Autenticação EAP-FAST com Wireless LAN Controllers e Identity Services Engine

Contents

Introduction

Este documento explica como configurar o Controller de LAN Wireless (WLC) para uma autenticação Extensible Authentication Protocol (EAP) - Flexible Authentication via Secure Tunneling (FAST) com o uso de um servidor RADIUS externo. Este exemplo de configuração usa o Identity Services Engine (ISE) como o servidor RADIUS externo para autenticar o cliente sem fio.

Este documento enfatiza como configurar o ISE para o provisionamento de PACs (Credenciais de Acesso Protegido) Anônimas e Autenticadas em Banda (Automáticas) para os clientes sem fio.

Prerequisites

Requirements

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Conhecimento básico da configuração de pontos de acesso leves (LAPs) e Cisco WLCs
- Conhecimento básico do protocolo CAPWAP
- Conhecimento de como configurar um servidor RADIUS externo, como o Cisco ISE
- Conhecimentos funcionais sobre o quadro geral de PEA
- Conhecimento básico sobre protocolos de segurança, como MS-CHAPv2 e EAP-GTC, e conhecimento sobre certificados digitais

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco 5520 Series WLC que executa o firmware versão 8.8.111.0AP Cisco 4800 SeriesAnyconnect NAM.Cisco Secure ISE versão 2.3.0.298Switch Cisco 3560-CX Series que executa a versão 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.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

O protocolo EAP-FAST é um tipo de EAP IEEE 802.1X acessível ao público que a Cisco desenvolveu para suportar clientes que não podem aplicar uma política de senha forte e querem implantar um tipo de EAP 802.1X que não requer certificados digitais.

O protocolo EAP-FAST é uma arquitetura de segurança cliente-servidor que criptografa transações EAP com um túnel TLS (Transport Level Security). O estabelecimento do túnel EAP-FAST baseia-se em segredos fortes que são exclusivos dos usuários. Esses segredos fortes são chamados de PACs, que o ISE gera usando uma chave mestra conhecida apenas pelo ISE.

O EAP-FAST ocorre em três fases:

- **Fase zero (fase de provisionamento automático da PAC)** — fase zero do EAP-FAST, uma fase opcional é um meio protegido por túnel para fornecer uma PAC ao usuário final do EAP-FAST com uma PAC para o usuário que solicita acesso à rede. **Fornecer uma PAC ao cliente do usuário final é a única finalidade da fase zero**.**Observação:** a fase zero é opcional porque as PACs também podem ser provisionadas manualmente para os clientes em vez de usar a fase zero.Consulte a seção Modos de Provisionamento PAC deste documento para obter

detalhes.

- **Fase um** — Na fase um, o ISE e o cliente de usuário final estabelecem um túnel TLS com base na credencial PAC do usuário. Essa fase exige que o cliente do usuário final tenha recebido uma PAC para o usuário que está tentando obter acesso à rede e que a PAC seja baseada em uma chave mestre que não expirou. Nenhum serviço de rede é ativado pela fase um do EAP-FAST.
- **Fase dois** — Na fase dois, as credenciais de autenticação de usuário são passadas com segurança usando um método EAP interno suportado pelo EAP-FAST dentro do túnel TLS para o RADIUS criado usando a PAC entre o cliente e o servidor RADIUS. EAP-GTC, TLS e MS-CHAP são suportados como métodos EAP internos. Nenhum outro tipo de EAP é suportado para EAP-FAST.

Consulte Como o EAP-FAST funciona para obter mais informações.

PAC

As PACs são fortes segredos compartilhados que permitem que o ISE e um cliente de usuário final EAP-FAST se autentiquem e estabeleçam um túnel TLS para uso na fase dois EAP-FAST. O ISE gera PACs usando a chave mestra ativa e um nome de usuário.

A PAC inclui:

- **PAC-Key** — Segredo compartilhado associado a um cliente (e dispositivo cliente) e identidade do servidor.
- **PAC opaco** — Campo opaco que o cliente armazena em cache e passa para o servidor. O servidor recupera a chave PAC e a identidade do cliente para se autenticar mutuamente com o cliente.
- **PAC-Info** — No mínimo, inclui a identidade do servidor para permitir que o cliente armazene em cache diferentes PACs. Opcionalmente, ele inclui outras informações, como a hora de expiração da PAC.

Modos de provisionamento de PAC

Como mencionado anteriormente, a fase zero é uma fase opcional.

O EAP-FAST oferece duas opções para provisionar um cliente com uma PAC:

- **Provisionamento automático de PAC (fase 0 EAP-FAST ou aprovisionamento de PAC em banda)**
- **Provisionamento de PAC manual (fora da banda)**

O provisionamento PAC em banda/automático envia uma nova PAC a um cliente de usuário final através de uma conexão de rede segura. O provisionamento automático de PAC não requer intervenção do usuário da rede ou de um administrador do ISE, desde que você configure o ISE e o cliente do usuário final para suportar o provisionamento automático.

A versão EAP-FAST mais recente suporta duas opções diferentes de configuração de provisionamento PAC na banda:

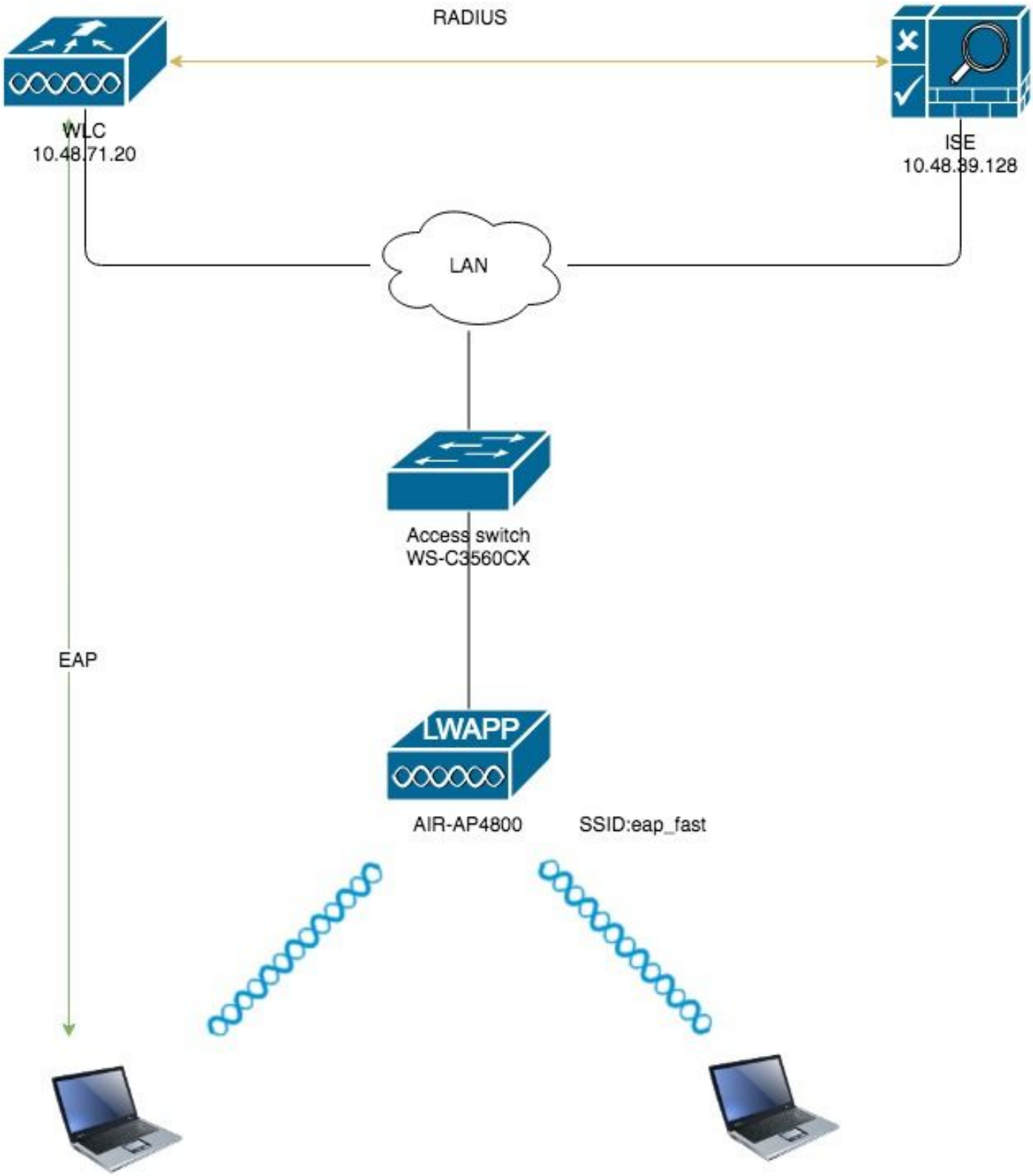
- **Provisionamento de PAC em banda anônima**
- **Provisionamento de PAC em banda autenticado**

Observação: este documento discute esses métodos de provisionamento de PAC em banda e como configurá-los.

O **provisionamento de PAC fora da banda/manual** exige que um administrador do ISE gere arquivos PAC, que devem ser distribuídos para os usuários de rede aplicáveis. Os usuários devem configurar clientes de usuário final com seus arquivos PAC.

Configurar

Diagrama de Rede



Configurações

Configurar a WLC para a autenticação EAP-FAST

Execute estas etapas para configurar a WLC para autenticação EAP-FAST:

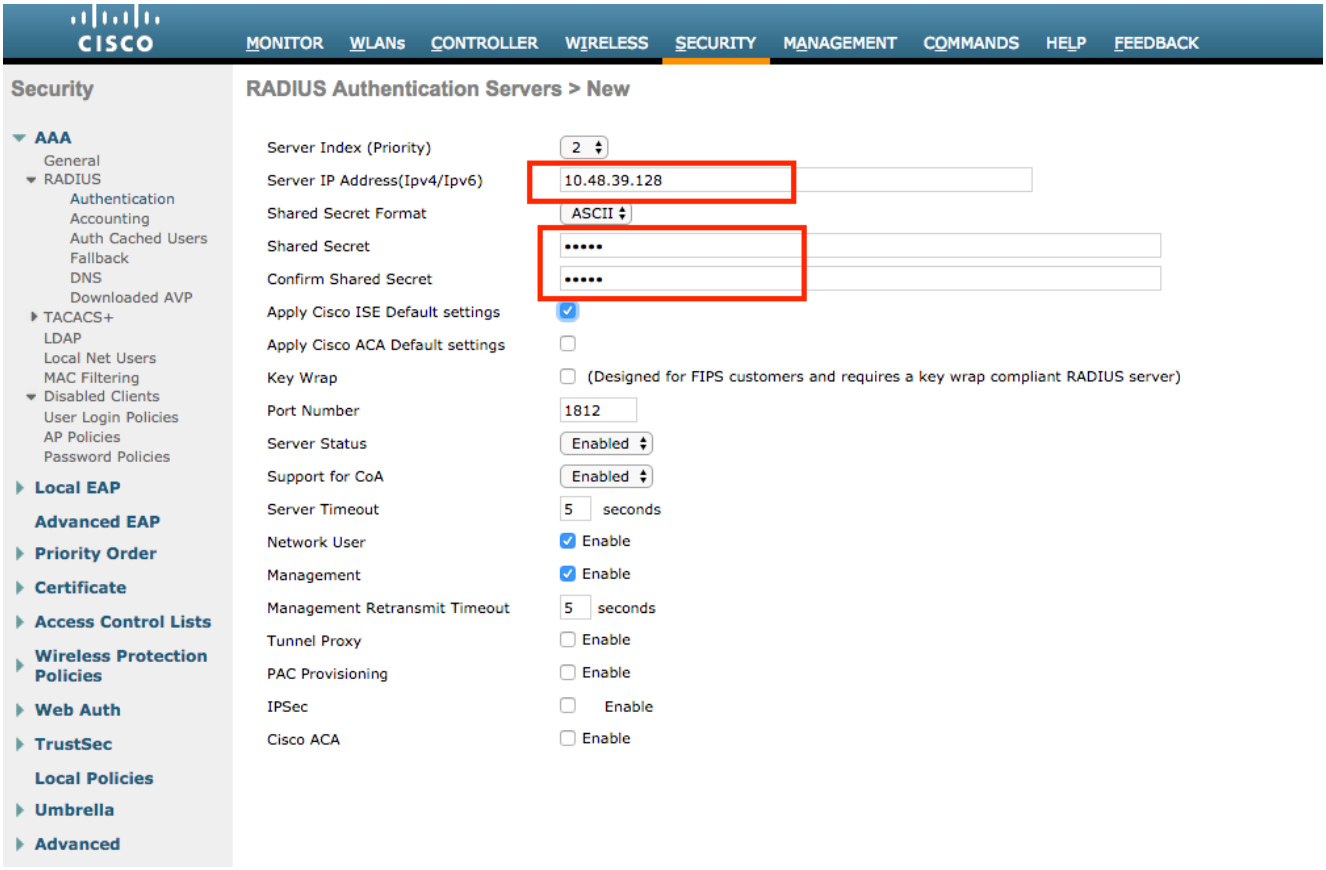
1. Configurar a WLC para autenticação RADIUS através de um servidor RADIUS externo
2. Configurar a WLAN para a autenticação EAP-FAST

