Configurar PEAP e EAP-FAST com ACS 5.2 e WLC

Contents

Introduction

Este documento explica como configurar o Controller de LAN Wireless (WLC) da autenticação Extensible Authentication Protocol (EAP) com o uso de um servidor RADIUS externo, como o Access Control Server (ACS) 5,2.

Prerequisites

Requirements

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

- Ter um conhecimento básico da WLC e dos Lightweight Access Points (LAPs)
- Ter conhecimento funcional do servidor AAA
- Ter um conhecimento profundo das redes sem fio e dos problemas de segurança sem fio

Componentes Utilizados

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

- WLC Cisco 5508 com firmware versão 7.0.220.0
- LAP Cisco 3502 Series
- Solicitante nativo do Microsoft Windows 7 com o driver Intel 6300-N versão 14.3
- Cisco Secure ACS que executa a versão 5.2
- Switch Cisco Série 3560

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.

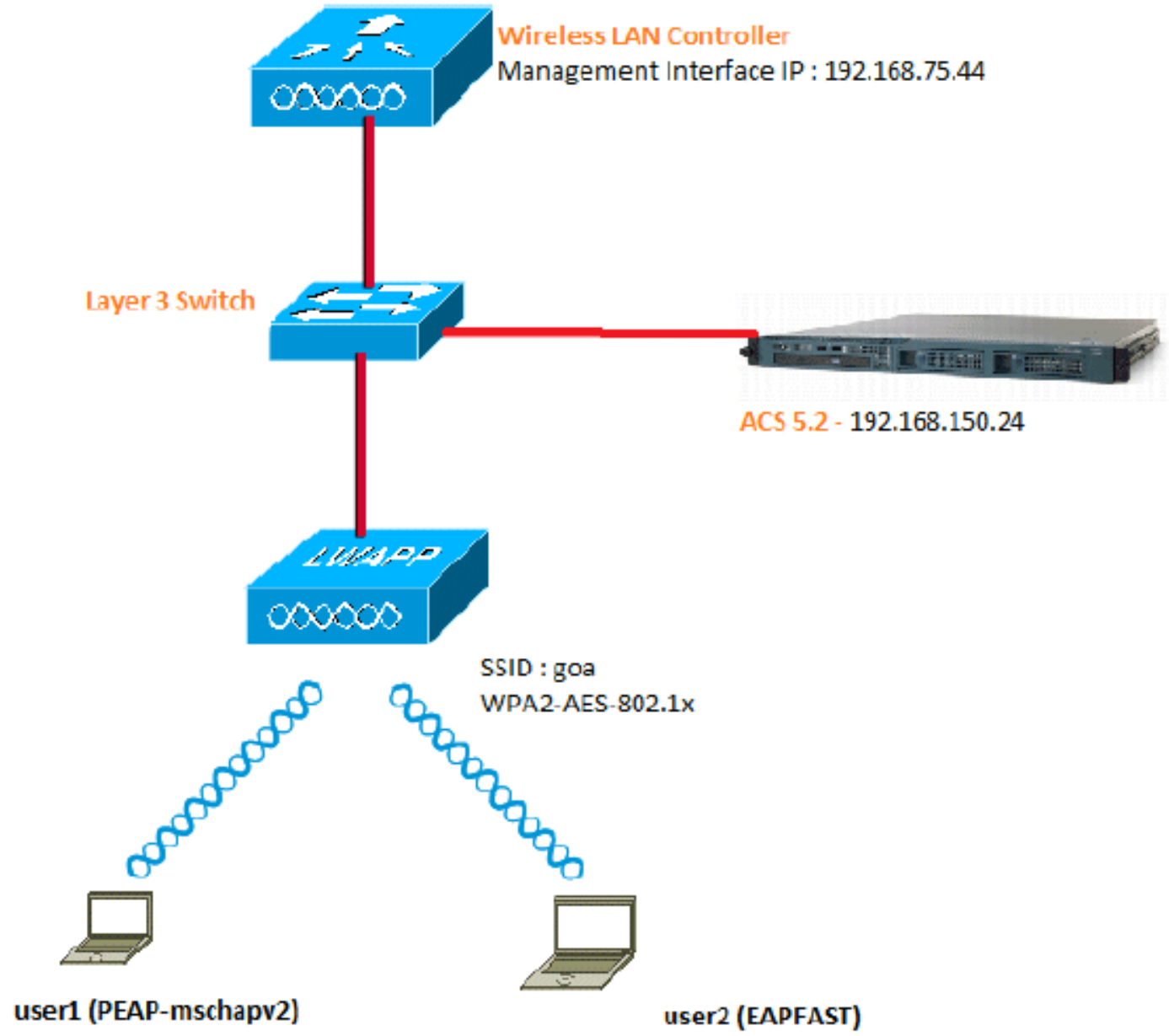
Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Estes são os detalhes de configuração dos componentes usados neste diagrama:

- O endereço IP do servidor ACS (RADIUS) é 192.168.150.24.
- O endereço da interface do gerenciador de AP e gerenciamento do WLC é 192.168.75.44.
- O endereço dos servidores DHCP é 192.168.150.25.
- A VLAN 253 é usada em toda essa configuração. Ambos os usuários se conectam ao mesmo SSID "objetivo". No entanto, o usuário1 está configurado para autenticar usando PEAP-MSCHAPv2 e o usuário2 usando EAP-FAST.
- Os usuários serão atribuídos na VLAN 253:VLAN 253: 192.168.153.x/24. Gateway: 192.168.153.1VLAN 75: 192.168.75.x/24. Gateway: 192.168.75.1

Hipóteses

- Os switches são configurados para todas as VLANs de Camada 3.
- O servidor DHCP recebe um escopo DHCP.
- Existe conectividade de Camada 3 entre todos os dispositivos na rede.
- O LAP já está unido à WLC.
- Cada VLAN tem uma máscara /24.

- O ACS 5.2 tem um certificado autoassinado instalado.

Configuration Steps

Essa configuração é separada em três etapas de alto nível:

1. Configure o servidor RADIUS.
2. Configurar o WLC.
3. Configure o Wireless Client Utility (Utilitário cliente sem fio).

Configurar o servidor RADIUS

A configuração do servidor RADIUS é dividida em quatro etapas:

1. Configurar recursos de rede.
2. Configurar usuários.
3. Definir elementos de política.
4. Aplicar políticas de acesso.

O ACS 5.x é um sistema de controle de acesso baseado em políticas. Ou seja, o ACS 5.x usa um modelo de política baseado em regras em vez do modelo baseado em grupos usado nas versões 4.x.

O modelo de política baseado em regras do ACS 5.x oferece um controle de acesso mais poderoso e flexível em comparação com a abordagem mais antiga baseada em grupos.

No modelo mais antigo baseado em grupos, um grupo define a política porque ela contém e une três tipos de informações:

- Informações de identidade - Essas informações podem ser baseadas na associação em grupos AD ou LDAP ou em uma atribuição estática para usuários ACS internos.
- Outras restrições ou condições - restrições de tempo, restrições de dispositivo e assim por diante.
- Permissões - VLANs ou níveis de privilégio do Cisco IOS®.

O modelo de política do ACS 5.x é baseado em regras do seguinte formato:

- Condição If então resultado

Por exemplo, usamos as informações descritas para o modelo baseado em grupo:

- Se identidade-condição, restrição-condição então autorização-perfil.

Como resultado, isso nos dá a flexibilidade de limitar sob quais condições o usuário tem permissão para acessar a rede, bem como qual nível de autorização é permitido quando condições específicas são atendidas.

Configurar recursos de rede

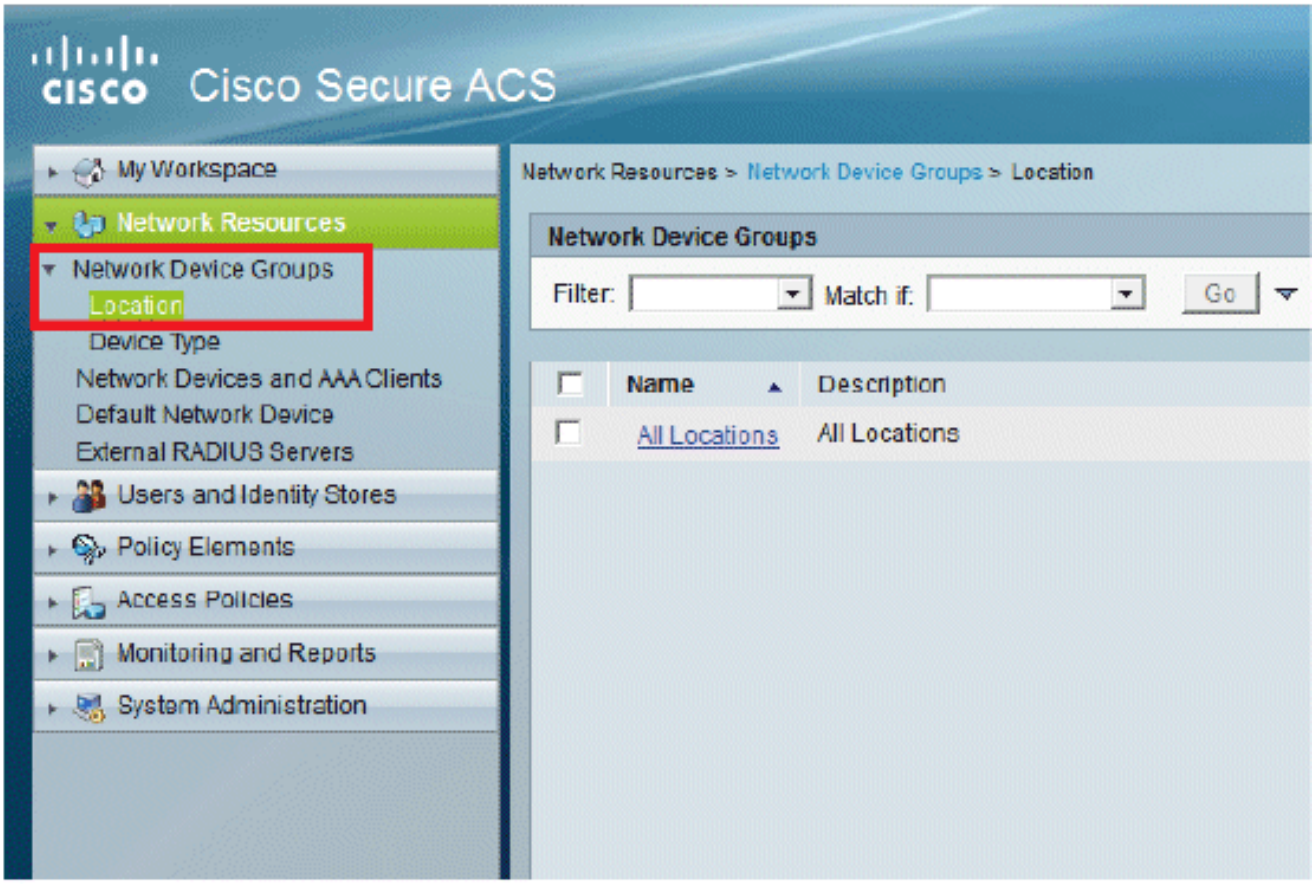
Nesta seção, configuramos o AAA Client para o WLC no servidor RADIUS.

Este procedimento explica como adicionar o WLC como um cliente de AAA no servidor RADIUS

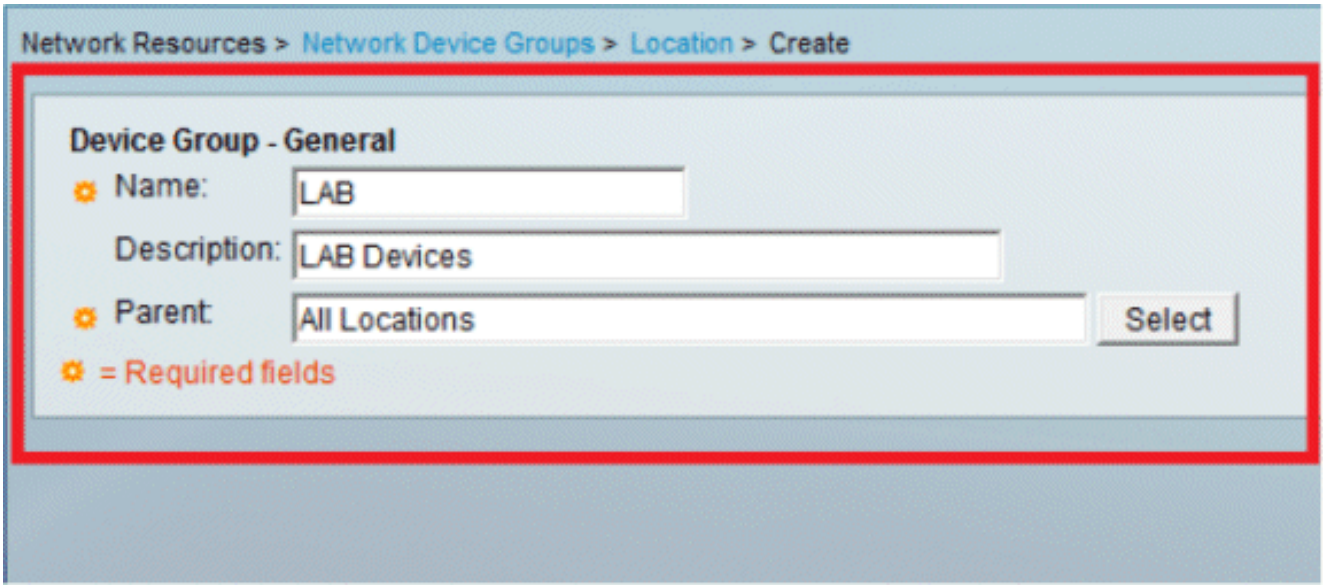
para que o WLC possa passar as credenciais do usuário ao servidor RADIUS.

Conclua estes passos:

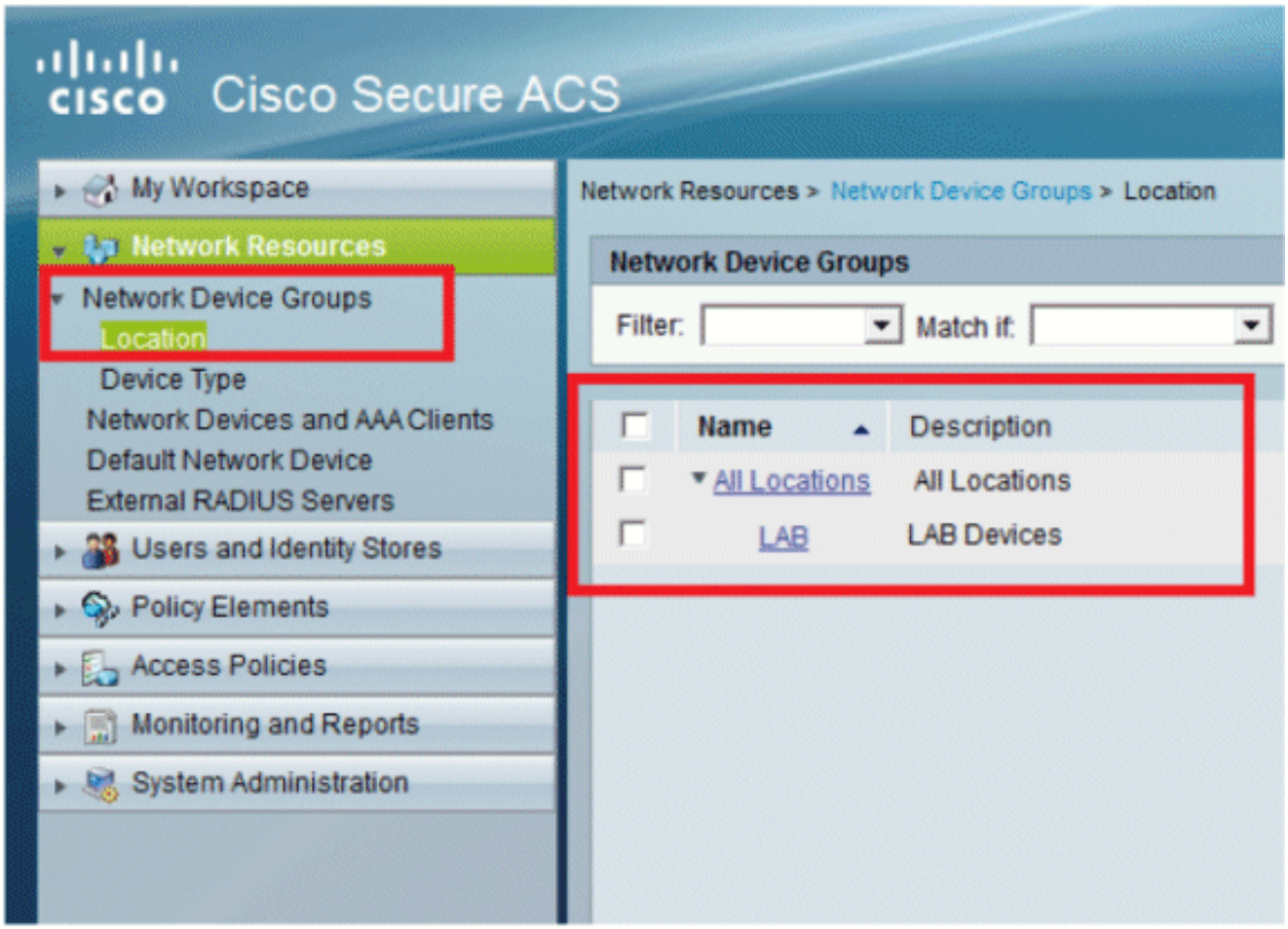
1. Na GUI do ACS, vá para **Network Resources > Network Device Groups > Location** e clique em **Create** (na parte inferior
).



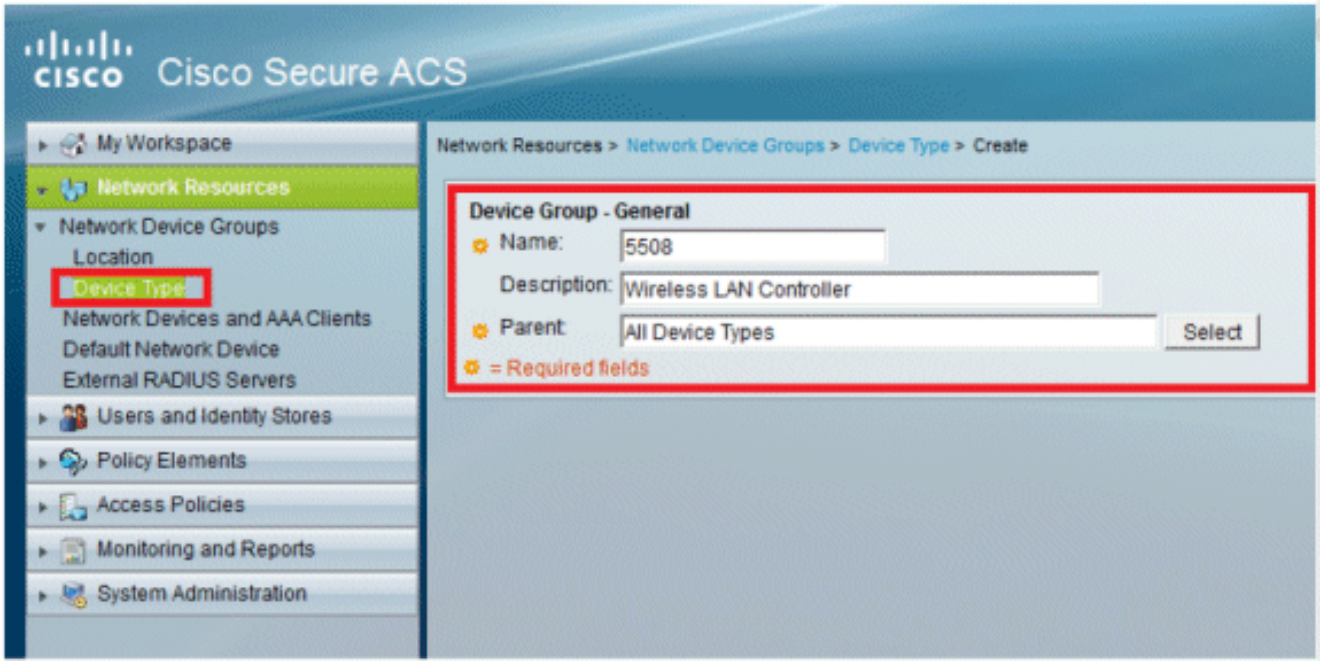
2. Adicione os campos necessários e clique em
   Enviar.



