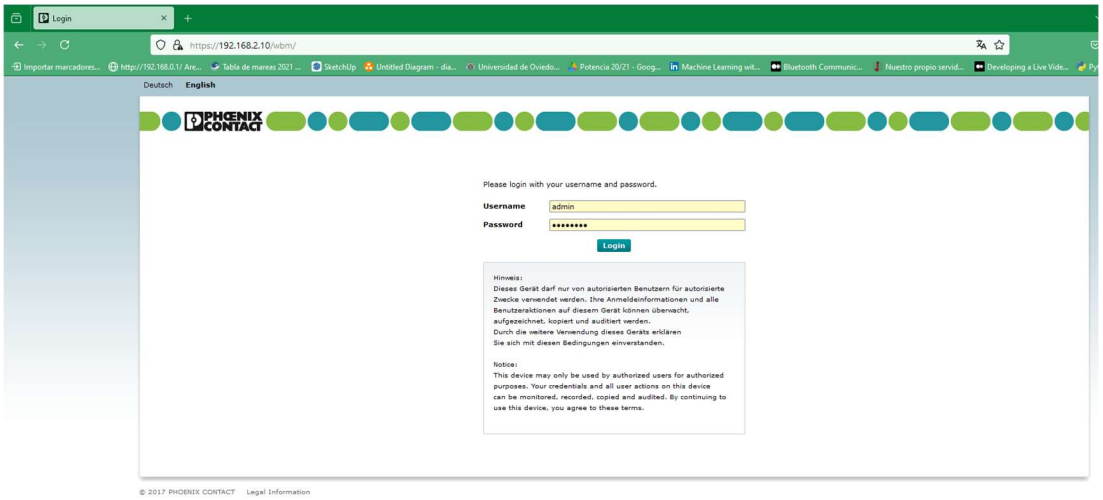

Ilustración 2.3.- Pantalla de 'Login' del EPC 1502

c) Seleccionar **Install App** y cargar el archivo .app descargado.

d) Una vez instalada la aplicación, seleccionarla y pulsar **Start**. Verificar que su estado en **App Status** aparezca como Run.

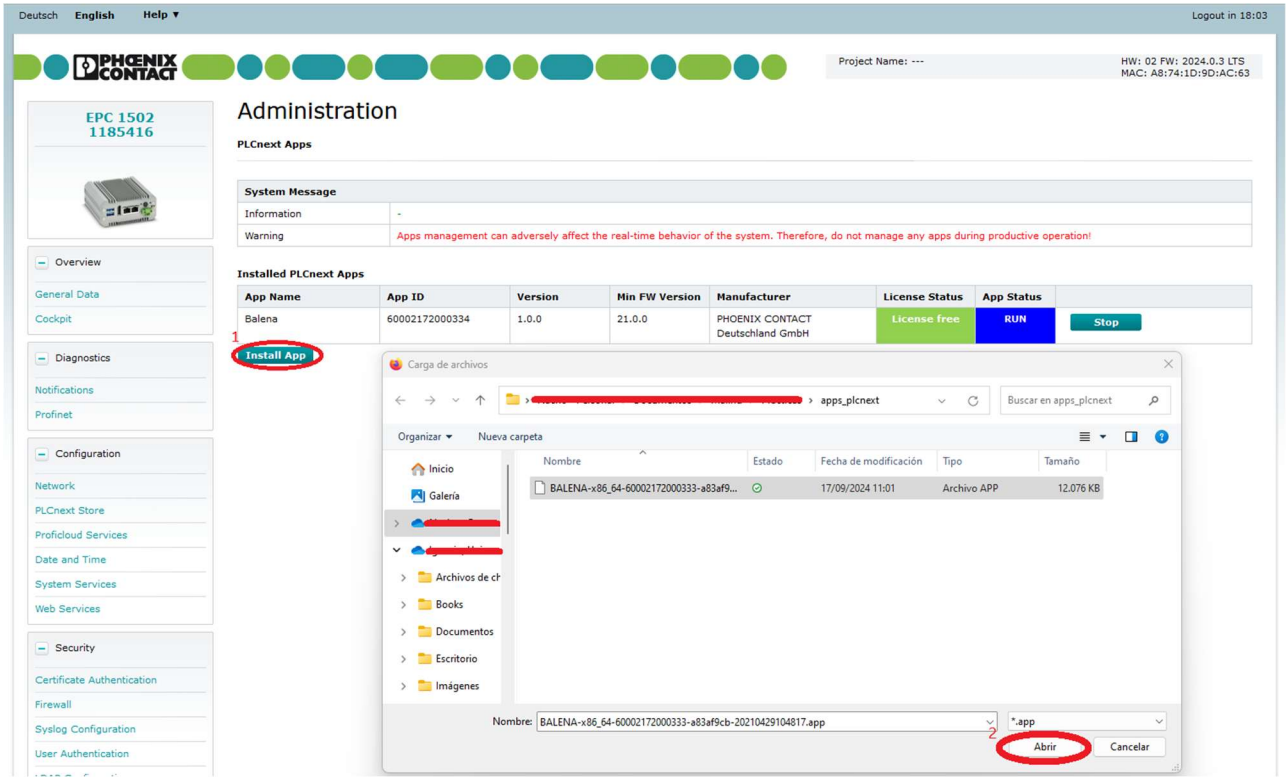

Ilustración 2.4.- Resumen gráfico de los pasos c) y d)

Con este procedimiento, BalenaEngine estará en ejecución en el EPC 1502.

2.1.3. Verificación de BalenaEngine

Para confirmar la correcta ejecución de BalenaEngine en el dispositivo:

1. Utilizar un cliente como **WinSCP** para iniciar una sesión **Putty** en el EPC 1502.
2. Una vez autenticado, ejecutar el siguiente comando en la terminal:

balena-engine --version

Este comando permite verificar el estado de ejecución de BalenaEngine.