Configurar a WLC para autenticação RADIUS através de um servidor RADIUS externo

A WLC precisa ser configurada para encaminhar as credenciais do usuário a um servidor RADIUS externo. O servidor RADIUS externo valida as credenciais do usuário usando EAP-FAST e fornece acesso aos clientes sem fio.

Conclua estes passos para configurar a WLC para um servidor RADIUS externo:

1. Escolha **Segurança** e **Autenticação RADIUS** na GUI do controlador para exibir a página Servidores de Autenticação RADIUS. Em seguida, clique em **New** para definir um servidor RADIUS.
2. Defina os parâmetros do servidor RADIUS na página **Servidores de Autenticação RADIUS > Novo**. Esses parâmetros incluem:Endereço IP do servidor RADIUSshared secretnúmero da portaStatus do servidorEste documento usa o servidor ISE com um endereço IP 10.48.39.128.



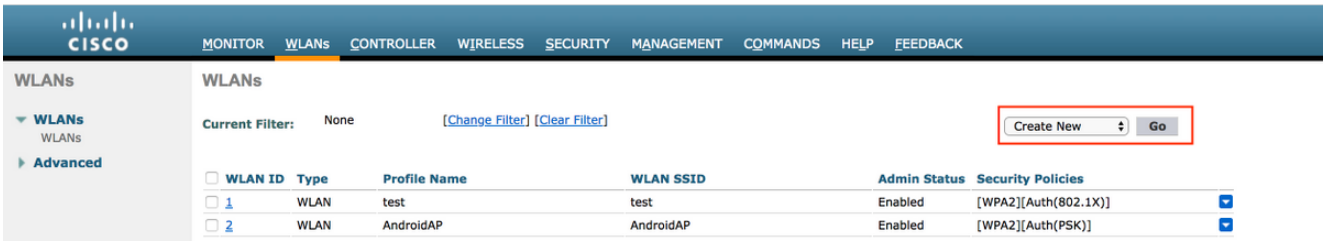
3. Clique em **Aplicar**.

Configurar a WLAN para a autenticação EAP-FAST

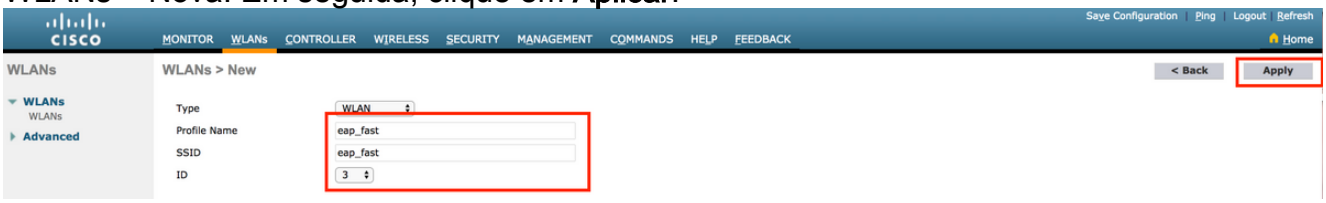
Em seguida, configure a WLAN que os clientes usam para se conectar à rede sem fio para autenticação EAP-FAST e atribua a uma interface dinâmica. O nome da WLAN configurado neste exemplo é **muito rápido**. Este exemplo atribui esta WLAN à interface de gerenciamento.

Conclua estes passos para configurar a WLAN **eap fast** e seus parâmetros relacionados:

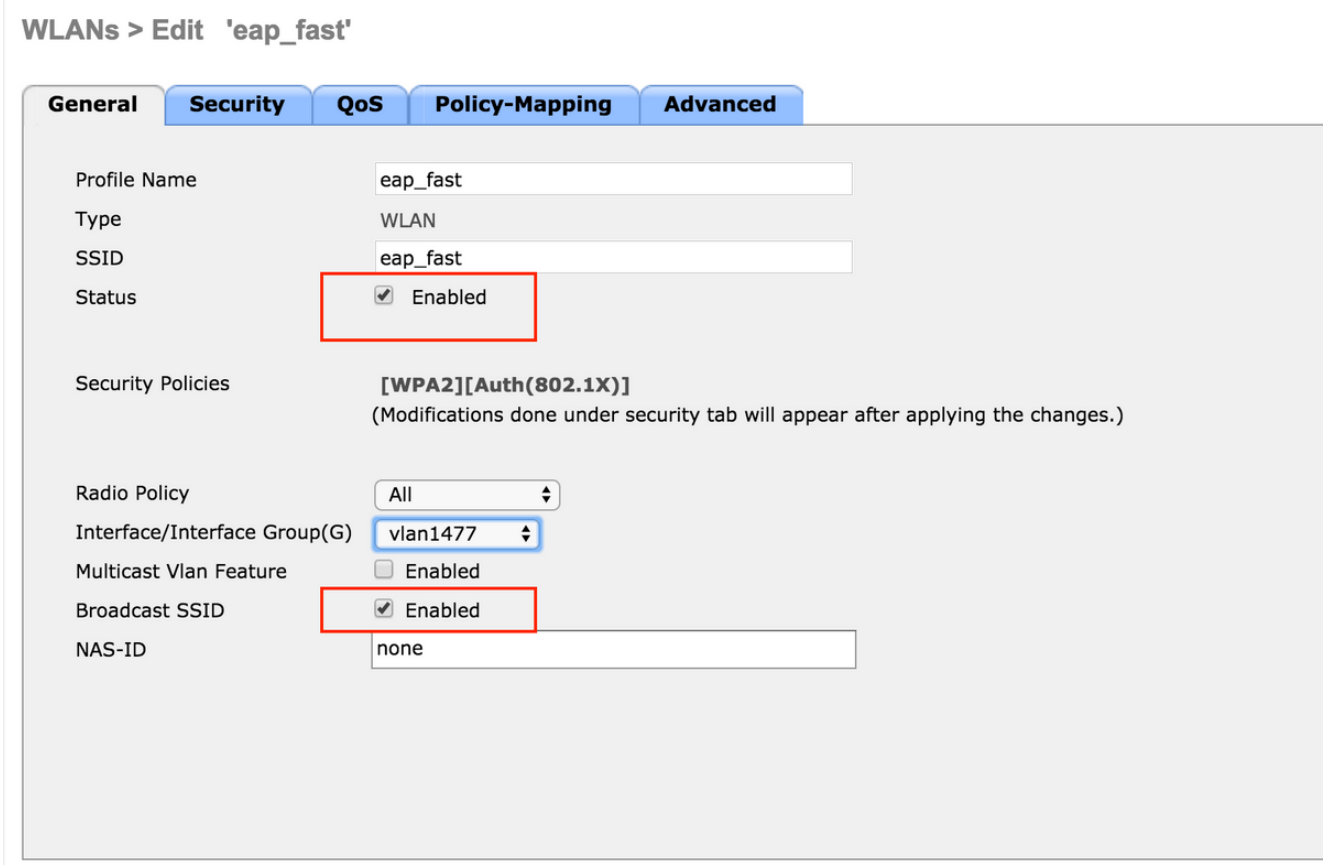
1. Clique em **WLANs** na GUI do controlador para exibir a página WLANs.Esta página lista as WLANs que existem na controladora.
2. Clique em **New** para criar uma nova WLAN.



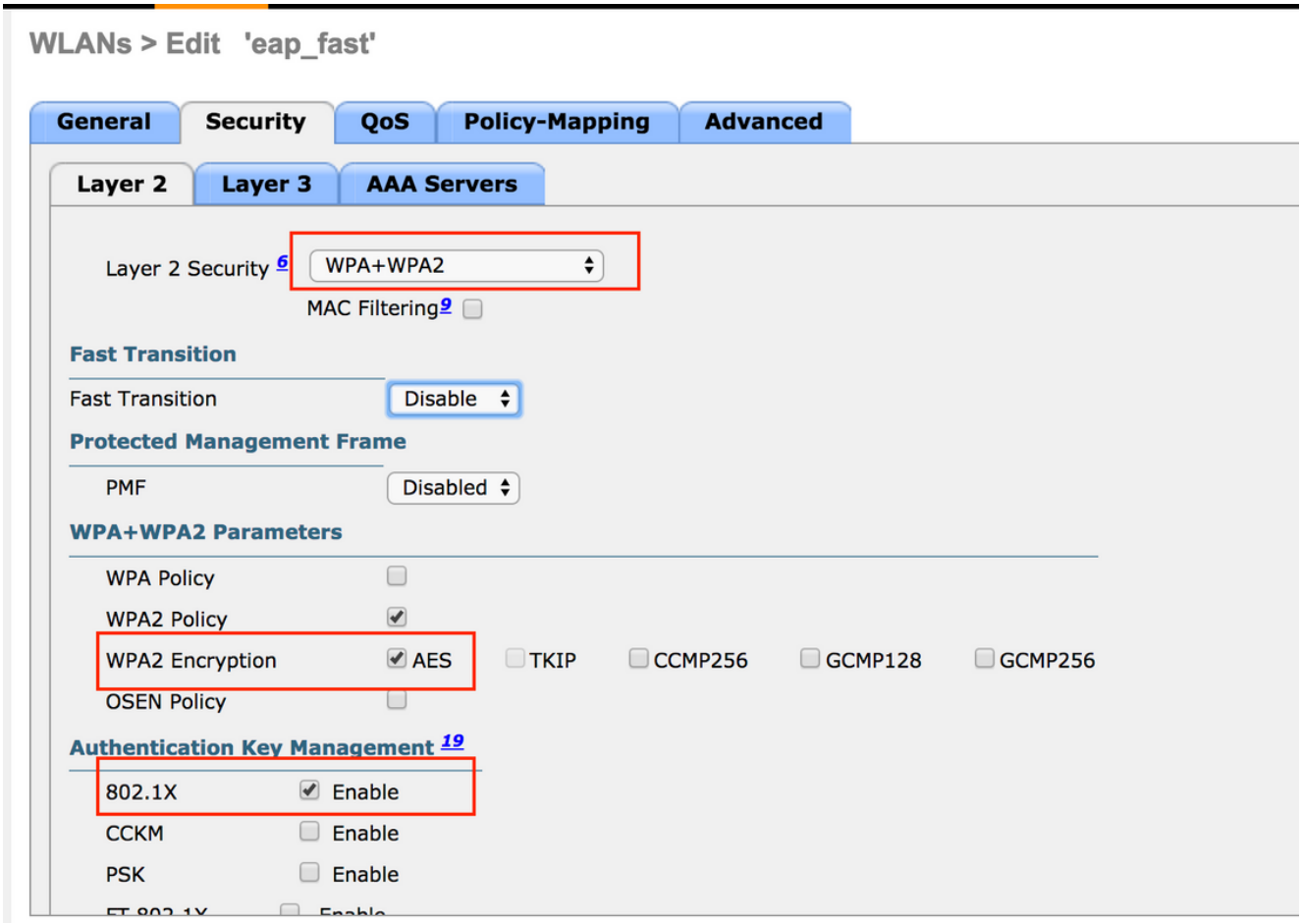
3. Configure o nome SSID da WLAN **eap_fast**, o nome do perfil e a ID da WLAN na página WLANs > Nova. Em seguida, clique em **Aplicar**.



