Autenticación EAP-FAST con controladores de LAN inalámbrica e Identity Services Engine

Contenido

Introducción

Este documento explica cómo configurar el controlador de LAN inalámbrico (WLC) para EAP (Extensible Authentication Protocol) - autenticación FAST (Flexible Authentication via Secure Tunneling) mediante un servidor RADIUS externo. Este ejemplo de configuración utiliza Identity Services Engine (ISE) como servidor RADIUS externo para autenticar el cliente inalámbrico.

Este documento se centra en cómo configurar el aprovisionamiento de ISE para las credenciales de acceso protegido (PAC) anónimas y autenticadas en banda (Automático) a los clientes inalámbricos.

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento básico de la configuración de los puntos de acceso ligeros (LAP) y los WLC de Cisco
- Conocimiento básico del protocolo CAPWAP
- Conocimiento de cómo configurar un servidor RADIUS externo, como Cisco ISE
- Conocimientos funcionales sobre el marco general de EAP
- Conocimientos básicos sobre protocolos de seguridad, como MS-CHAPv2 y EAP-GTC, y conocimientos sobre certificados digitales

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- WLC de la serie 5520 de Cisco que ejecuta la versión de firmware 8.8.111.0AP Cisco serie 4800Anyconnect NAM.Cisco Secure ISE versión 2.3.0.298Switch de la serie Cisco 3560-CX que ejecuta la versión 15.2(4)E1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Antecedentes

El protocolo EAP-FAST es un tipo EAP IEEE 802.1X de acceso público desarrollado por Cisco para admitir clientes que no pueden aplicar una política de contraseña segura y desean implementar un tipo EAP 802.1X que no requiere certificados digitales.

El protocolo EAP-FAST es una arquitectura de seguridad cliente-servidor que cifra las transacciones EAP con un túnel de seguridad de nivel de transporte (TLS). El establecimiento del túnel EAP-FAST se basa en secretos seguros que son exclusivos de los usuarios. Estos secretos seguros se denominan PAC, que el ISE genera utilizando una clave maestra conocida únicamente por el ISE.

EAP-FAST se produce en tres fases:

- **Fase cero (fase de aprovisionamiento automático de PAC)**: fase cero de EAP-FAST, una fase opcional es un medio seguro de túnel para proporcionar un cliente de usuario final EAP-FAST con una PAC para el usuario que solicita acceso a la red. **Proporcionar un PAC al cliente del**

usuario final es el único propósito de la fase cero.**Nota:** La fase cero es opcional porque las PAC también se pueden aprovisionar manualmente a los clientes en lugar de utilizar la fase cero.Consulte la sección Modos de aprovisionamiento PAC de este documento para obtener más detalles.

- **Fase uno**: en la fase uno, el ISE y el cliente de usuario final establecen un túnel TLS basado en la credencial PAC del usuario. Esta fase requiere que se haya proporcionado al cliente de usuario final una PAC para el usuario que intenta obtener acceso a la red y que la PAC se base en una clave maestra que no ha caducado. No hay servicio de red habilitado por la fase uno de EAP-FAST.
- **Fase dos**: en la fase dos, las credenciales de autenticación de usuario se pasan de forma segura utilizando un método EAP interno compatible con EAP-FAST dentro del túnel TLS al RADIUS creado mediante el PAC entre el cliente y el servidor RADIUS. EAP-GTC, TLS y MS-CHAP se soportan como métodos EAP internos. No se soportan otros tipos EAP para EAP-FAST.

Consulte Cómo funciona EAP-FAST para obtener más información.

PAC

Los PAC son secretos compartidos sólidos que permiten que el ISE y un cliente de usuario final EAP-FAST se autentiquen mutuamente y establezcan un túnel TLS para su uso en la fase dos de EAP-FAST. El ISE genera PACs utilizando la clave maestra activa y un nombre de usuario.

PAC comprende:

- **Clave PAC**: secreto compartido enlazado a un cliente (y dispositivo cliente) y a la identidad del servidor.
- **PAC opaco**: campo opaco que el cliente almacena en caché y pasa al servidor. El servidor recupera la clave PAC y la identidad del cliente para autenticarse mutuamente con el cliente.
- **Información PAC**: como mínimo, incluye la identidad del servidor para permitir que el cliente almacene en caché diferentes PACs. Opcionalmente, incluye otra información como la hora de vencimiento del PAC.

Modos de suministro de PAC

Como se ha mencionado anteriormente, la fase cero es una fase opcional.

EAP-FAST ofrece dos opciones para aprovisionar un cliente con un PAC:

- **Aprovisionamiento PAC automático (EAP-FAST Fase 0 o Aprovisionamiento PAC en banda)**
- **Aprovisionamiento manual (fuera de banda) de PAC**

El aprovisionamiento PAC en banda/automático envía un nuevo PAC a un cliente de usuario final a través de una conexión de red segura. El aprovisionamiento automático de PAC no requiere la intervención del usuario de la red ni de un administrador de ISE, siempre que configure el ISE y el cliente de usuario final para que admita el aprovisionamiento automático.

La última versión de EAP-FAST admite dos opciones de configuración de aprovisionamiento PAC en banda diferentes:

- **Aprovisionamiento anónimo de PAC en banda**

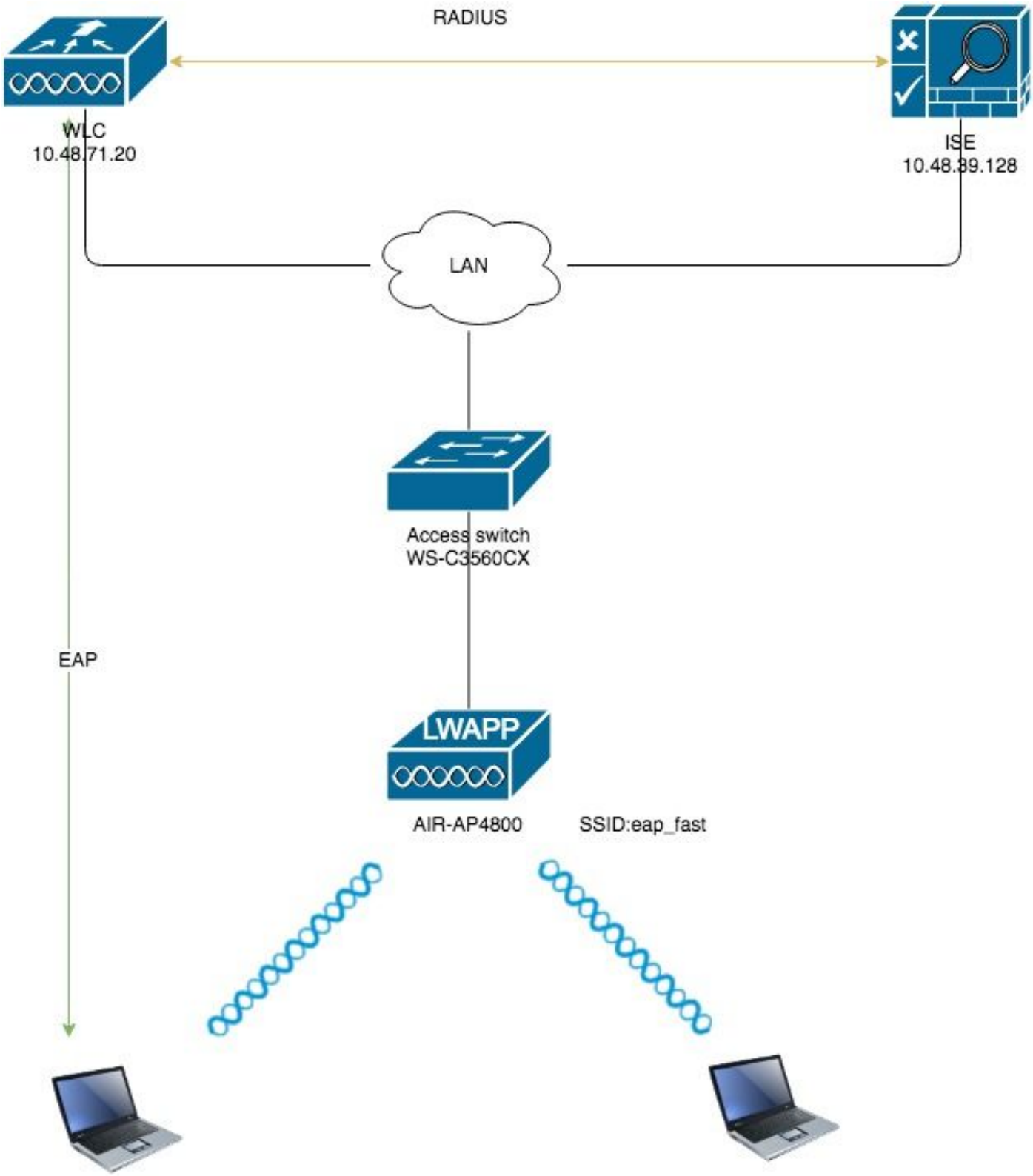
- Aprovisionamiento PAC autenticado en banda

Nota: Este documento trata estos métodos de aprovisionamiento PAC en banda y cómo configurarlos.

El aprovisionamiento PAC manual/fuera de banda requiere que un administrador de ISE genere archivos PAC, que luego deben distribuirse a los usuarios de red correspondientes. Los usuarios deben configurar los clientes de usuario final con sus archivos PAC.

Configurar

Diagrama de la red



Configuraciones

Configuración del WLC para la Autenticación EAP-FAST

Realice estos pasos para configurar el WLC para la autenticación EAP-FAST:

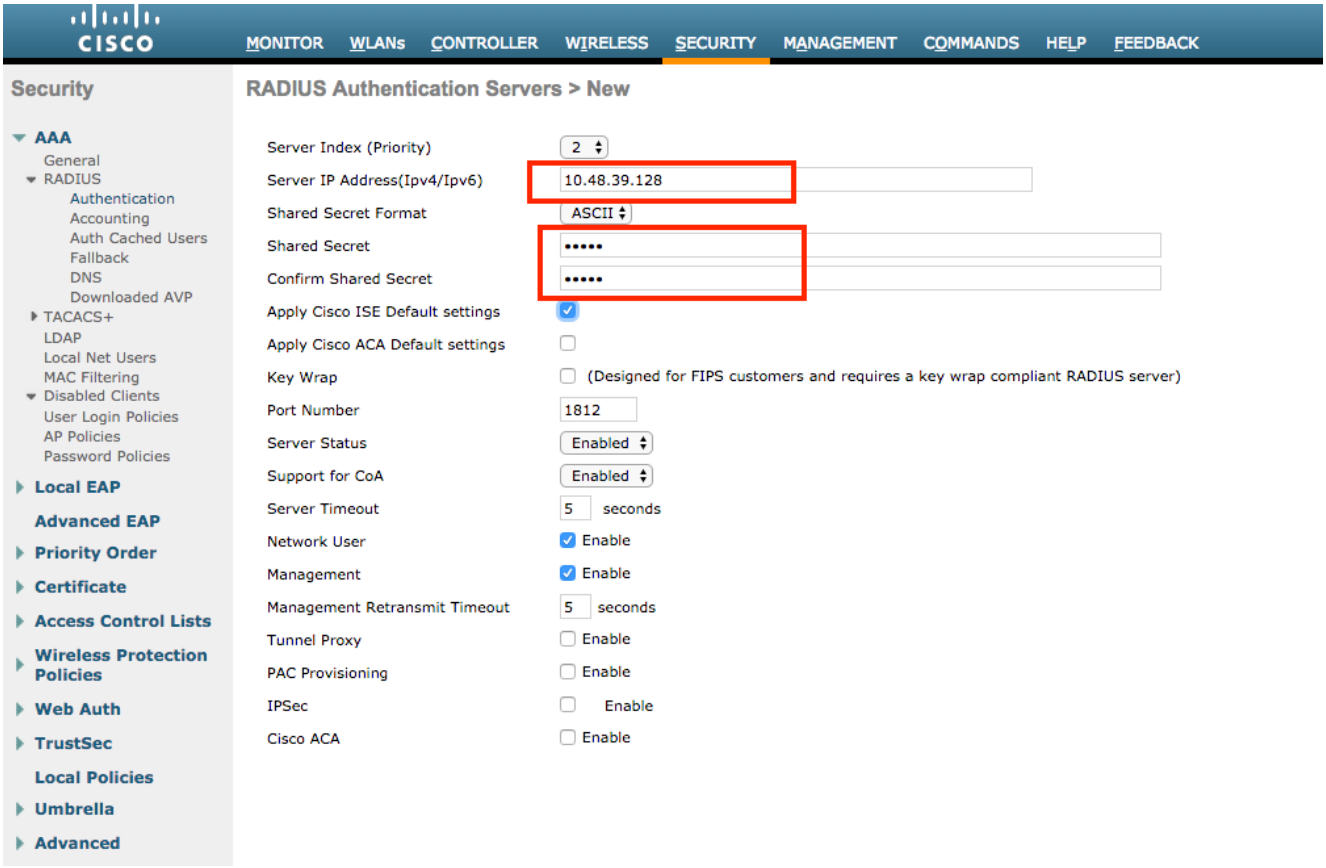
1. Configuración del WLC para la Autenticación RADIUS a través de un Servidor RADIUS Externo
2. Configuración de la WLAN para la Autenticación EAP-FAST