   Agora você verá esta
   tela:

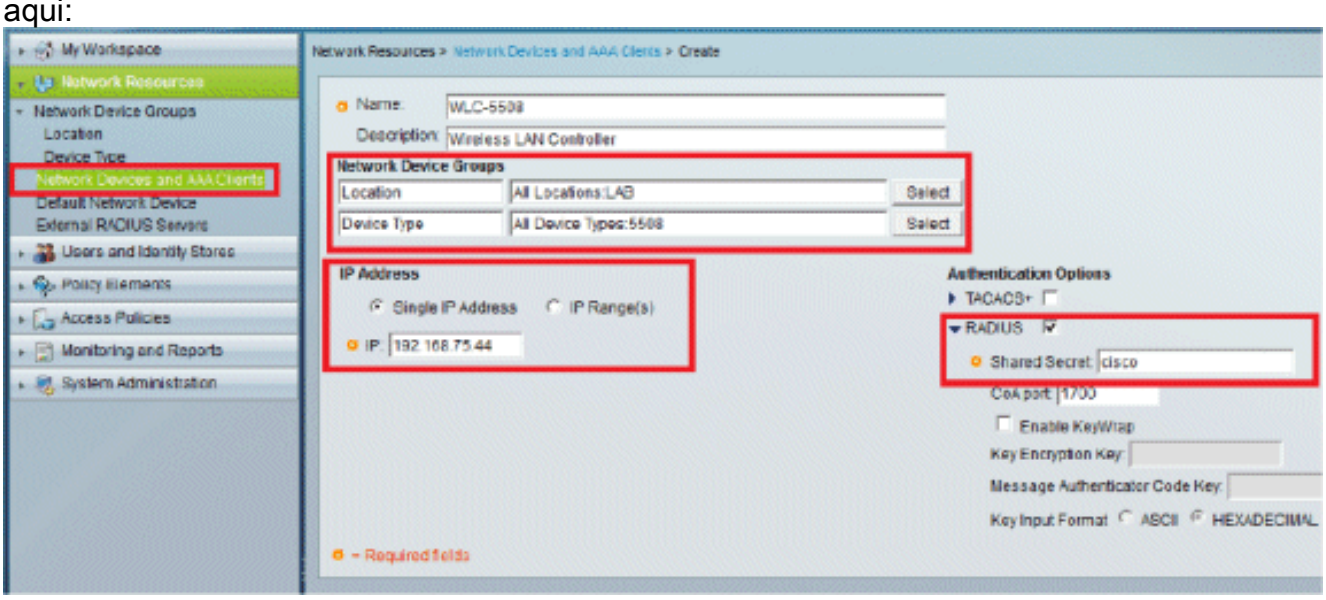


3. Clique em **Tipo de dispositivo > Criar**.

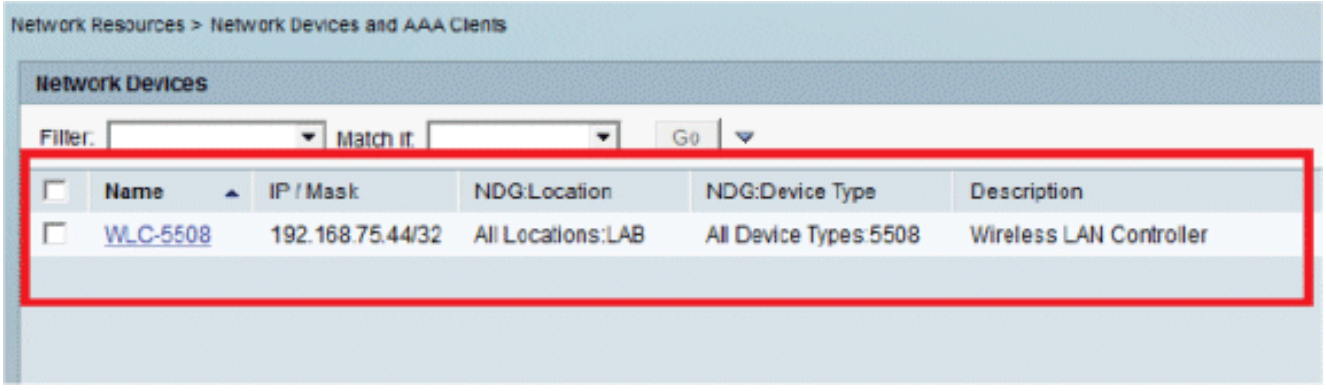


4. Clique em Submit. Agora você verá esta tela:

5. Vá para **Network Resources > Network Devices and AAA Clients**.
6. Clique em **Criar** e preencha os detalhes como mostrado aqui:



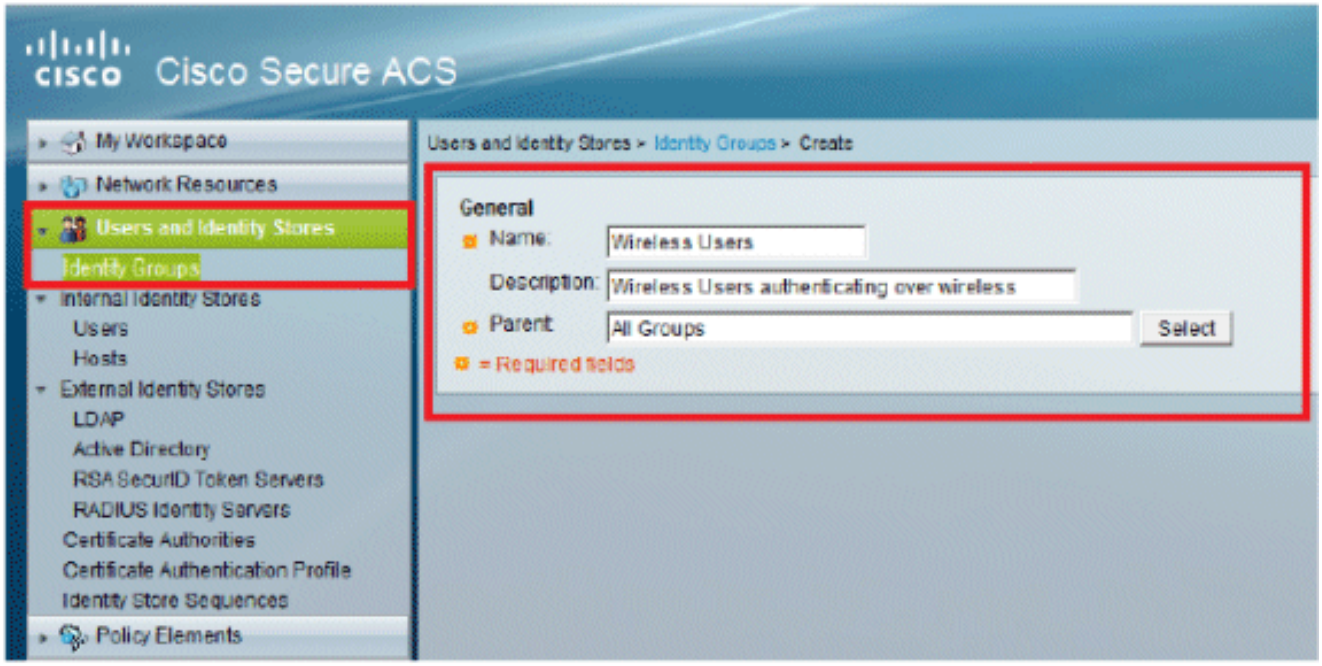
7. Clique em Submit. Agora você verá esta tela:



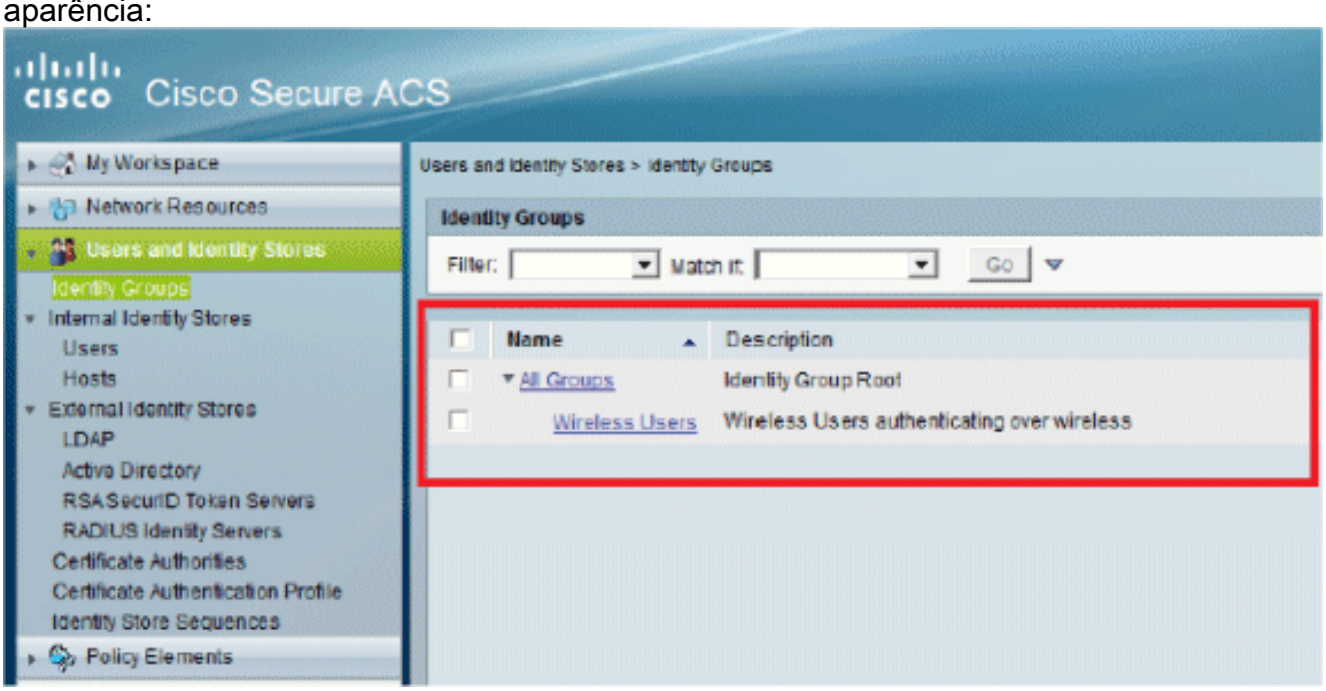
Configurar usuários

Nesta seção, criaremos usuários locais no ACS. Ambos os usuários (usuário1 e usuário2) são atribuídos em um grupo chamado "Usuários sem fio".

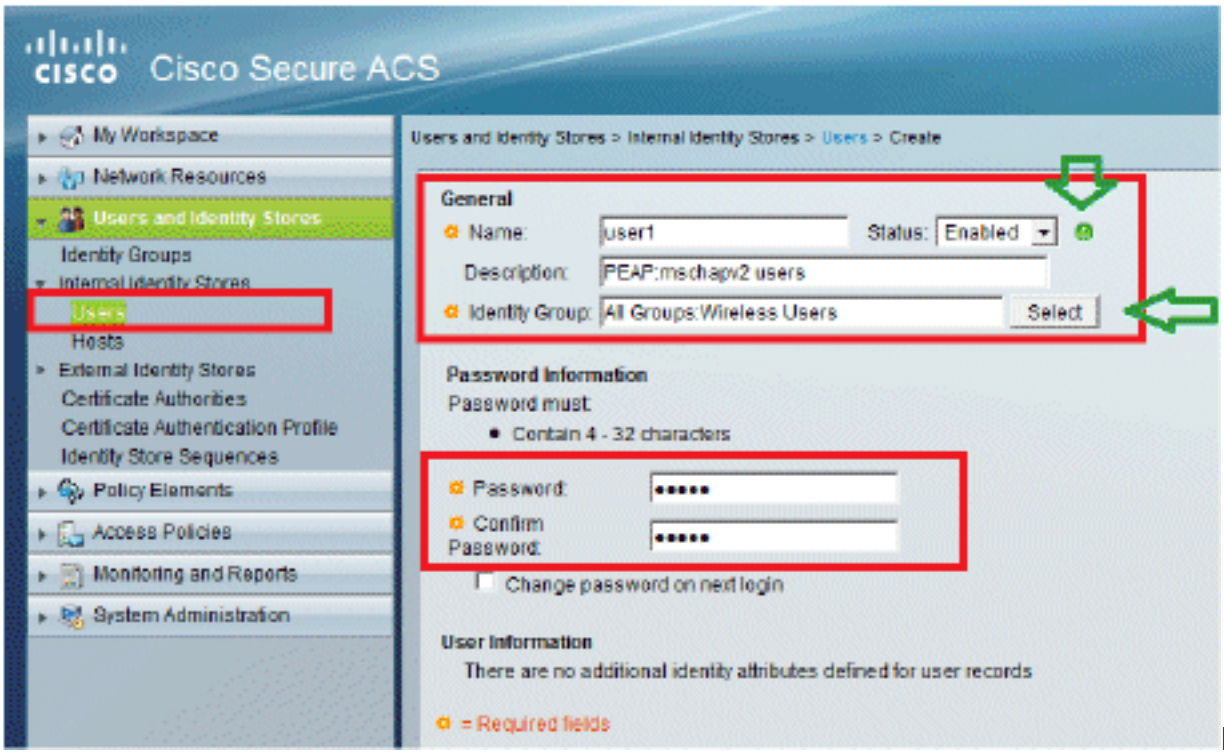
1. Vá para **Users and Identity Stores > Identity Groups > Create**.



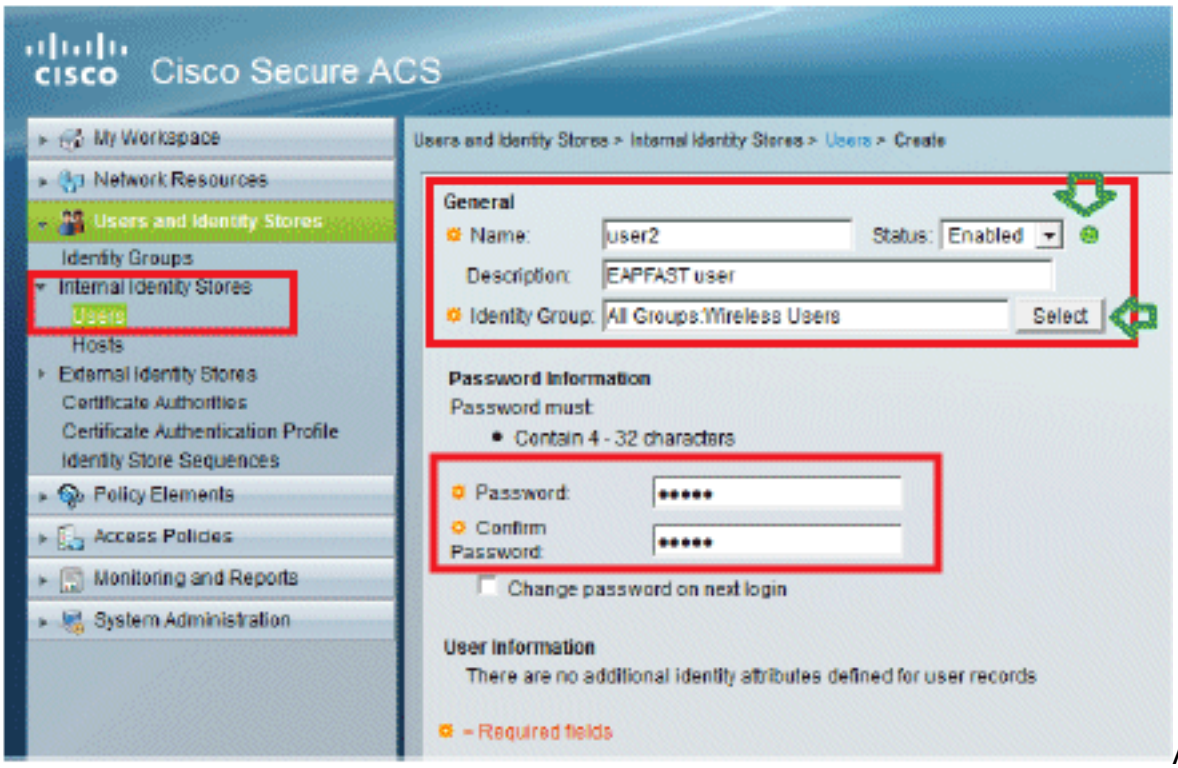
2. Quando você clicar em **Enviar**, a página terá esta aparência:

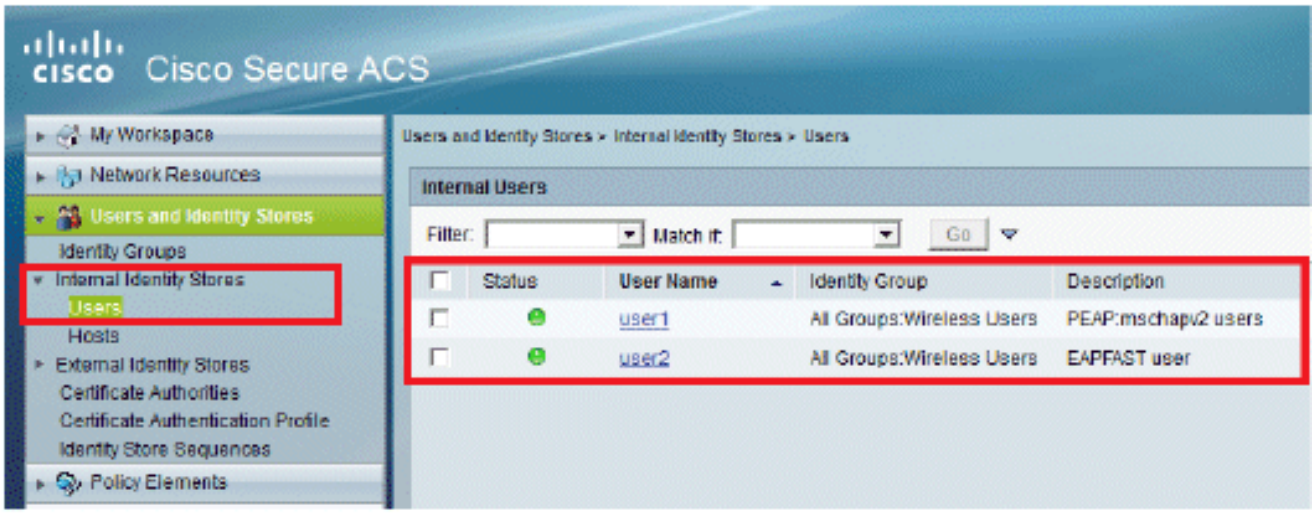


3. Crie os usuários **user1** e **user2** e atribua-os ao grupo "Usuários sem fio".Clique em **Users and Identity Stores > Identity Groups > Users > Create**.



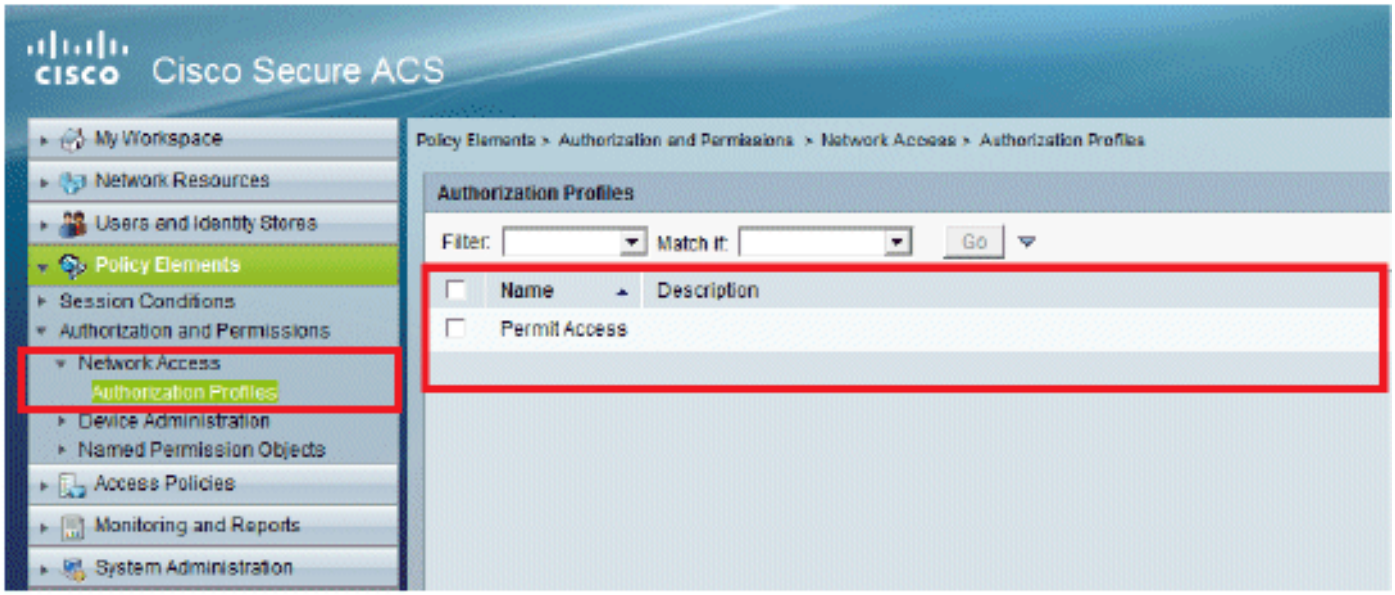
Da mesma forma, crie user2. A tela ficará assim:





Definir Elementos da Política

Verifique se **Permit Access** está definido.

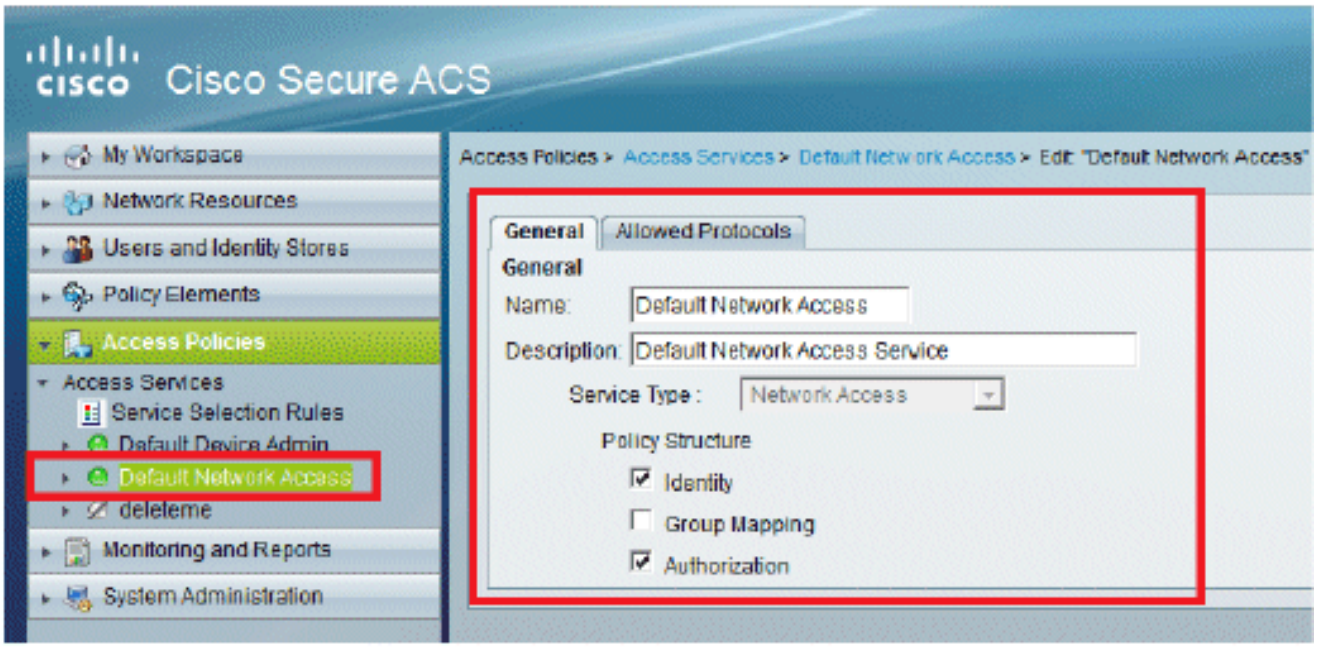


Aplicar políticas de acesso

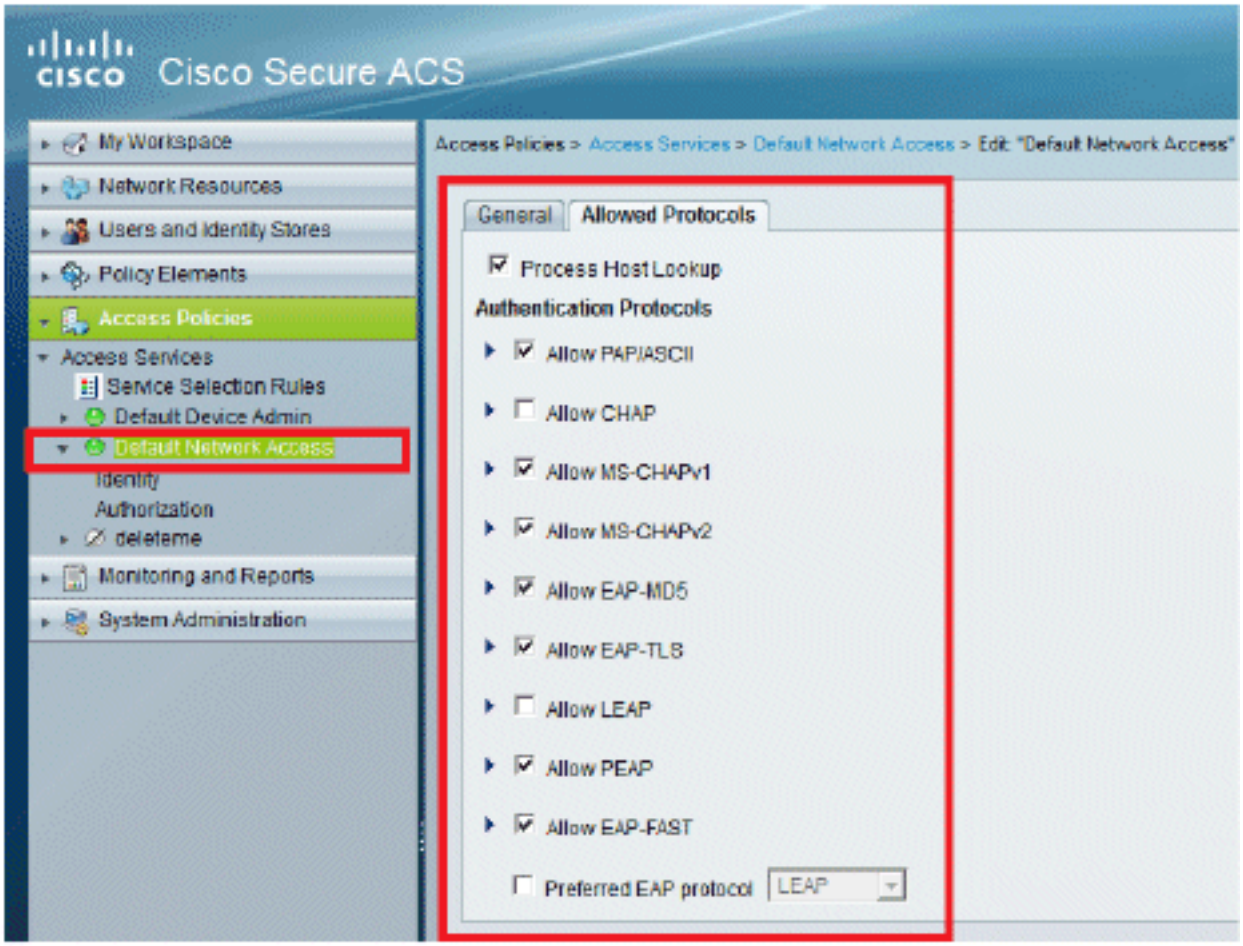
Nesta seção, selecionaremos quais métodos de autenticação serão usados e como as regras serão configuradas. Criaremos regras com base nas etapas anteriores.