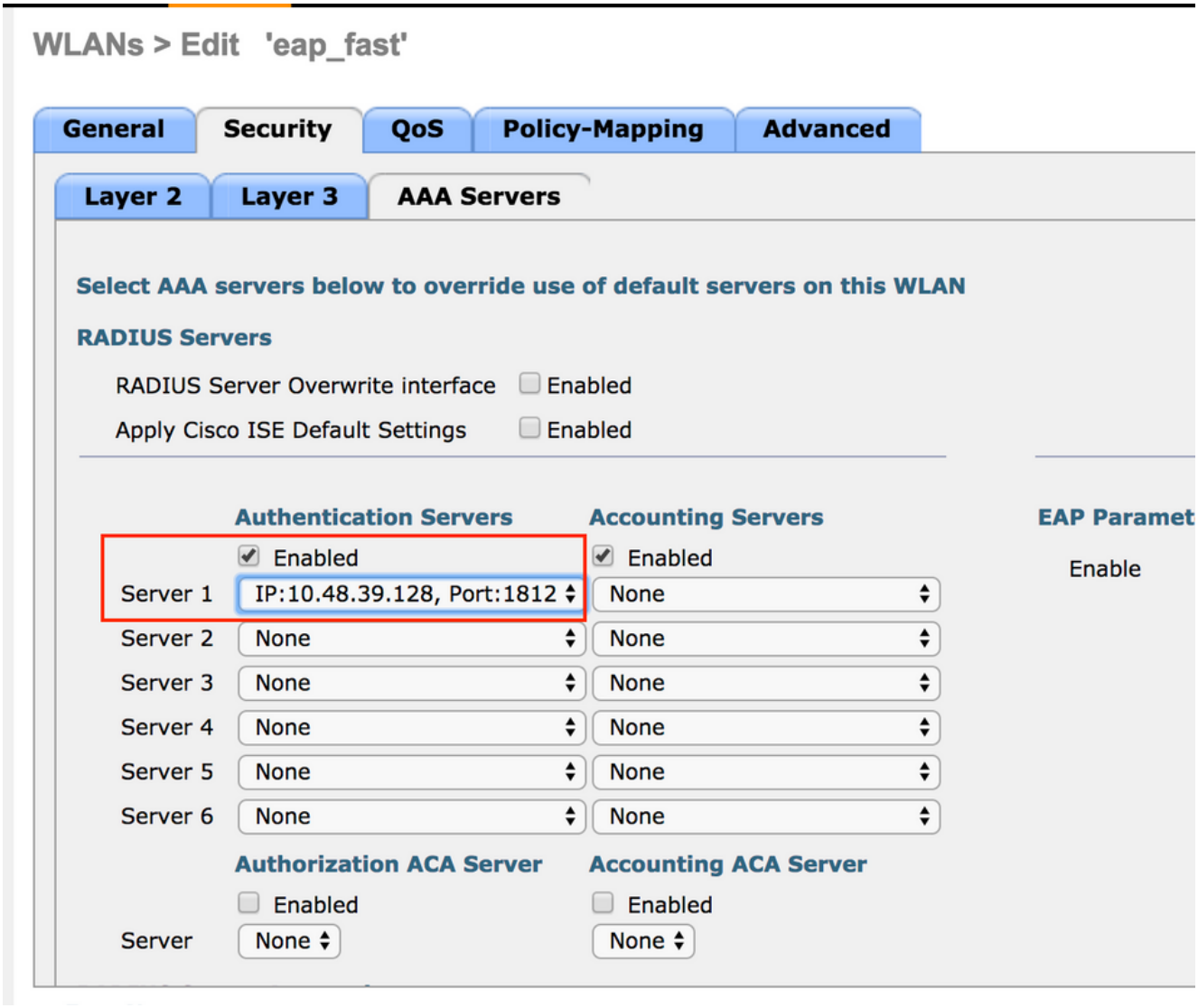
4. Depois de criar uma nova WLAN, a página **WLAN > Edit** para a nova WLAN é exibida. Nesta página, você pode definir vários parâmetros específicos para esta WLAN. Isso inclui políticas gerais, servidores RADIUS, políticas de segurança e parâmetros 802.1x.
5. Marque a caixa de seleção **Admin Status** na guia **General Policies** para habilitar a WLAN. Se você quiser que o AP transmita o SSID em seus quadros de beacon, marque a caixa de seleção **Transmitir SSID**.



6. Sob **"WLAN -> Editar -> Segurança -> Camada 2"** escolha os parâmetros WPA/WPA2 e selecione dot1x para AKM.
   Este exemplo usa WPA2/AES + dot1x como segurança da camada 2 para esta WLAN. Os outros parâmetros podem ser modificados com base no requisito da rede WLAN.



7. Na guia "**WLAN -> Edit -> Security -> AAA Servers**", escolha o servidor RADIUS apropriado no menu suspenso em RADIUS Servers.



8. Clique em Apply.**Observação:** esta é a única configuração de EAP que precisa ser configurada no controlador para autenticação de EAP. Todas as outras configurações específicas do EAP-FAST precisam ser feitas no servidor RADIUS e nos clientes que precisam ser autenticados.

Configurar o servidor RADIUS para autenticação EAP-FAST

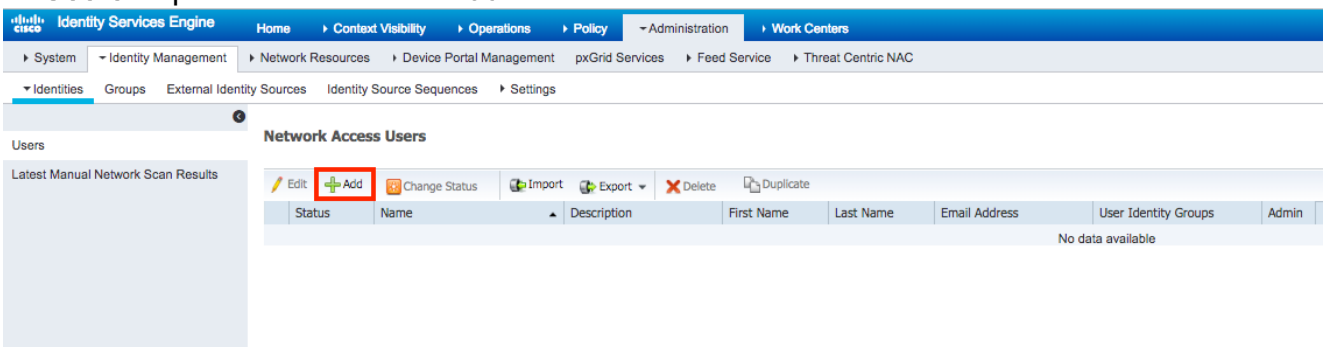
Execute estas etapas para configurar o servidor RADIUS para autenticação EAP-FAST:

1. Criar um banco de dados de usuário para autenticar clientes EAP-FAST
2. Adicione a WLC como cliente AAA ao servidor RADIUS
3. Configurar a autenticação EAP-FAST no servidor RADIUS com provisionamento PAC em banda anônima
4. Configurar a autenticação EAP-FAST no servidor RADIUS com o provisionamento PAC em banda autenticado

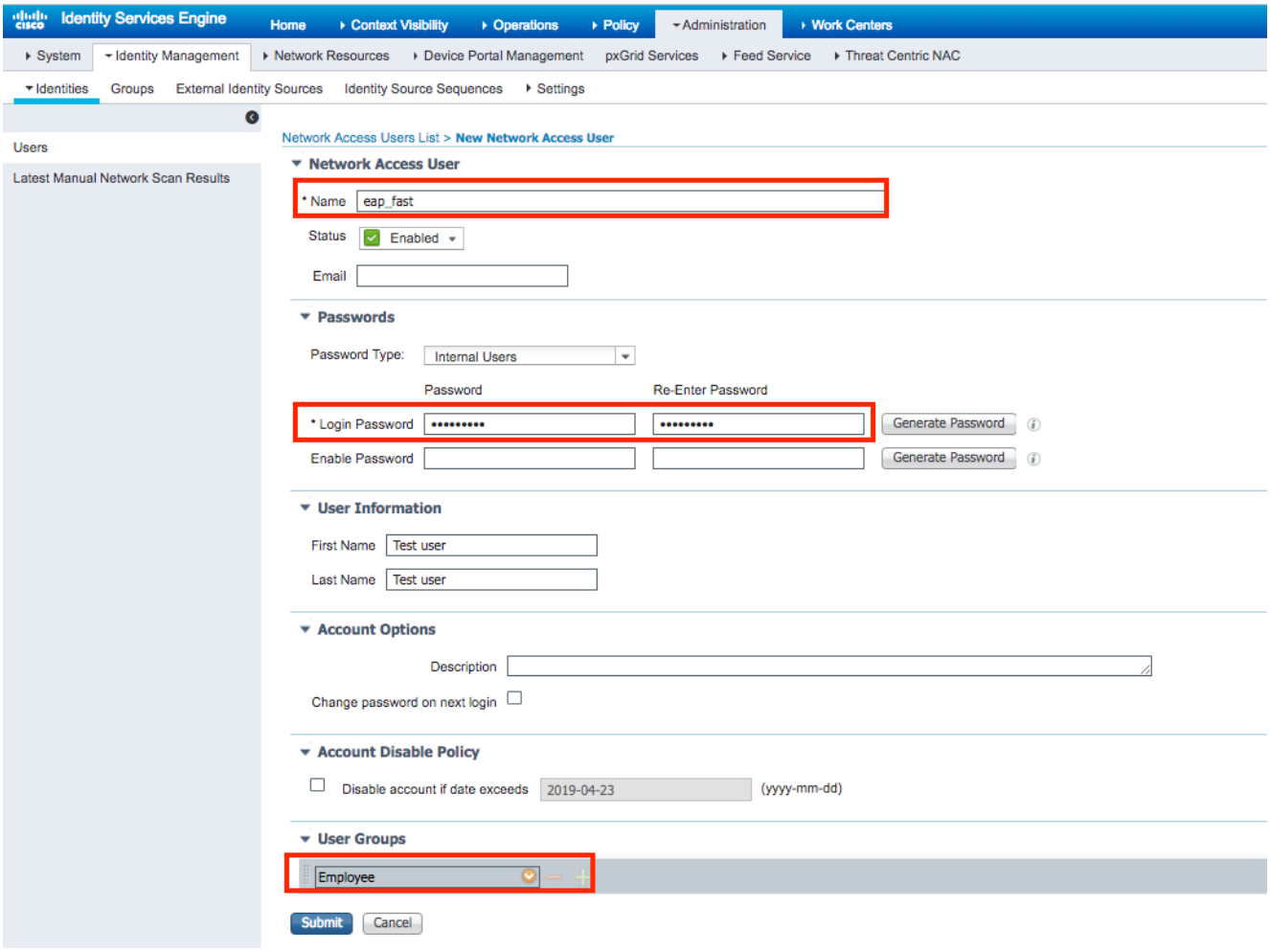
Criar um banco de dados de usuário para autenticar clientes EAP-FAST

Este exemplo configura o nome de usuário e a senha do cliente EAP-FAST como <*eap_fast*> e <*EAP-fast1*>, respectivamente.