Configuración del WLC para la Autenticación RADIUS a través de un Servidor RADIUS Externo

El WLC necesita ser configurado para reenviar las credenciales del usuario a un servidor RADIUS externo. A continuación, el servidor RADIUS externo valida las credenciales del usuario mediante EAP-FAST y proporciona acceso a los clientes inalámbricos.

Complete estos pasos para configurar el WLC para un servidor RADIUS externo:

1. Elija **Security** y **RADIUS Authentication** en la GUI del controlador para mostrar la página RADIUS Authentication Servers . Luego, haga clic en **Nuevo** para definir un servidor RADIUS.
2. Defina los parámetros del servidor RADIUS en la página **Servidores de autenticación RADIUS > Nuevo**. Estos parámetros incluyen:Dirección IP de servidor RADIUSsecreto compartidonúmero de puertoEstado del servidorEste documento utiliza el servidor ISE con una dirección IP de 10.48.39.128.



3. Haga clic **Aplicar**.

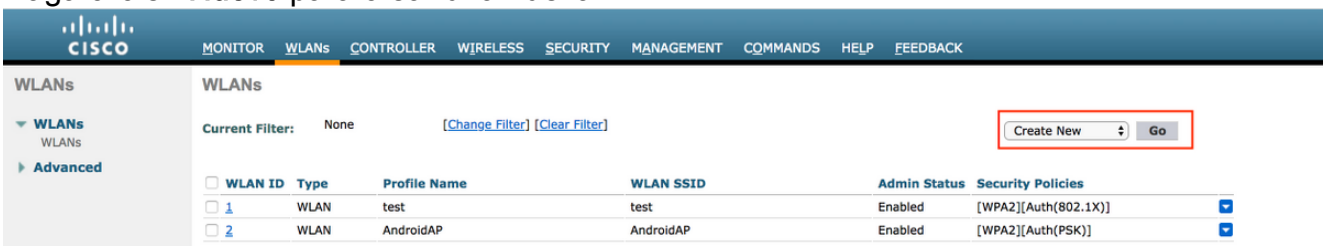
Configuración de la WLAN para la Autenticación EAP-FAST

A continuación, configure la WLAN que los clientes utilizan para conectarse a la red inalámbrica para la autenticación EAP-FAST y asignarla a una interfaz dinámica. El nombre WLAN configurado en este ejemplo es **eap fast**. Este ejemplo asigna esta WLAN a la interfaz de administración.

Complete estos pasos para configurar la WLAN **eap fast** y sus parámetros relacionados:

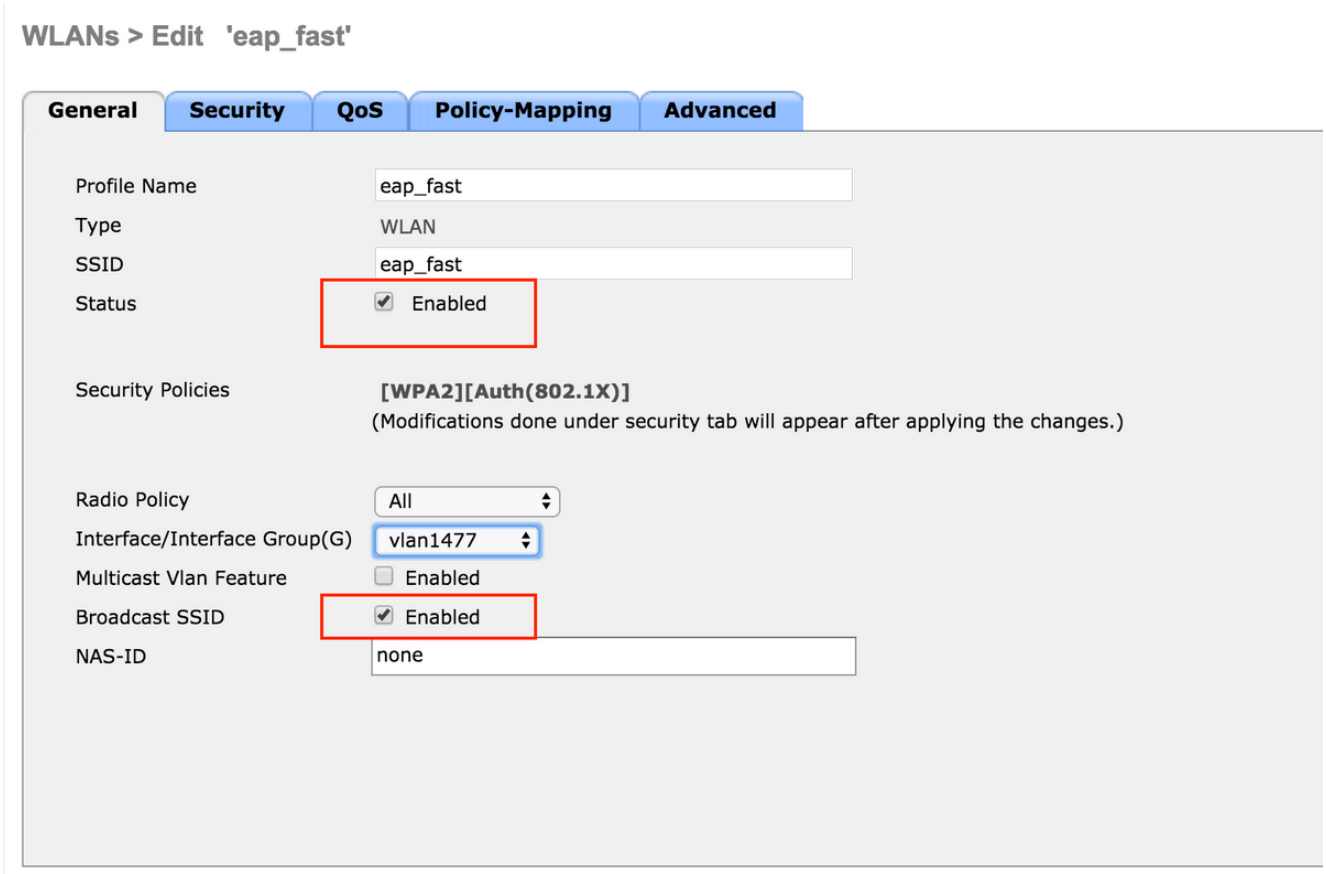
1. Haga clic en **WLANs** desde la GUI del controlador para mostrar la página de WLANs.Esta página enumera las WLANs que existen en el controlador.

2. Haga clic en **Nuevo** para crear una nueva WLAN.

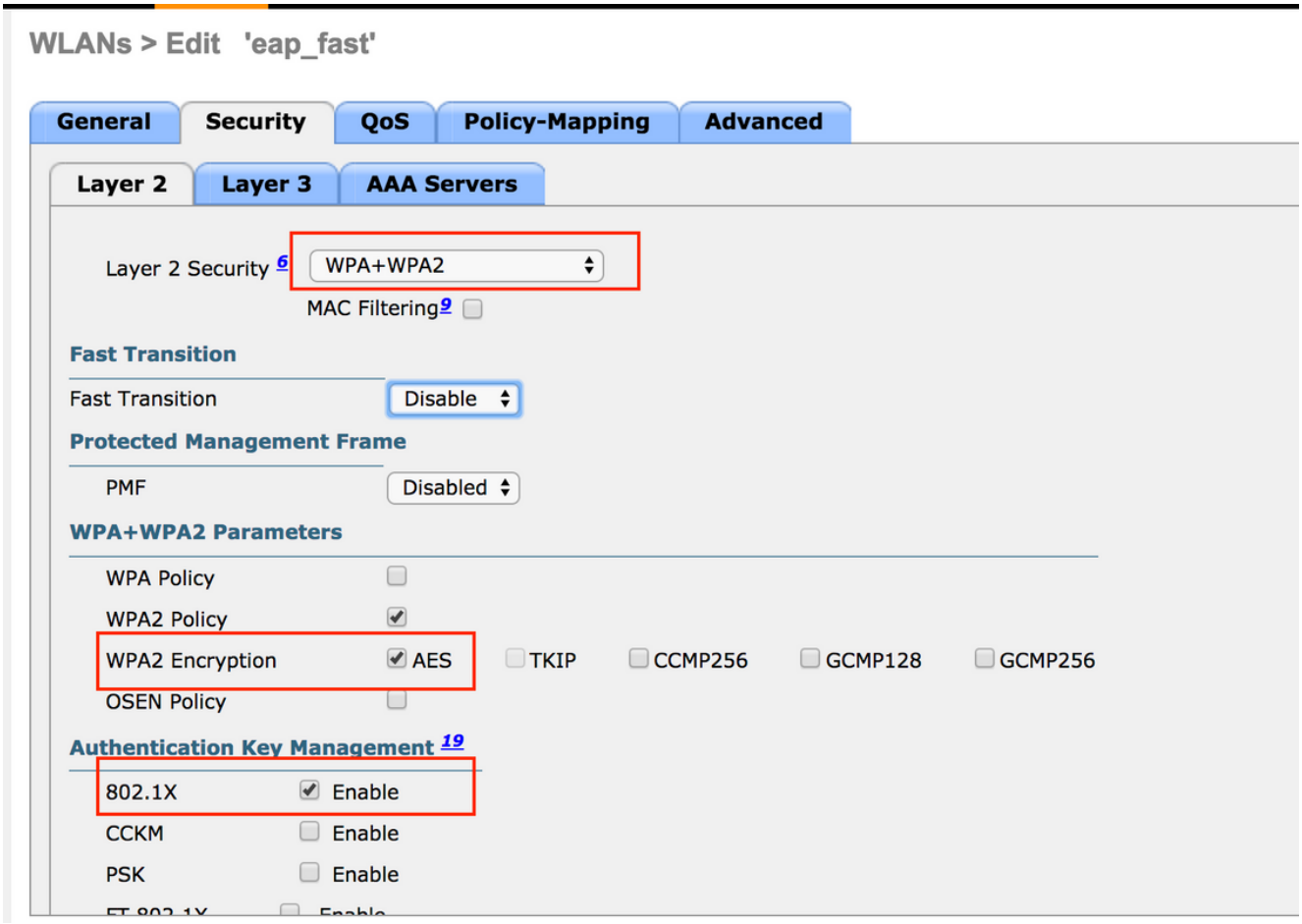


3. Configure el nombre **eap_fast** WLAN SSID, el nombre del perfil y el ID de WLAN en la página WLANs > New. A continuación, haga clic en **Aplicar**.