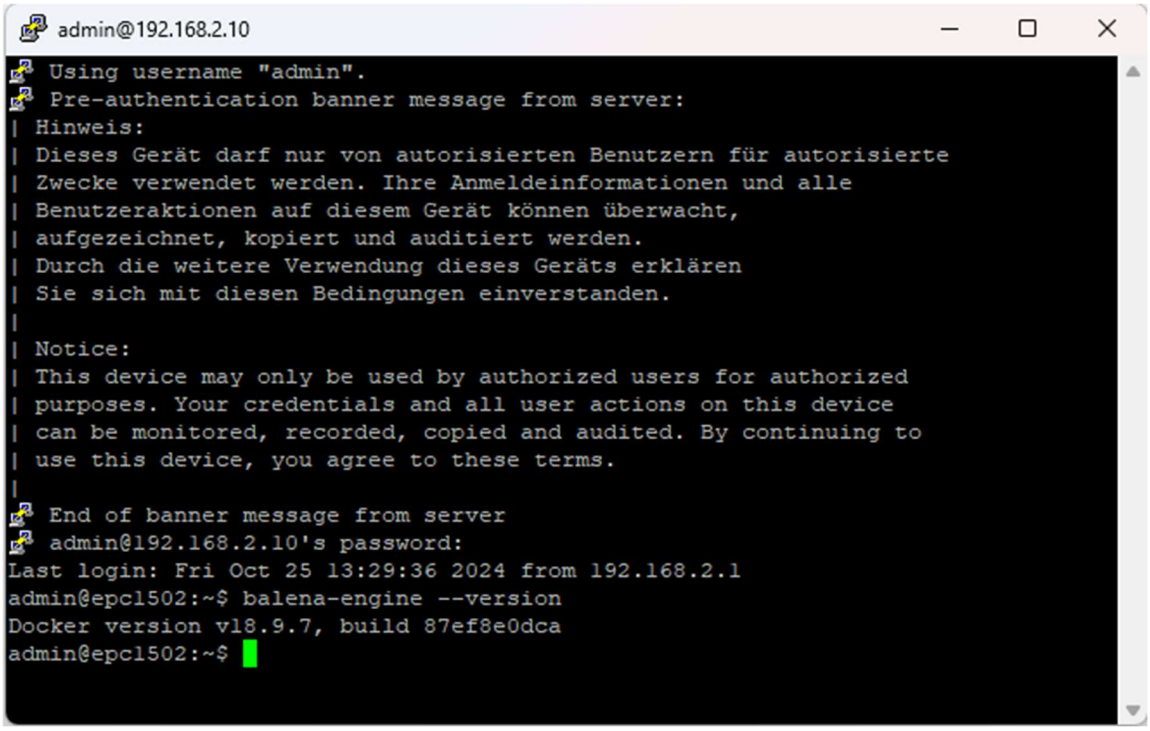

Ilustración 2.5.- Resultado del comando balena-engine --version

2.1.4. Descarga e instalación de la imagen del servidor FreeRADIUS

Con BalenaEngine en funcionamiento, se procede a descargar la imagen oficial del servidor FreeRADIUS:

- **Opción A:** Descargar la imagen en una máquina local con Docker Desktop y transferirla al EPC 1502
    1. **Acceso a Docker Hub**: Buscar la imagen freeradius/freeradius-server en Docker Hub [3].
    2. Ejecutar el siguiente comando en el ordenador local para descargar la imagen de FreeRADIUS:

        docker pull freeradius/freeradius-server

    3. Para transferir la imagen al EPC 1502, primero guardarla en un archivo .tar:

        docker save -o <ruta_del_archivo>.tar freeradius/freeradius-server

    4. Transferir el archivo al EPC 1502 mediante WinSCP.
    5. Cargar la imagen en el EPC 1502: Una vez transferido el archivo, iniciar sesión en el EPC 1502 mediante **Putty** y ejecutar:

        balena-engine load -i <ruta_del_archivo>.tar

- **Opción B: Descargar la imagen directamente en el EPC 1502 (requiere conexión a internet):** Si el EPC 1502 tiene acceso a internet, se puede descargar la imagen de FreeRADIUS directamente desde Docker Hub utilizando el comando:

    balena-engine pull freeradius/freeradius-server

Después de realizar estos pasos, la imagen de FreeRADIUS estará disponible en el EPC 1502.

2.1.5. Ejecución del servidor FreeRADIUS en un contenedor

Para iniciar el servidor FreeRADIUS en un contenedor, utilizar el siguiente comando:

balena-engine run --name my-radius -t --privileged -p 192.168.2.10:1812:1812/udp -p 192.168.2.10:1813:1813/udp freeradius/freeradius-server -X

Explicación de los parámetros:

- --name my-radius: Asigna el nombre my-radius al contenedor para facilitar su identificación.
- -t: Asigna un terminal interactivo al contenedor.
- --privileged: Concede permisos elevados al contenedor, permitiendo el acceso a dispositivos y configuraciones del sistema.
- -p 192.168.2.10:1812:1812/udp: Expone el puerto UDP 1812 para autenticación en la IP 192.168.2.10 del EPC.
- -p 192.168.2.10:1813:1813/udp: Expone el puerto UDP 1813, que FreeRADIUS usa para el registro de contabilidad.
- freeradius/freeradius-server: Define la imagen de FreeRADIUS a ejecutar.
- -X: Ejecuta el servidor en modo depuración, proporcionando un registro detallado de eventos y errores.

Consideraciones de reinicio:

- Cuando el EPC 1502 se apaga, el contenedor no se reinicia automáticamente al volver a encenderse con el comando anterior. Para ponerlo en funcionamiento nuevamente, puedes usar:
    - ***balena-engine restart my-radius*** para reiniciar el contenedor, o
    - ***balena-engine start my-radius*** para iniciarlo si está detenido.
- **Configuración de reinicio automático al crear el contenedor**: Para evitar la necesidad de reiniciar manualmente el contenedor tras un apagado, puedes agregar uno de los siguientes flags al comando ***balena-engine run*** inicial:
    - ***--restart always***: El contenedor intentará reiniciarse siempre que se detenga o apague.
    - ***--restart unless-stopped***: El contenedor intentará reiniciarse automáticamente, excepto si ha sido detenido manualmente.

2.1.6. Acceso y configuración de prueba del servidor FreeRADIUS en el contenedor

Una vez que el contenedor con FreeRADIUS esté en ejecución, el servidor estará activo, pero configurado solo para acceso local. Los siguientes pasos permiten realizar una prueba básica de funcionamiento en el entorno local. En una etapa posterior, se configurará el servidor FreeRADIUS para aceptar conexiones desde direcciones externas.

1. **Acceder al contenedor de FreeRADIUS**: Abrir una nueva sesión **Putty** y ejecutar el siguiente comando para acceder al contenedor en ejecución:

   balena-engine exec -it my-radius /bin/bash

2. **Instalar el editor de texto Nano**: Para facilitar las modificaciones en los archivos de configuración, instalar el editor **Nano** dentro del contenedor:

   apt update && apt install nano

3. **Configurar un usuario de prueba**:

   Navegar al directorio de configuración de FreeRADIUS:

   cd /etc/freeradius

   Editar el archivo users usando Nano:

   nano users

   Se pueden combinar los dos comandos anteriores en uno solo:

   nano /etc/freeradius/users

   Una vez en el archivo, localizar y descomentar las siguientes líneas eliminando cualquier símbolo # al inicio:

   bob Cleartext-Password := "hello"

   Reply-Message := "Hello, %{User-Name}"

   Lo importante de este paso es tener en cuenta que los usuarios se configurar en el archivo /etc/freeradius/users.