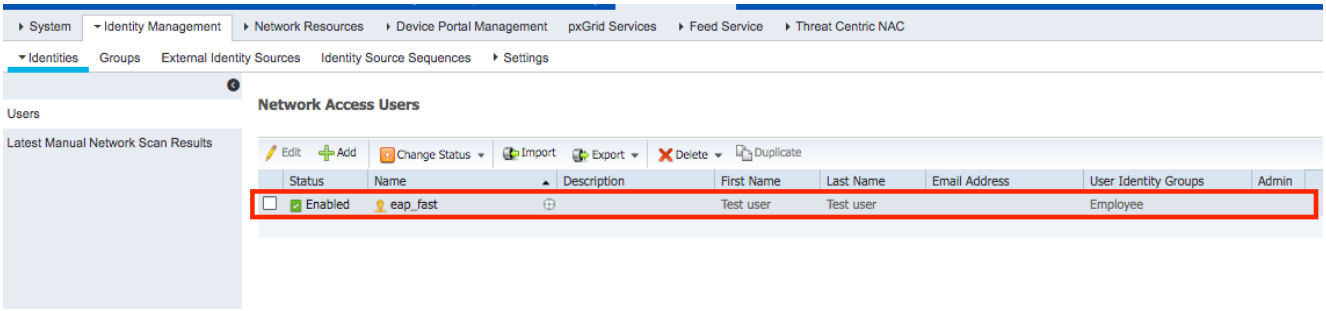
1. Na IU do administrador da Web do ISE, navegue em **"Administration -> Identity Management -> Users"** e pressione o ícone **"Add"**.



2. Preencha os formulários necessários para que o usuário seja criado - **"Nome"** e **"Senha de login"** e selecione **"Grupo de usuários"** na lista suspensa;[opcionalmente, você pode preencher outras informações para a conta de usuário]
Prima **"Sumbit"**



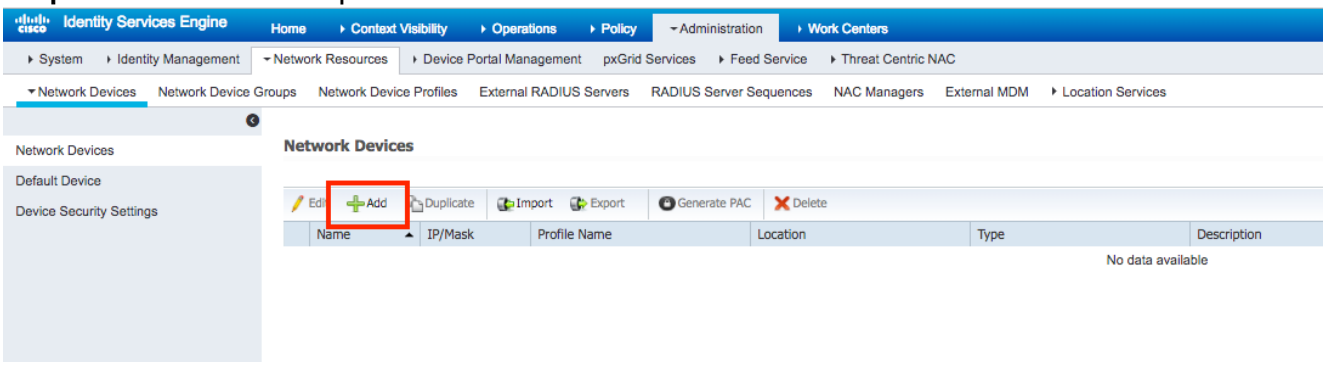
3. O usuário é criado.



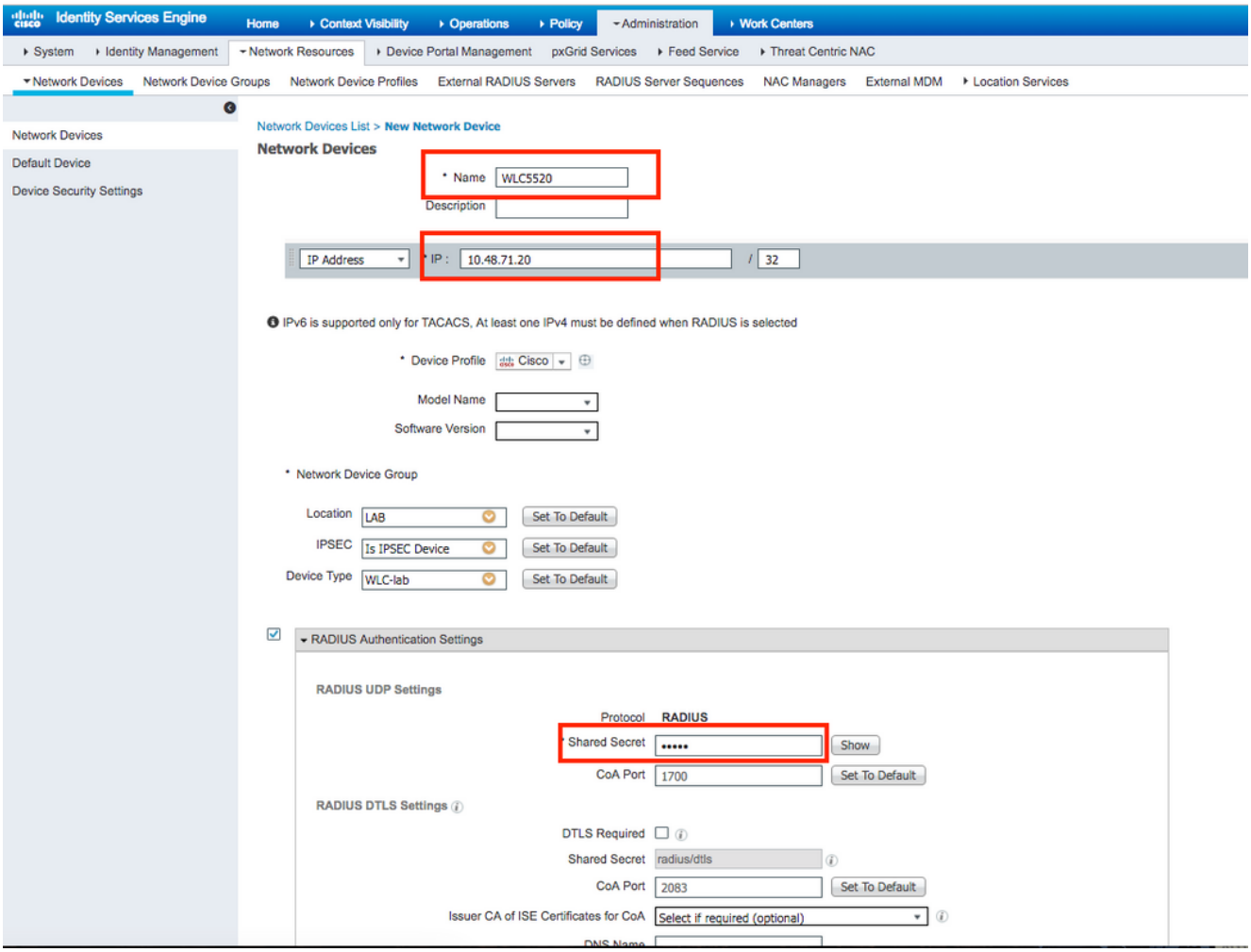
Adicione a WLC como cliente AAA ao servidor RADIUS

Conclua estes passos para definir o controlador como um cliente AAA no servidor ACS:

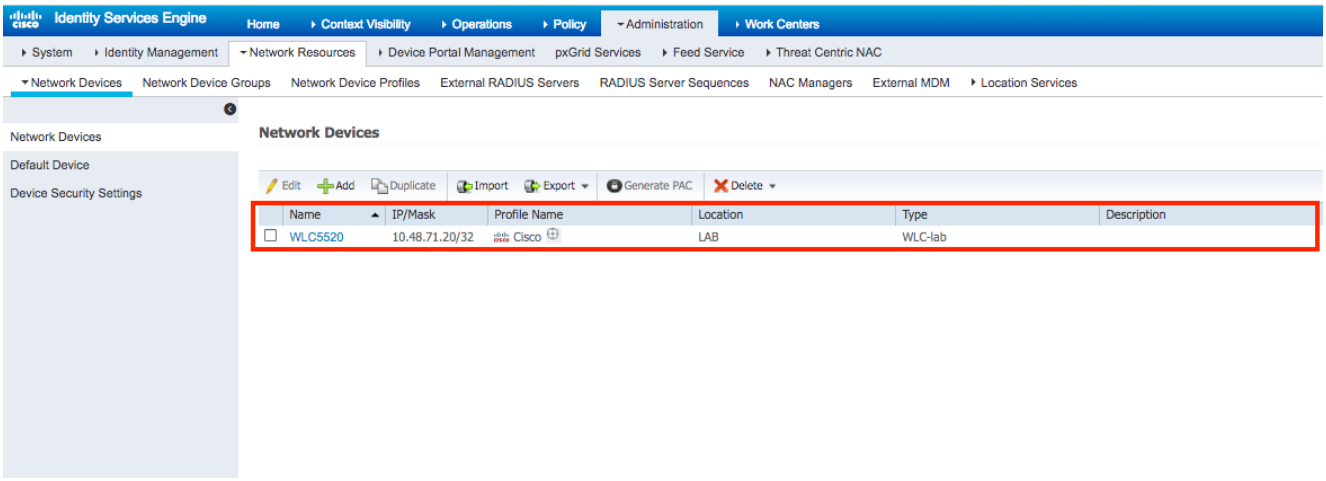
1. Na IU do administrador da Web do ISE, navegue em **"Administração -> Recursos de rede -> Dispositivos de rede"** e pressione o ícone **"Adicionar"**.