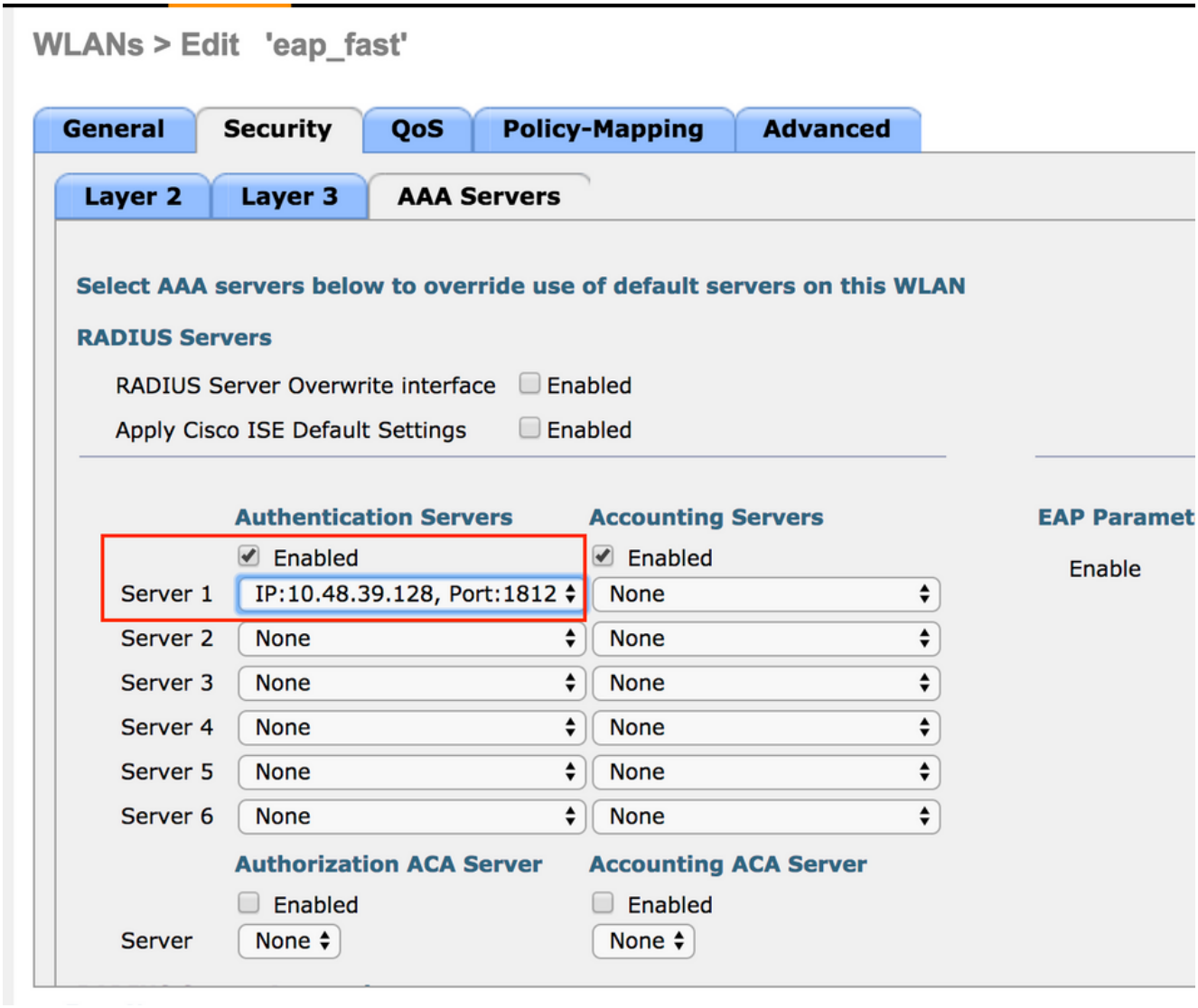
4. Una vez que crea una nueva WLAN, aparece la página **WLAN > Edit** para la nueva WLAN. En esta página, puede definir varios parámetros específicos para esta WLAN. Esto incluye políticas generales, servidores RADIUS, políticas de seguridad y parámetros 802.1x.
5. Marque la casilla de verificación **Admin Status** bajo la **ficha General Policies** para habilitar la WLAN. Si desea que el AP transmita el SSID en sus tramas de baliza, marque la casilla de verificación **Broadcast SSID**.



6. En **"WLAN -> Editar -> Seguridad -> Capa 2"** seleccione parámetros WPA/WPA2 y seleccione dot1x para AKM.
   Este ejemplo utiliza WPA2/AES + dot1x como seguridad de Capa 2 para esta WLAN. Los otros parámetros se pueden modificar en función de los requisitos de la red WLAN.



7. En la ficha **"WLAN -> Edit -> Security -> AAA Servers"**, elija el servidor RADIUS apropiado del menú desplegable en RADIUS Servers.



8. Haga clic en Apply (Aplicar).**Nota:** Este es el único parámetro EAP que se debe configurar en el controlador para la autenticación EAP. El resto de las configuraciones específicas de EAP-FAST deben realizarse en el servidor RADIUS y en los clientes que deben autenticarse.

Configuración del Servidor RADIUS para la Autenticación EAP-FAST

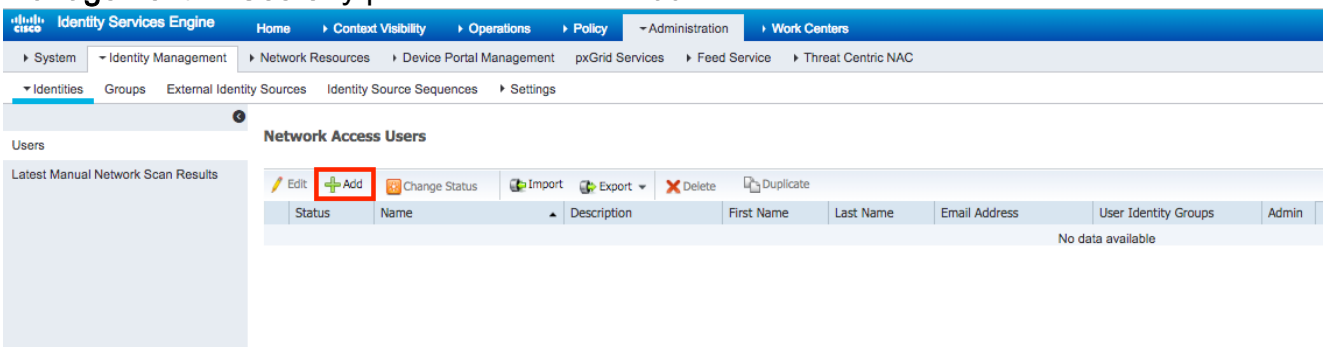
Realice estos pasos para configurar el servidor RADIUS para la autenticación EAP-FAST:

1. Crear una base de datos de usuario para autenticar clientes EAP-FAST
2. Agregue el WLC como cliente AAA al servidor RADIUS
3. Configure la autenticación EAP-FAST en el servidor RADIUS con aprovisionamiento PAC anónimo en banda
4. Configuración de la Autenticación EAP-FAST en el Servidor RADIUS con Aprovisionamiento PAC Autenticado en Banda

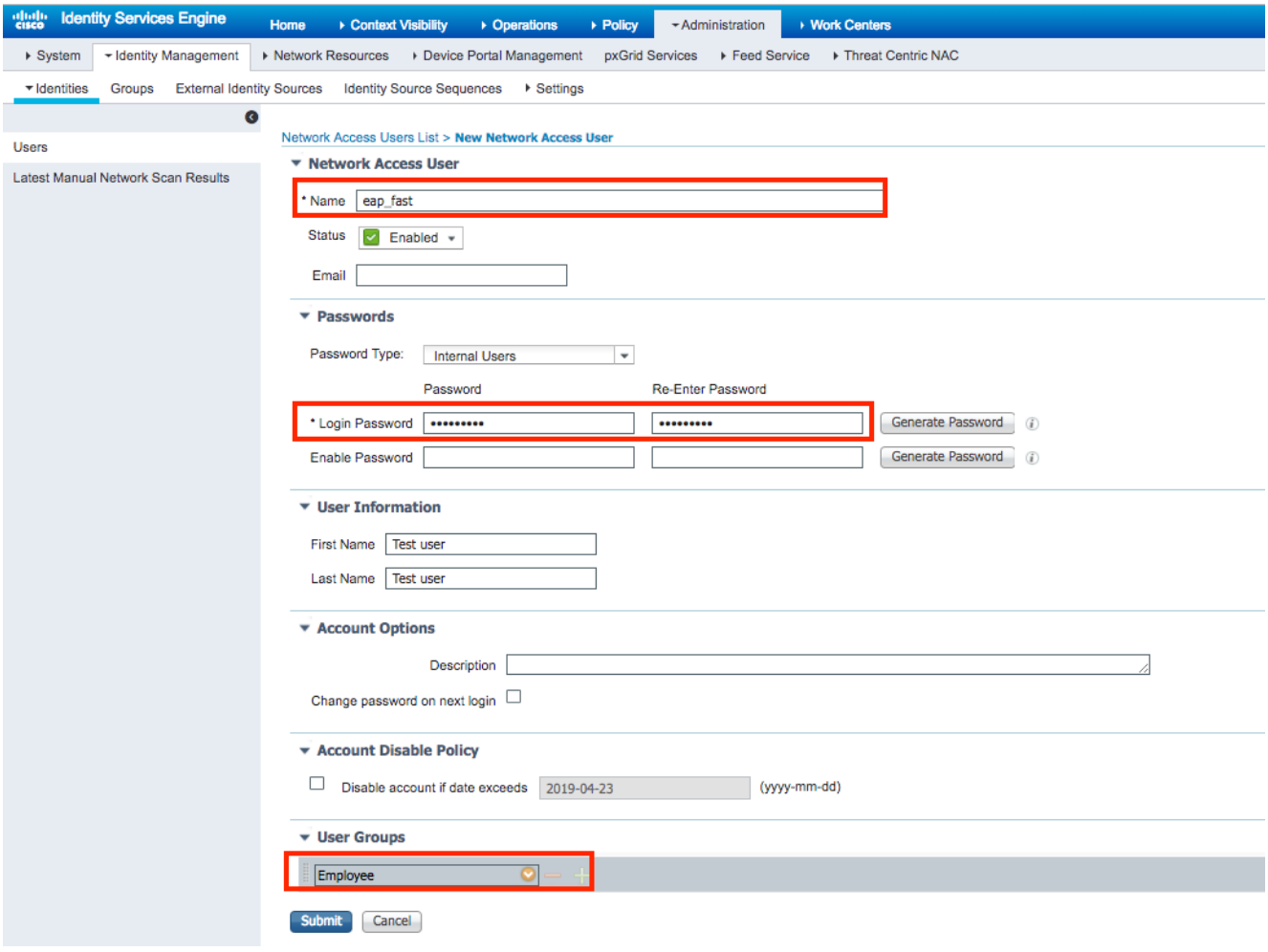
Crear una base de datos de usuario para autenticar clientes EAP-FAST

Este ejemplo configura el nombre de usuario y la contraseña del cliente EAP-FAST como <*eap_fast*> y <*EAP-fast1* >, respectivamente.