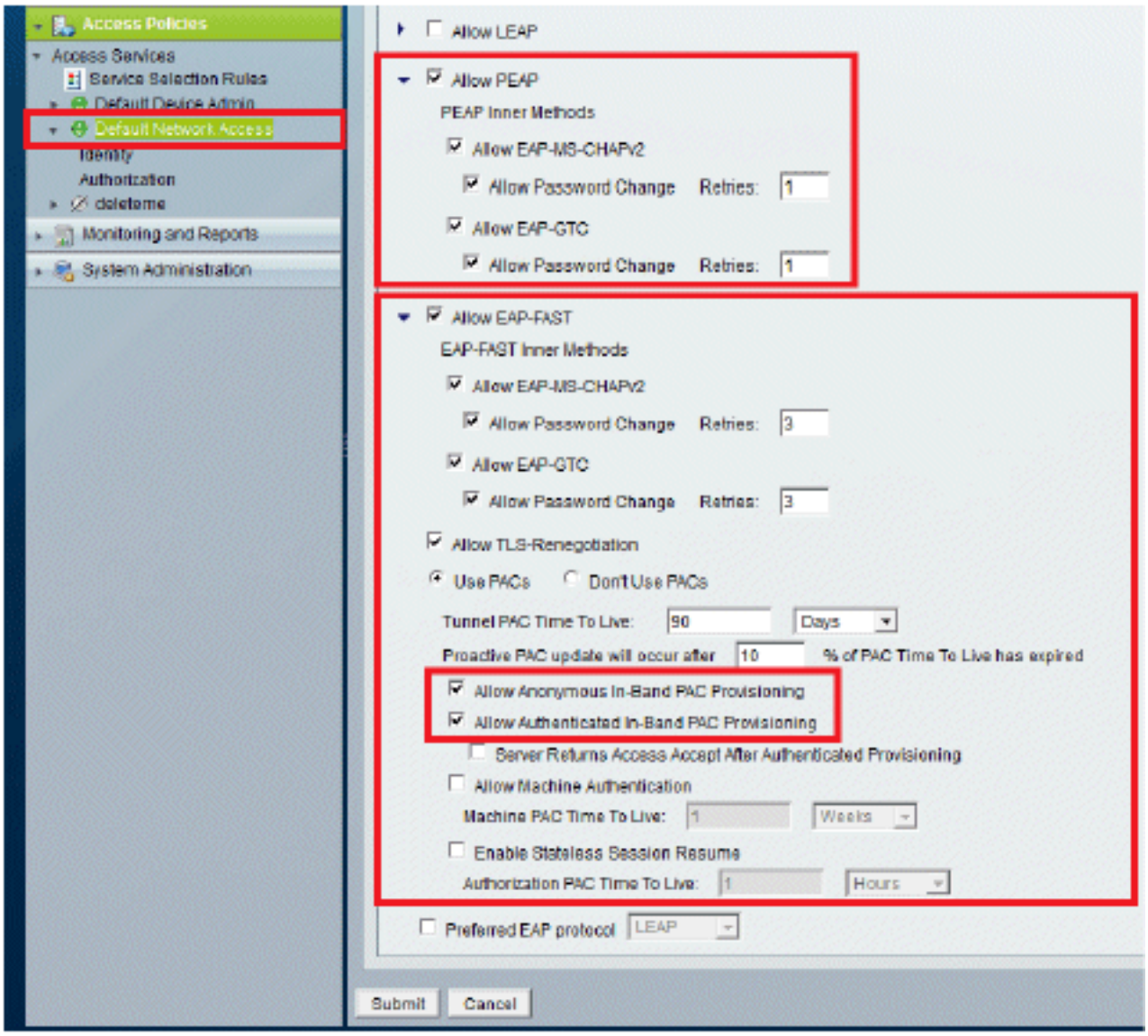
Conclua estes passos:

1. Vá para **Access Policies > Access Services > Default Network Access > Edit: "Default Network Access"**.

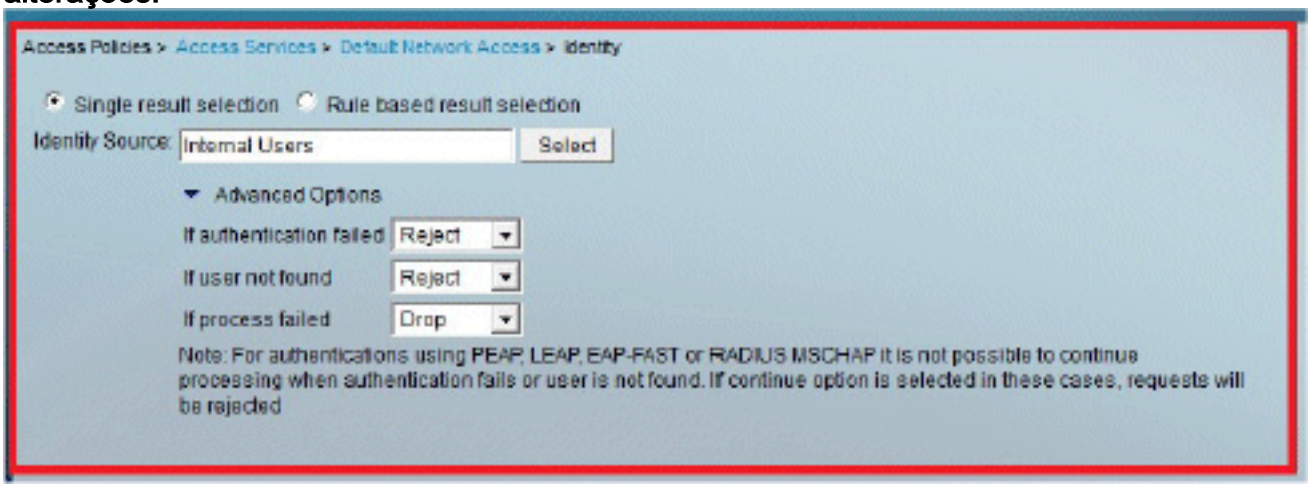


2. Selecione o método EAP que você deseja que os clientes sem fio autentiquem. Neste exemplo, usamos **PEAP- MSCHAPv2** e **EAP-FAST**.



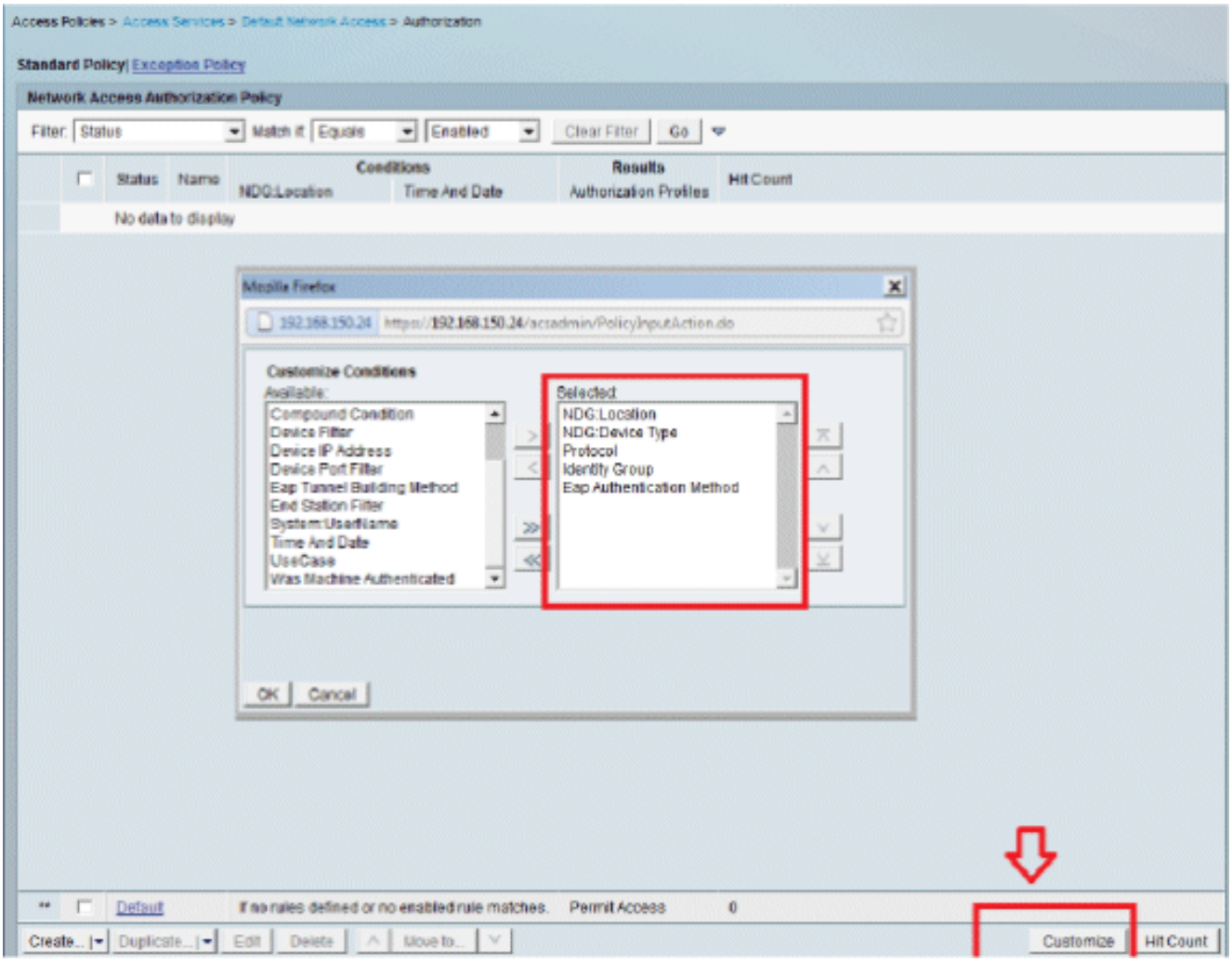


3. Clique em Submit.
4. Verifique o grupo Identidade selecionado. Neste exemplo, usamos **Internal Users**, que criamos no ACS. **Salve as alterações.**

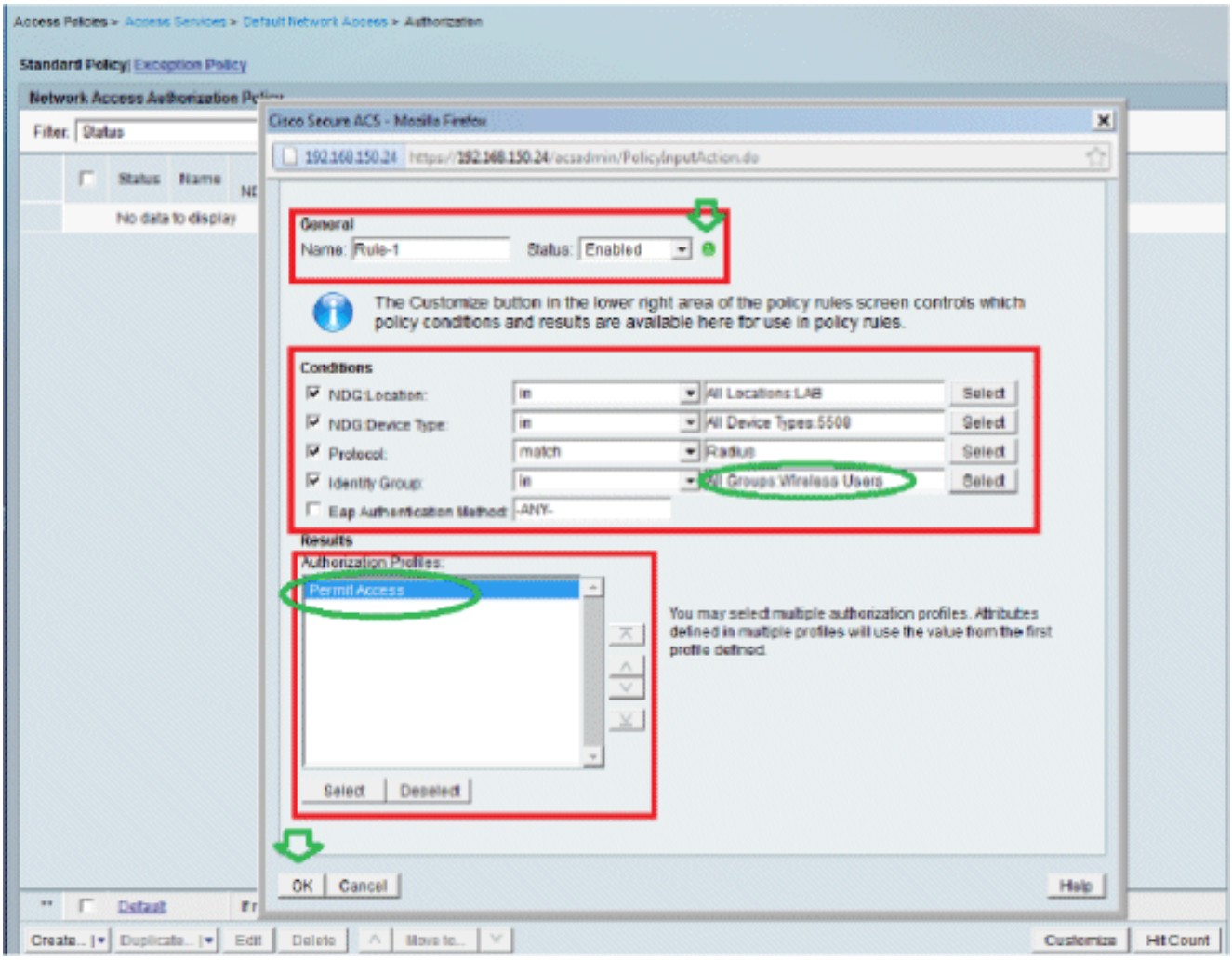


5. Para verificar o perfil de autorização, vá para **Access Policies > Access Services > Default Network Access > Authorization**.Você pode personalizar sob quais condições permitirá o acesso do usuário à rede e que perfil (atributos) de autorização você passará depois de autenticado. Essa granularidade está disponível apenas no ACS 5.x. Neste exemplo, selecionamos Location, **Device Type**, **Protocol**, Identity Group e EAP Authentication

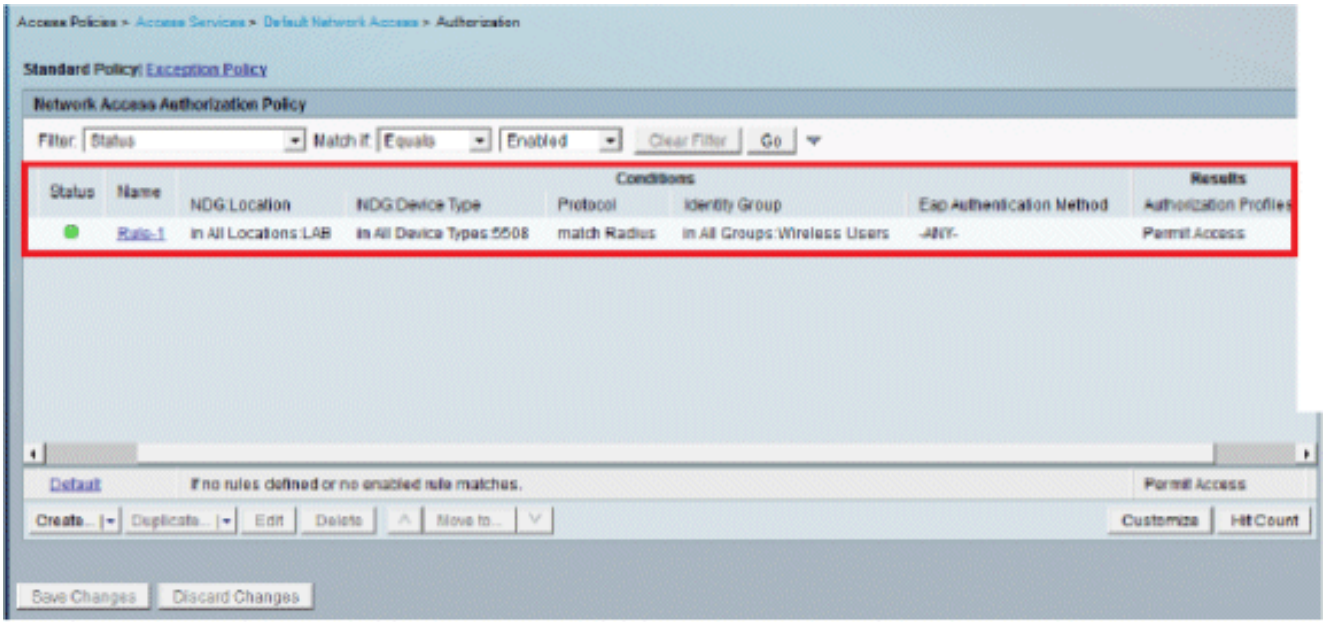
Method.



6. Clique em **OK** e em **Save Changes**.
7. A próxima etapa é criar uma regra. Se nenhuma regra for definida, o cliente terá acesso sem nenhuma condição.Clique em **Criar > Regra-1**. Esta regra é para usuários do grupo "Usuários sem
fio".

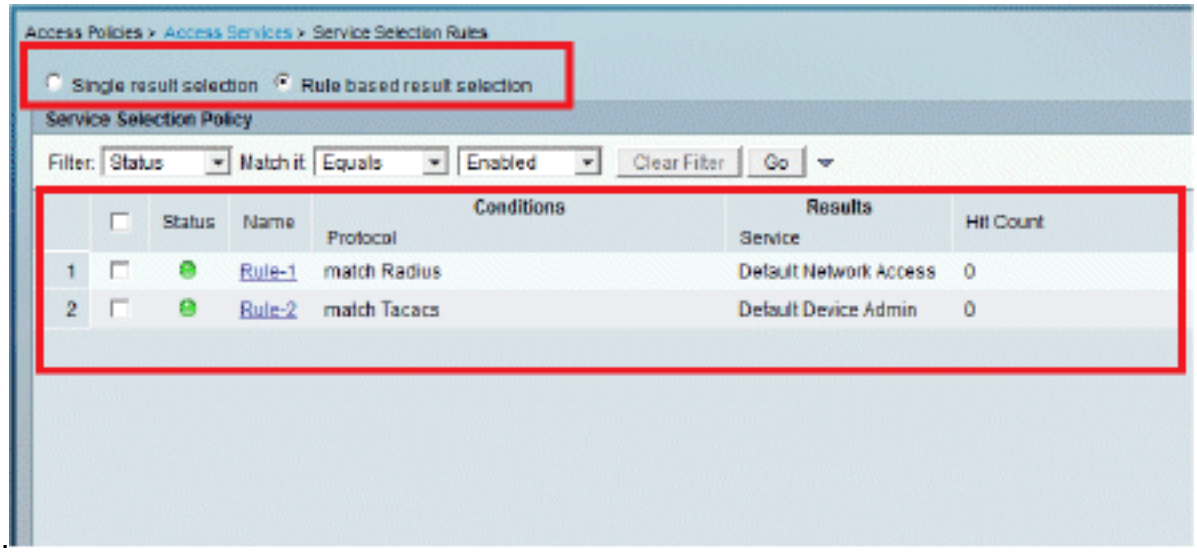


8. Salve as alterações. A tela ficará assim:



Se você quiser que os usuários que não corresponderem às condições sejam negados, edite a regra padrão para dizer "negar acesso".

9. Agora definiremos **Regras de Seleção de Serviço**. Use esta página para configurar uma política simples ou baseada em regras para determinar qual serviço aplicar às solicitações recebidas. Neste exemplo, uma política baseada em regras é

usada. 