4. **Guardar y salir del archivo**: en **Nano**, guardar los cambios con CTRL + O y salir con CTRL + X.
5. **Reiniciar el servidor FreeRADIUS para aplicar los cambios**:

balena-engine restart my-radius

6. **Realizar una prueba de funcionamiento en el entorno local:**

Acceder nuevamente al contenedor:

balena-engine exec -it my-radius /bin/bash

Ejecutar el siguiente comando para probar el acceso con el usuario bob en la dirección localhost (127.0.0.1):

radtest bob hello 127.0.0.1 0 testing123

Si el servidor responde correctamente, en el mensaje devuelto debe aparecer:

Received Access-Accept

Reply-Message = "Hello, bob"

2.1.7. Configuración de acceso a FreeRADIUS desde una subred específica

Para configurar el servidor FreeRADIUS de forma que esté disponible para los dispositivos de una red distinta al localhost, por ejemplo, la subred 192.168.2.0/24, se debe modificar el archivo **clients.conf** de FreeRADIUS para definir la subred como cliente autorizado. Para ello:

1. **Acceder al contenedor FreeRADIUS**: Si el servidor FreeRADIUS está en ejecución dentro de un contenedor, primero se debe acceder al contenedor:

   balena-engine exec -it my-radius /bin/bash

2. **Abrir el archivo clients.conf**:

   Navegar al directorio de configuración de FreeRADIUS donde se encuentra el archivo clients.conf:

   cd /etc/freeradius

   Abrir el archivo clients.conf con un editor de texto como **Nano**:

   nano clients.conf

   Se pueden combinar los dos comandos anteriores en uno solo:

   nano /etc/freeradius/clients.conf

3. **Agregar la configuración para la red 192.168.2.0/24:**

```
client 192.168.2.0/24 {
        secret = testing123
        shortname = private-network
}
```

Explicación:

- client 192.168.2.0/24: Define la red de clientes en el rango 192.168.2.0 a 192.168.2.255.
- secret = testing123: Establece la clave compartida que los dispositivos cliente usarán para autenticarse con el servidor FreeRADIUS.
- shortname = private-network: Asigna un nombre corto para esta red, útil para identificarla en los registros.

4. **Guardar y salir del archivo:** en Nano, guardar los cambios con CTRL + O y salir con CTRL +X.
5. **Reiniciar FreeRADIUS:** para que los cambios en el archivo **clients.conf** tengan efecto, reiniciar el servidor FreeRADIUS.

balena-engine restart my-radius

Con esta configuración, el servidor FreeRADIUS aceptará solicitudes de autenticación provenientes de cualquier dispositivo en la subred 192.168.2.0/24, usando la clave compartida testing123.

Nota: si se apaga el PLC será necesario reiniciar el contenedor mediante:

balena-engine restart my-radius

2.2. Configuración del Fl Switch 2220

Este paso configura el **FL Switch 2220** para autenticar usuarios mediante el servidor FreeRADIUS configurado en el EPC 1502.

1. **Acceso a la interfaz del FL Switch 2220**:
   - Acceder a la interfaz de usuario del **EPC 1502** a través de su dirección IP en un navegador web.

Ilustración 2.6.- Vista inicial del FL Switch 2220 desde el navegador

   - Introducir las credenciales en **Login** y navegar a **Configuration → Security** para realizar la configuración.

2. **Configurar el servidor RADIUS**:
   - En el apartado **RADIUS Server Configuration**:
     - Ingresar la **IP del servidor RADIUS** (en este ejemplo, la IP del EPC 1502 es 192.168.2.10).
     - Establecer el **puerto** de FreeRADIUS en 1812.
     - Introducir el **secreto compartido** como testing123.
   - Guardar los cambios con **Apply&Save**.
   - Para verificar la conectividad, utilizar el botón **Test** en "**Check Radius Server Availability**". Si la conexión es exitosa, el estado del servidor RADIUS debería mostrarse como **Active**.

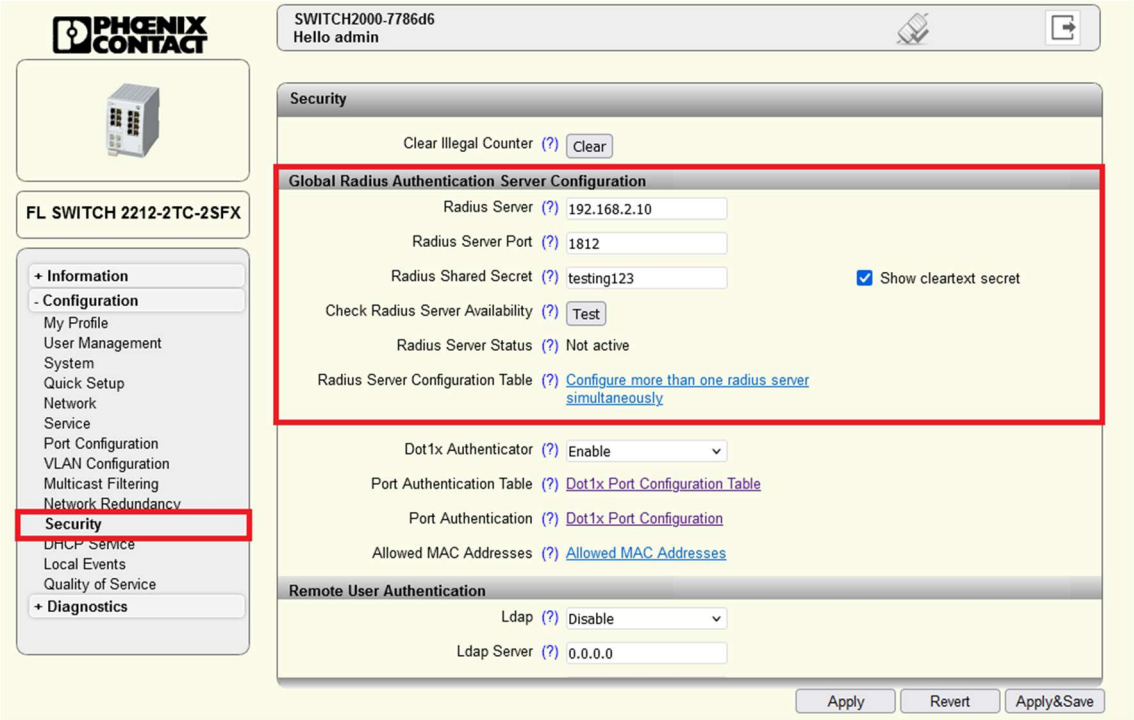

Ilustración 2.7.- Configuración del servidor RADIUS

3. **Habilitar la autenticación de usuarios a través del servidor RADIUS**: En la sección "Remote User Authentication", cambiar la opción "Radius" a "Enable".