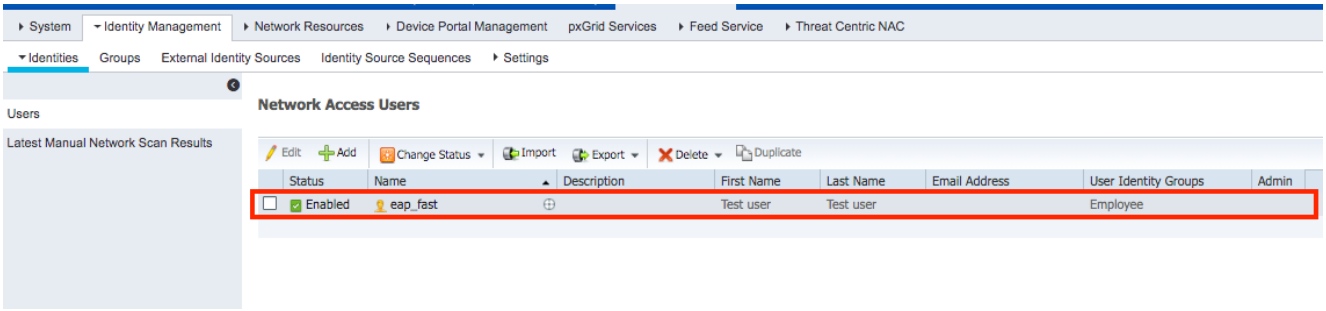
1. En la interfaz de usuario de ISE Web admin, navegue bajo **"Administration -> Identity Management -> Users"** y presione el icono **"Add"**.



2. Rellene los formularios necesarios para que se cree el usuario: **"Nombre"** y **"Contraseña de inicio de sesión"** y seleccione **"Grupo de usuarios"** en la lista desplegable;[opcionalmente puede rellenar otra información para la cuenta de usuario]
Pulse **"Sumbit"**



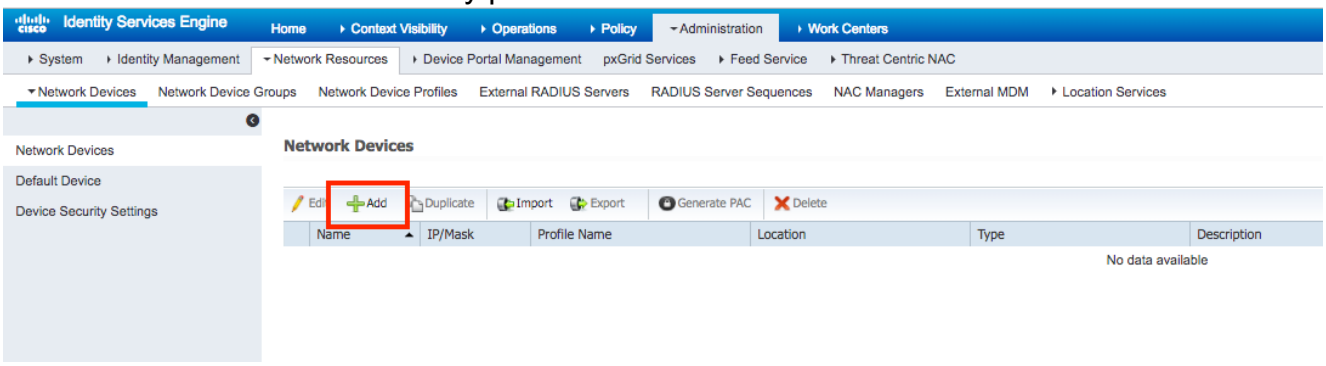
3. Se crea el usuario.



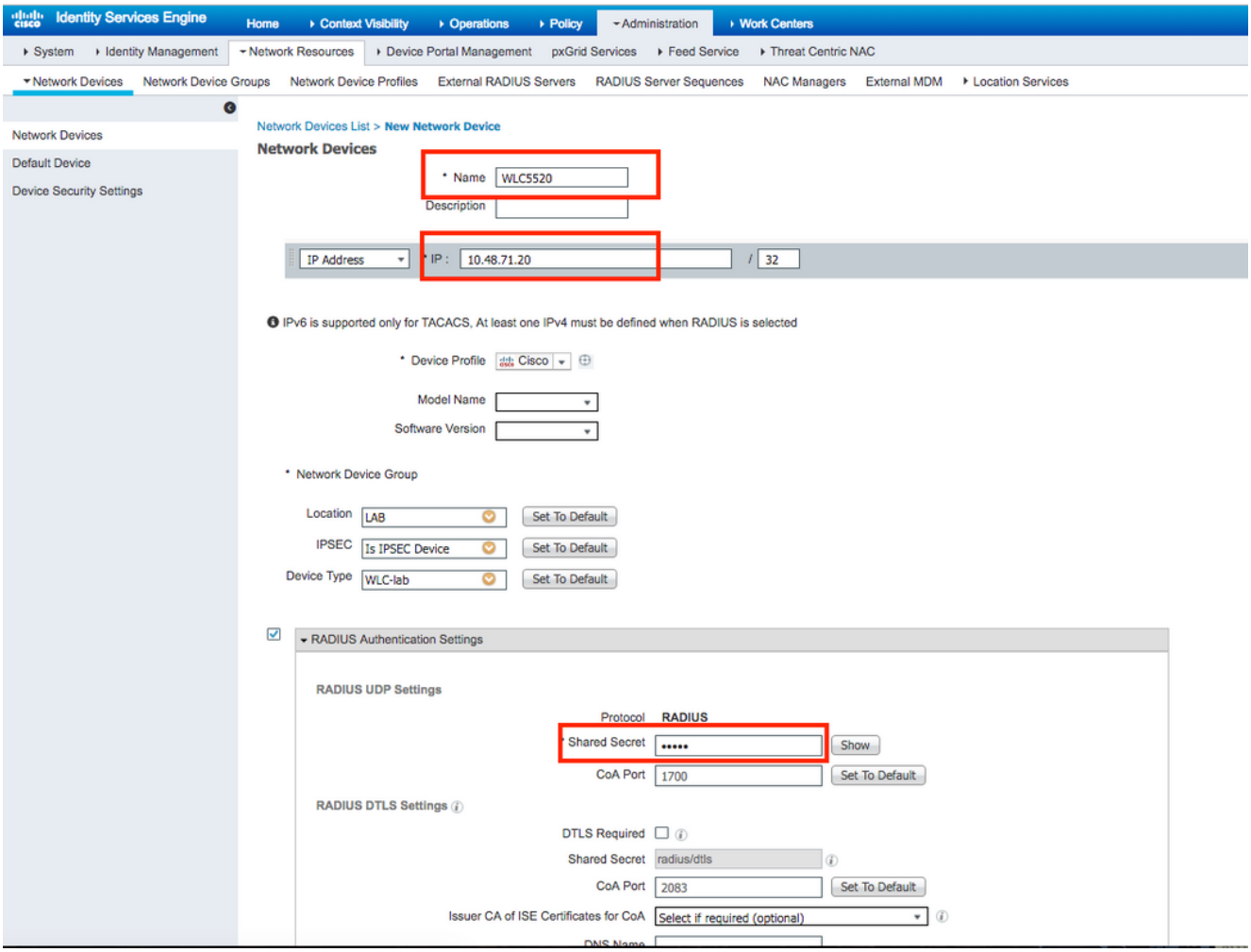
Agregue el WLC como cliente AAA al servidor RADIUS

Complete estos pasos para definir el controlador como un cliente AAA en el servidor ACS:

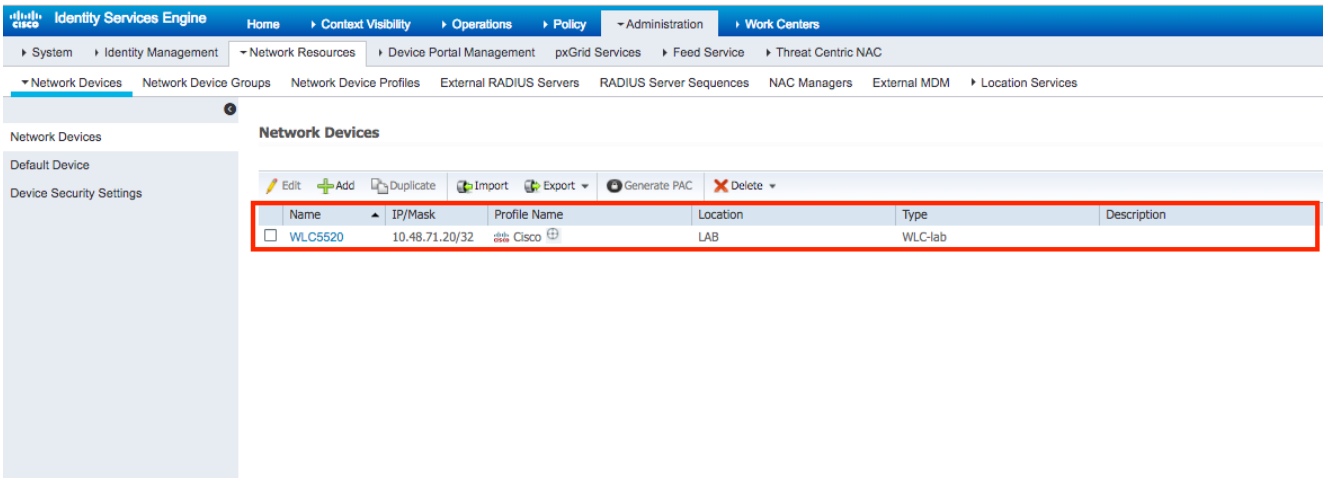
1. En la interfaz de usuario de ISE Web admin navegue bajo **"Administration -> Network Resources -> Network Devices"** y presione el icono **"Add"**.



2. Rellene los formularios requeridos para que el dispositivo sea agregado - **"Nombre"**, **"IP"** y configure la misma contraseña secreta compartida, como configuramos en WLC en la sección anterior, en el formulario **"Secreto Compartido"** [opcionalmente puede llenar otra información para el dispositivo como ubicación, grupo, etc].
Pulse **"Sumbit"**



3. El dispositivo se agrega a la lista de dispositivos de acceso de red ISE. (NAD)

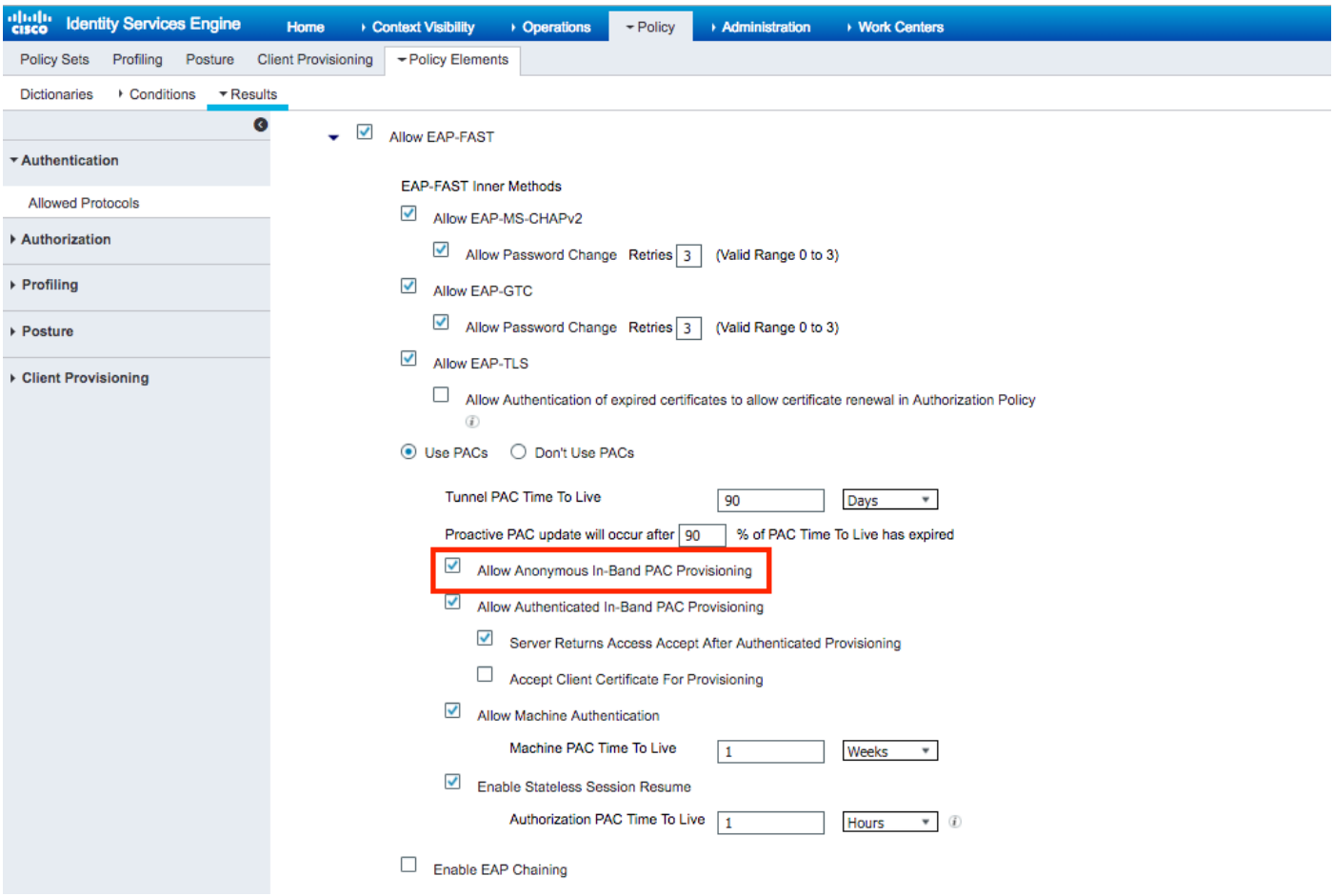


Configure la autenticación EAP-FAST en el servidor RADIUS con aprovisionamiento PAC anónimo en banda

Por lo general, uno quisiera utilizar este tipo de método en caso de que no tengan infraestructura PKI en su implementación.