Configurar o WLC

Essa configuração requer estes passos:

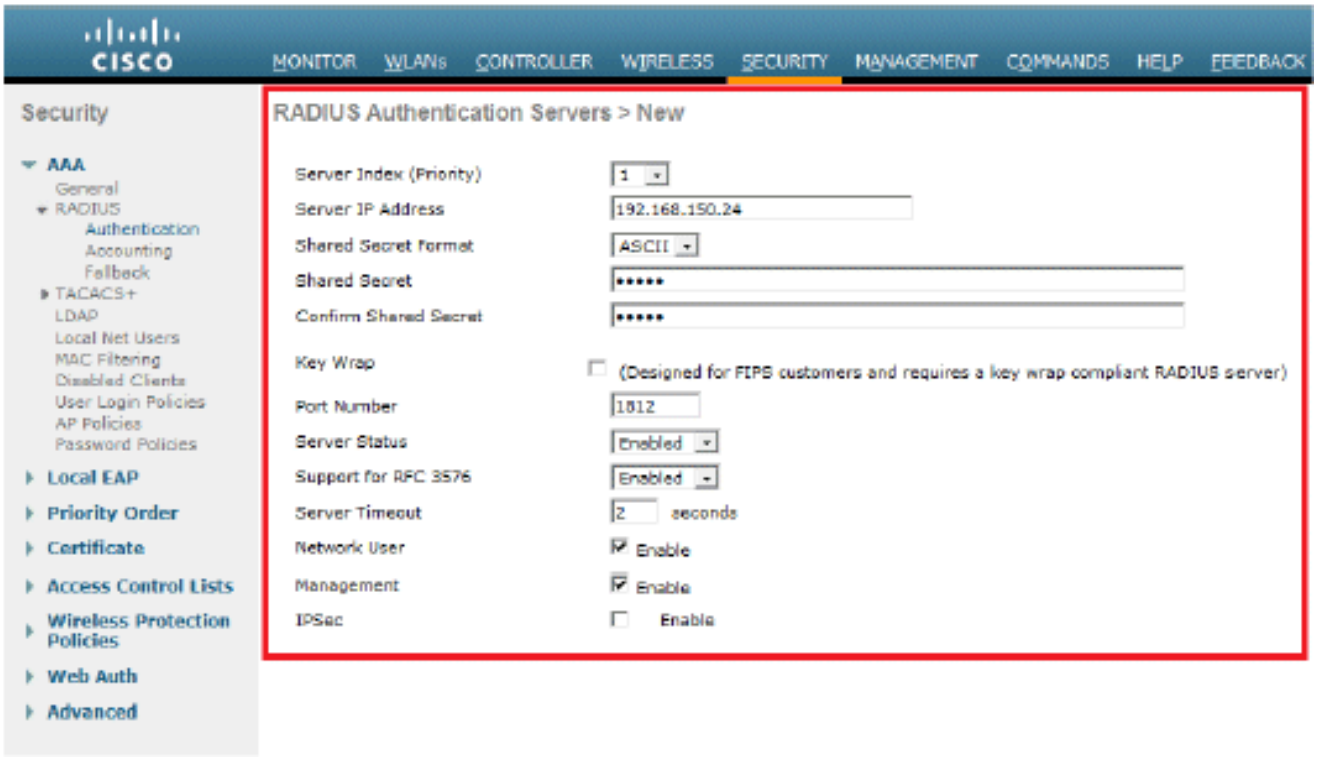
1. Configurar o WLC com os detalhes do Servidor de Autenticação.
2. Configure as interfaces dinâmicas (VLANs).
3. Configurar as WLANs (SSID).

Configurar o WLC com os detalhes do Servidor de Autenticação

Énecessário configurar a WLC para que ela possa se comunicar com o servidor RADIUS para autenticar os clientes e também para quaisquer outras transações.

Conclua estes passos:

1. No controller GUI, clique em **Security**.
2. Digite o endereço IP do servidor RADIUS e a chave secreta compartilhada usados entre o servidor RADIUS e o WLC.Essa chave secreta compartilhada deve ser a mesma que foi configurada no servidor
   RADIUS.

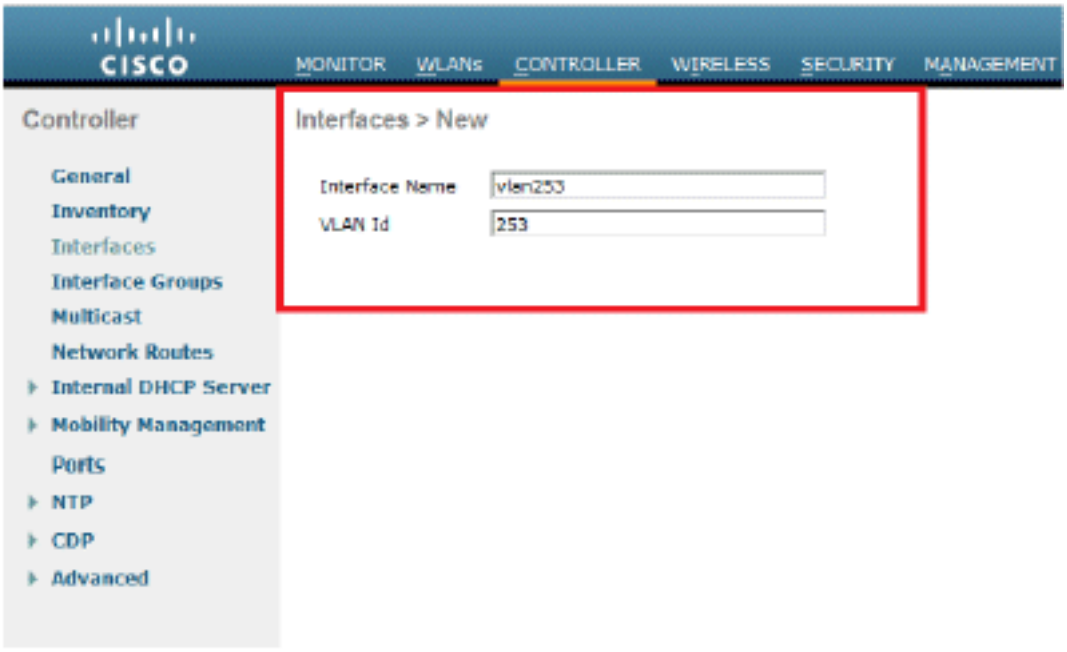


Configurar as interfaces dinâmicas (VLANs)

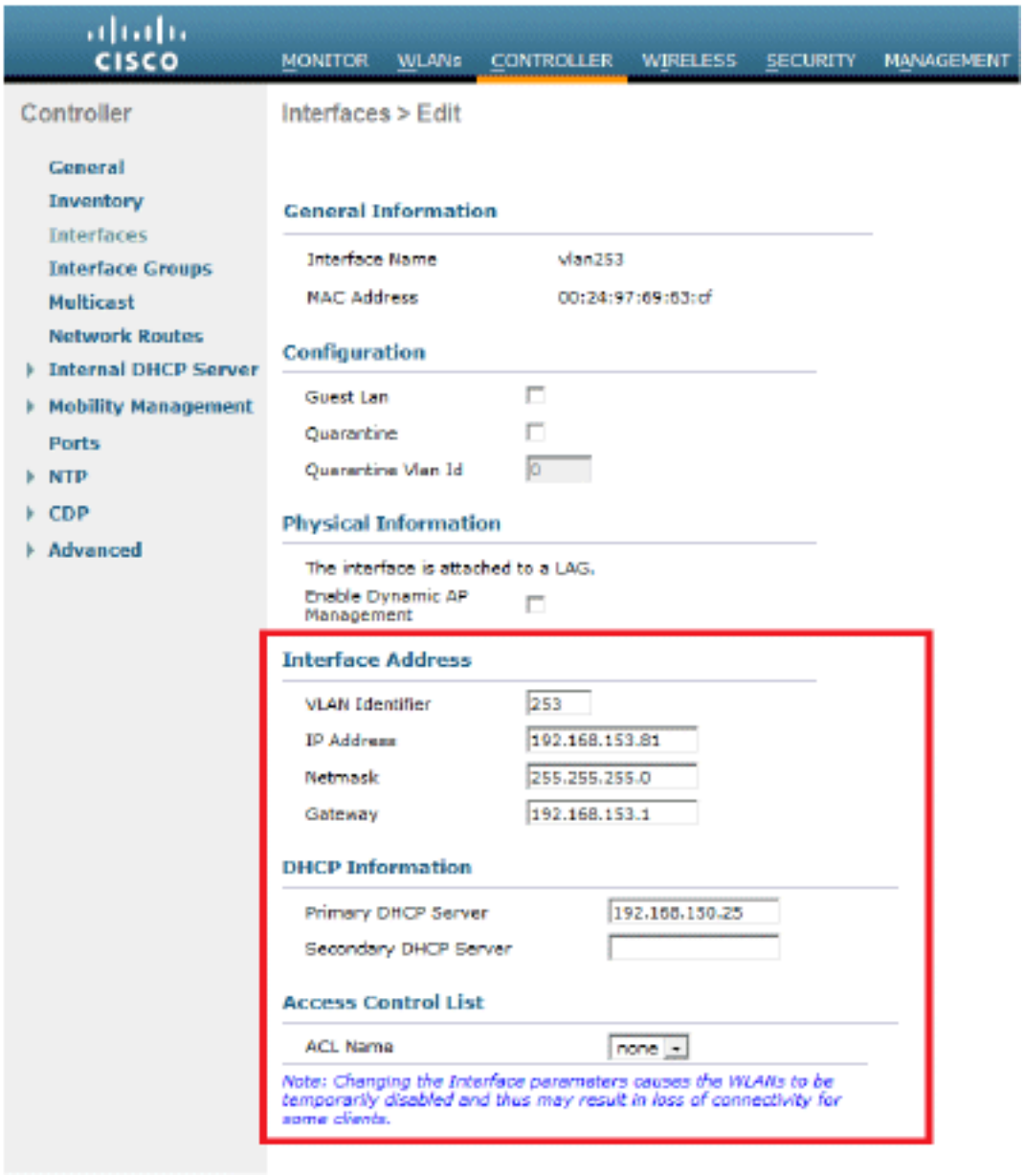
Este procedimento descreve como configurar interfaces dinâmicas no WLC.

Conclua estes passos:

1. A interface dinâmica é configurada na GUI do controlador, na janela **Controller >**

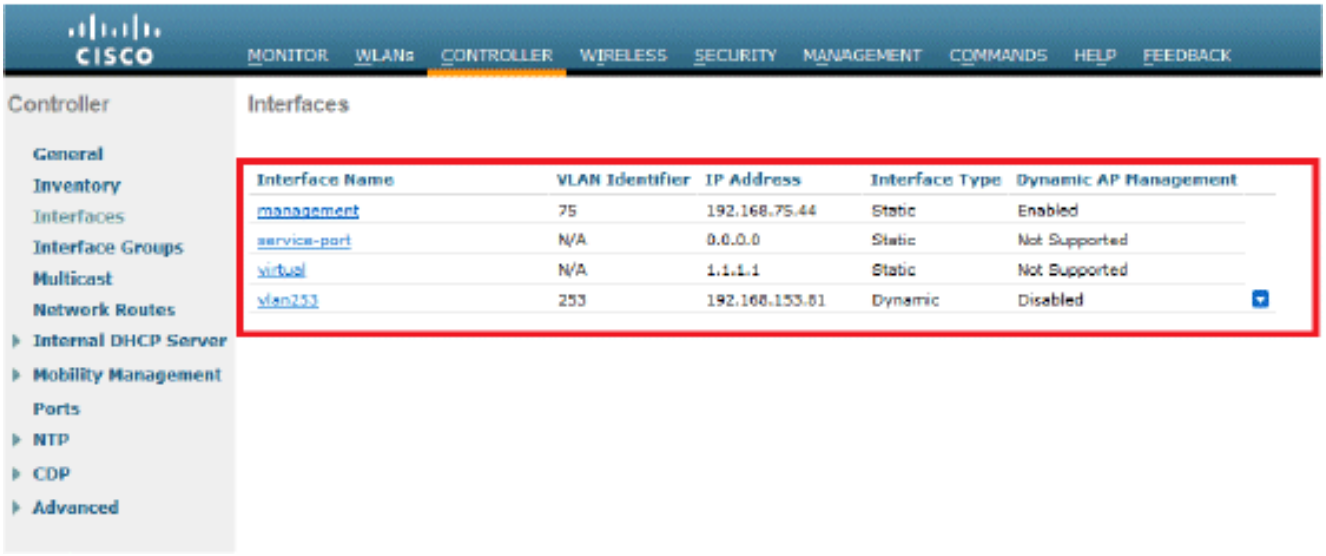


Interfaces.
2. Clique em Apply.Isto abre a janela Edit desta interface dinâmica (VLAN 253 aqui).
3. Digite o endereço IP e o gateway padrão desta interface



dinâmica.

4. Clique em Apply.
5. As interfaces configuradas terão esta aparência:

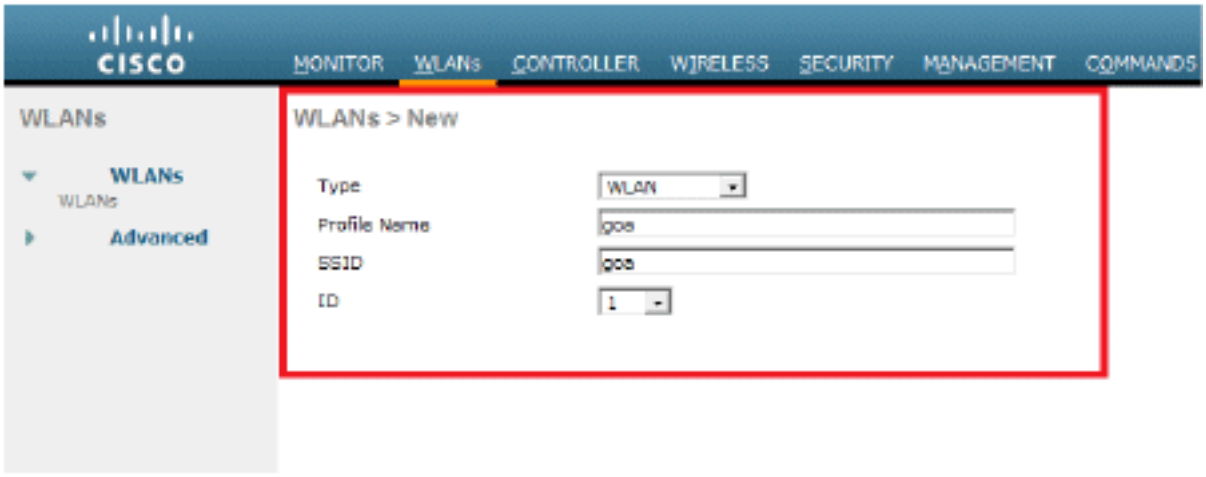


Configurar as WLANs (SSID)

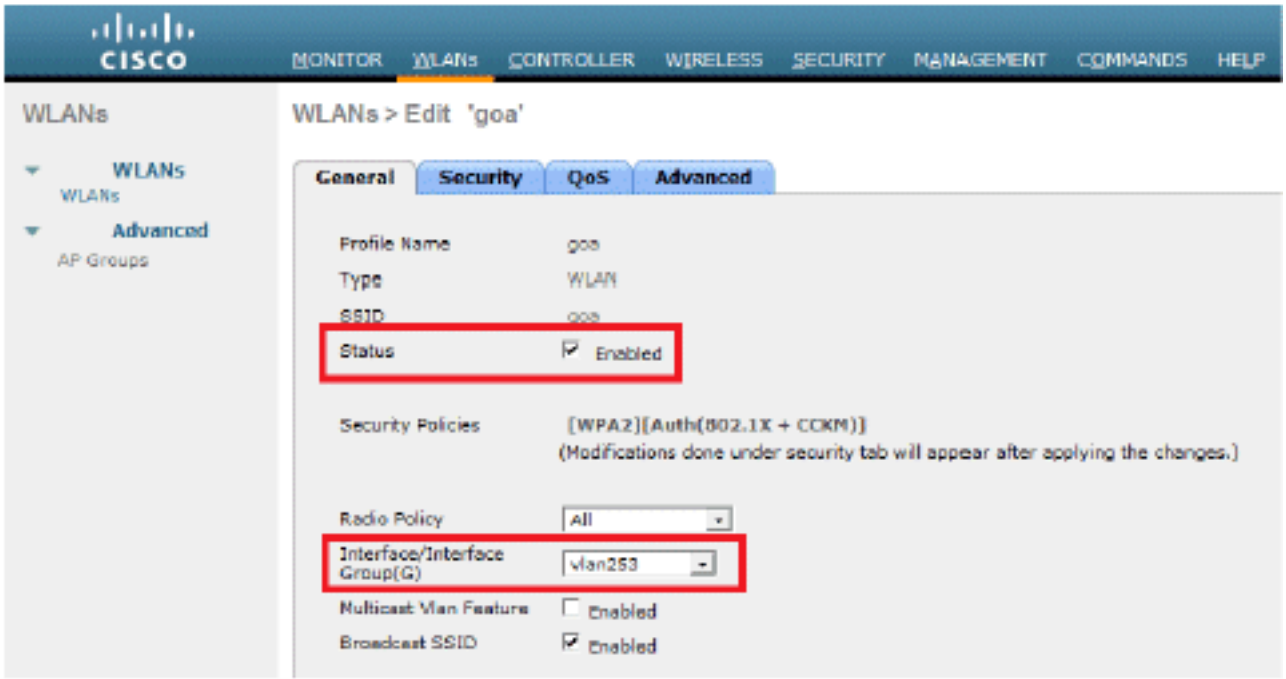
Este procedimento explica como configurar as WLANs no WLC.

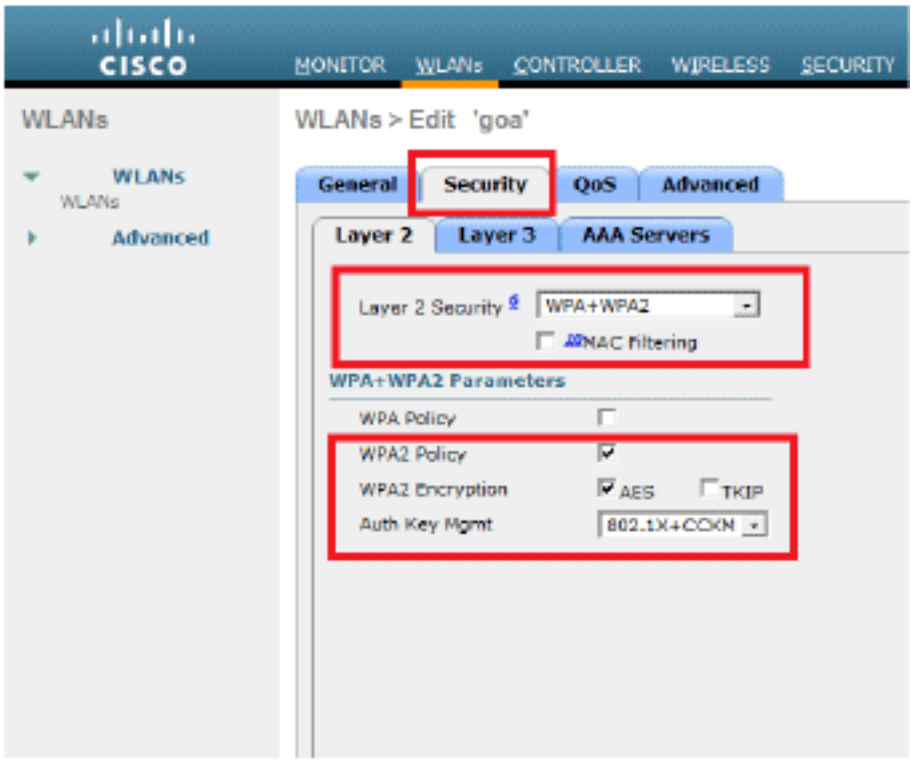
Conclua estes passos:

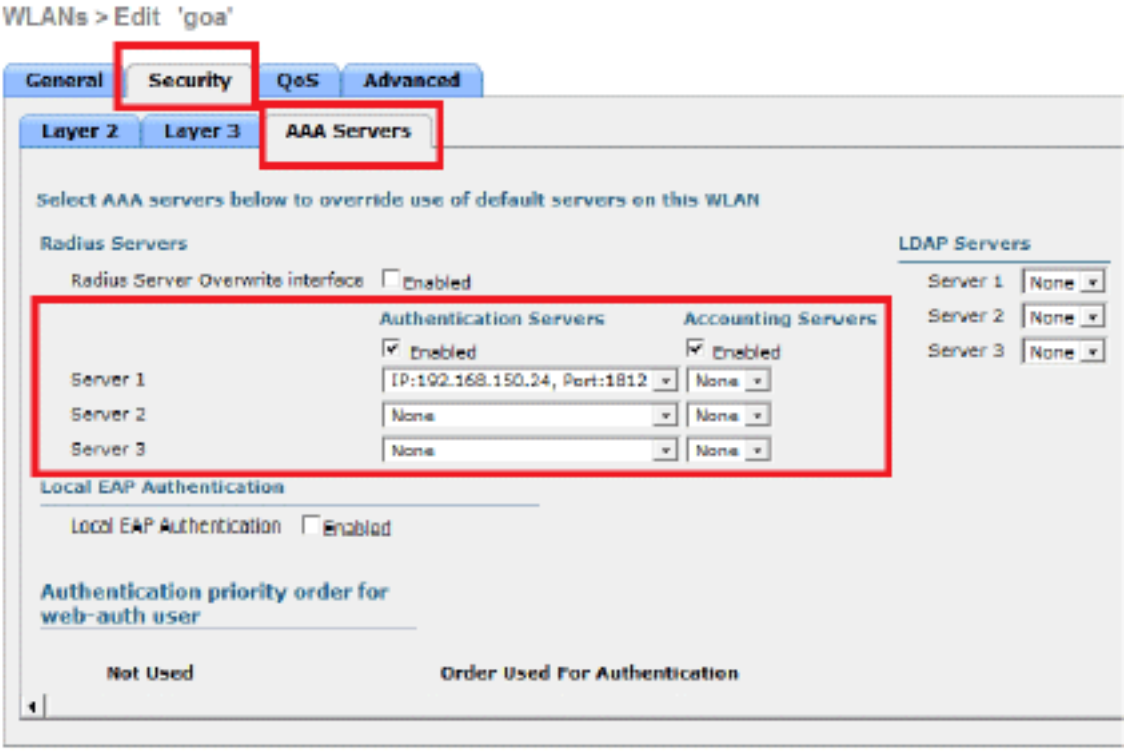
1. Na GUI do controlador, vá para **WLANs > Create New** para criar uma nova WLAN. A janela New WLANs é exibida.
2. Digite a ID da WLAN e a SSID da WLAN.Você pode digitar qualquer nome como o SSID da WLAN. Este exemplo usa **goa** como o SSID da WLAN.