2. Preencha os formulários necessários para que o dispositivo seja adicionado - **"Nome"**, **"IP"** e configure a mesma senha secreta compartilhada, como configuramos na WLC na seção anterior, no formulário **"Segredo compartilhado"** [opcionalmente, você pode preencher outras informações para o dispositivo, como localização, grupo, etc].
Prima **"Sumbit"**



3. O dispositivo é adicionado à lista de dispositivos de acesso à rede ISE. (NAD)

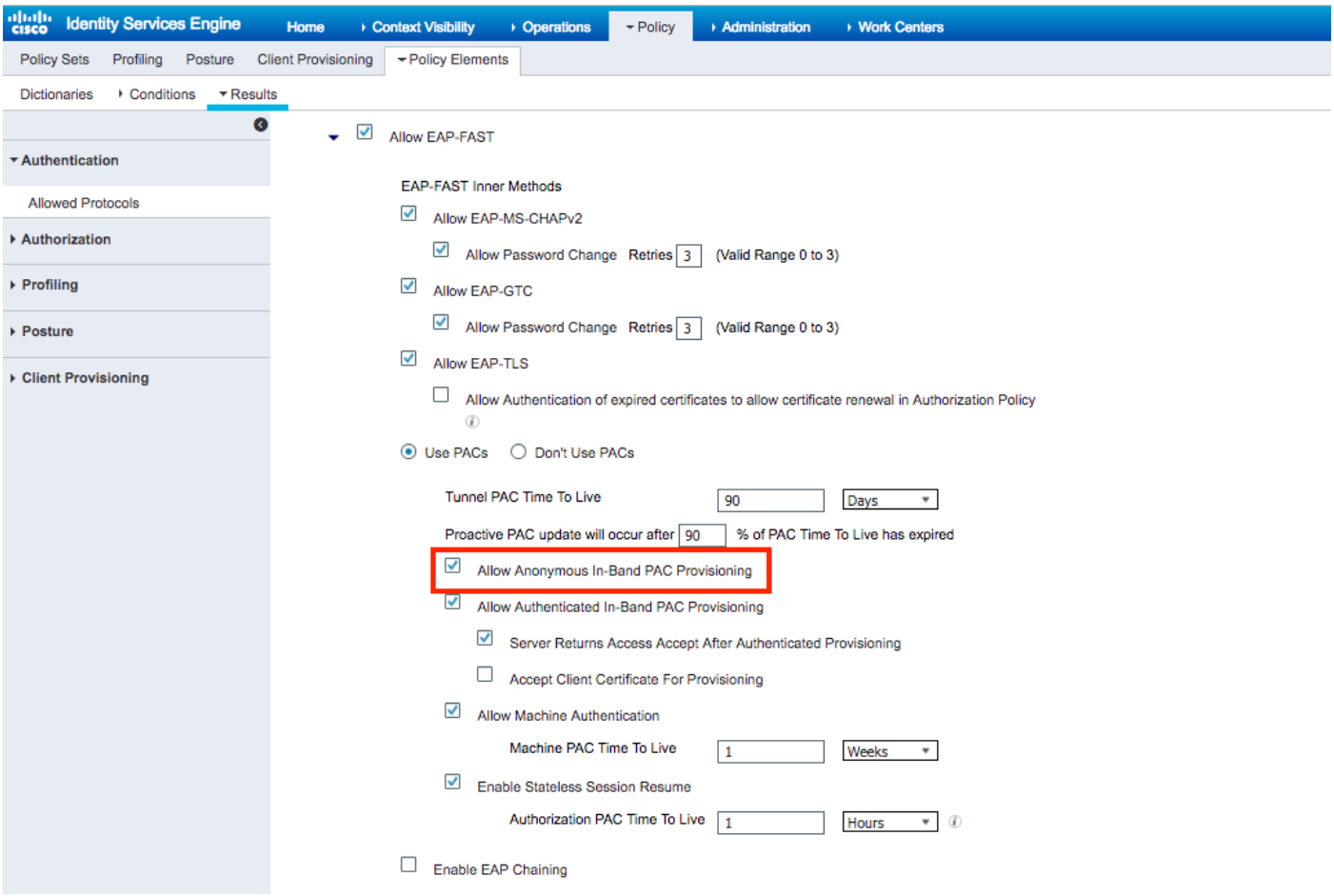


Configurar a autenticação EAP-FAST no servidor RADIUS com provisionamento PAC em banda anônima

Em geral, gostaríamos de usar esse tipo de método caso eles não tenham infraestrutura de PKI em sua implantação.

Esse método opera dentro de um túnel Authenticated Diffie-HellmanKey Agreement Protocol (ADHP) antes que o peer autentique o servidor ISE.

Para suportar este método, precisamos habilitar **""Allow Anonymous In-band PAC Provisioning"** no ISE sob **"Authentication Allowed Protocols"**:



Observação: certifique-se de que você tenha permitido a autenticação de tipo de senha, como EAP-MS-CHAPv2 para o método interno EAP-FAST, já que obviamente com o provisionamento

em banda anônima não podemos usar nenhum certificado.

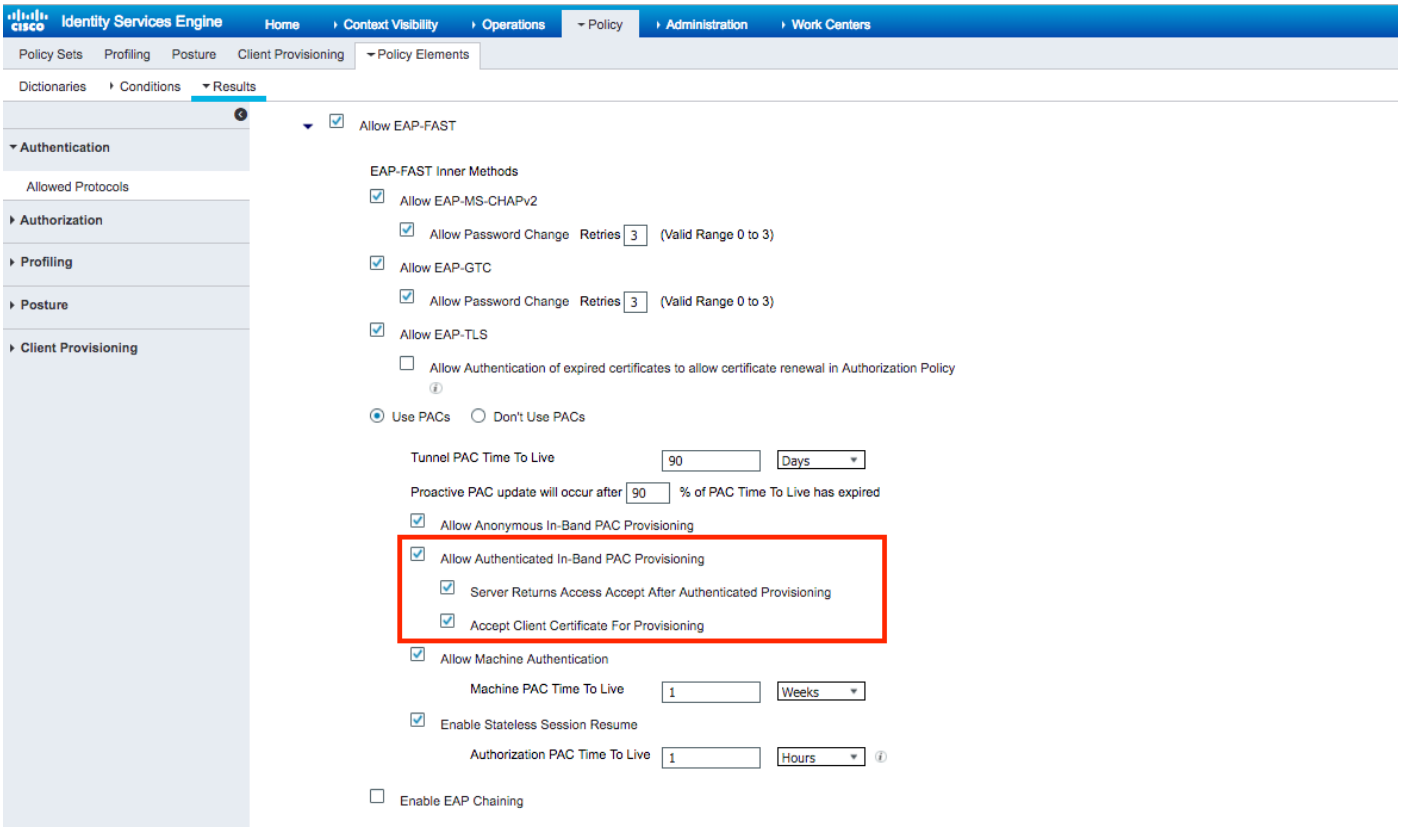
Configurar a autenticação EAP-FAST no servidor RADIUS com o provisionamento PAC em banda autenticado

Essa é a opção mais segura e recomendada. O túnel TLS é construído com base no certificado do servidor que é validado pelo requerente e o certificado do cliente é validado pelo ISE (padrão).

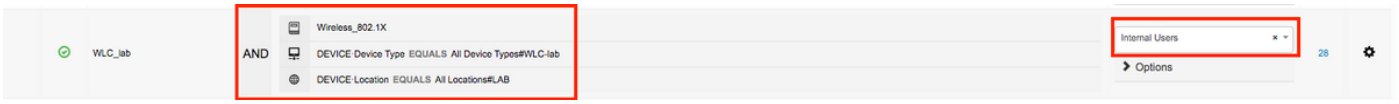
Essa opção exige uma infraestrutura de PKI para cliente e servidor, embora possa ser limitada apenas ao lado do servidor ou ignorada em ambos os lados.

No ISE, há duas opções adicionais para o provisionamento Autenticado em banda:

1. **"Server Devolve Access Accept After Authenticated Provisioning"** - Normalmente, após o provisionamento PAC, um Access-Reject deve ser enviado forçando o requerente a reautenticar usando PACs. No entanto, como o provisionamento de PAC é feito em túnel TLS autenticado, podemos responder imediatamente com Access-Accept para minimizar o tempo de autenticação. (nesse caso, verifique se você tem certificados confiáveis no lado cliente e servidor).
2. **"Aceitar Certificado do Cliente para Provisionamento" - se não se quiser fornecer infraestrutura de PKI para dispositivos do cliente e apenas se tiver um certificado confiável no ISE, ative essa opção, que permite ignorar a validação do certificado do cliente no lado do servidor.**



No ISE, também definimos uma política de autenticação simples para usuários sem fio, abaixo, por exemplo, está usando como parâmetro de condição o tipo de dispositivo e o local e o tipo de autenticação, o fluxo de autenticação correspondente a essa condição será validado no banco de dados de usuário interno.



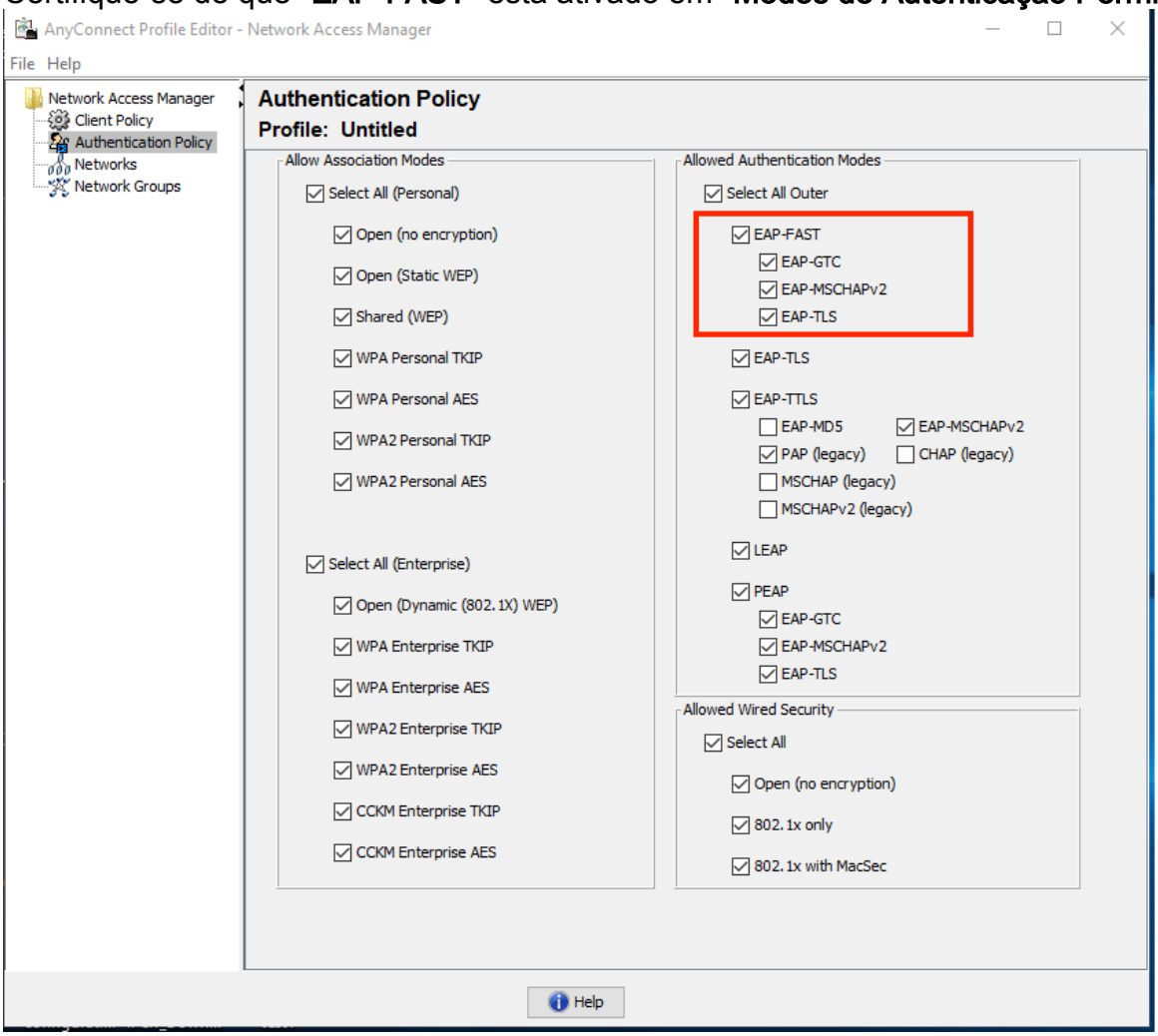
Verificar

Este exemplo mostrará as configurações de fluxo de Provisionamento de PAC Autenticado em Banda e de NAM (Network Access Manager) juntamente com as respectivas depurações de WLC.