Este método funciona dentro de un túnel de protocolo de acuerdo de clave Diffie-Hellman autenticado (ADHP) antes de que el par autentique el servidor ISE.

Para admitir este método, necesitamos habilitar "**"Permitir aprovisionamiento PAC anónimo en banda**" en ISE bajo los "**Protocolos permitidos de autenticación**":



Nota: Asegúrese de haber permitido la autenticación de tipo de contraseña, como EAP-MS-CHAPv2 para el método interno EAP-FAST, ya que obviamente con Aprovisionamiento en banda

anónimo no podemos utilizar ningún certificado.

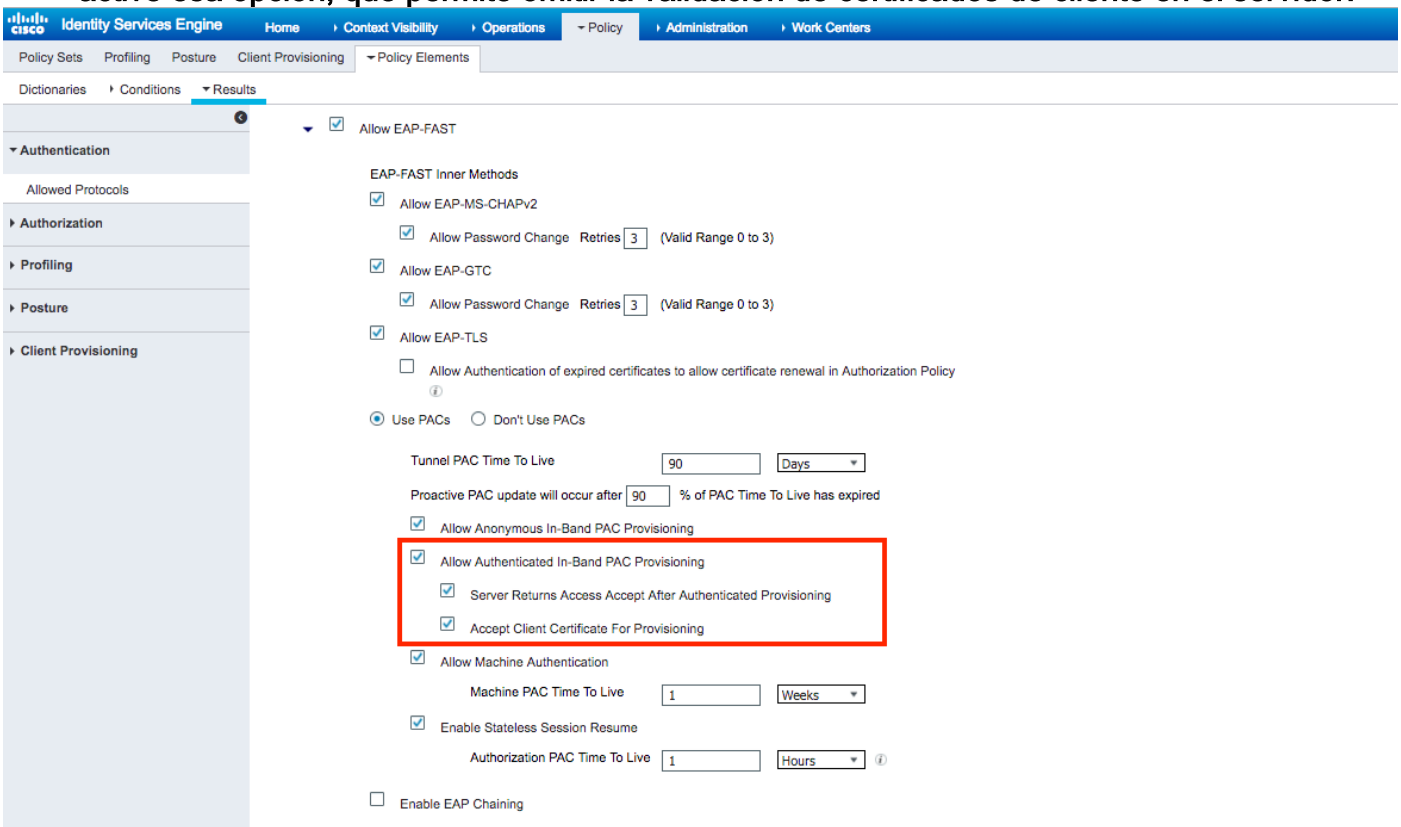
Configuración de la Autenticación EAP-FAST en el Servidor RADIUS con Aprovisionamiento PAC Autenticado en Banda

Esta es la opción más segura y recomendada. El túnel TLS se genera basándose en el certificado del servidor que es validado por el solicitante y el certificado del cliente es validado por ISE (valor predeterminado).

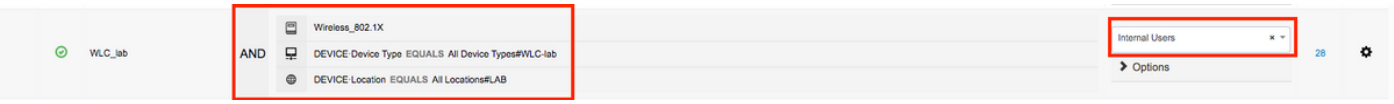
Esta opción requiere disponer de infraestructura PKI para el cliente y el servidor, aunque sólo puede limitarse al lado del servidor o omitirse en ambos lados.

En ISE hay dos opciones adicionales para el aprovisionamiento en banda autenticado:

1. **"Server Devuelve el Acceso Aceptar después de un Aprovisionamiento Autenticado"** - Normalmente, después de un Aprovisionamiento PAC, se debe enviar un Rechazo de Acceso que obliga al solicitante a volver a autenticarse mediante PAC. Sin embargo, dado que el aprovisionamiento PAC se realiza en el túnel TLS autenticado, podemos responder inmediatamente con Access-Accept para minimizar el tiempo de autenticación. (en tal caso, asegúrese de que dispone de certificados de confianza en el cliente y en el servidor).
2. **"Aceptar certificado de cliente para aprovisionamiento": si no se desea proporcionar infraestructura PKI a los dispositivos cliente y sólo se tiene certificado de confianza en ISE, active esa opción, que permite omitir la validación de certificados de cliente en el servidor.**



En ISE también definimos un conjunto de políticas de autenticación simple para los usuarios inalámbricos. A continuación, el ejemplo utiliza como tipo de dispositivo de parámetro de condición y tipo de ubicación y autenticación, el flujo de autenticación que coincide con esa condición se validará en la base de datos de usuarios interna.



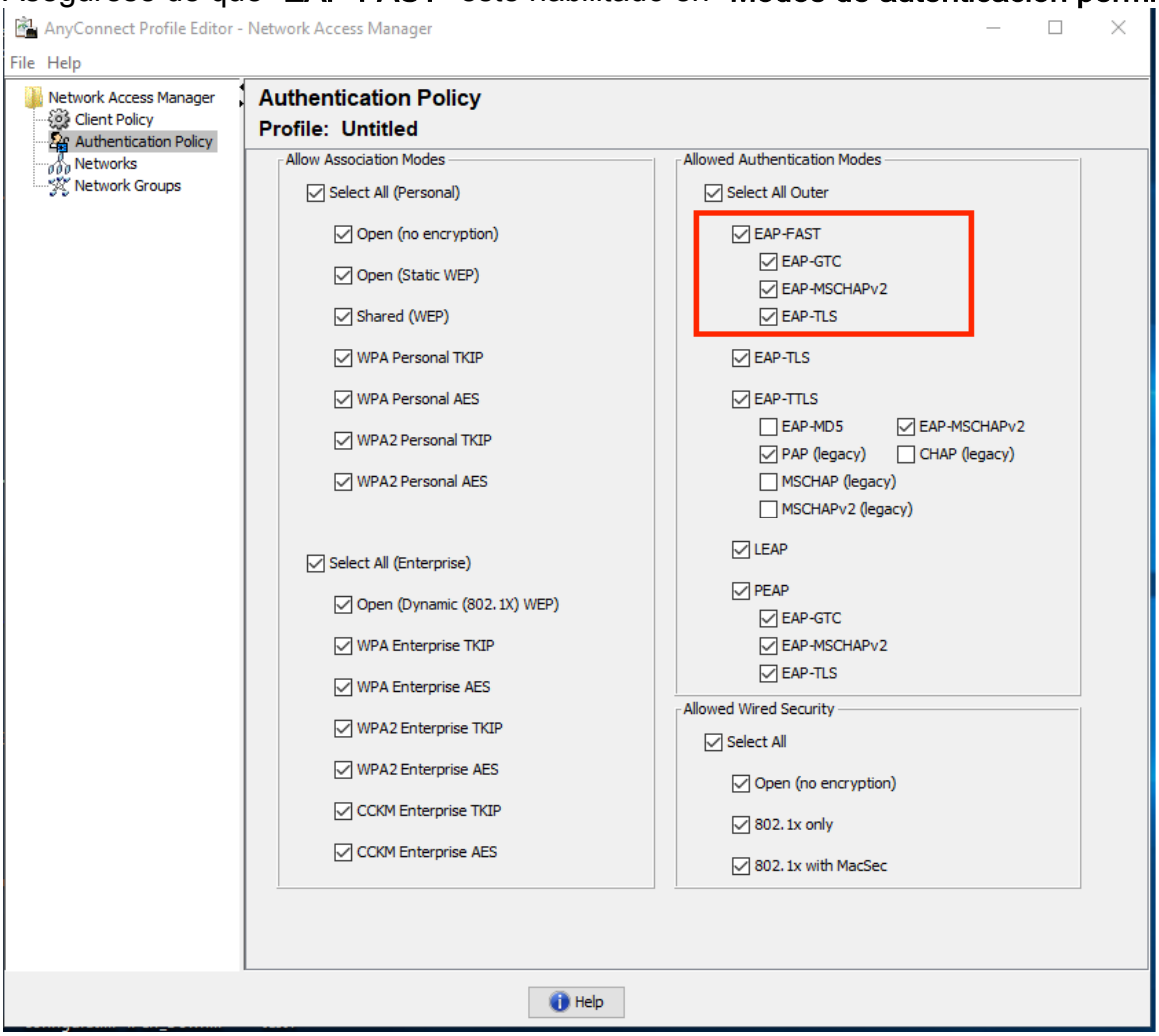
Verificación

En este ejemplo se mostrarán los parámetros de configuración del flujo de aprovisionamiento PAC autenticado en banda y del administrador de acceso de red (NAM) junto con los debugs de WLC respectivos.