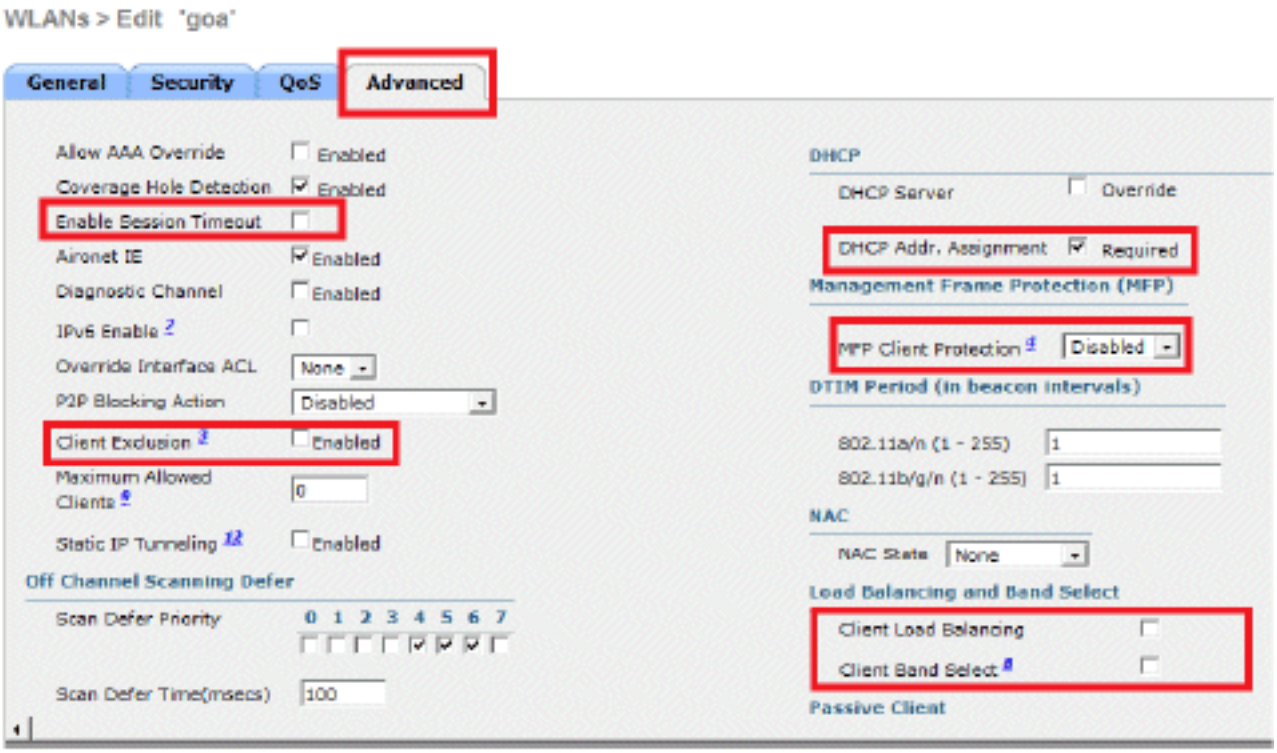


3. Clique em **Apply** para ir para a janela Edit do objetivo da WLAN.




MONITOR
WLANs
CONTROLLER
WIRELESS
SECURITY
WLANs
WLANs > Edit 'goa'
WLANs
WLANs
Advanced
General
Security
QoS
Advanced
Layer 2
Layer 3
AAA Servers
Layer 2 Security
WPA+WPA2
MAC Filtering
WPA+WPA2 Parameters
WPA Policy
WPA2 Policy
WPA2 Encryption
AES
TKIP
Auth Key Mgmt
802.1X+CCKM


WLANs > Edit 'goa'
General
Security
QoS
Advanced
Layer 2
Layer 3
AAA Servers
Select AAA servers below to override use of default servers on this WLAN
Radius Servers
Radius Server Overwrite interface
Enabled
Authentication Servers
Accounting Servers
Enabled
Enabled
Server 1
IP:192.168.150.24, Port:1812
None
Server 2
None
None
Server 3
None
None
LDAP Servers
Server 1
None
Server 2
None
Server 3
None
Local EAP Authentication
Local EAP Authentication
Enabled
Authentication priority order for web-auth user
Not Used
Order Used For Authentication



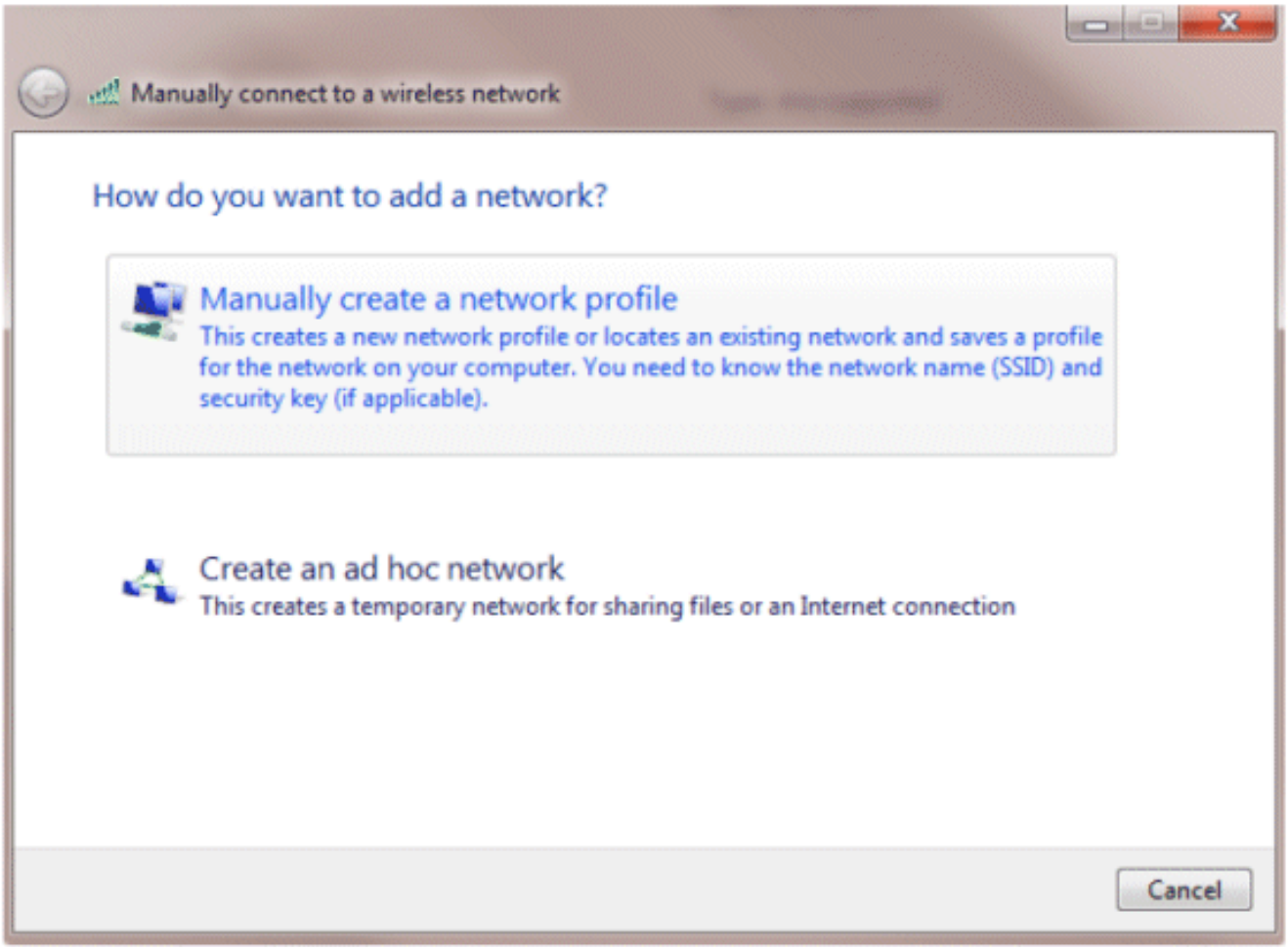
Configurar o utilitário de cliente sem fio

PEAP-MSCHAPv2 (usuário1)

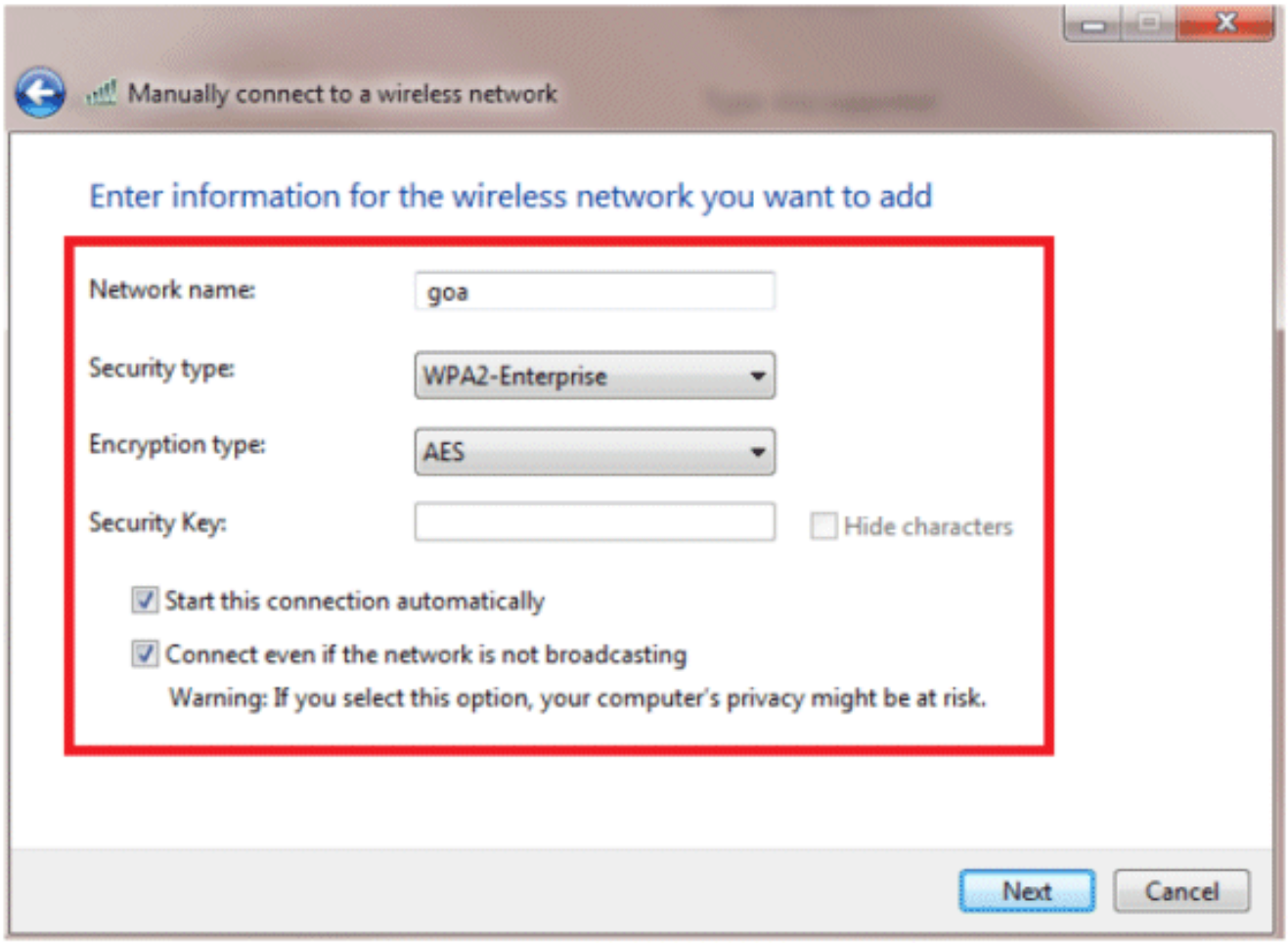
Em nosso cliente de teste, estamos usando o solicitante nativo do Windows 7 com uma placa Intel 6300-N executando a versão de driver 14.3. É recomendável testar usando os drivers mais recentes dos fornecedores.

Conclua estas etapas para criar um perfil no Windows Zero Config (WZC):

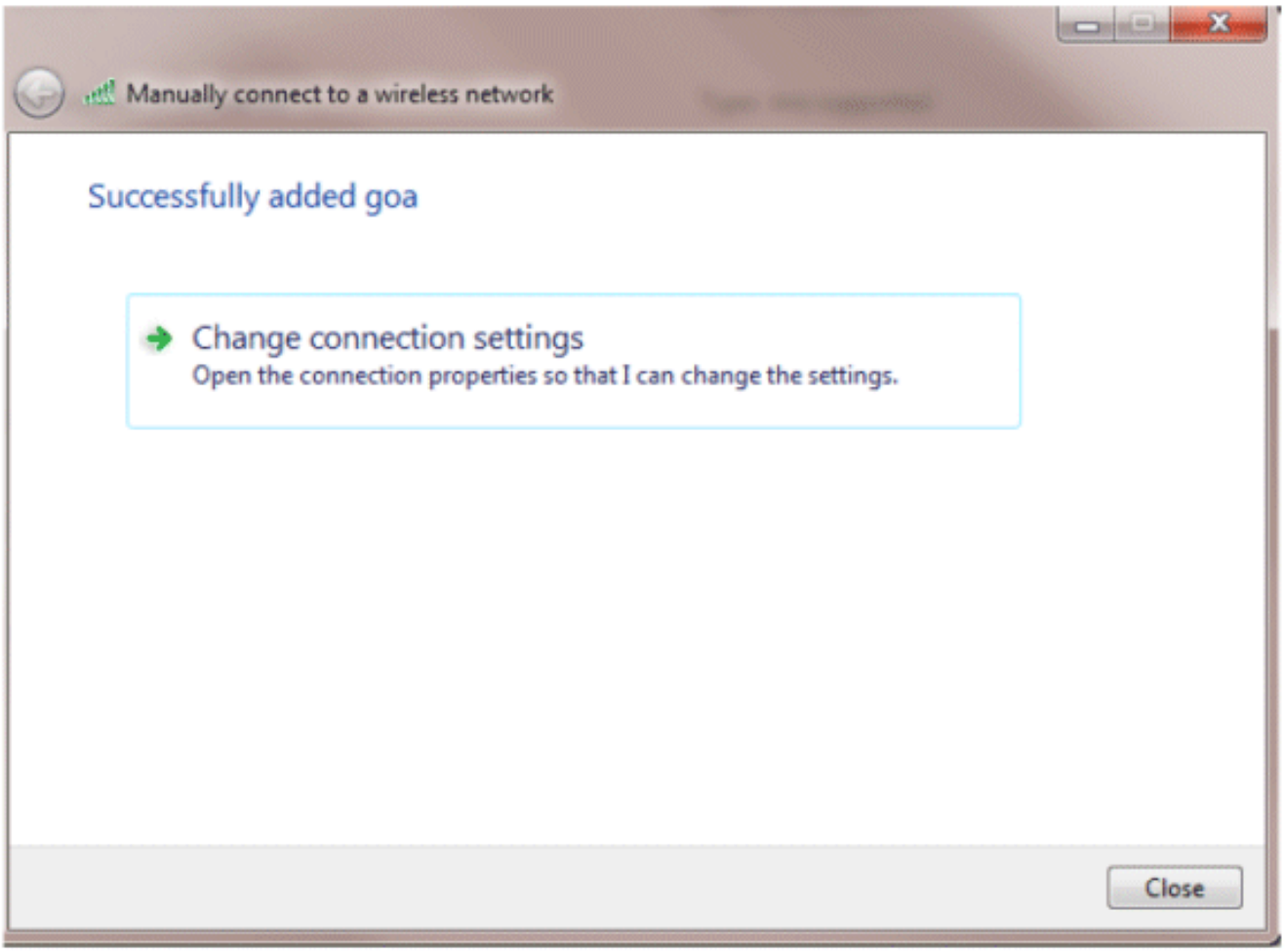
1. Vá para **Painel de controle > Rede e Internet > Gerenciar redes sem fio**.
2. Clique na guia **Add**.
3. Clique em **Criar manualmente um perfil de rede**.



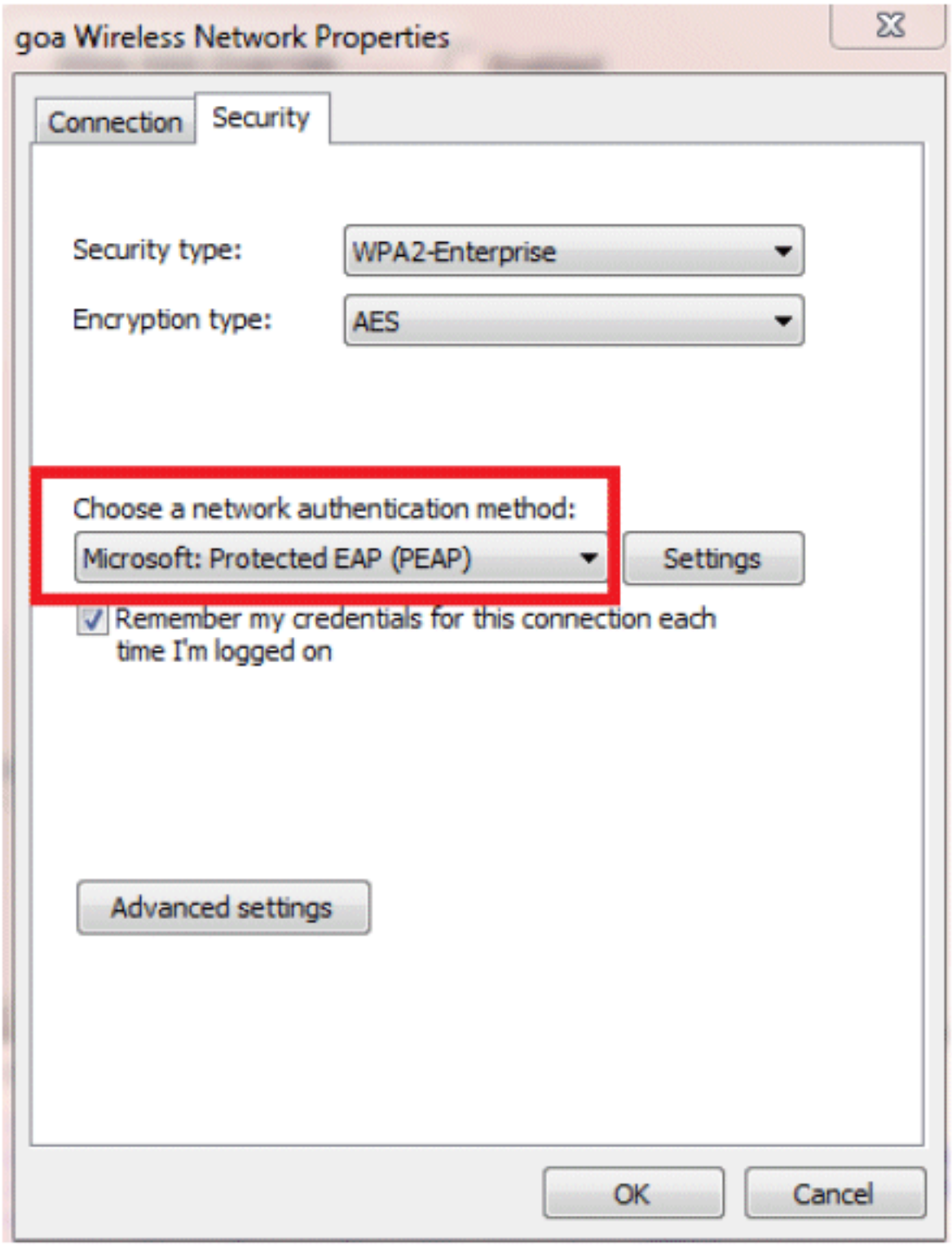
4. Adicione os detalhes conforme configurado na WLC.**Observação:** o SSID diferencia maiúsculas de minúsculas.
5. Clique em
   Next.