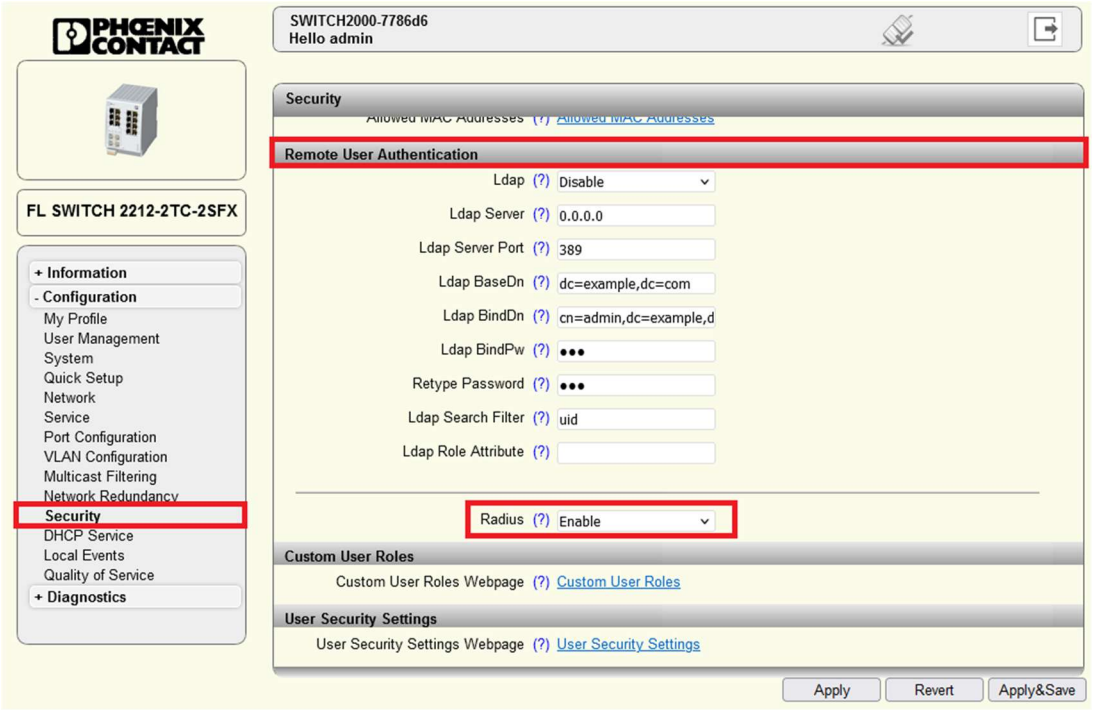

Ilustración 2.8.- Habilitar autenticación de usuarios

4. **Configurar los puertos del switch para autenticación RADIUS**:
   - Buscar '**Dot1x Authenticator'** y habilitar esta opción seleccionando **Enable**.

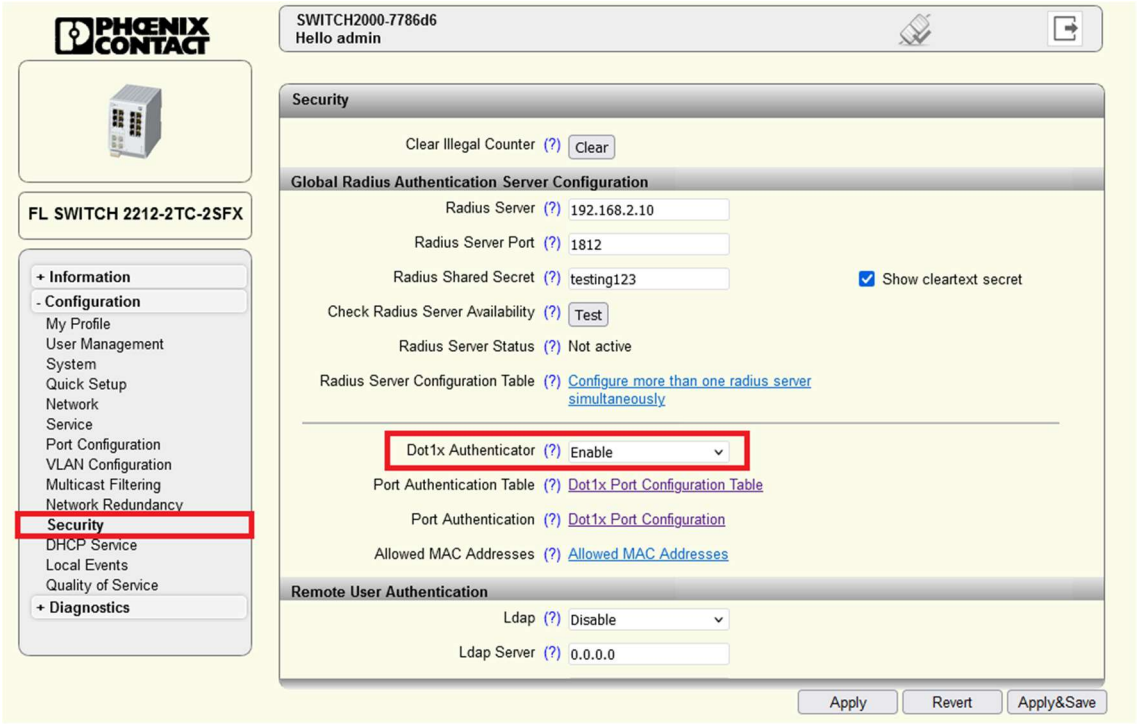

Ilustración 2.9.- Activación de Dot1x Authenticator

- Existen dos maneras de configurar los puertos, ambas aparecen justo debajo de '**Dot1x Authenticator'**:
  - **Opción A: Configuración en tabla**:
    - Ir a **Dot1x Port Configuration Table**.
    - En el campo **Mode** del puerto deseado, seleccionar **Auto** para habilitar la autenticación RADIUS en ese puerto.