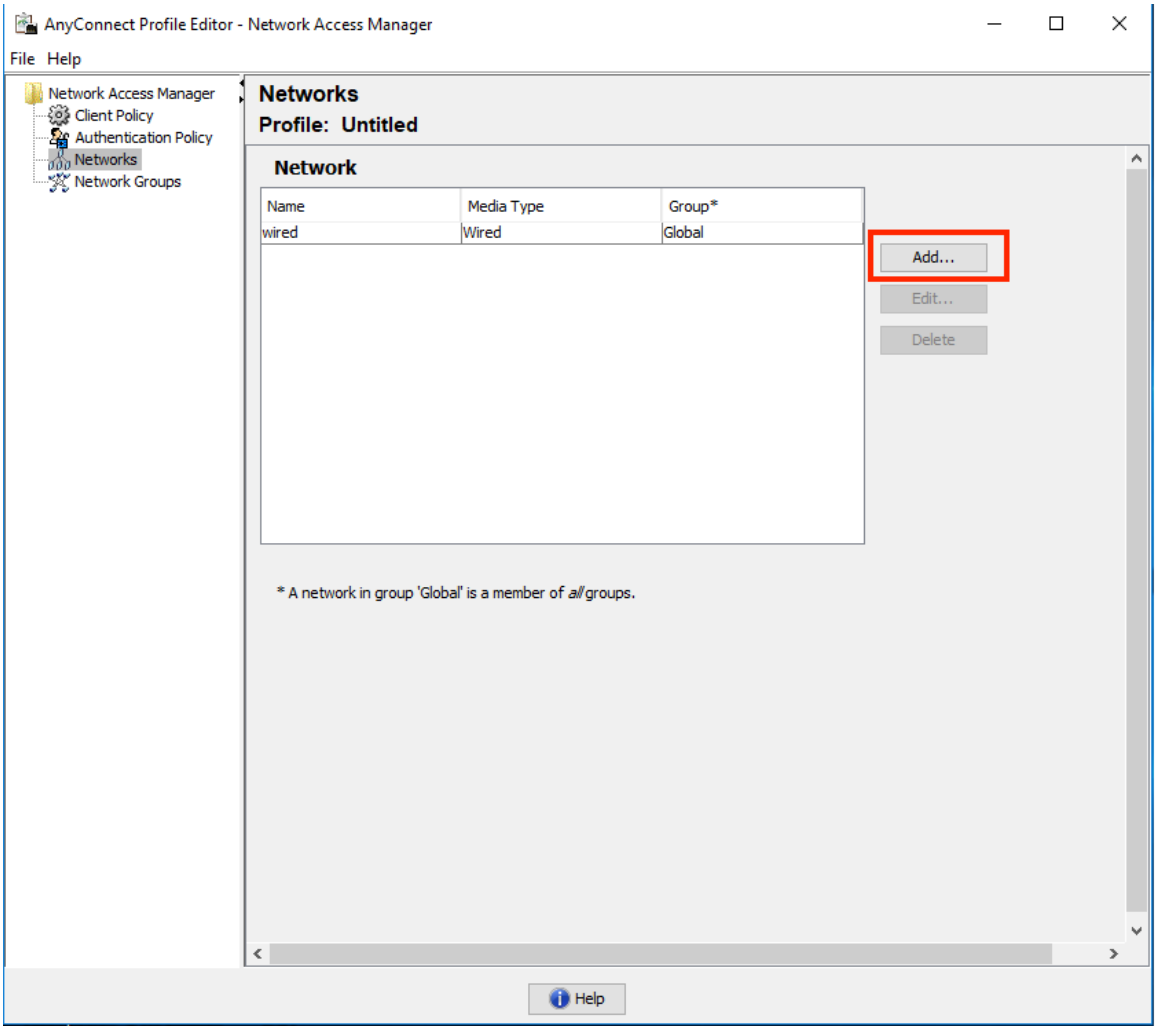
configuración del perfil NAM

Se deben realizar los siguientes pasos para configurar el perfil NAM de Anyconnect para autenticar la sesión de usuario con ISE mediante EAP-FAST:

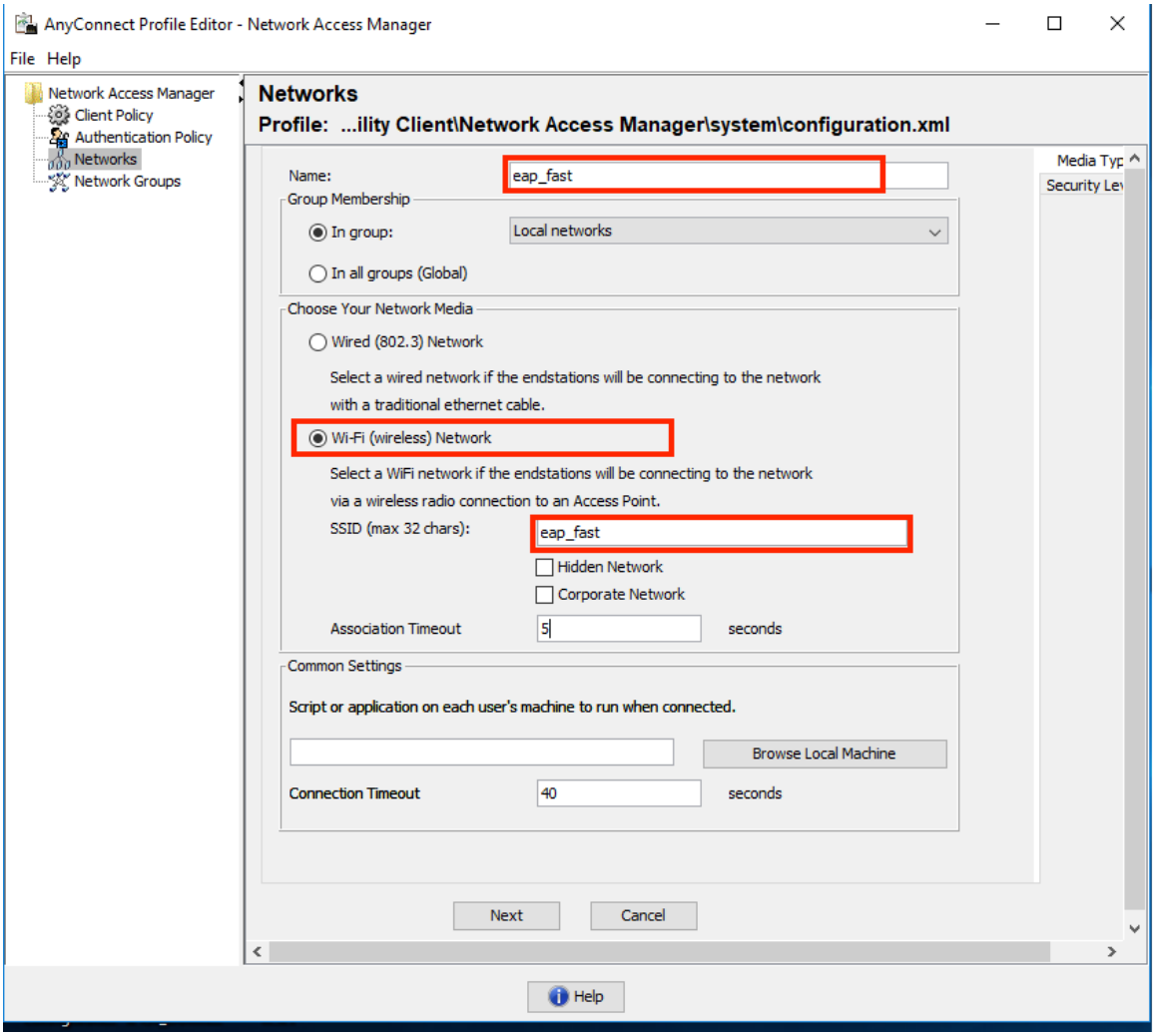
1. Abra Network Access Manager Profile Editor y cargue el archivo de configuración actual.
2. Asegúrese de que **"EAP-FAST"** esté habilitado en **"Modos de autenticación permitidos"**



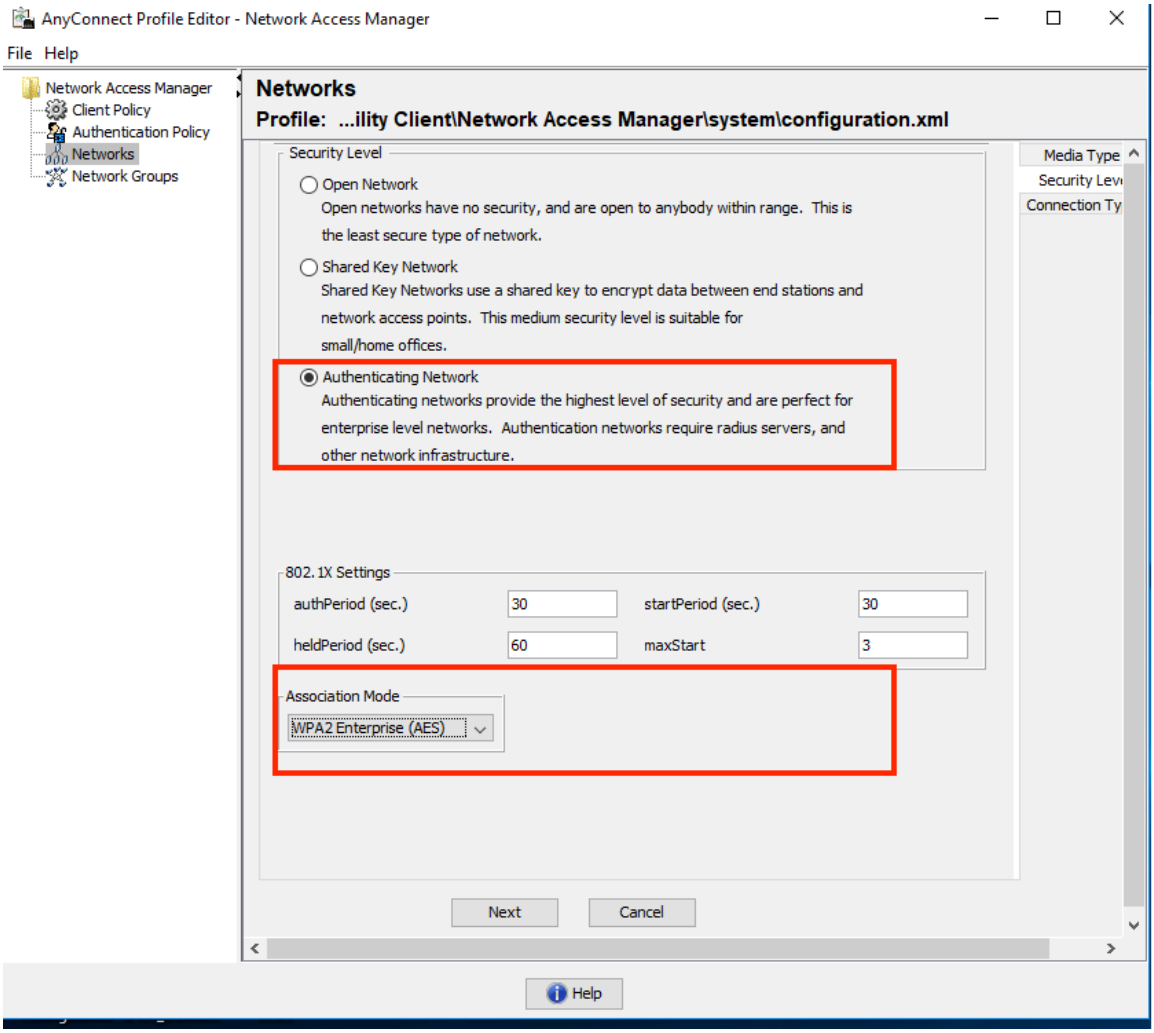
3. **"Agregar"** un nuevo perfil de red:



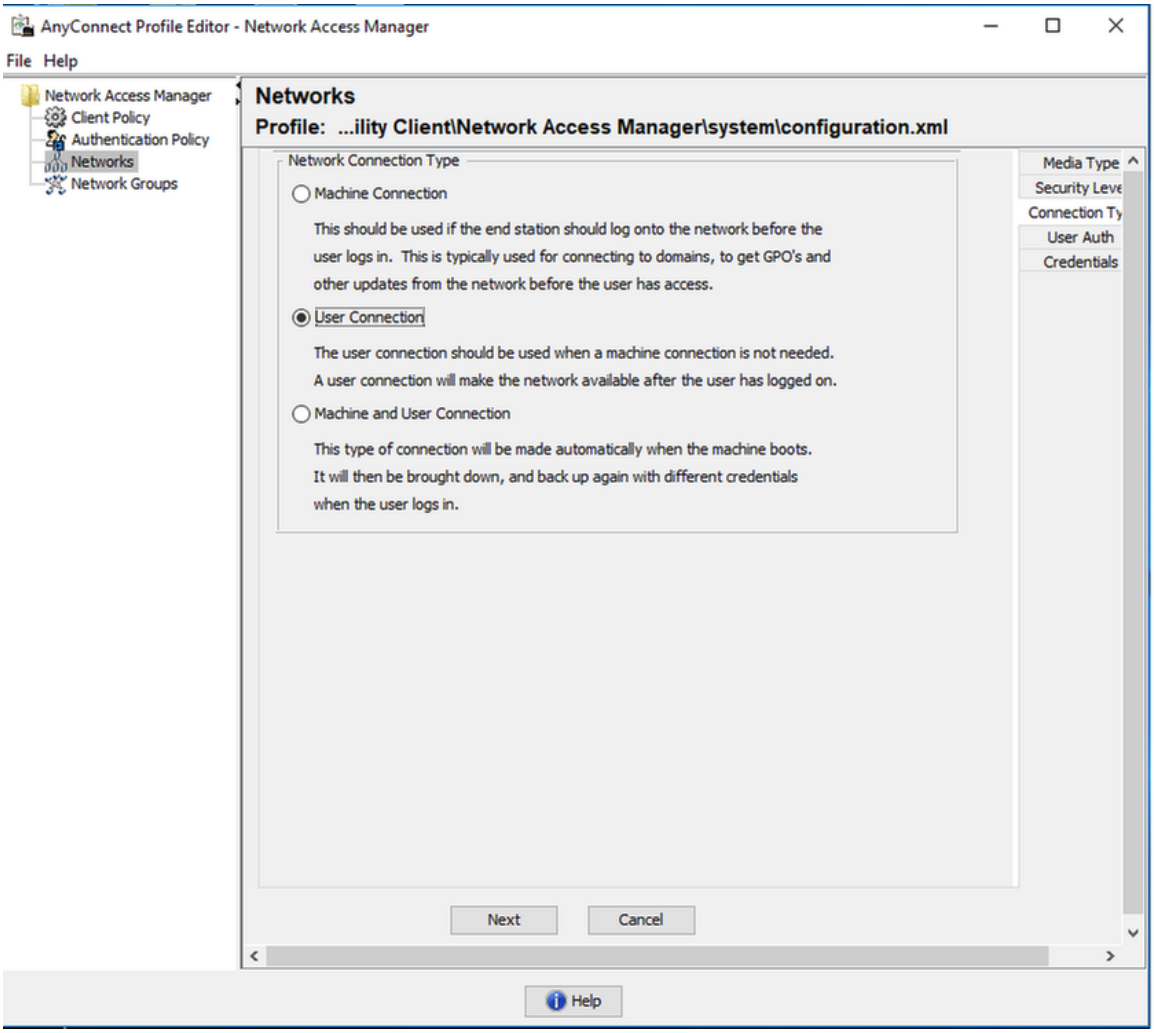
4. En la sección de configuración **"Tipo de medios"**, defina el perfil "**Nombre**", como el tipo de red de medios y especifique el nombre SSID.



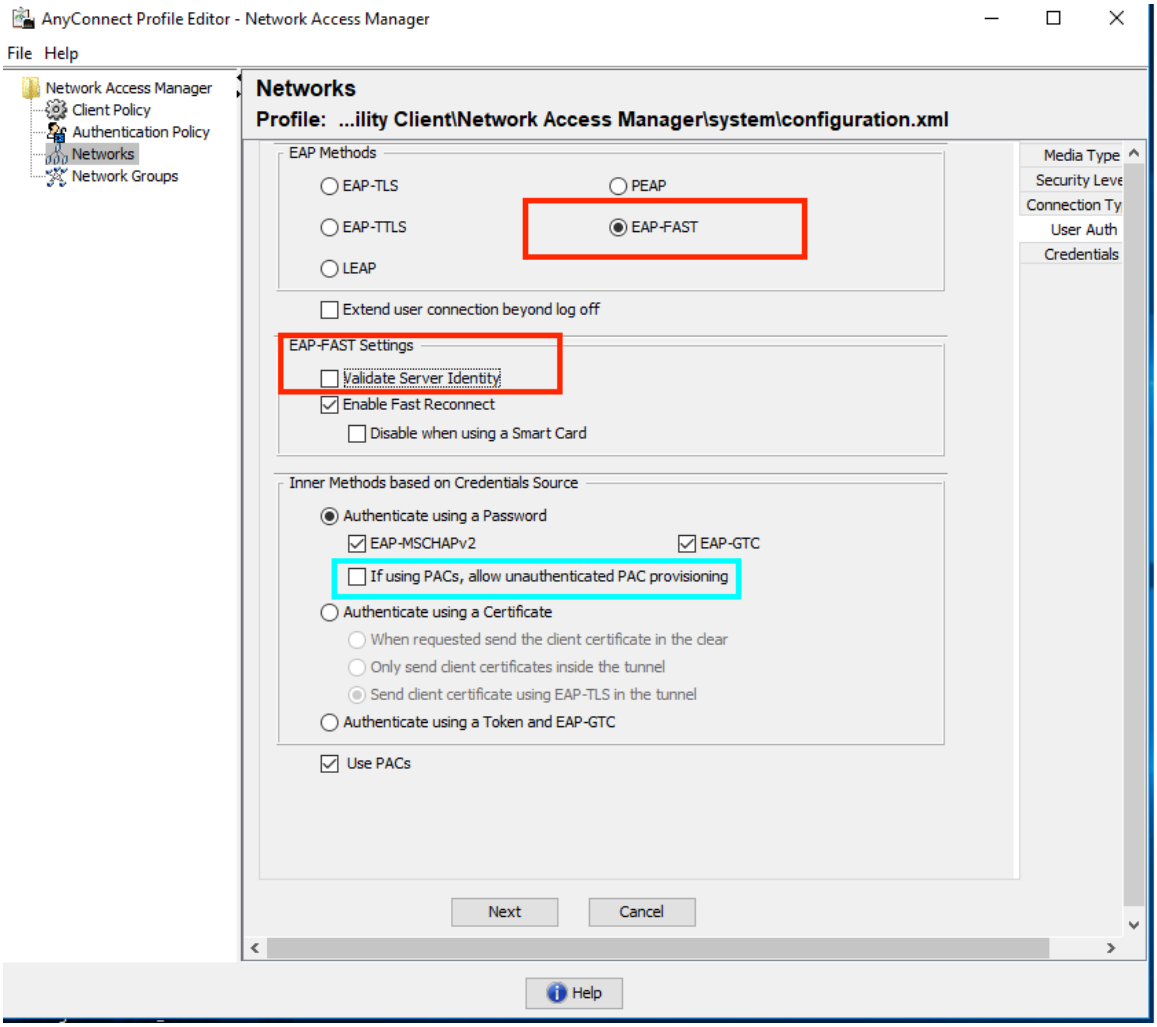
5. En la ficha de configuración **"Nivel de seguridad"**, seleccione "Autenticación de red" y especifique el modo de asociación como WPA2 Enterprise (AES)



6. En este ejemplo estamos utilizando la autenticación de tipo de usuario, por lo tanto, en la ficha siguiente "**Tipo de conexión**" seleccione "**Conexión de usuario**"



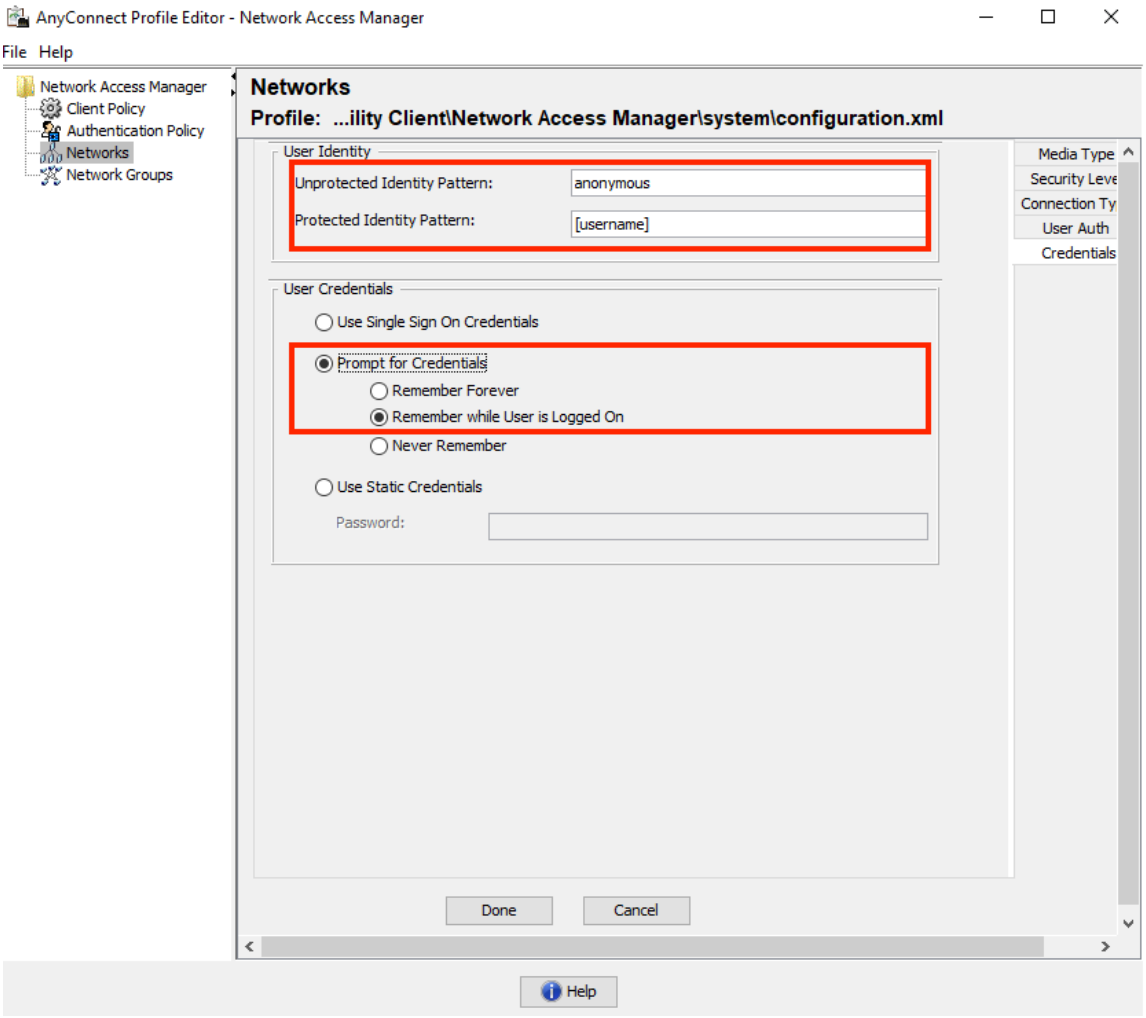
7. En la ficha "**User Auth**", especifique EAP-FAST como método de autenticación permitido e inhabilite la validación del certificado del servidor, ya que en este ejemplo no utilizamos certificados de confianza.