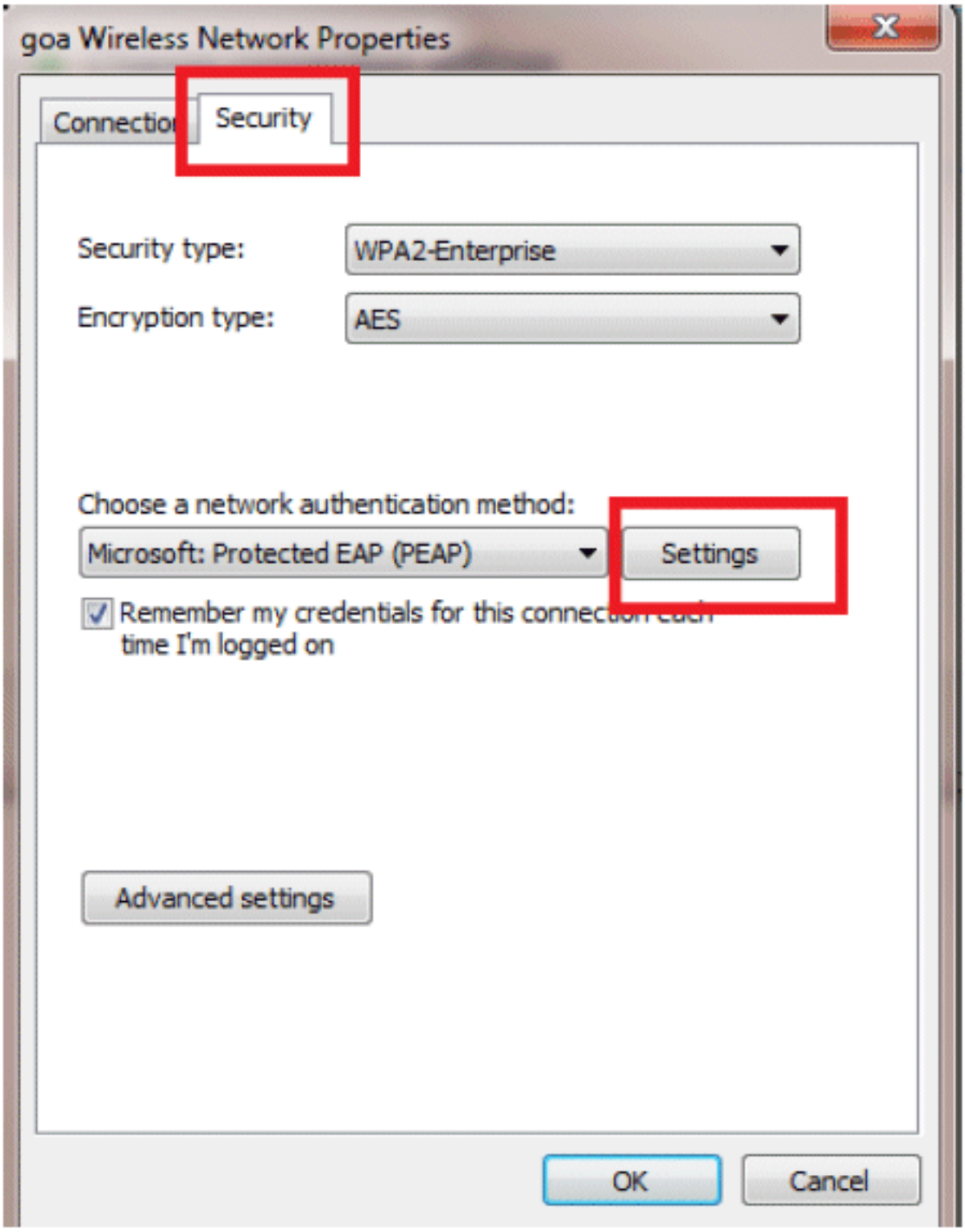


6. Clique em **Change connection settings** para verificar novamente as configurações.

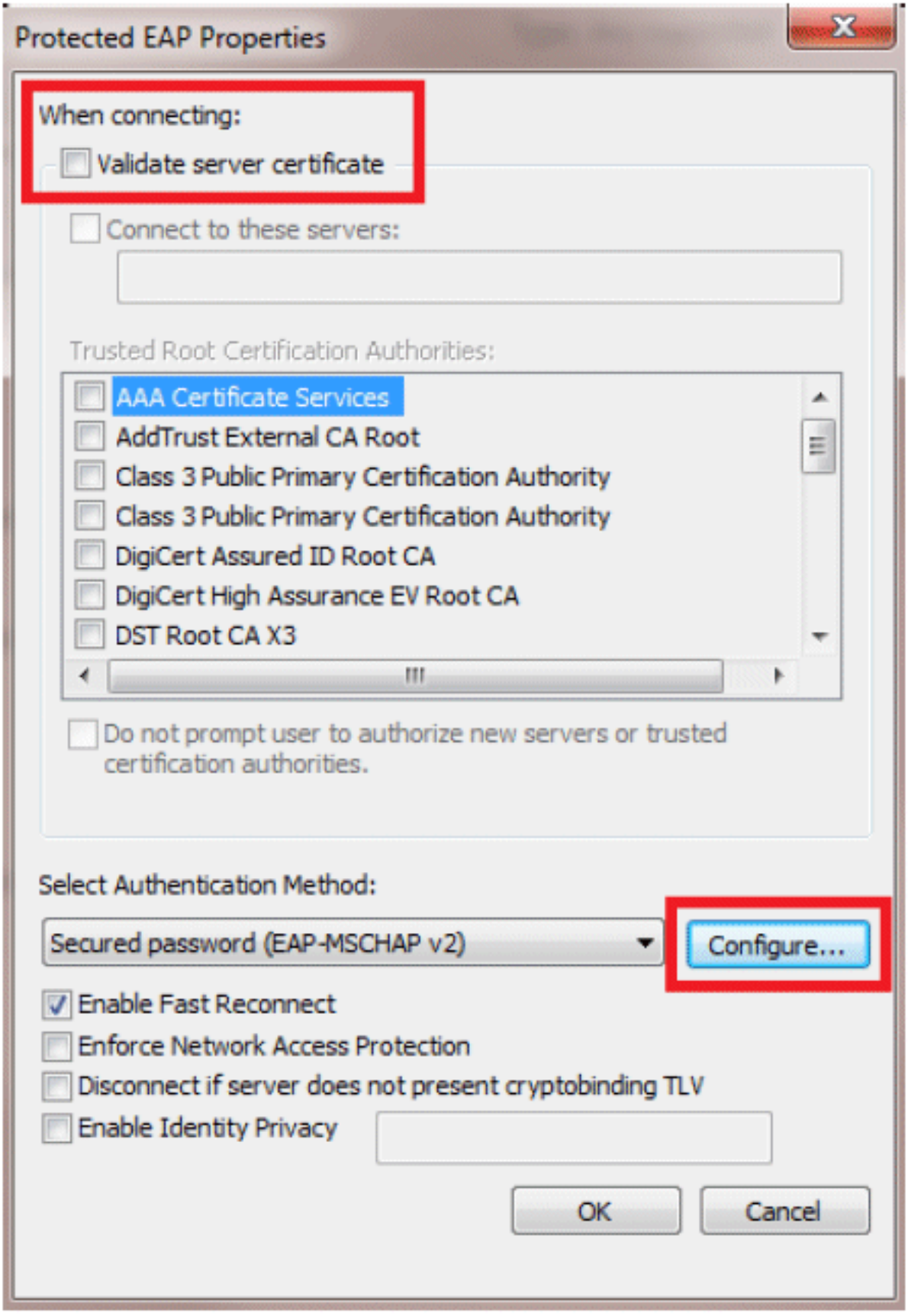


7. Verifique se o **PEAP** está habilitado.

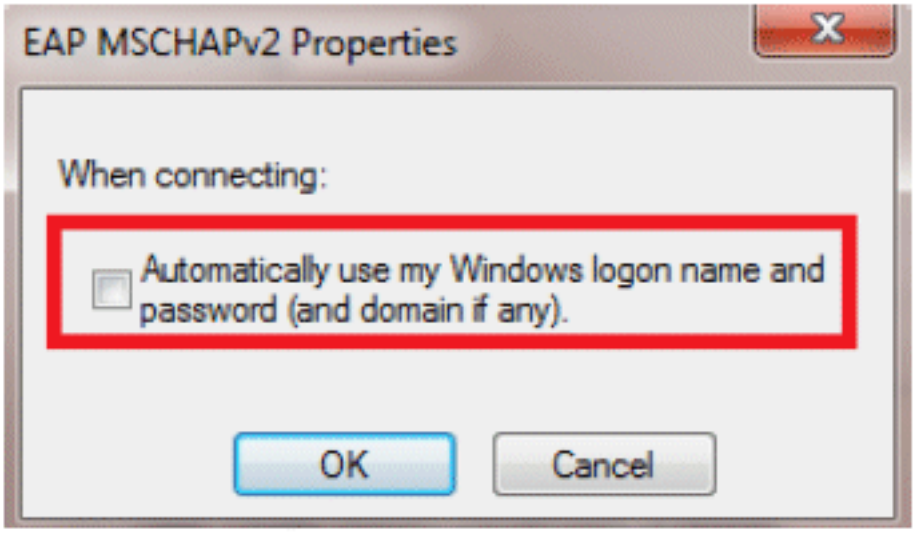




8. Neste exemplo, não estamos validando o certificado do servidor. Se você marcar esta caixa e não conseguir se conectar, tente desabilitar o recurso e teste novamente.

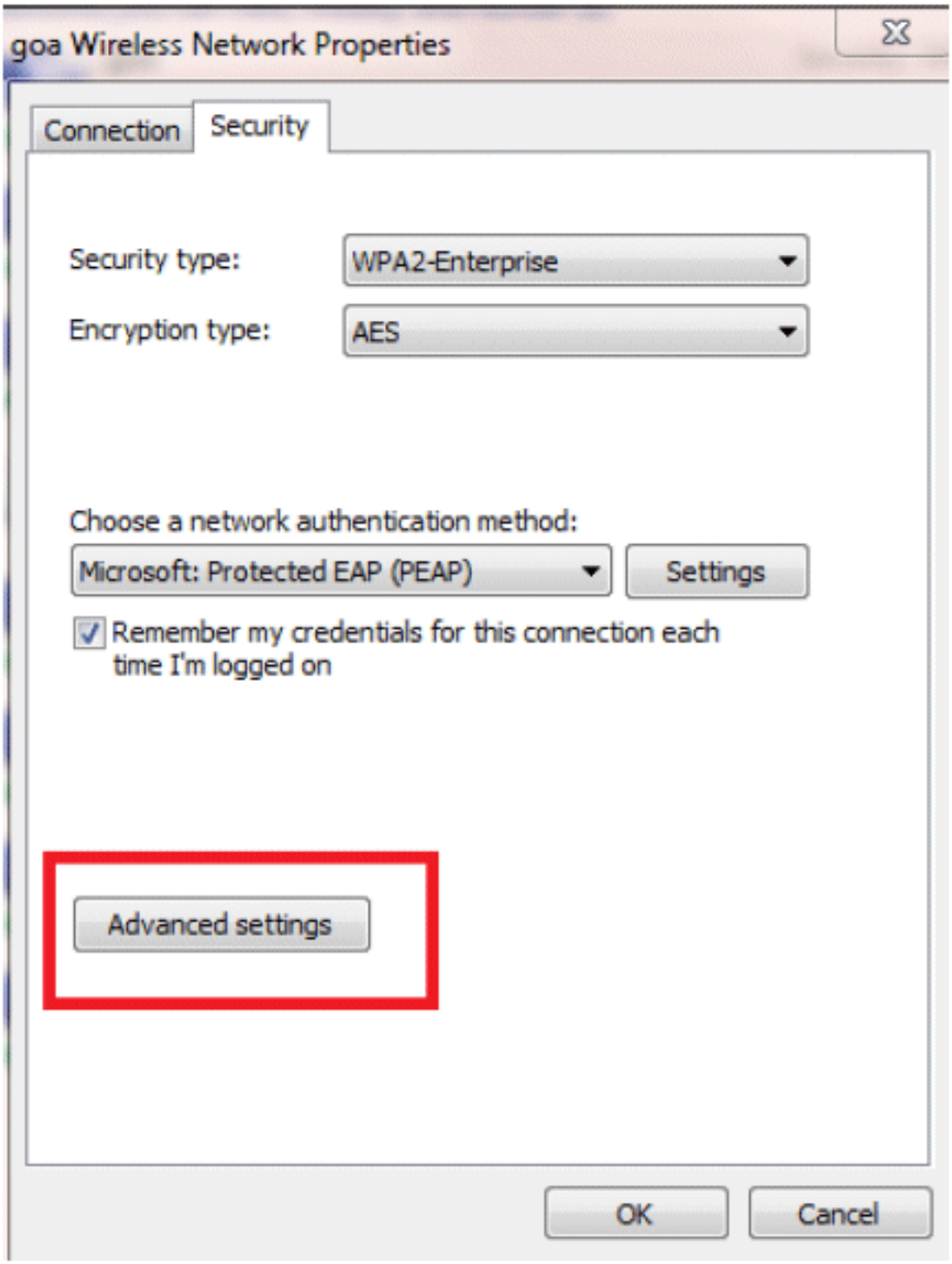


9. Como alternativa, você pode usar suas credenciais do Windows para fazer login. No entanto, neste exemplo, não vamos usar isso. Click

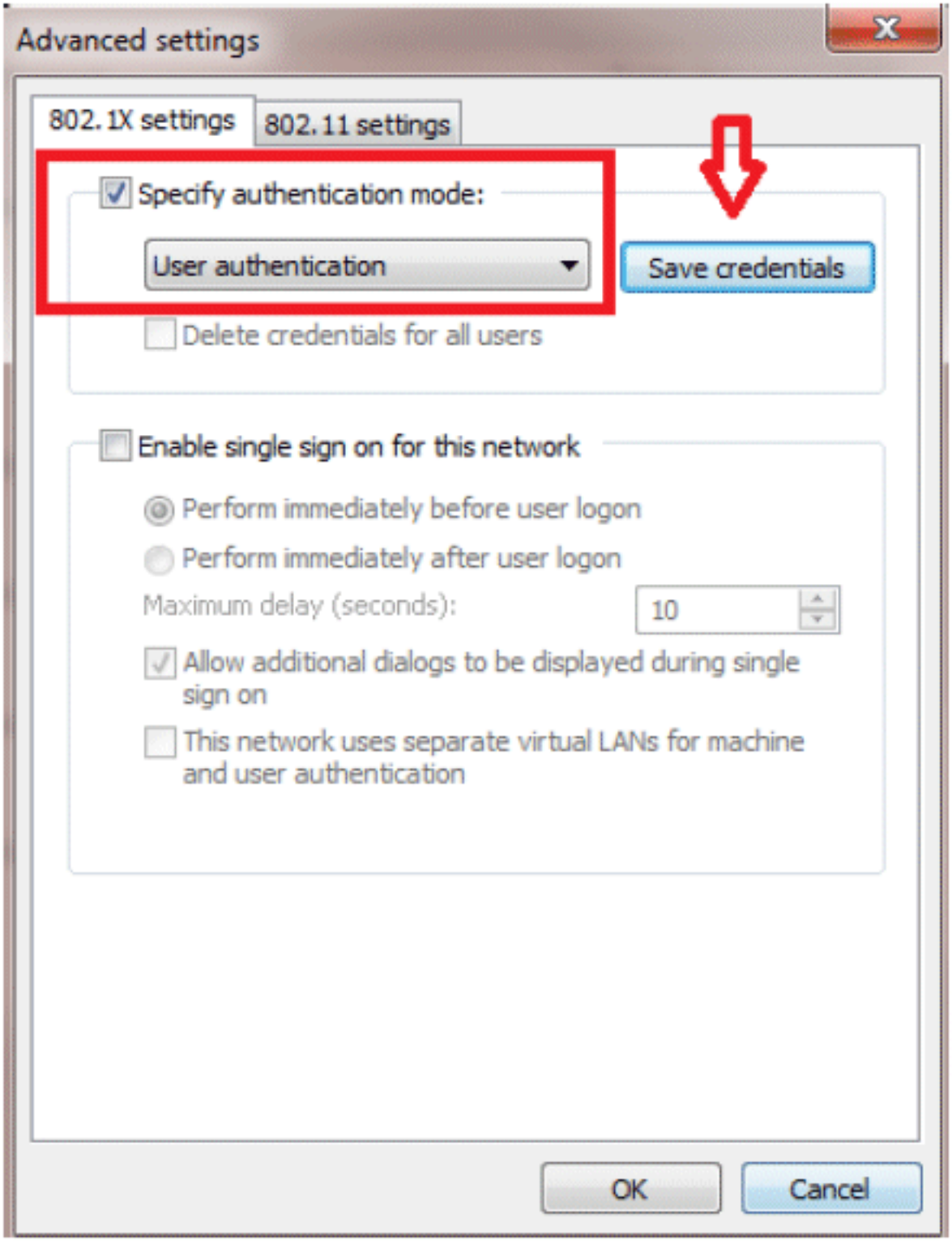


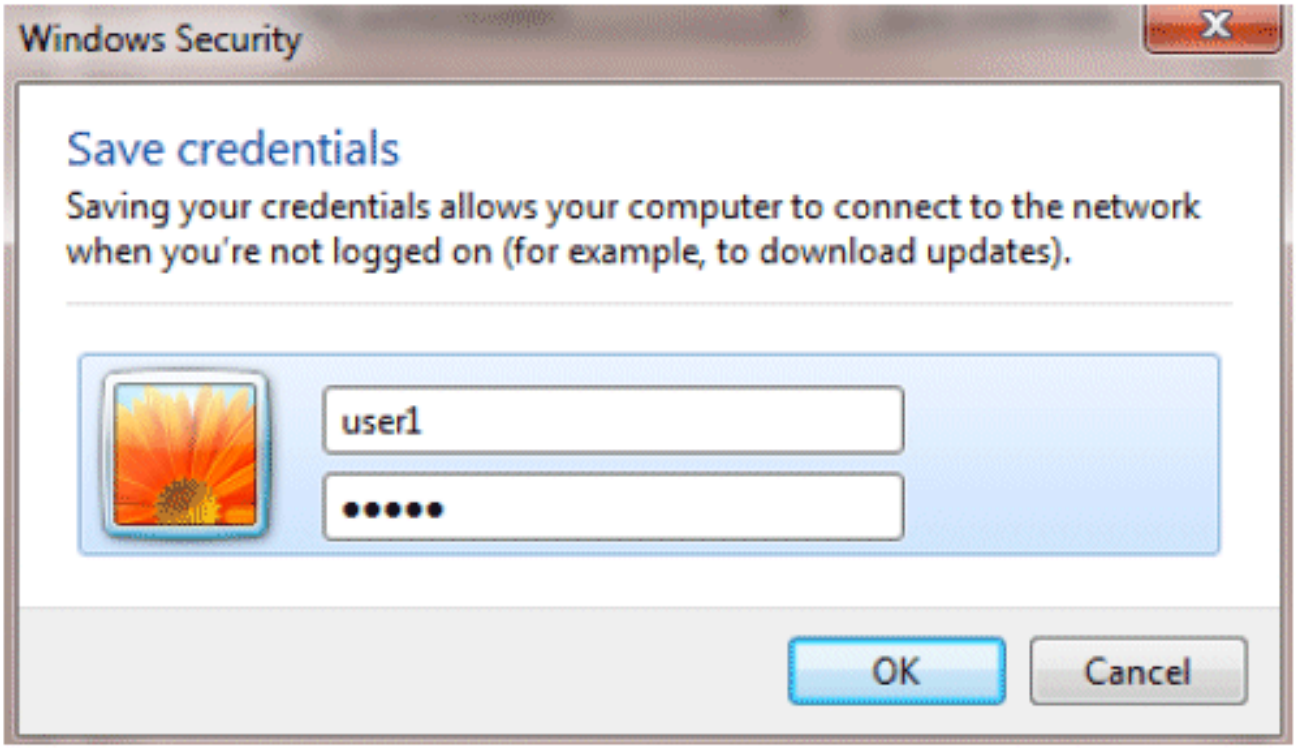
OK.

10. Clique em **Advanced settings** para configurar o nome de usuário e a


goa Wireless Network Properties
Connection
Security
Security type:
WPA2-Enterprise
Encryption type:
AES
Choose a network authentication method:
Microsoft: Protected EAP (PEAP)
Settings
Remember my credentials for this connection each time I'm logged on
Advanced settings
OK
Cancel

senha.


Advanced settings
802.1X settings
802.11 settings
Specify authentication mode:
User authentication
Save credentials
Delete credentials for all users
Enable single sign on for this network
Perform immediately before user logon
Perform immediately after user logon
Maximum delay (seconds):
10
Allow additional dialogs to be displayed during single sign on
This network uses separate virtual LANs for machine and user authentication
OK
Cancel



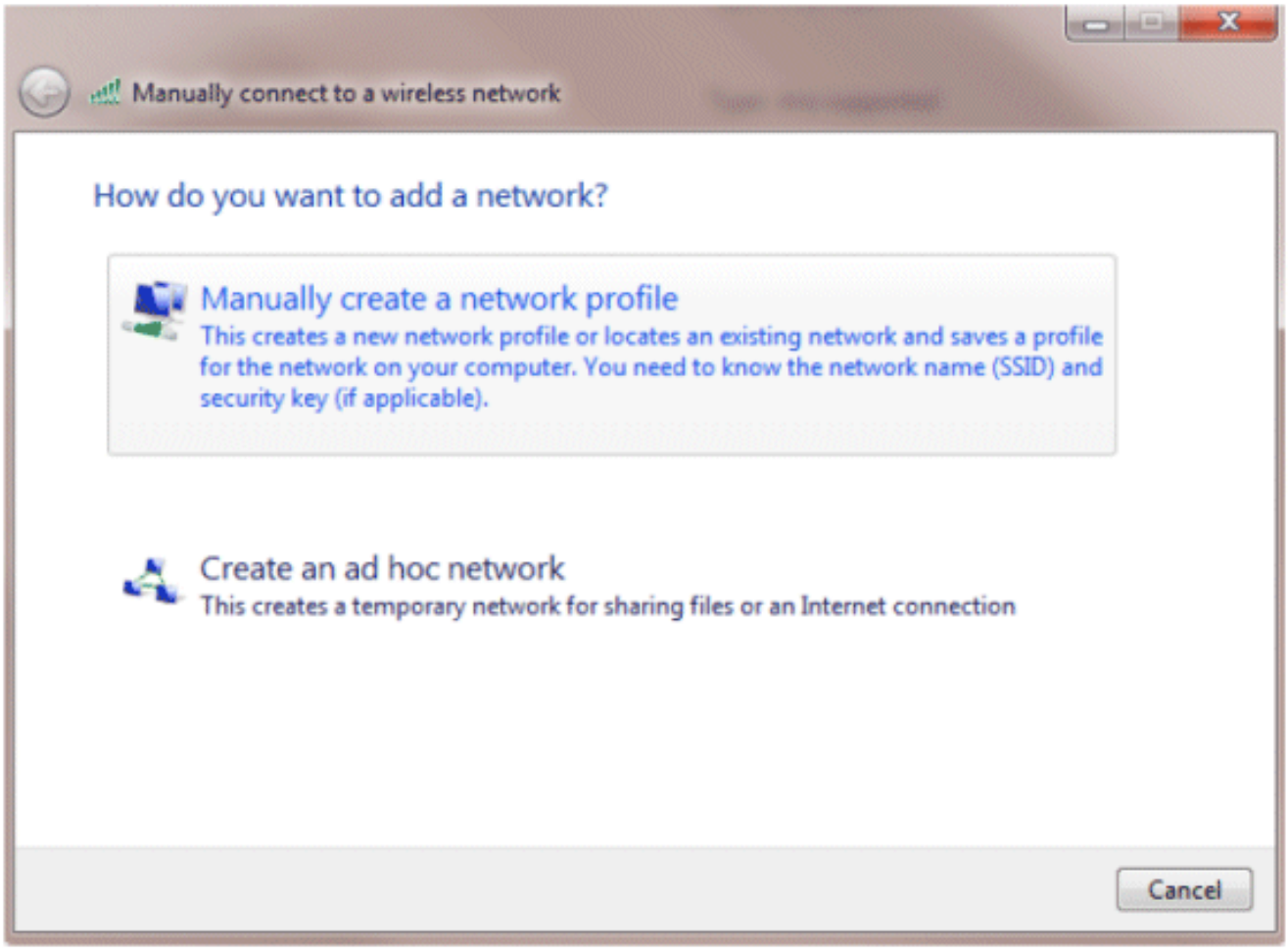
Seu utilitário Cliente está pronto para se conectar.

EAP-FAST (usuário2)

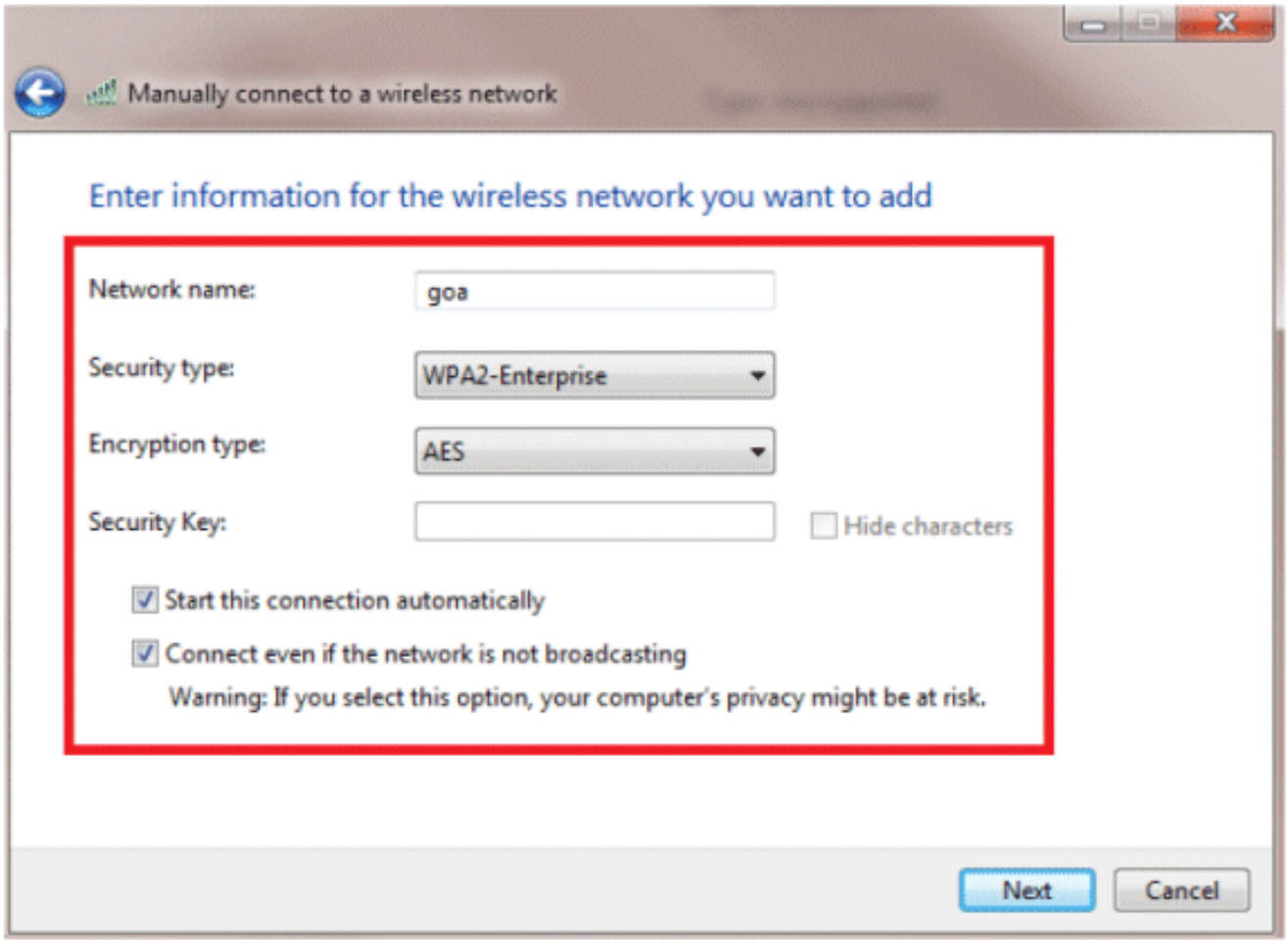
Em nosso cliente de teste, estamos usando o solicitante nativo do Windows 7 com uma placa Intel 6300-N executando a versão de driver 14.3. É recomendável testar usando os drivers mais recentes dos fornecedores.