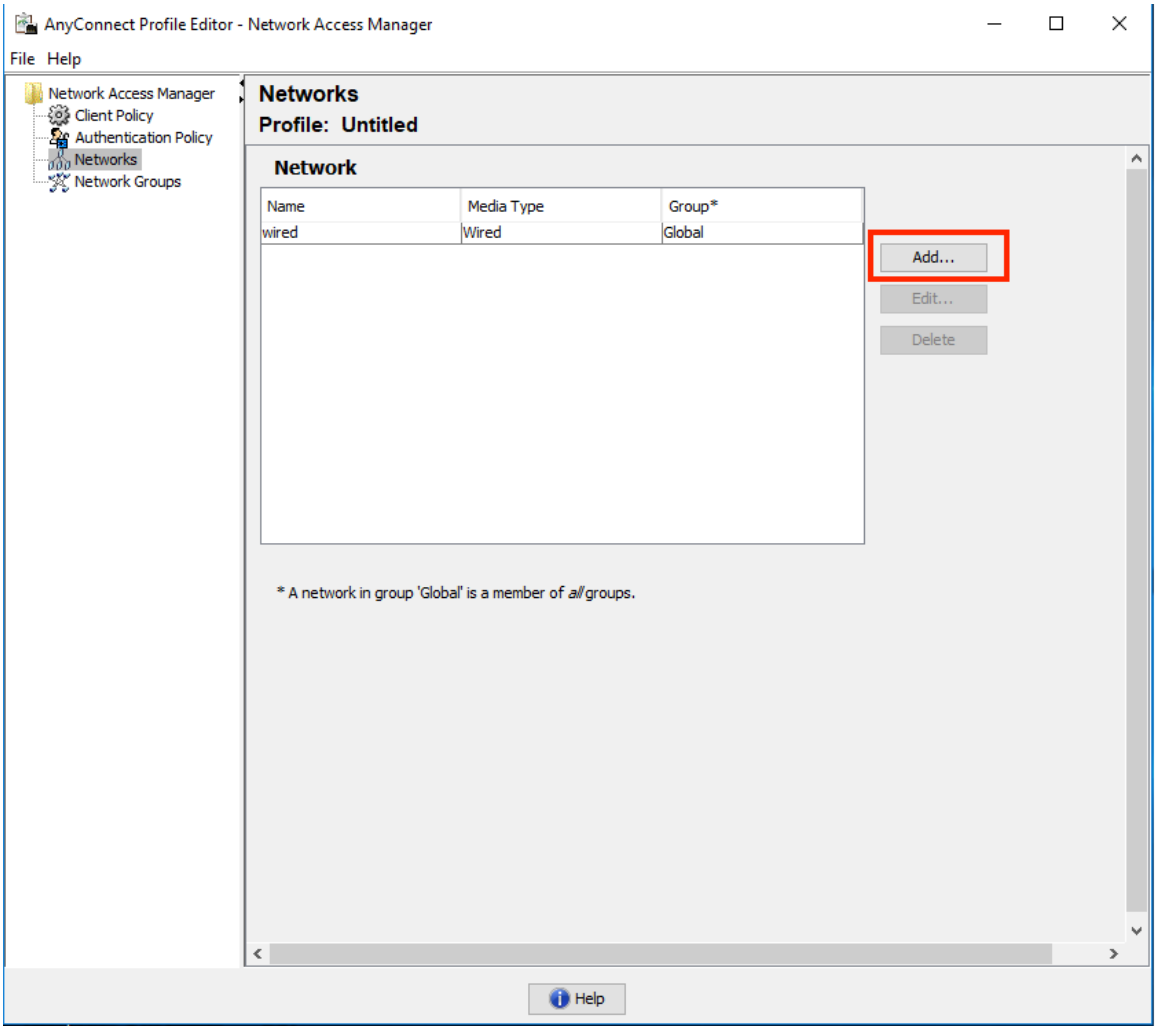
configuração de perfil NAM

As etapas a seguir precisam ser feitas para configurar o perfil do AnyConnect NAM para autenticar a sessão do usuário em relação ao ISE usando EAP-FAST:

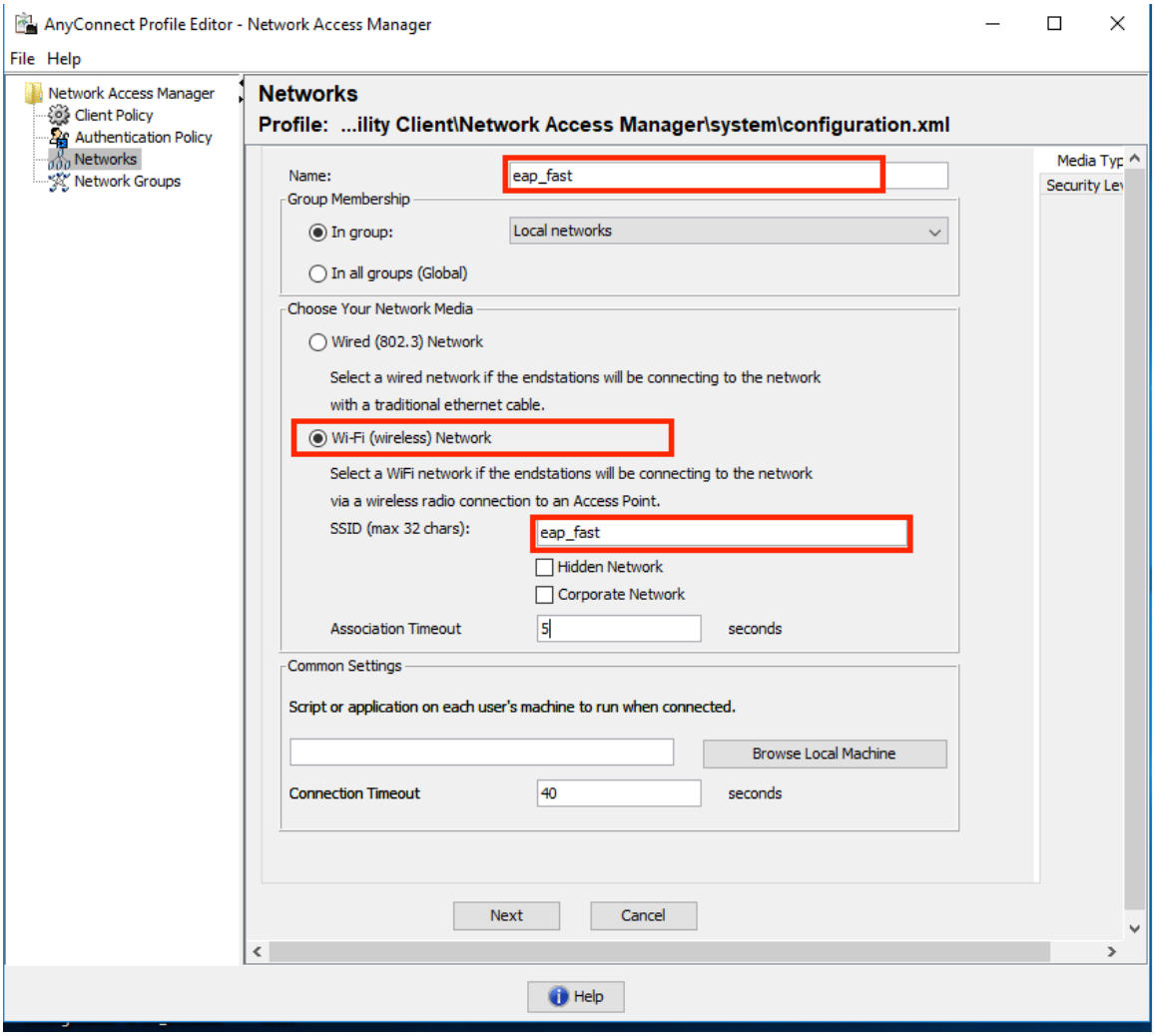
1. Abra o Editor de perfis do Network Access Manager e carregue o arquivo de configuração atual.
2. Certifique-se de que "**EAP-FAST**" está ativado em **"Modos de Autenticação Permitidos"**



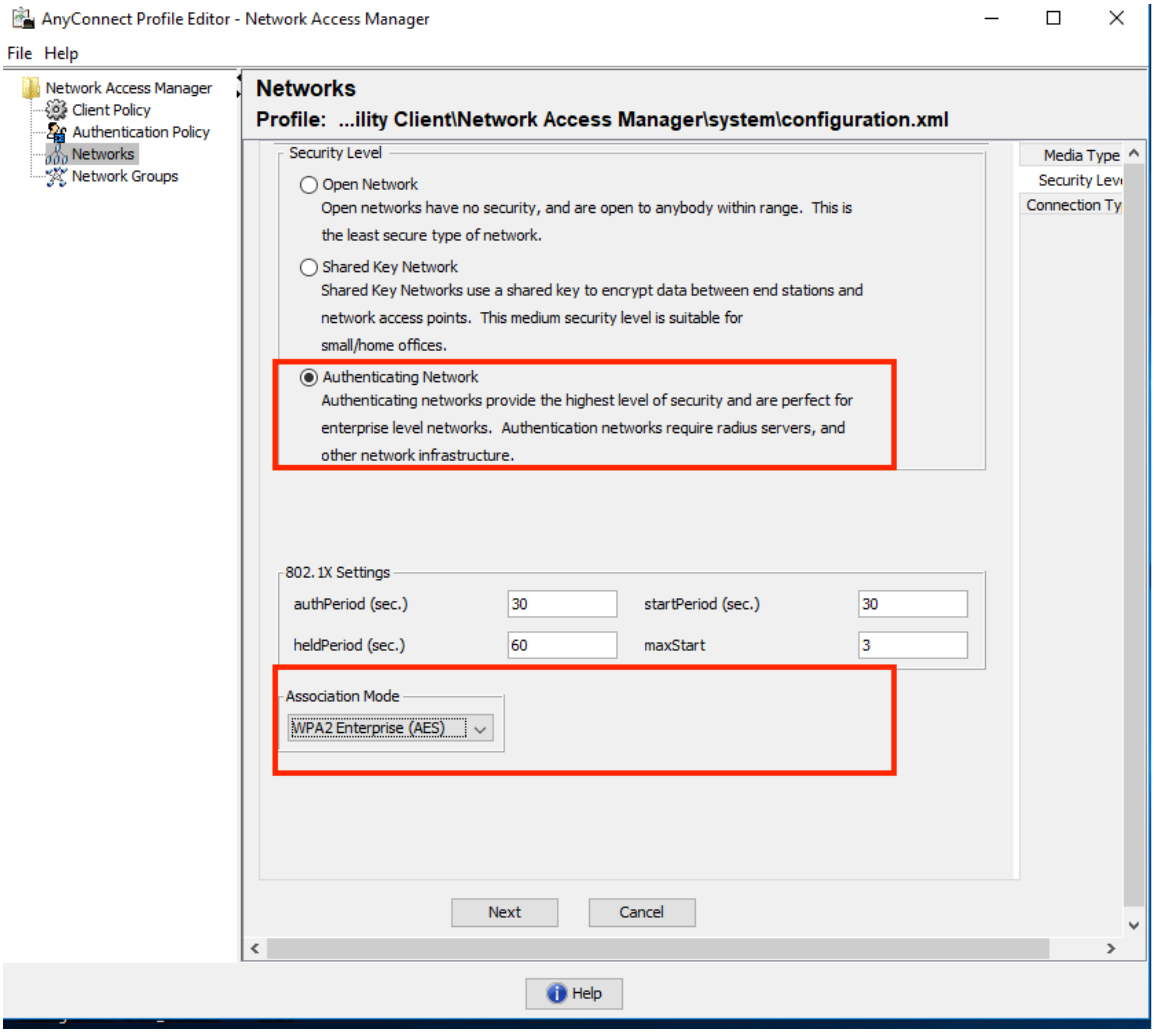
3. **"Adicionar"** um novo perfil de rede:



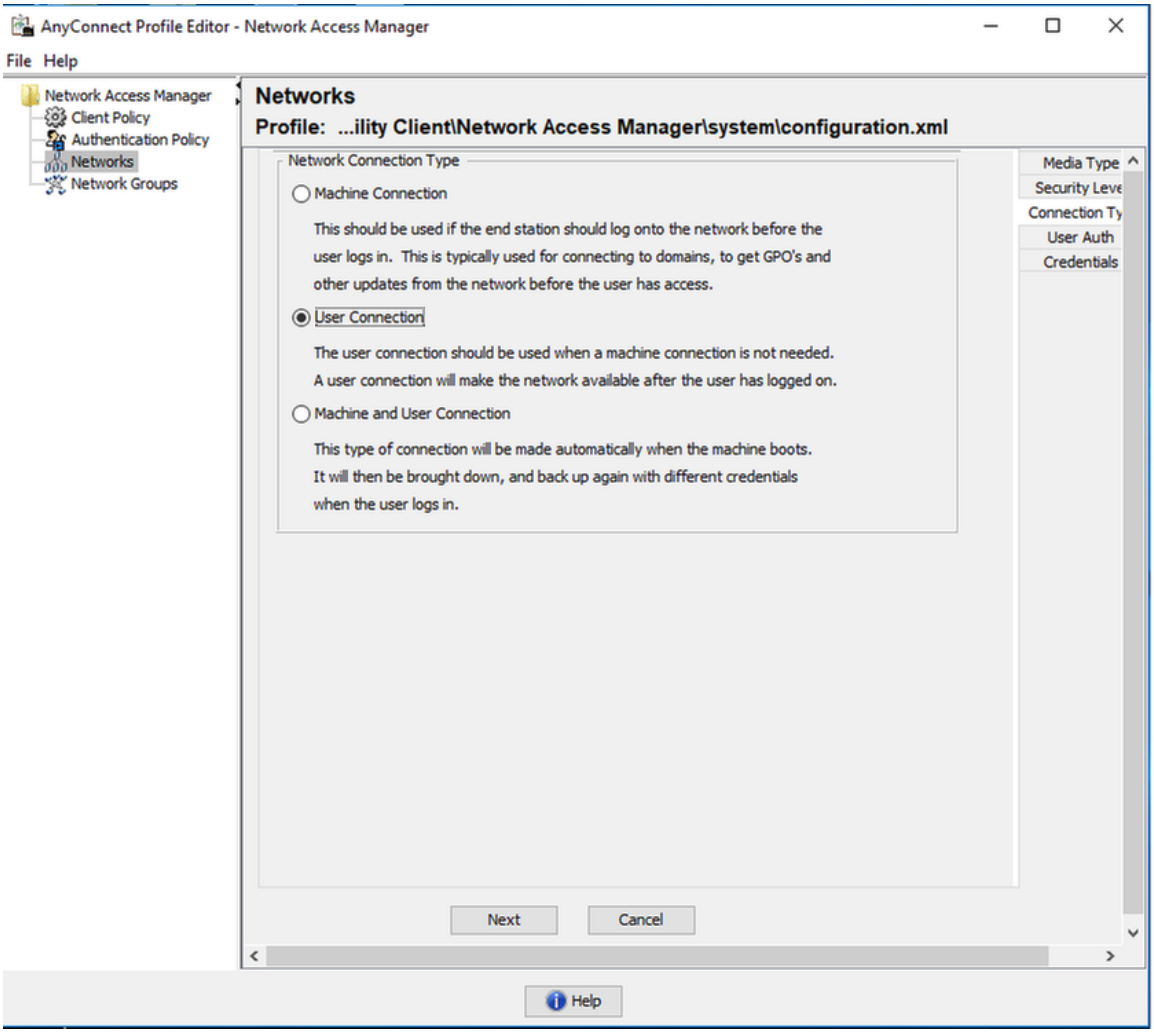
4. Na seção de configuração **"Tipo de mídia", defina o perfil "Nome"**, sem fio como o tipo de rede de mídia e especifique o nome SSID.



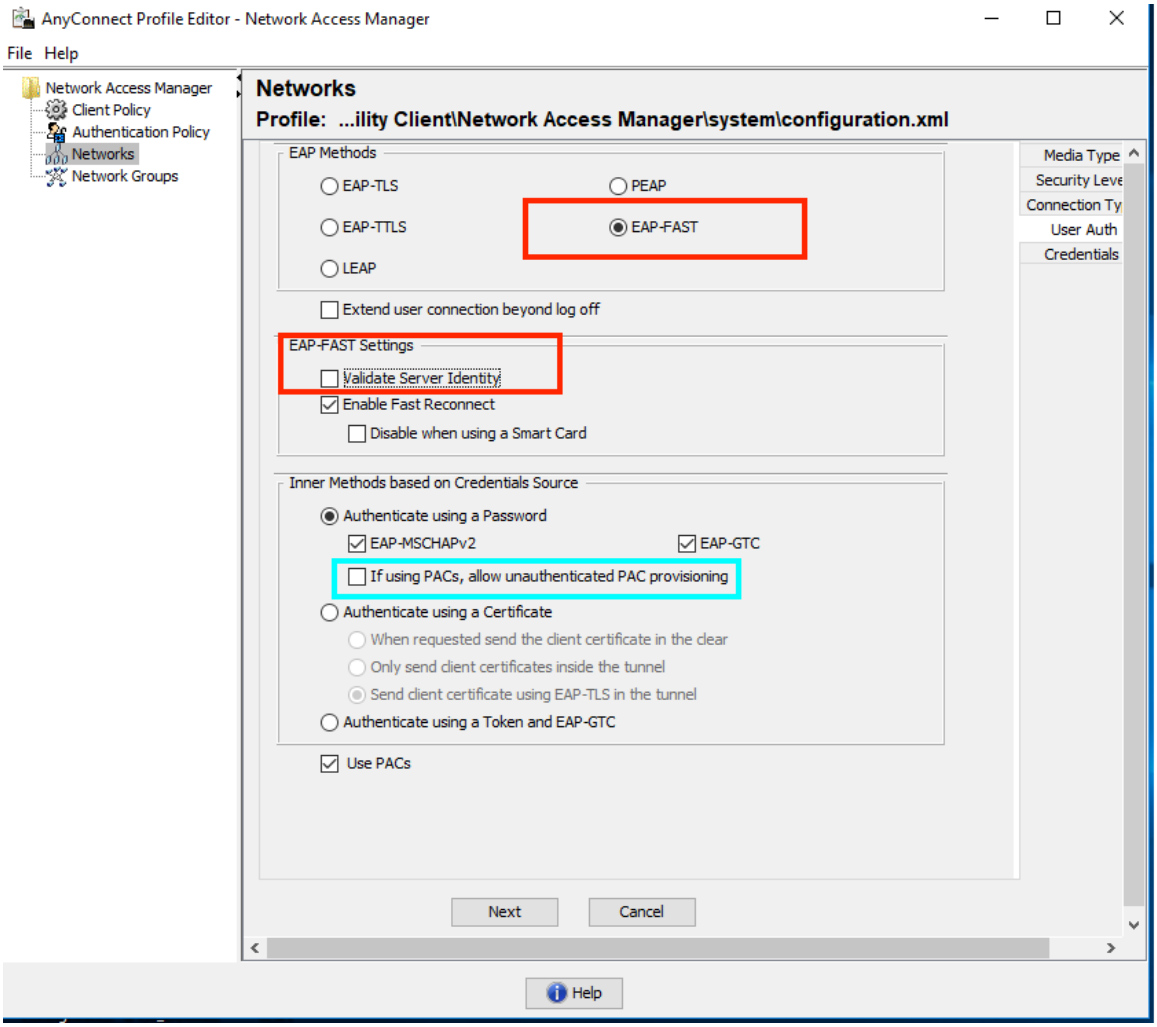
5. Na guia de configuração "**Nível de segurança**" selecione "Autenticando rede" e especifique o modo de associação como WPA2 Enterprise (AES)



6. Neste exemplo, estamos usando a autenticação de tipo de usuário, portanto, na próxima guia "**Tipo de conexão**", selecione "**Conexão do usuário**"