Nota: en el entorno de producción real, asegúrese de tener instalado el certificado de confianza en ISE y mantenga la opción de validación del certificado del servidor habilitada en la configuración de NAM.

Nota: opción "Si se utilizan PACs, se debe seleccionar permitir el aprovisionamiento PAC no autenticado" sólo en caso de aprovisionamiento PAC anónimo en banda.

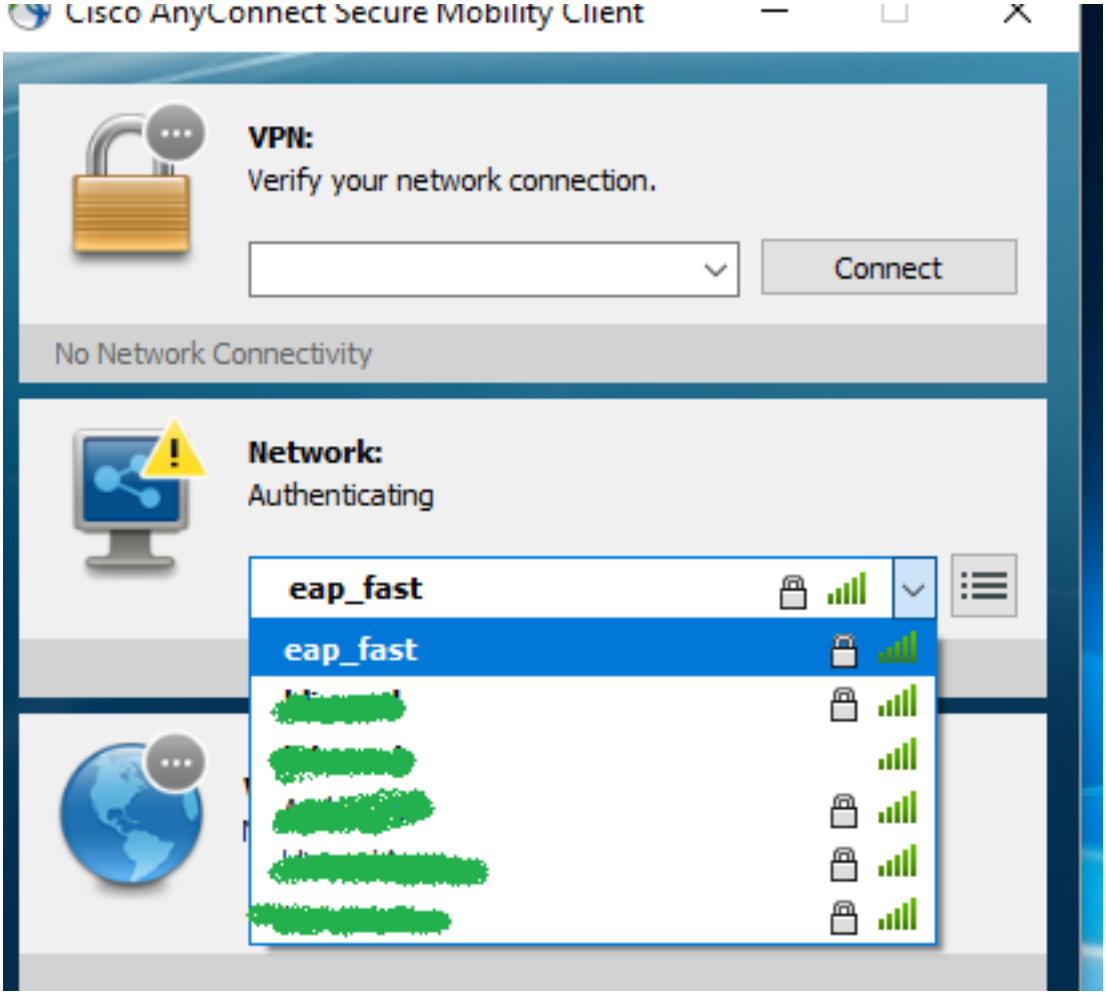
8. Defina las credenciales de usuario, ya sea como SSO en caso de que desee utilizar las mismas credenciales que se usaron para el inicio de sesión, o seleccione "Pedir credenciales" en caso de que desee que se pida al usuario las credenciales mientras se conecta a la red, o defina las credenciales estáticas para ese tipo de acceso. En este ejemplo, solicitamos al usuario credenciales al intentar conectarse a la red.



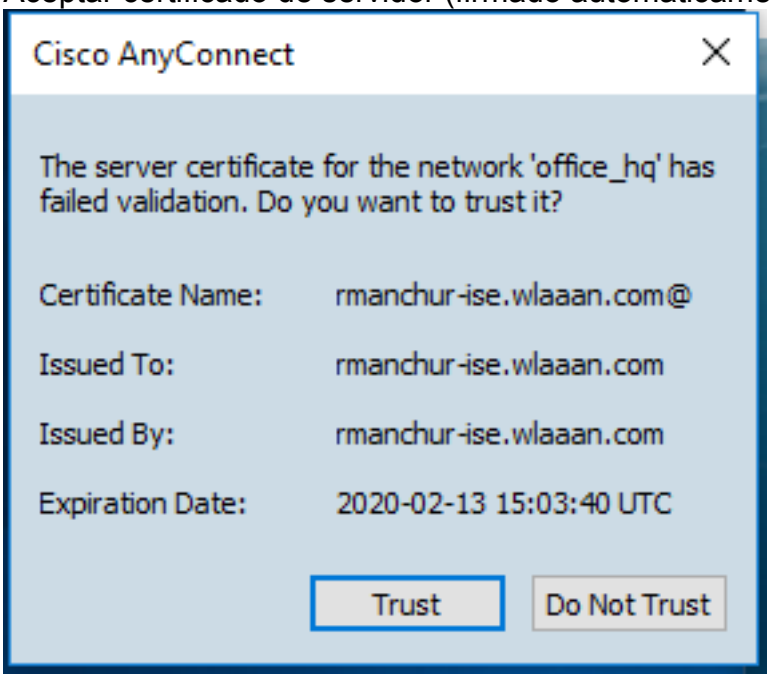
9. Guarde el perfil configurado en la carpeta NAM correspondiente.

Pruebe la conectividad con SSID mediante la autenticación EAP-FAST.

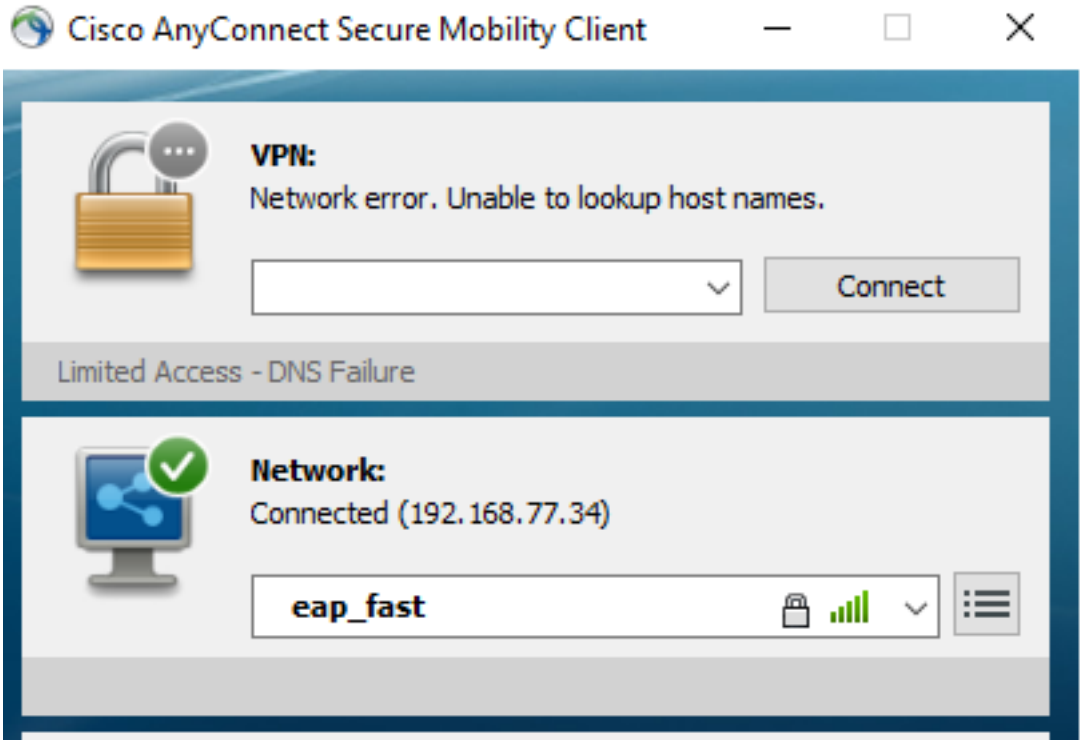
1. Seleccionar el perfil respectivo de la lista de redes de Anyconnect



2. Introduzca el nombre de usuario y la contraseña necesarios para la autenticación
3. Aceptar certificado de servidor (firmado automáticamente)



4. Fin



Registros de autenticación ISE

Los registros de autenticación ISE que muestran el flujo de aprovisionamiento de EAP-FAST y PAC se pueden ver en "**Operaciones -> RADIUS -> Registros en directo**" y se pueden ver en más detalles usando el icono "**Zoom**":

1. El cliente ha iniciado la autenticación e ISE estaba proponiendo EAP-TLS como método de autenticación, pero el cliente rechazó y propuso EAP-FAST en su lugar, ese era el método en el que el cliente y el ISE estaban de acuerdo.

Steps

11001	Received RADIUS Access-Request
11017	RADIUS created a new session
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
11507	Extracted EAP-Response/Identity
12500	Prepared EAP-Request proposing EAP-TLS with challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12101	Extracted EAP-Response/NAK requesting to use EAP-FAST instead
12100	Prepared EAP-Request proposing EAP-FAST with challenge
11006	Returned RADIUS Access-Challenge
11001	Received RADIUS Access-Request
11018	RADIUS is re-using an existing session
12102	Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST as negotiated

2. El intercambio de señales TLS se inició entre el cliente y el servidor para proporcionar un entorno protegido para el intercambio PAC y se completó correctamente.

12800 Extracted first TLS record; TLS handshake started
12805 Extracted TLS ClientHello message
12806 Prepared TLS ServerHello message
12807 Prepared TLS Certificate message
12808 Prepared TLS ServerKeyExchange message
12810 Prepared TLS ServerDone message
12811 Extracted TLS Certificate message containing client certificate
12105 Prepared EAP-Request with another EAP-FAST challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request
11018 RADIUS is re-using an existing session
12104 Extracted EAP-Response containing EAP-FAST challenge-response
12105 Prepared EAP-Request with another EAP-FAST challenge
11006 Returned RADIUS Access-Challenge
11001 Received RADIUS Access-Request (⏰ Step latency=13317 ms)
11018 RADIUS is re-using an existing session
12104 Extracted EAP-Response containing EAP-FAST challenge-response
12812 Extracted TLS ClientKeyExchange message
12813 Extracted TLS CertificateVerify message
12804 Extracted TLS Finished message
12801 Prepared TLS ChangeCipherSpec message
12802 Prepared TLS Finished message
12816 TLS handshake succeeded

3. Se inició la autenticación interna y las credenciales de usuario fueron validadas correctamente por ISE mediante MS-CHAPv2 (autenticación basada en nombre de usuario/contraseña)