Conclua estas etapas para criar um perfil no WZC:

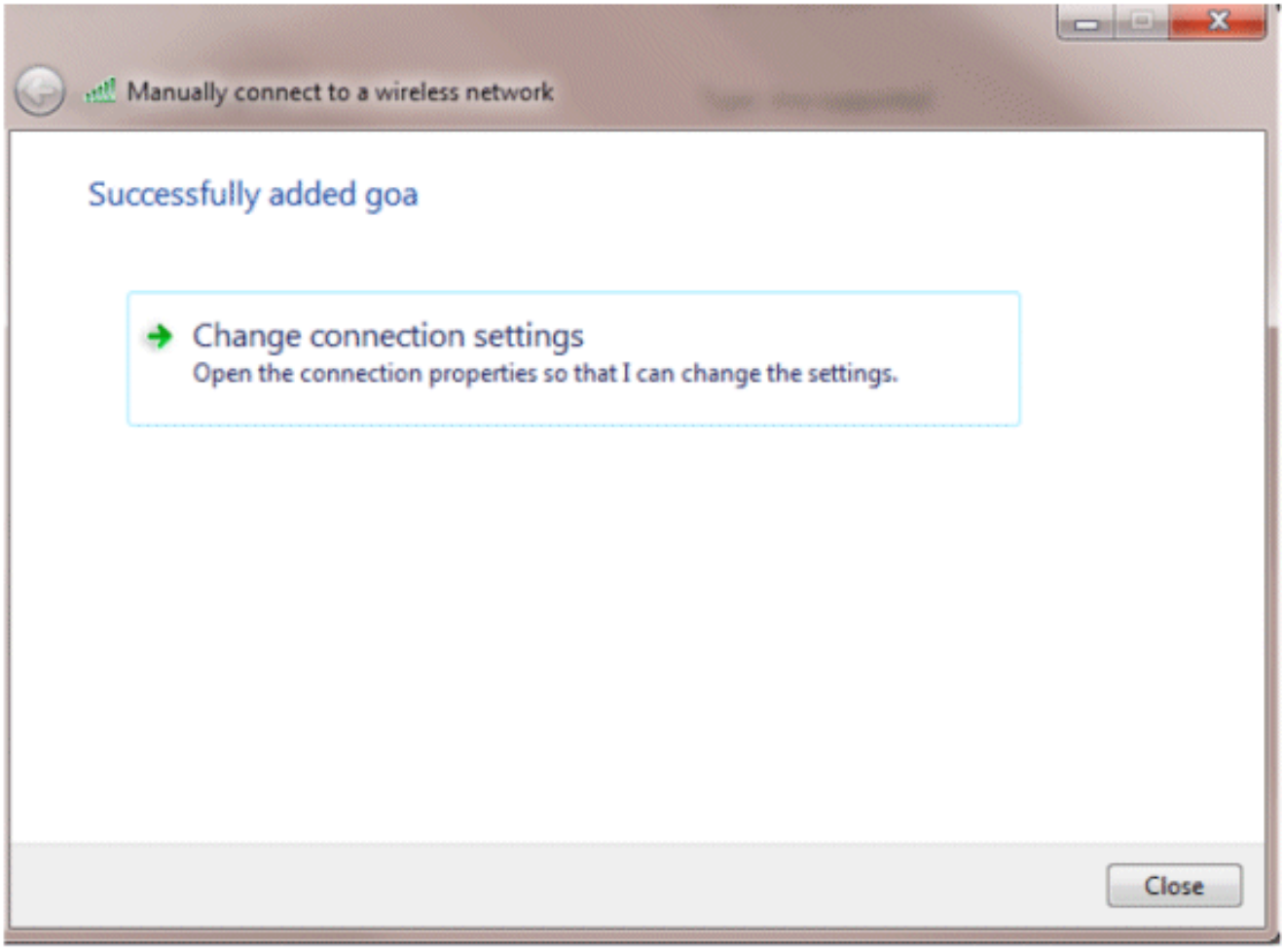
1. Vá para **Painel de controle > Rede e Internet > Gerenciar redes sem fio**.
2. Clique na guia **Add**.
3. Clique em **Criar manualmente um perfil de rede**.



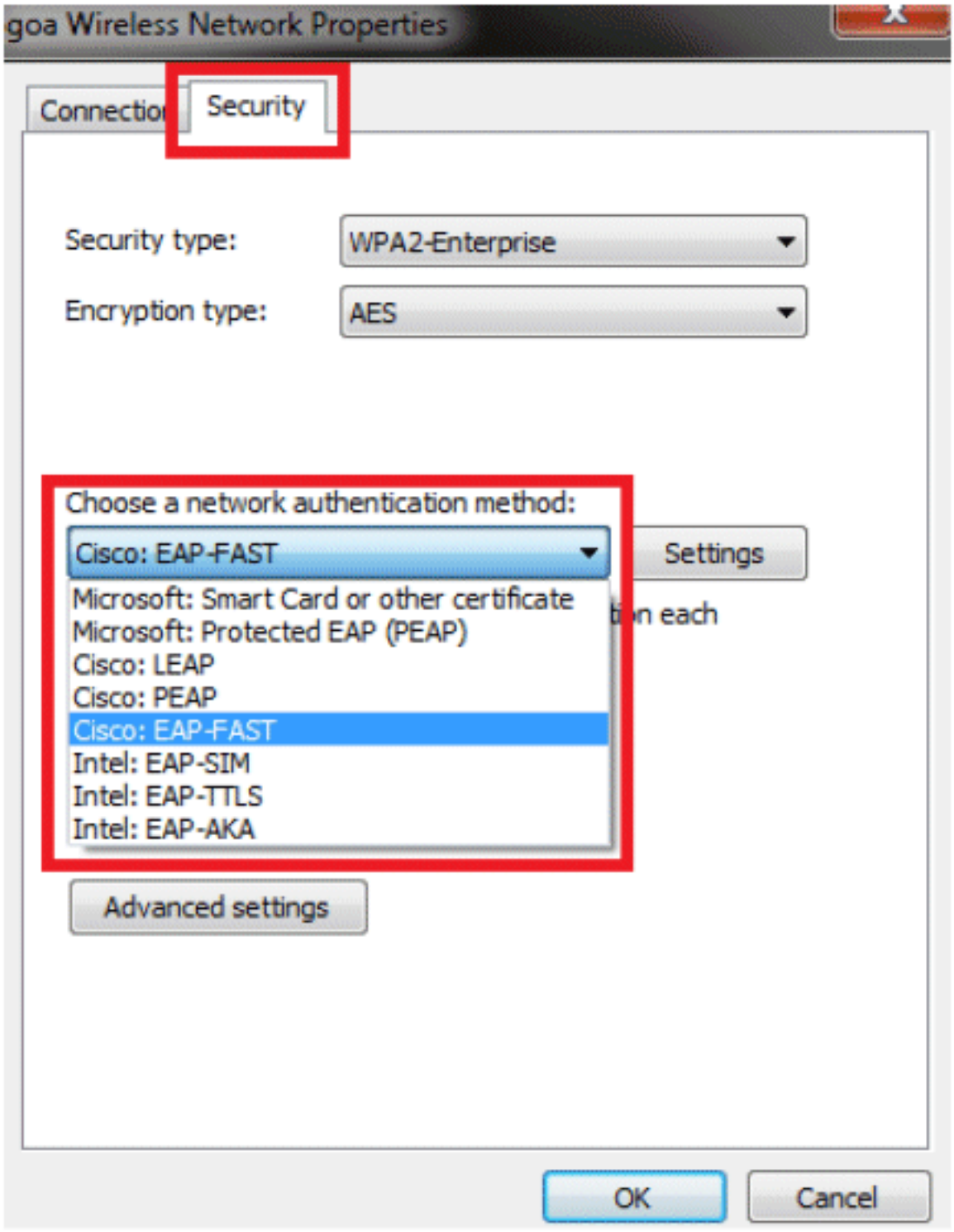
4. Adicione os detalhes conforme configurado na WLC.**Observação:** o SSID diferencia maiúsculas de minúsculas.
5. Clique em
   Next.



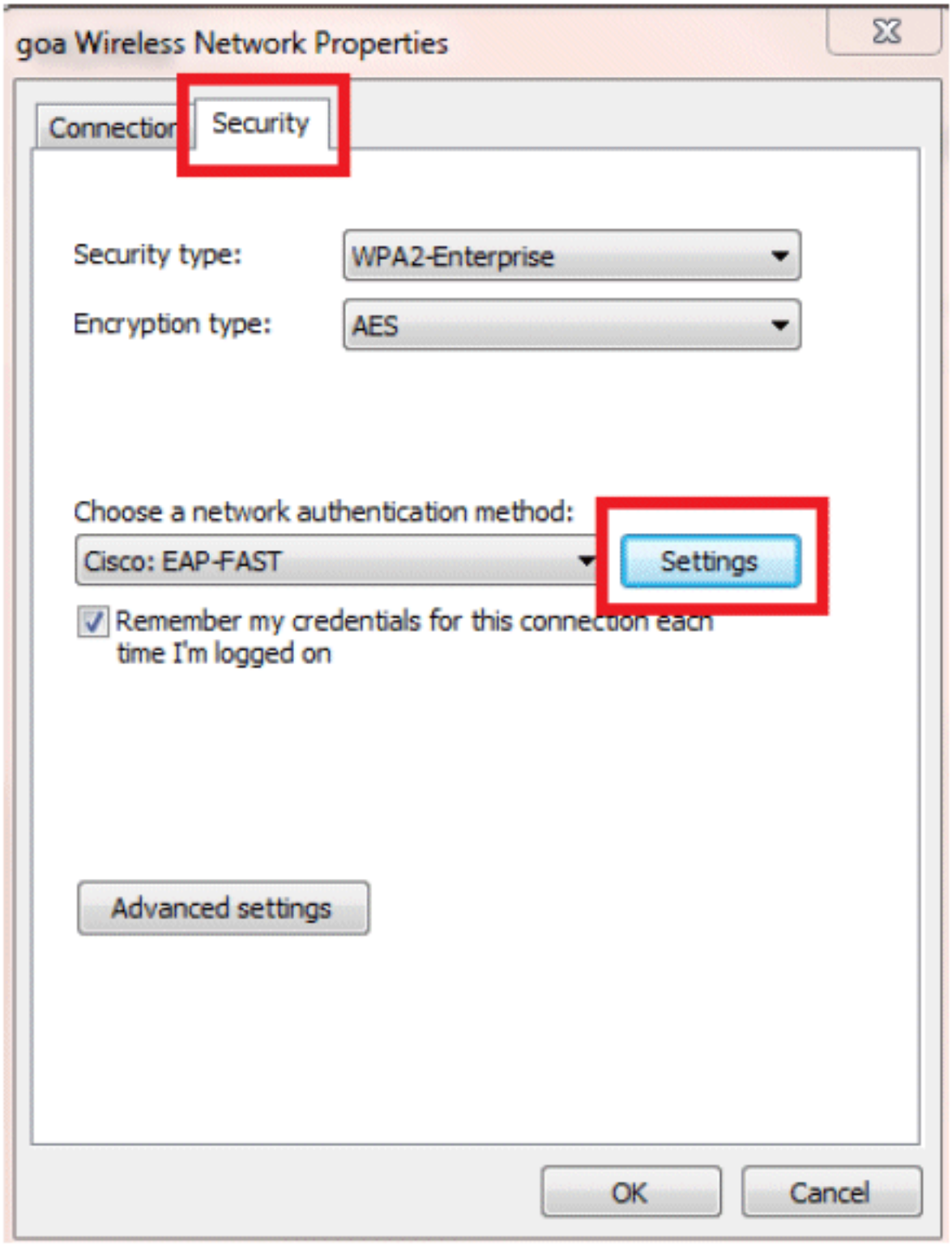
6. Clique em **Change connection settings** para verificar novamente as configurações.



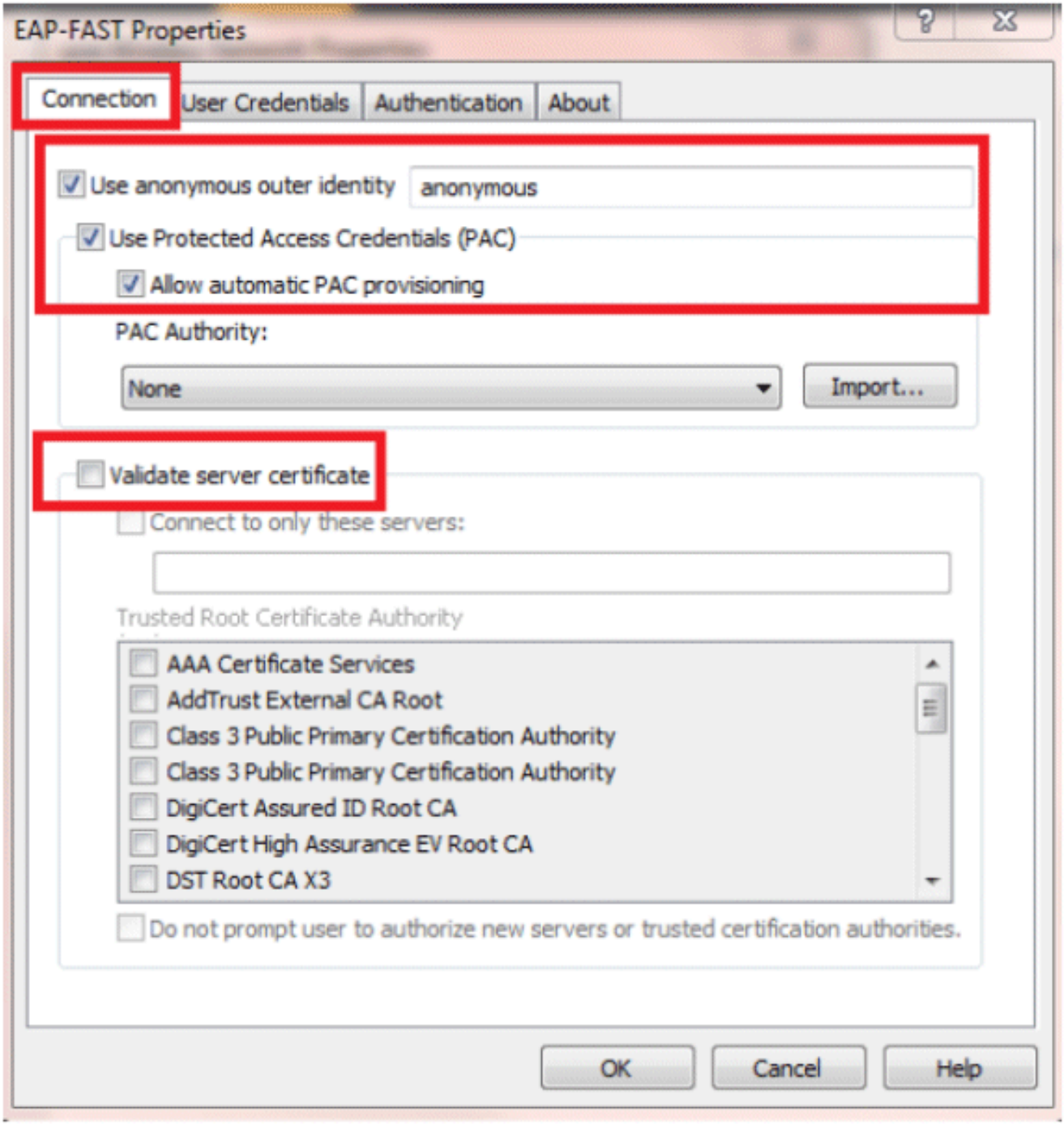
7. Verifique se o EAP-FAST está habilitado.**Observação:** por padrão, o WZC não tem EAP-FAST como um método de autenticação. Você precisa fazer o download do utilitário de um fornecedor terceirizado. Neste exemplo, como se trata de uma placa Intel, temos o Intel PROSet instalado no



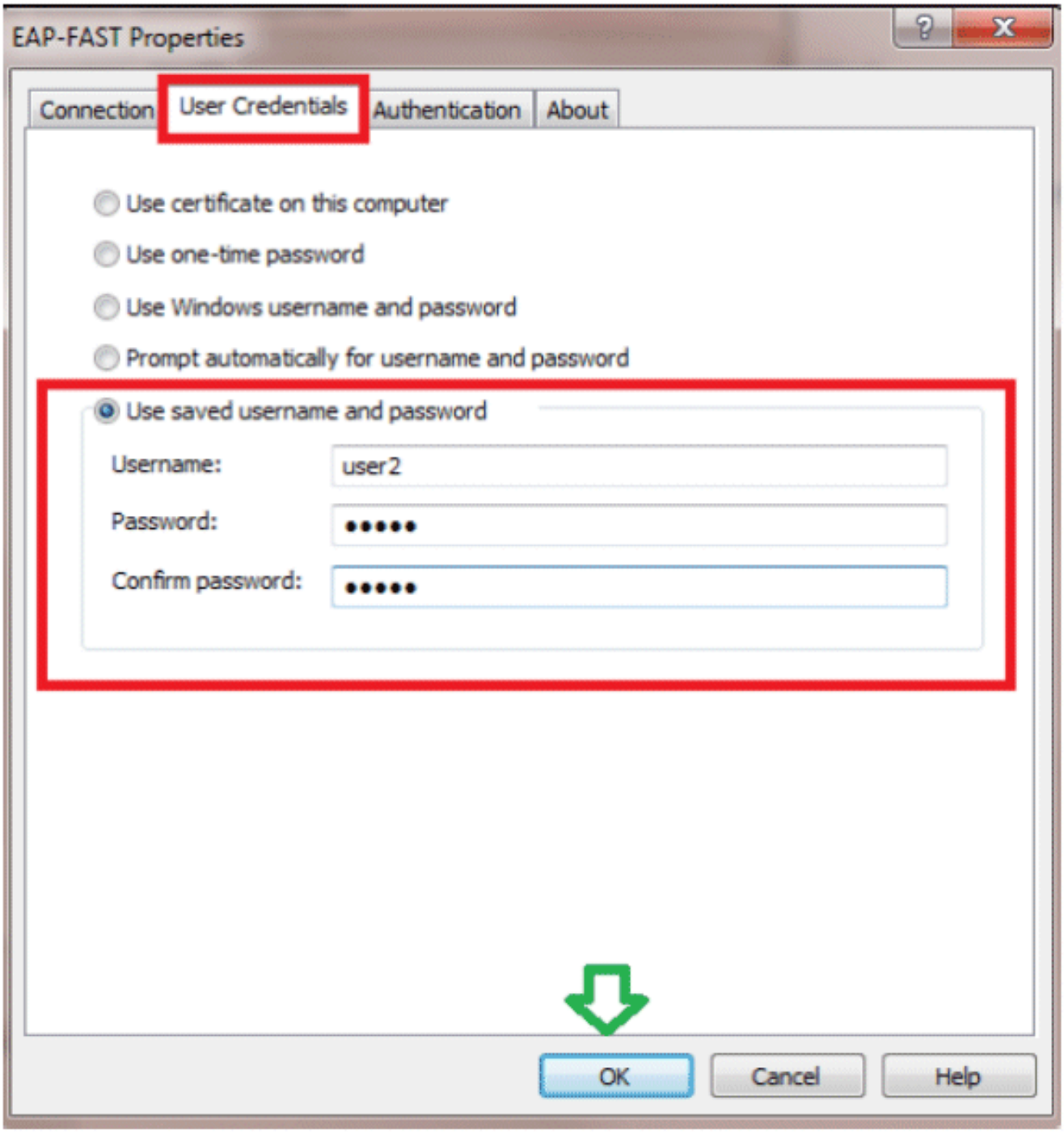
sistema.



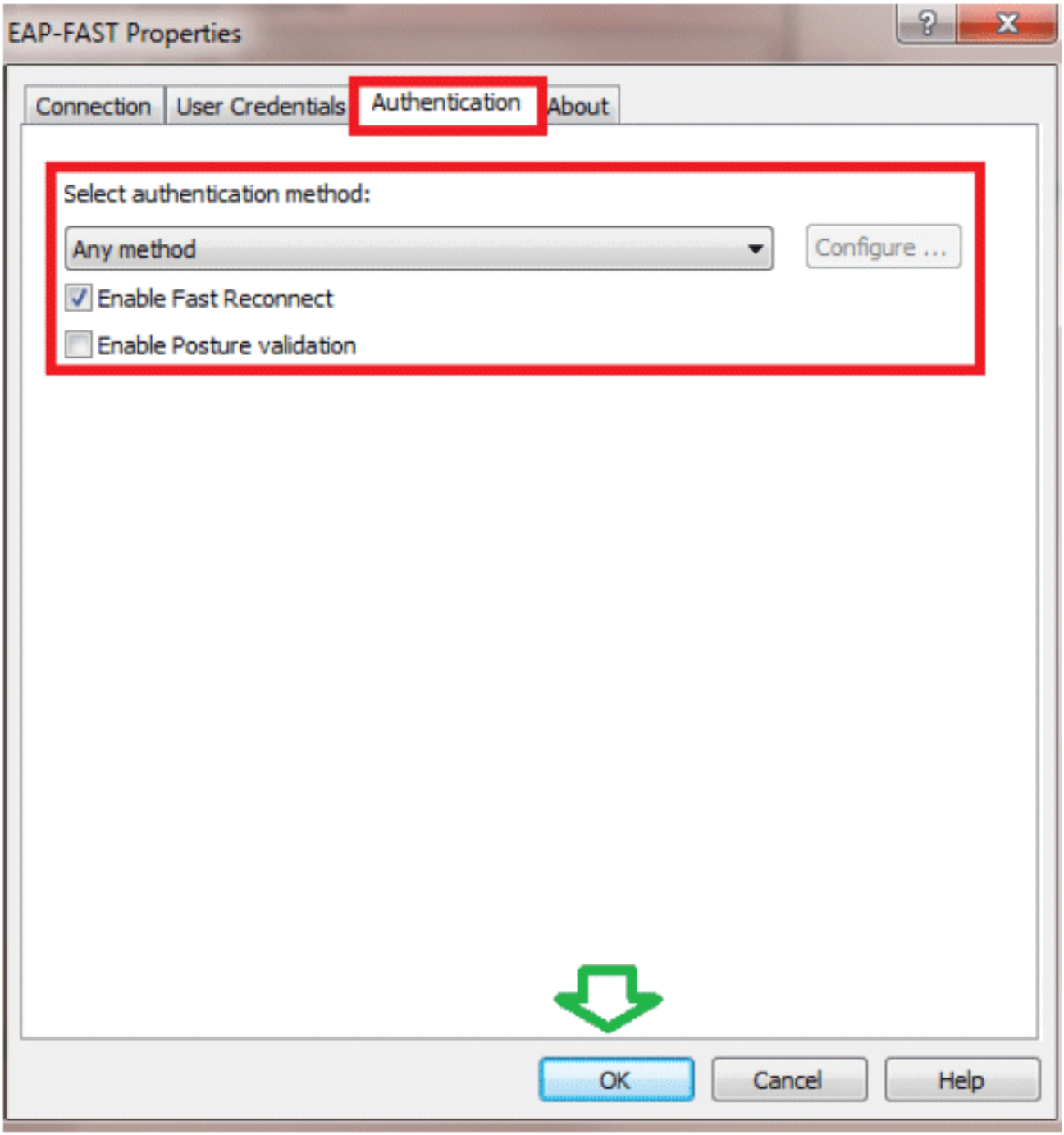
8. Habilite **Permitir fornecimento automático de PAC** e certifique-se de que **Validar certificado do servidor** esteja desmarcado.