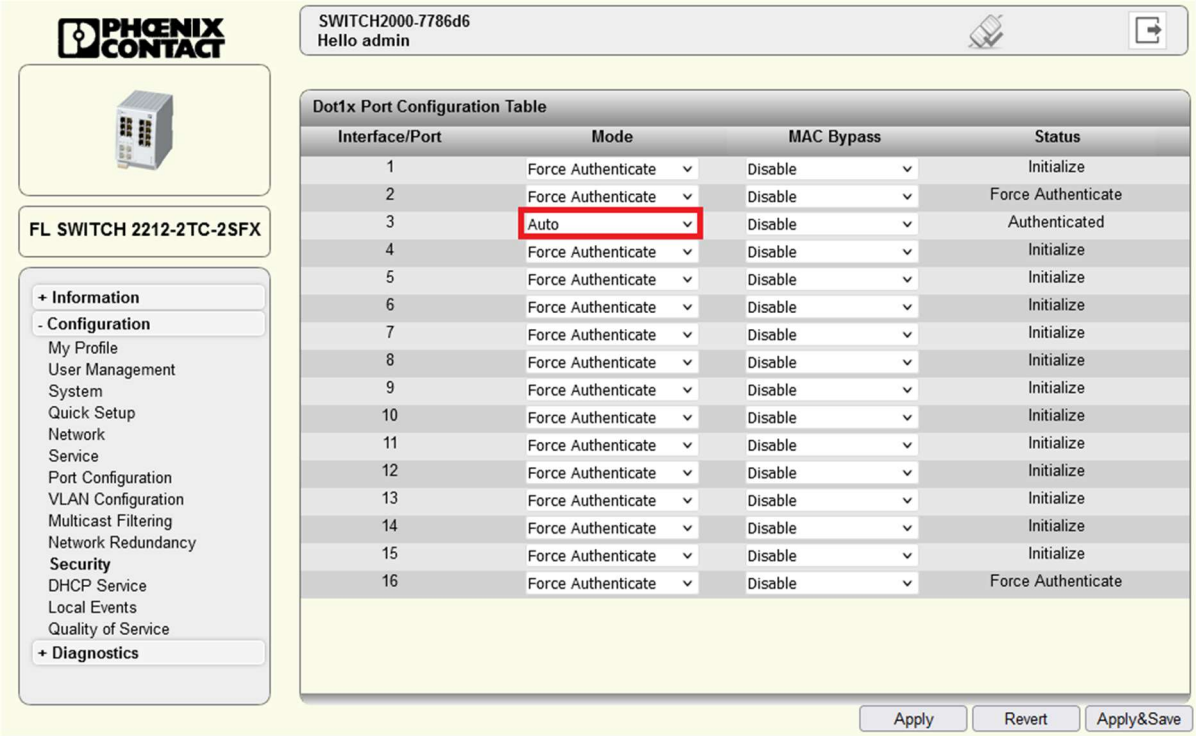

Ilustración 2.10.- Configuración de puertos desde Dot1x Port Configuration Table

- **Opción B: Configuración individual de puertos**: Navegar a **Dot1x Port Configuration** para ver los puertos individualmente, lo que permite opciones adicionales como:
  - **Failed Authentication Handling**: Define el comportamiento ante una autenticación fallida, pudiendo deshabilitar el puerto o asignarlo a una red de invitados.
  - En **Authentication Mode**, seleccionar **Auto** para que cada puerto deba autenticarse mediante RADIUS. Esta configuración es equivalente a modificar **Mode** en la tabla de configuración de la **Opción A**.

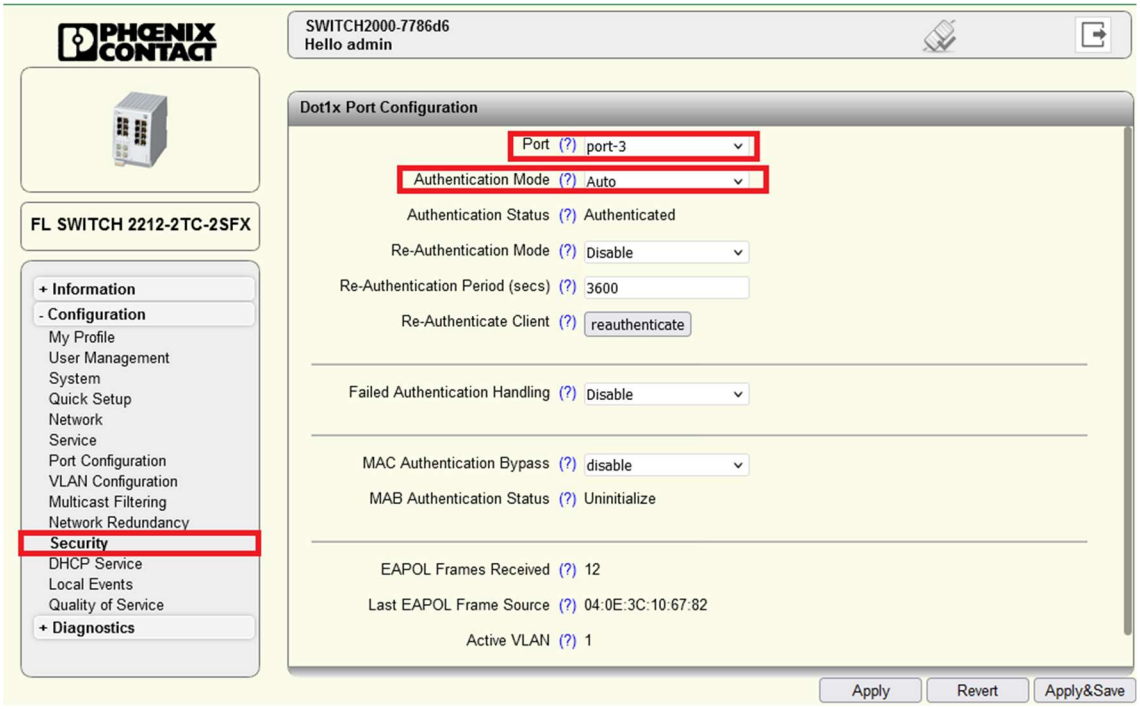

Ilustración 2.11.- Configuración del puerto desde Dot1x Port Configuration

Nota: Si se configura un puerto para habilitar la autentificación RADIUS mediante una de las dos opciones, no es necesario configurarla en la otra.

5. Pulsar '**Apply&Save**' para guardar y aplicar los cambios realizados.

6. **Ejemplo de verificación en el puerto 3**: En este ejemplo, se habilita la autenticación RADIUS únicamente en el puerto 3. Para probar el funcionamiento de la configuración realizada:
    - Conectar un cliente (por ejemplo, un ordenador) al puerto 3 (sin que este tenga la configuración adicional que se verá en el siguiente paso) y acceder a la IP del EPC 1502 en un navegador web.
    - La página no debería cargar, ya que el cliente necesita autenticarse a través de RADIUS.
    - Para confirmar, conectar el mismo cliente a otro puerto (cualquier otro puerto que no esté configurado con la autenticación por RADIUS) y acceder nuevamente a la IP del EPC 1502; la página debería cargar sin problemas.

2.3. Configuración del cliente solicitante

Este paso permite configurar un sistema para acceder a un puerto del switch que requiere autenticación mediante el servidor FreeRADIUS. El ejemplo usa el puerto 3 configurado previamente en el switch.

- **Configuración en Windows (Ejemplo con Windows 11):**
  1. Activar el servicio de configuración automática de redes cableadas:
     - Ir a **Servicios** en Windows.
     - Buscar el servicio '**Configuración automática de redes cableadas'** y hacer doble clic en él.