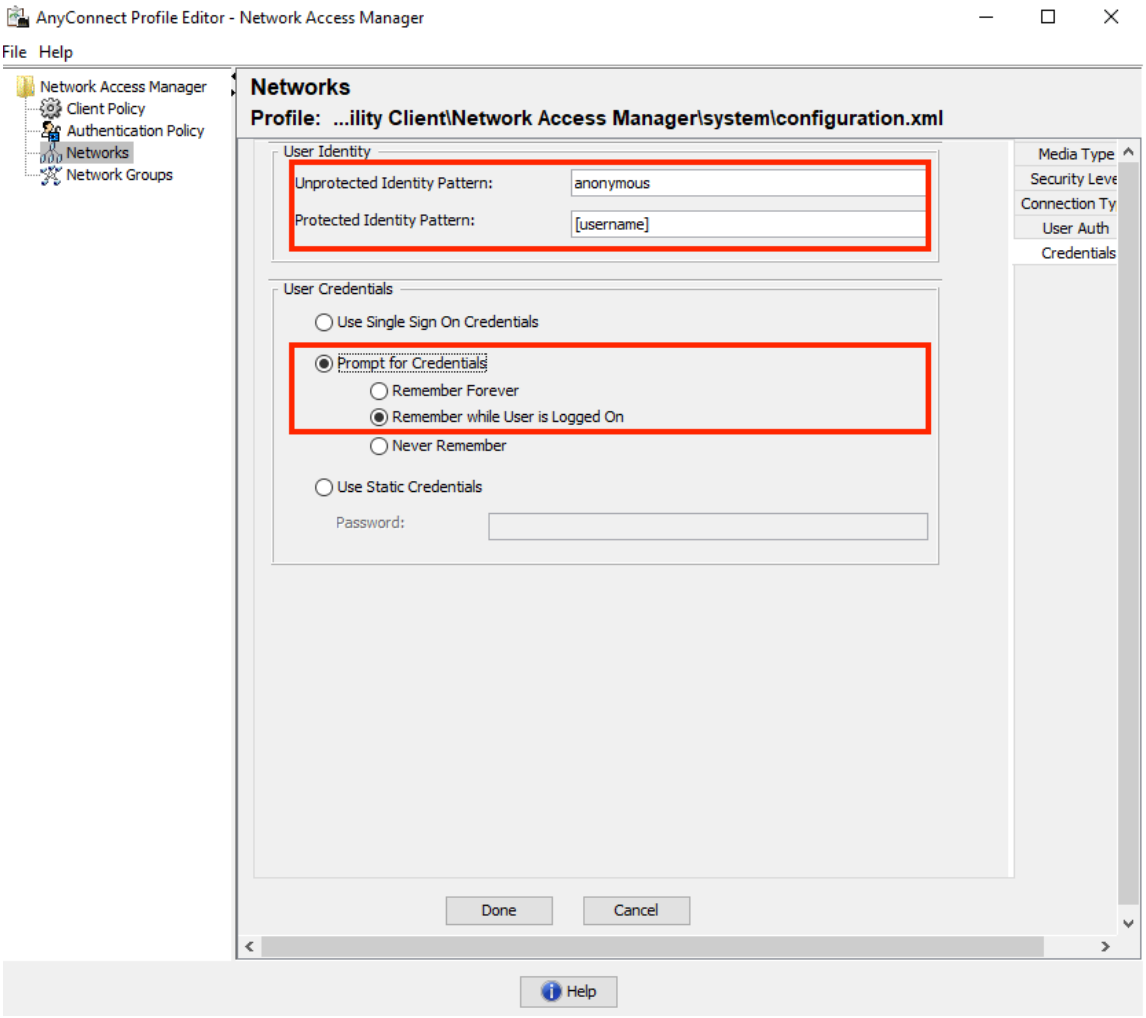


7. Na guia "**User Auth**", especifique EAP-FAST como método de autenticação permitido e desative a validação do certificado do servidor, já que não estamos usando certificados confiáveis neste exemplo.



Nota: no ambiente de produção real, certifique-se de que tem um certificado fidedigno instalado no ISE e mantenha a opção de validação do certificado do servidor ativada nas definições do NAM.
Note: a opção "Se estiver usando PACs, permitir provisionamento de PAC não autenticado" deve ser selecionada somente no caso do provisionamento de PAC em banda anônima.

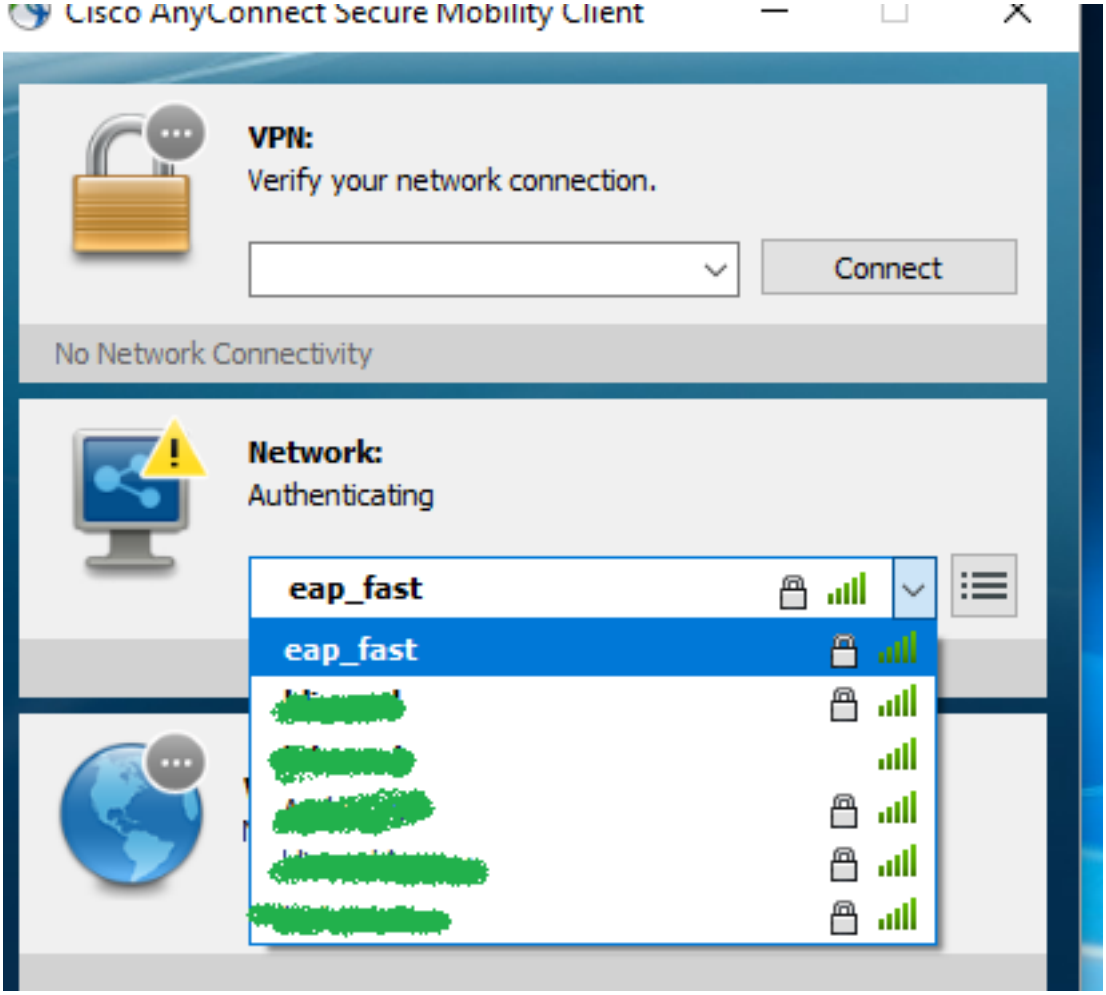
8. Defina as credenciais do usuário, como SSO, caso deseje usar as mesmas credenciais usadas para login, ou selecione "Solicitar credenciais", caso queira que o usuário seja solicitado a fornecer credenciais durante a conexão com a rede, ou defina credenciais estáticas para esse tipo de acesso. Neste exemplo, solicitamos credenciais ao usuário na tentativa de conexão à rede.



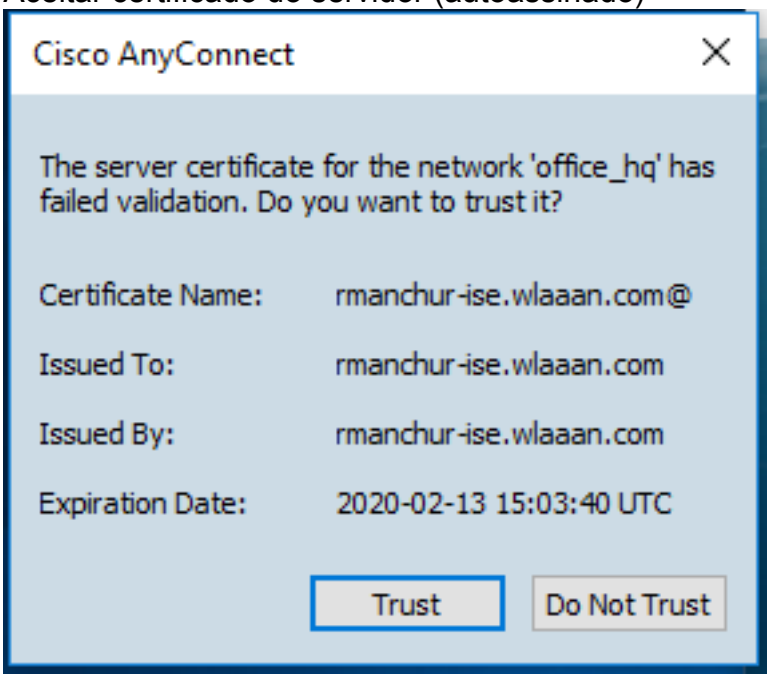
9. Salve o perfil configurado na respectiva pasta NAM.

Teste a conectividade com o SSID usando a autenticação EAP-FAST.

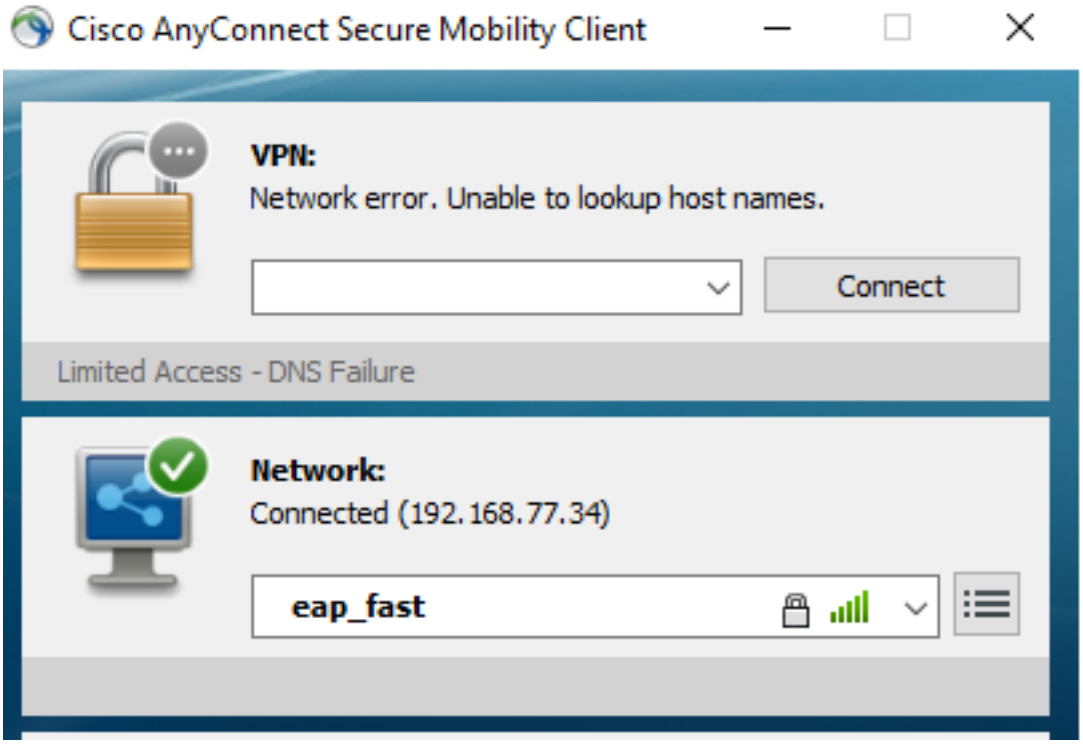
1. Selecione o perfil respectivo na lista de redes do Anyconnect



2. Insira o nome de usuário e a senha necessários para a autenticação
3. Aceitar certificado do servidor (autoassinado)



4. done



Logs de autenticação do ISE

Os registros de autenticação do ISE que mostram o fluxo de provisionamento EAP-FAST e PAC podem ser vistos em "**Operations -> RADIUS -> Live Logs**" e podem ser consultados em mais detalhes usando o ícone **"Zoom"**:

1. O cliente iniciou a autenticação e o ISE estava propondo EAP-TLS como método de autenticação, mas o cliente rejeitou e propôs o EAP-FAST, que foi o método acordado entre o cliente e o ISE.

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. O handshake TLS foi iniciado entre o cliente e o servidor para fornecer um ambiente protegido para troca de PAC e foi concluído com êxito.

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. A autenticação interna foi iniciada e as credenciais de usuário foram validadas com êxito pelo ISE usando MS-CHAPv2 (autenticação baseada em nome de usuário/senha)