9. Clique na guia **Credenciais do usuário** e insira as credenciais do usuário2. Como alternativa, você pode usar suas credenciais do Windows para fazer login. No entanto, neste exemplo, não vamos usar
isso.

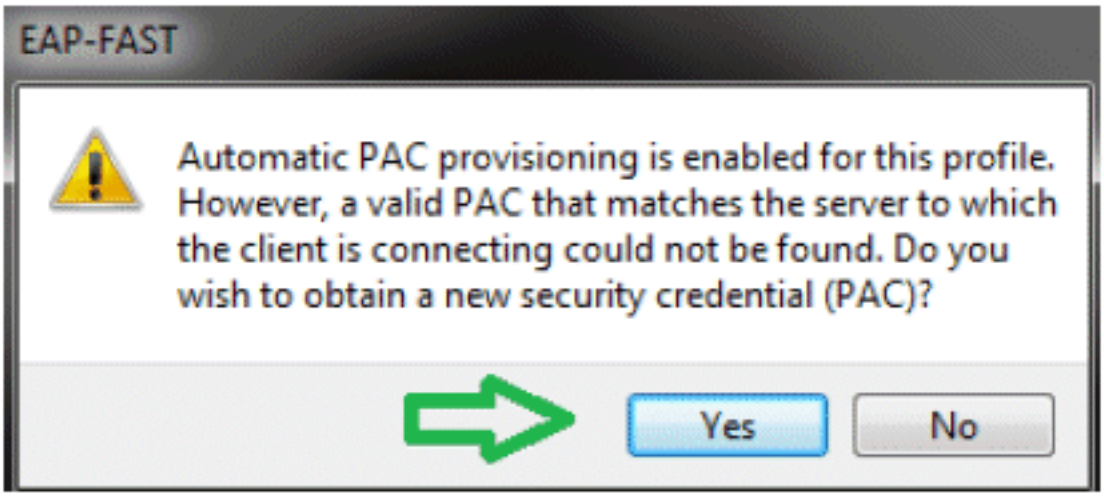

EAP-FAST Properties
Connection
User Credentials
Authentication
About
Use certificate on this computer
Use one-time password
Use Windows username and password
Prompt automatically for username and password
Use saved username and password
Username:
user2
Password:
Confirm password:
OK
Cancel
Help

10. Click **OK**.



Seu utilitário Cliente está pronto para conectar-se ao usuário2.

Observação: quando o usuário2 estiver tentando se autenticar, o servidor RADIUS enviará uma PAC. Aceite a PAC para concluir a autenticação.



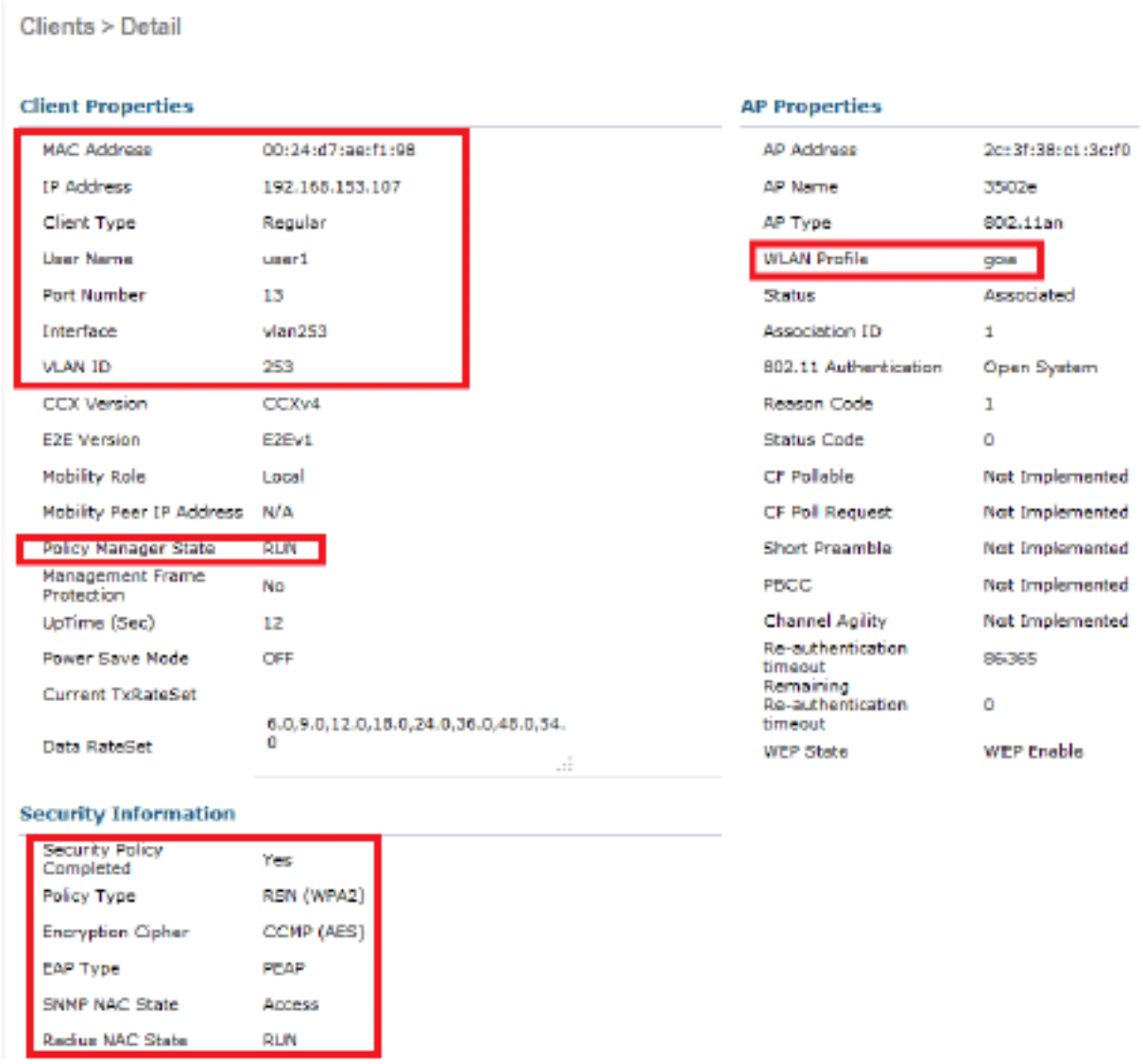
Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Verificar user1 (PEAP-MSCHAPv2)

Na GUI da WLC, vá para **Monitor** > **Clients** e selecione o endereço MAC.

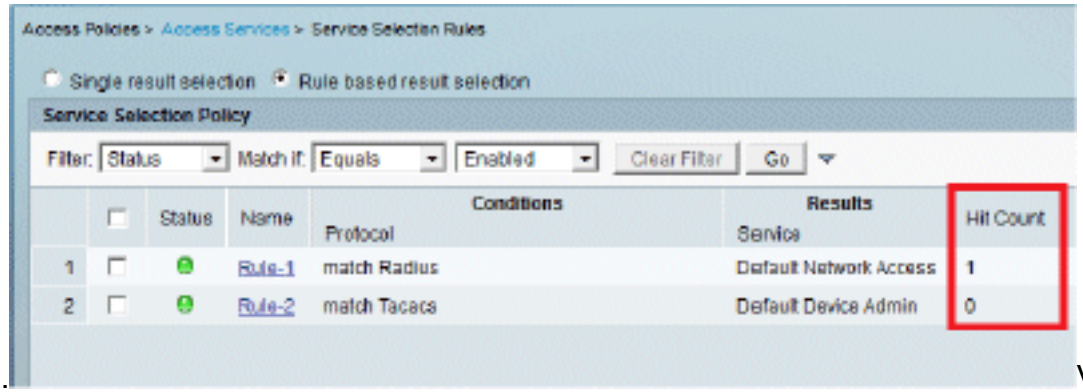


Estatísticas de RADIUS da WLC:

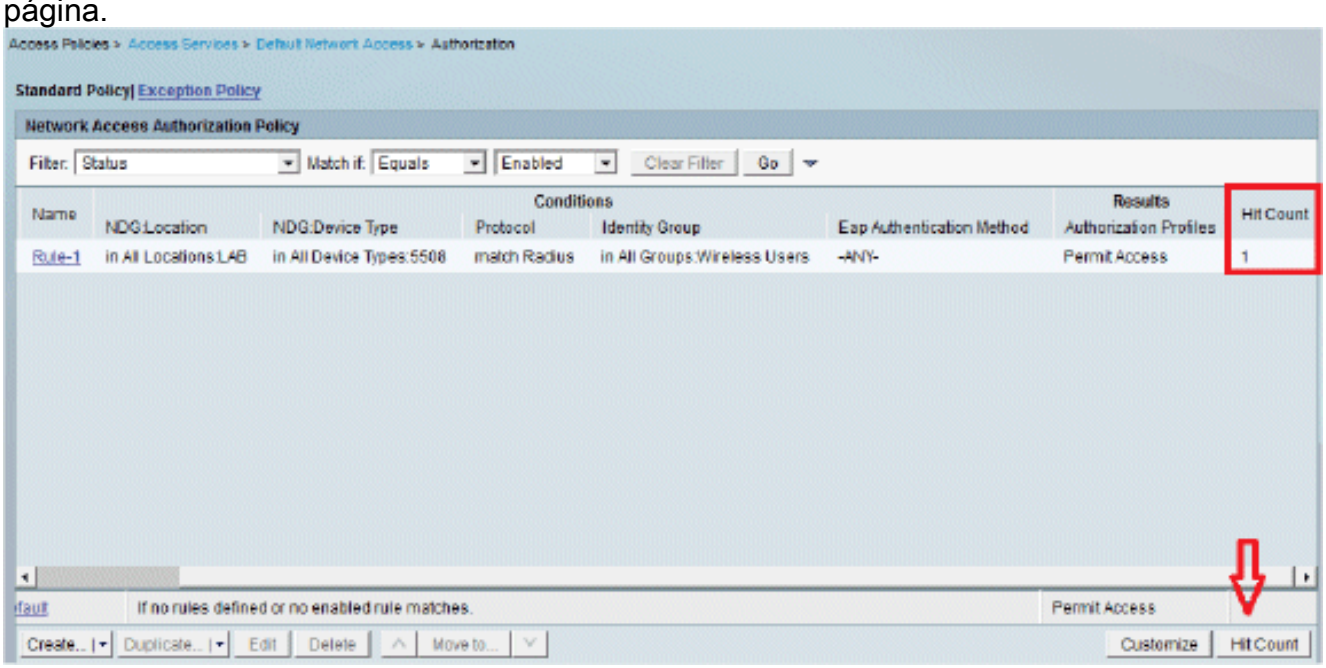
```
(Cisco Controller) >show radius auth statistics
Authentication Servers:
Server Index..................................... 1
Server Address................................... 192.168.150.24
Msg Round Trip Time.............................. 1 (msec)
First Requests................................... 8
Retry Requests................................... 0
Accept Responses................................. 1
Reject Responses................................. 0
Challenge Responses.............................. 7
Malformed Msgs................................... 0
Bad Authenticator Msgs........................... 0
Pending Requests................................. 0
Timeout Requests................................. 0
Unknowntype Msgs................................. 0
Other Drops...................................... 0
```

Logs ACS:

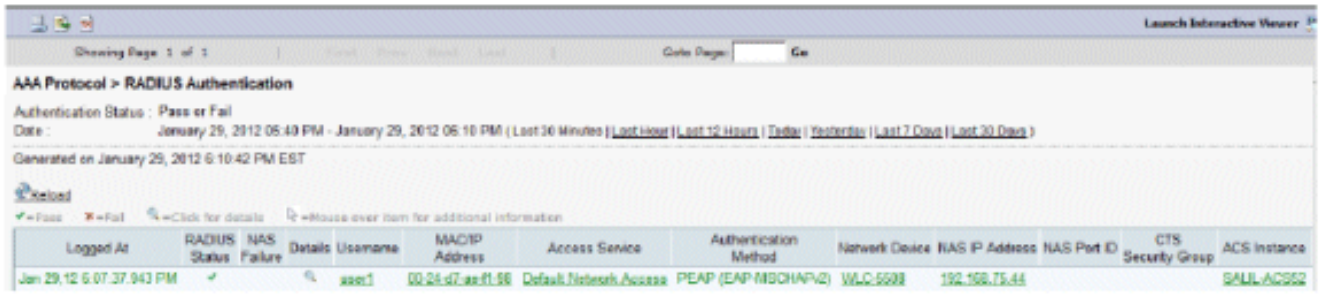
1. Conclua estes passos para visualizar as contagens de ocorrências:Se você verificar os logs dentro de 15 minutos da autenticação, certifique-se de atualizar a contagem de



ocorrências. Você tem uma guia para **contagem de ocorrências** na parte inferior da mesma página.



2. Clique em **Monitoring and Reports** e uma janela pop-up Nova será exibida. Vá para **Authentications -Radius -Today**. Você também pode clicar em **Detalhes** para verificar qual regra de seleção de serviço foi aplicada.



Verificar usuário2 (EAP-FAST)

Na GUI da WLC, vá para **Monitor > Clients** e selecione o endereço MAC.

Clients > Detail

Client Properties

MAC Address	00:24:d7:ae:f1:98
IP Address	192.168.153.111
Client Type	Regular
User Name	user2
Port Number	13
Interface	vlan253
VLAN ID	253
CCX Version	CCXv4
E2E Version	E2Ev1
Mobility Role	Local
Mobility Peer IP Address	N/A
Policy Manager State	RUN
Management Frame Protection	No
UpTime (Sec)	29
Power Save Mode	OFF
Current TxRateSet	m15
Data RateSet	6.0,9.0,12.0,18.0,24.0,36.0,48.0,54.0

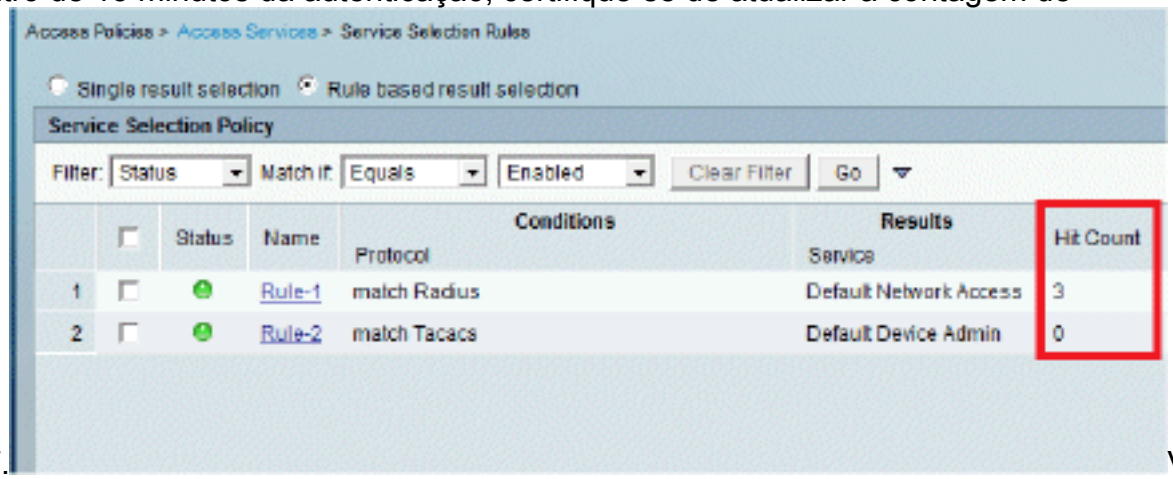
AP Properties

AP Address	2c:3f:38:c1:3c:f0
AP Name	3502e
AP Type	802.11an
WLAN Profile	goa
Status	Associated
Association ID	1
802.11 Authentication	Open System
Reason Code	1
Status Code	0
CF Pollable	Not Implemented
CF Poll Request	Not Implemented
Short Preamble	Not Implemented
PBCC	Not Implemented
Channel Agility	Not Implemented
Re-authentication timeout	86392
Remaining Re-authentication timeout	0
WEP State	WEP Enable

Security Information

Security Policy Completed	Yes
Policy Type	RSN (WPA2)
Encryption Cipher	CCMP (AES)
EAP Type	EAP-FAST
SNMP NAC State	Access
Radius NAC State	RUN

Logs ACS:

1. Conclua estes passos para visualizar as contagens de ocorrências:Se você verificar os logs dentro de 15 minutos da autenticação, certifique-se de atualizar a contagem de HIT. 
Access Policies > Access Services > Service Selection Rules

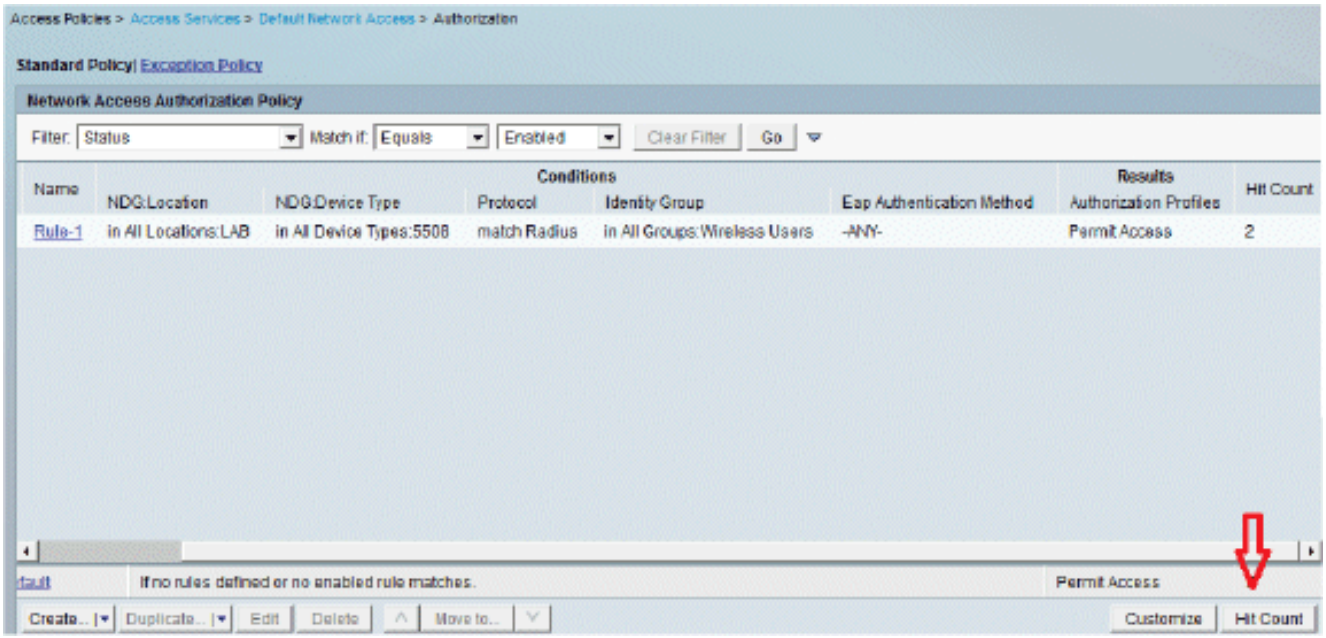
Single result selection Rule based result selection

Service Selection Policy

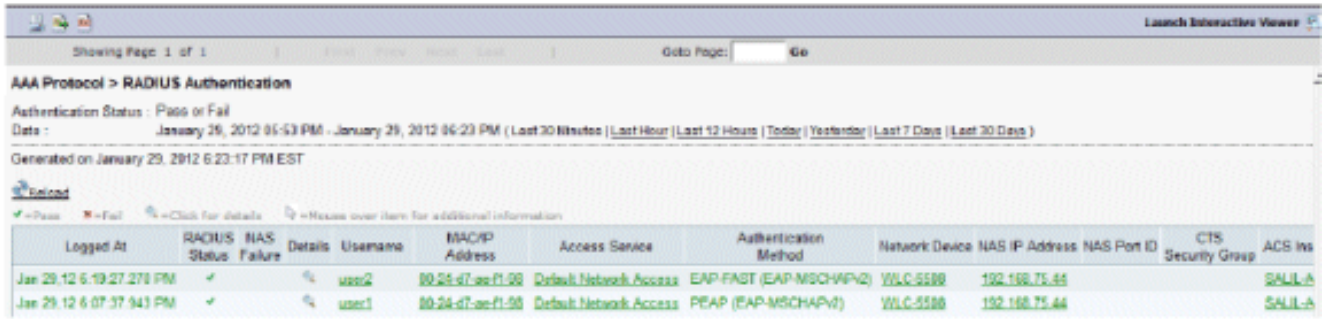
Filter: Status Match if: Equals Enabled Clear Filter Go

		Status	Name	Conditions: Protocol	Results: Service	Hit Count
1			Rule-1	match Radius	Default Network Access	3
2			Rule-2	match Tacacs	Default Device Admin	0

Você tem uma guia para **contagem de ocorrências** na parte inferior da mesma página.



2. Clique em **Monitoring and Reports** e uma janela pop-up Nova será exibida. Vá para **Authentications -Radius -Today**. Você também pode clicar em **Detalhes** para verificar qual regra de seleção de serviço foi aplicada.



Troubleshoot

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Comandos para Troubleshooting

A Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Nota:Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos debug.

1. Se você tiver algum problema, emita estes comandos no WLC:**debug client** ***<mac add of the client>*****debug aaa all enableshow client detail** ***<mac addr>*** **- Verifique o estado do gerenciador de políticas.show radius auth statistics** - Verifique o motivo da falha.**debug disable-all** - Desativa as depurações.**clear stats radius auth all** - Limpar estatísticas de raio no WLC.
2. Verifique os registros no ACS e anote o motivo da falha.

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.