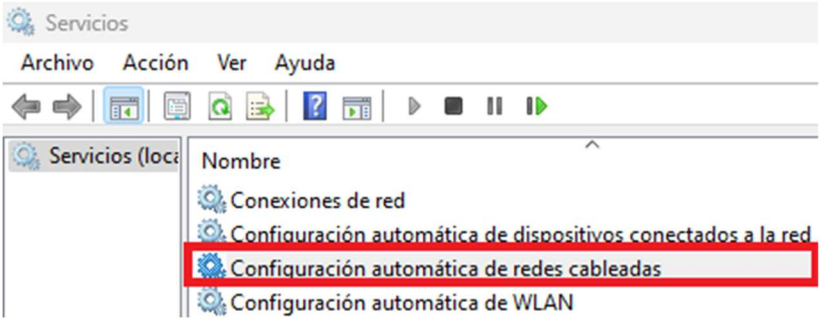

Ilustración 2.12.- Servicio 'Configuración automática de redes cableadas'

     - En la pestaña '**General**', establecer el '**Tipo de inicio**' en **Automático** y pulsar '**Iniciar**' para que el '**Estado del servicio**' pase a '**En ejecución**'.

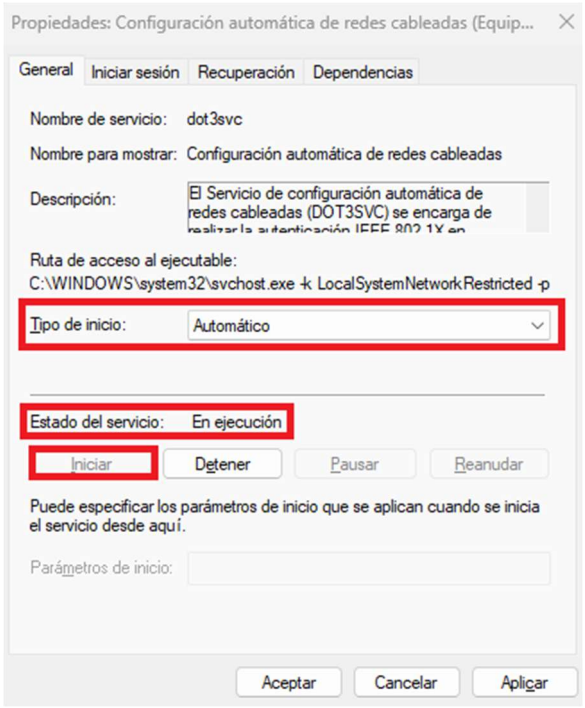

Ilustración 2.13.- Pestaña General de Configuración automática de redes cableadas

2. Acceder a la configuración de Ethernet:
   - Ir a **Panel de Control → Redes e Internet → Centro de redes y recursos compartidos**.
   - En el menú de la izquierda, seleccionar '**Cambiar configuración del adaptador**'.

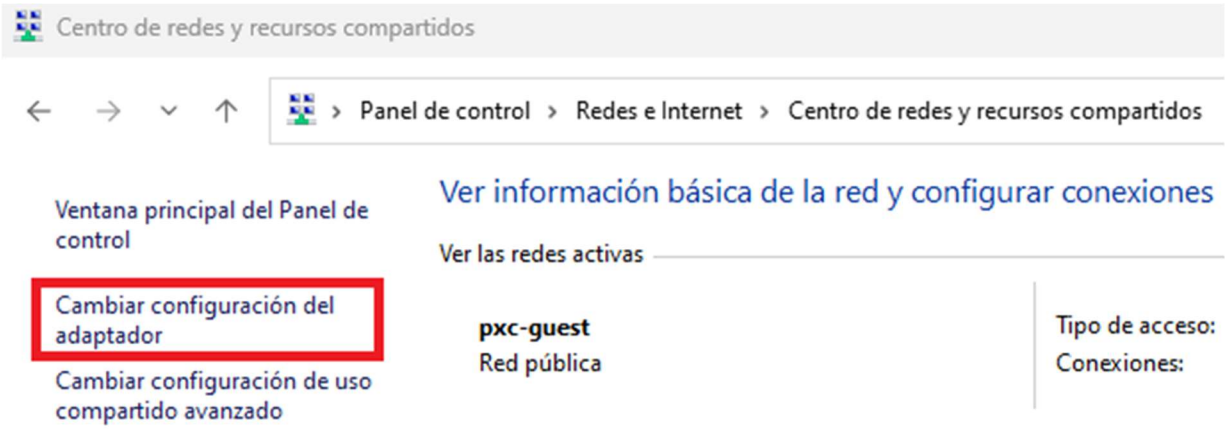

Ilustración 2.14.- Cambiar configuración del adaptador

   - Hacer clic derecho en la conexión Ethernet correspondiente y seleccionar '**Propiedades**'.

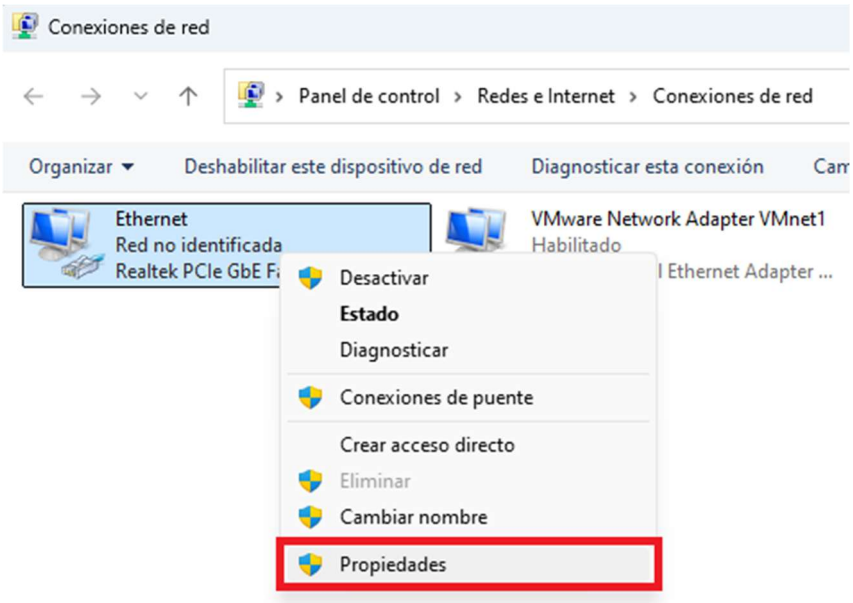

Ilustración 2.15.- Doble clic en Propiedades

3. Configurar la autenticación IEEE 802.1X en Ethernet: En la ventana '**Propiedades de Ethernet**':
   - Activar la casilla '**Habilitar autenticación de IEEE 802.1X**'.
   - Cambiar el '**Método de autenticación de la red a Microsoft: EAP protegido (PEAP)**'.
   - Desmarcar '**Recordar mis credenciales para esta conexión cada vez que inicie sesión**'.
   - Marcar '**Retroceso a acceso de red no autorizado**'.
   - Seleccionar '**Configuración**' junto a '**Microsoft: EAP protegido (PEAP)**' para abrir las '**Propiedades de EAP protegido**'.

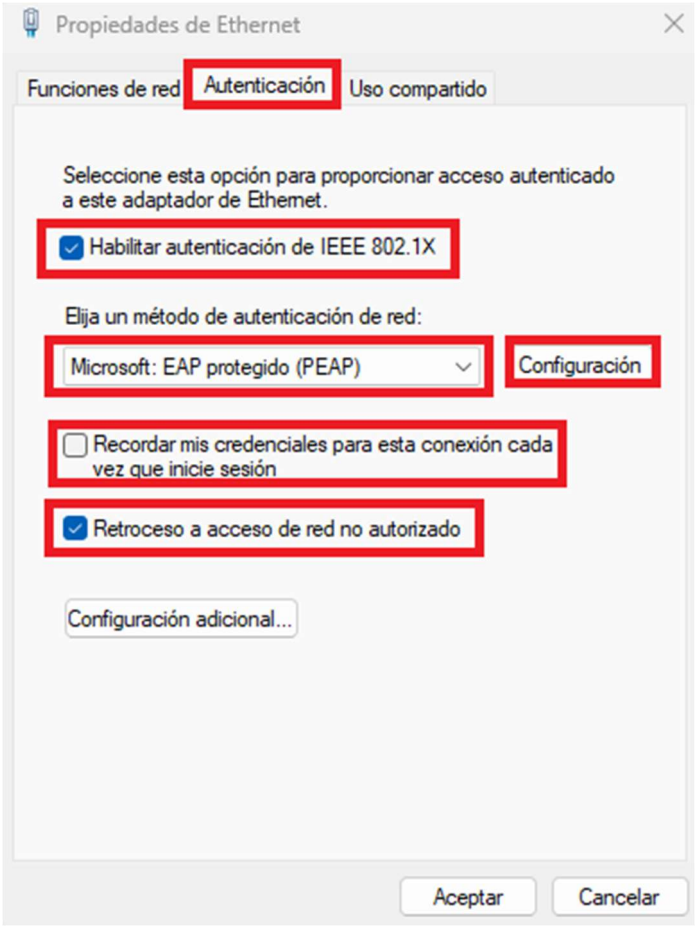

Ilustración 2.16.- Pestaña Autenticación de Propiedades de Ethernet

4. Configurar la ventana '**Propiedades de EAP protegido**':
   - Desmarcar '**Verificar la identidad del servidor validando el certificado**'.
   - En '**Seleccione el método de autenticación**', seleccionar '**Contraseña segura (EAP-MSCHAP v2)**'.
     - Pulsar en '**Configurar…**' junto a '**Contraseña segura (EAP-MSCHAP v2)**' y desmarcar '**Usar automáticamente el nombre de inicio de sesión y la contraseña de Windows (y dominio, si existe alguno)**'. Pulsar '**Aceptar**'.
   - Marcar '**Habilitar reconexión rápida**'.
   - Desmarcar '**Desconectar si el servidor no presenta TLV de cryptobinding**'.
   - Desmarcar '**Habilitar privacidad de identidad**'.
   - Pulsar '**Aceptar'** para cerrar esta ventana.

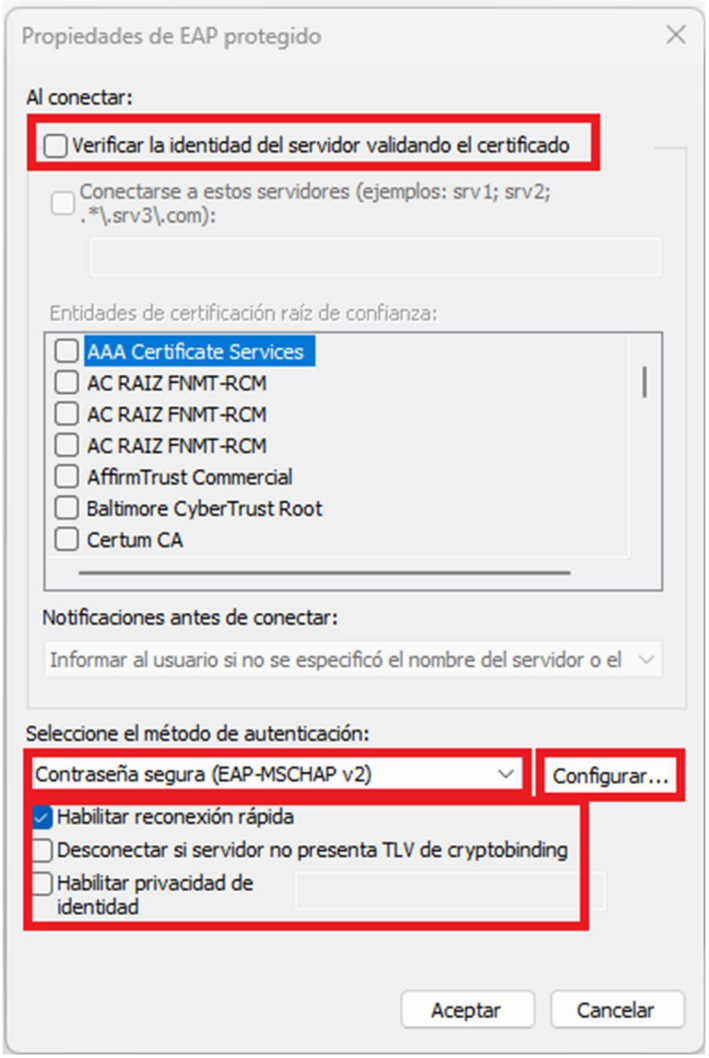

Ilustración 2.17.- Propiedades de EAP protegido

5. Configurar ajustes avanzados de autenticación en Ethernet:
   - De vuelta en la ventana '**Propiedades de Ethernet**', seleccionar '**Configuración adicional…**'.
   - En '**Configuración Avanzada**':
     - Marcar '**Especificar modo de autenticación**' y seleccionar '**Autenticación de usuario en el menú desplegable**'.
     - Desmarcar '**Habilitar inicio de sesión único en esta red**'.
     - Pulsar '**Aceptar**' para confirmar y cerrar la ventana.

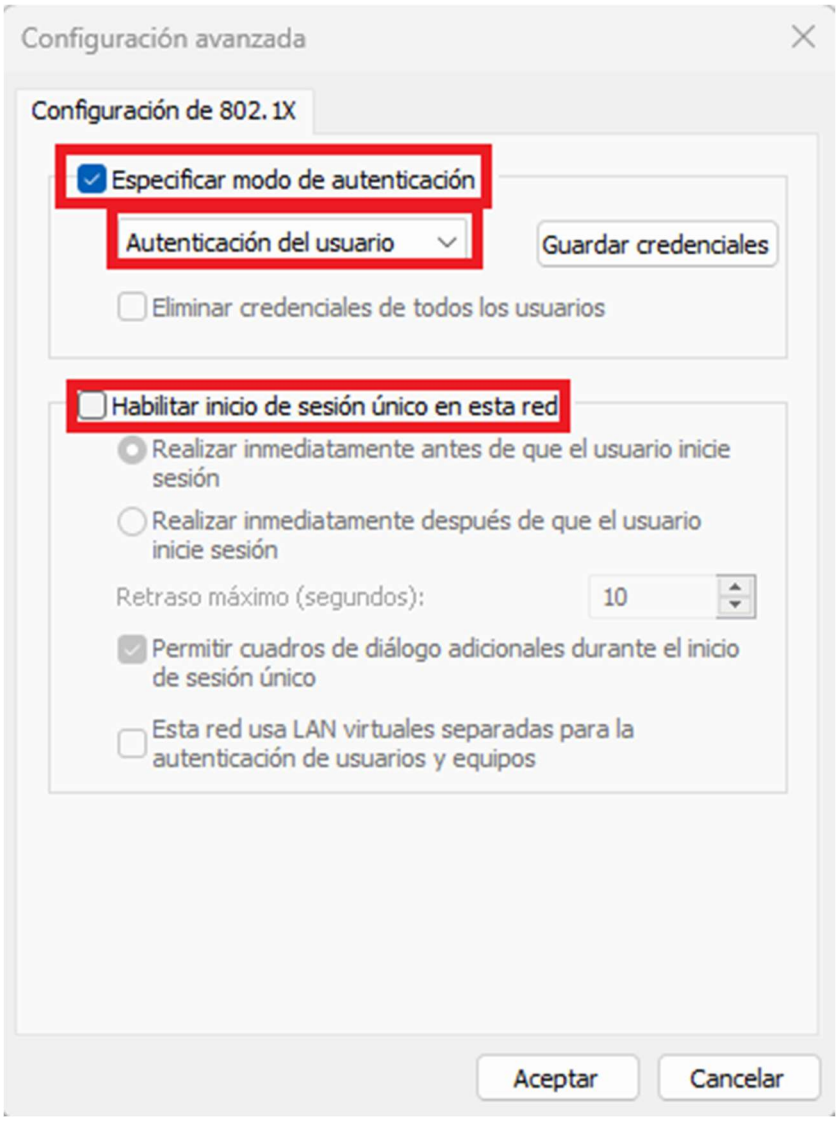

Ilustración 2.18.- Configuración avanzada

- Pulsar '**Aceptar**' en la ventana '**Propiedades de Ethernet**' para aplicar los cambios.

Con estos pasos, al conectar el cliente (ordenador) al puerto 3 del **FL Switch 2220**, aparecerá el siguiente mensaje en la parte inferior derecha de la pantalla.

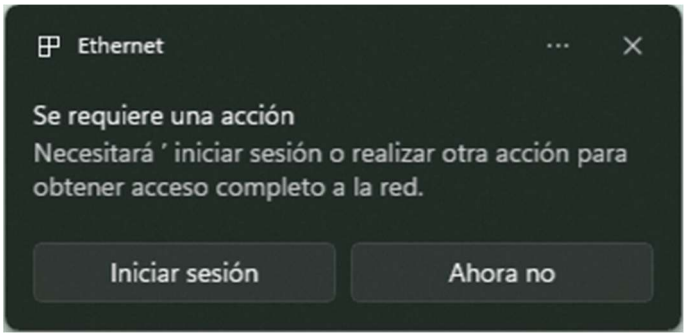

Ilustración 2.19.- Mensaje de autenticación

Tras dar en '**Iniciar sesión**' se abrirá una ventana de '**Configuración**':

Ilustración 2.20.- Ventana de Configuración

Al darle en '**Iniciar sesión**' en esta nueva ventana, aparece una nueva ventana en la que habrá que introducir las credenciales **que corresponden a uno de los usuarios configurados en el archivo /etc/freeradius/users** del servidor FreeRADIUS, para este ejemplo, el usuario es 'bob' y la contraseña 'hello':

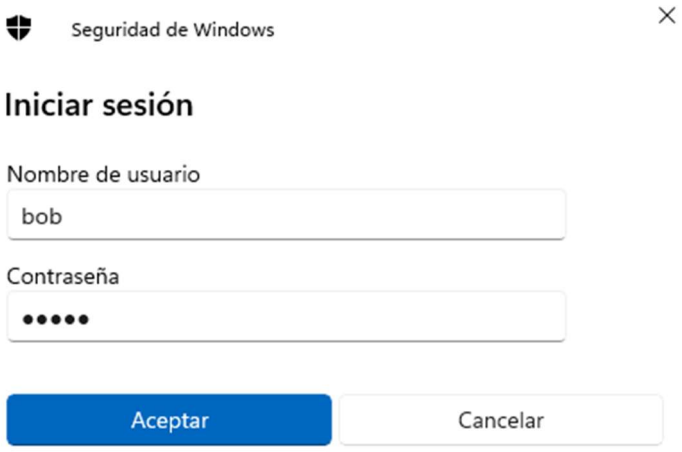

Ilustración 2.21.- Ventana de Inicio de sesión de Seguridad de Windows

Debe aparecer un mensaje que indique que se ha iniciado sesión:

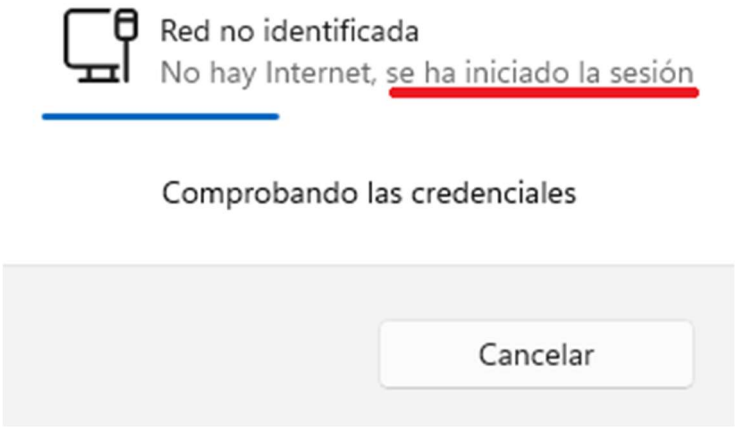

Ilustración 2.22.- Sesión iniciada

Ahora, al introducir la IP de uno de los dispositivos conectados a la red, por ejemplo la dirección del EPC 1502, 192.168.2.10, deberá cargar con éxito, al contrario de lo que ocurría en el apartado 2.2, '**Ejemplo de verificación en el puerto 3'.**

3.Referencias

[1] “balenaEngine - A container engine purpose-built for IoT devices.” Accessed: Oct. 25, 2024. [Online]. Available: https://www.balena.io/engine

[2] “PLCnext Store | The open software store for automation.” Accessed: Oct. 25, 2024. [Online]. Available: https://www.plcnextstore.com/eu/

[3] “Docker Hub Container Image Library | App Containerization.” Accessed: Oct. 28, 2024. [Online]. Available: https://hub.docker.com/