Configurar a atribuição de VLAN dinâmica com WLCs com base no ISE para o mapa de grupo do Ative Diretory

Contents

Introdução

Este documento descreve o conceito de atribuição de VLAN dinâmica.

Pré-requisitos

O documento descreve como configurar a controladora Wireless LAN (WLC) e o servidor Identity Services Engine (ISE) para atribuir dinamicamente clientes Wireless LAN (WLAN) a uma VLAN específica.

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico de controladores de LAN sem fio (WLCs) e pontos de acesso leves (LAPs)
- Conhecimento funcional de um servidor AAA (Authentication, Authorization, and Accounting), como um ISE

- Conhecimento completo da rede Wireless e problemas de segurança Wireless
- Conhecimento funcional e configurável da atribuição de VLAN dinâmica
- Entendimento básico dos serviços do Microsoft Windows AD, bem como dos conceitos de controlador de domínio e DNS
- Ter conhecimento básico de Controle e Provisionamento do Protocolo de Ponto de Acesso (CAPWAP)

Componentes Utilizados

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

- Cisco 5520 Series WLC que executa o firmware versão 8.8.111.0
- AP Cisco 4800 Series
- Suplicante nativo do Windows e NAM do Anyconnect
- Cisco Secure ISE versão 2.3.0.298
- Microsoft Windows 2016 Server configurado como um controlador de domínio
- Switch Cisco 3560-CX Series que executa a versão 15.2(4)E1

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Conventions

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

Atribuição da VLAN (Rede local virtual) dinâmica com servidor Radius

Na maioria de sistemas de WLAN, cada WLAN tem uma política estática que se aplica a todos os clientes associados com um Service Set Identifier (SSID), ou o WLAN na terminologia do controlador. Embora poderoso, este método tem limitações porque exige que os clientes se associem com os diferentes SSID para herdar diferentes QoS e políticas de segurança.

A solução WLAN da Cisco trata dessa limitação através do suporte à rede de identidade. Isso permite que a rede anuncie um único SSID, mas permite que usuários específicos herdem diferentes QoS, atributos de VLAN e/ou políticas de segurança com base na credencial do usuário.

A atribuição da VLAN dinâmica é um recurso que coloca um usuário wireless em uma VLAN específica baseado nas credenciais fornecidas pelo usuário. Essa tarefa de atribuir usuários a uma VLAN específica é realizada por um servidor de autenticação RADIUS, como o Cisco ISE. Isso pode ser usado, por exemplo, para permitir que o host sem fio permaneça na mesma VLAN à medida que se move dentro de uma rede de campus.

O servidor Cisco ISE autentica usuários sem fio em um dos vários bancos de dados possíveis, o que inclui seu banco de dados interno. Por exemplo:

- BD interno
- Diretório ativo
- LDAP (Lightweight Diretory Access Protocol) genérico
- Bancos de dados relacionais compatíveis com ODBC (Open Database Connectivity)
- Servidores de token SecurID Rivest, Shamir e Adelman (RSA)
- Servidores de token compatíveis com RADIUS

Os protocolos de autenticação do Cisco ISE e as fontes de identidade externas suportadas listam os vários protocolos de autenticação suportados pelos bancos de dados internos e externos do ISE.

Este documento se concentra na autenticação de usuários sem fio que usam o banco de dados externo do Windows Ative Diretory.

Após a autenticação bem-sucedida, o ISE recupera as informações de grupo desse usuário do banco de dados do Windows e associa o usuário ao respectivo perfil de autorização.

Quando um cliente tenta se associar a um LAP registrado com um controlador, o LAP passa as credenciais do usuário para o WLC com a ajuda do respectivo método EAP.

A WLC envia essas credenciais ao ISE com o uso do protocolo RADIUS (encapsulando o EAP) e o ISE passa as credenciais dos usuários ao AD para validação com a ajuda do protocolo KERBEROS.

O AD valida as credenciais do usuário e, após a autenticação bem-sucedida, informa o ISE.

Uma vez que a autenticação seja bem-sucedida, o servidor ISE passa determinados atributos da Internet Engineering Task Force (IETF) para a WLC. Esses atributos RADIUS decidem a ID da VLAN que deve ser atribuída ao cliente sem fio. A SSID (WLAN, em termos do WLC) do cliente não importa porque o usuário sempre recebe esta identificação predeterminada da VLAN.

Os atributos do usuário do RADIUS usados para a atribuição de ID da VLAN são:

- IETF 64 (tipo de túnel)—Defina isso como VLAN
- IETF 65 (tipo de meio de túnel)—Defina como 802

- IETF 81 (ID do grupo privado do túnel)—Defina como VLAN ID

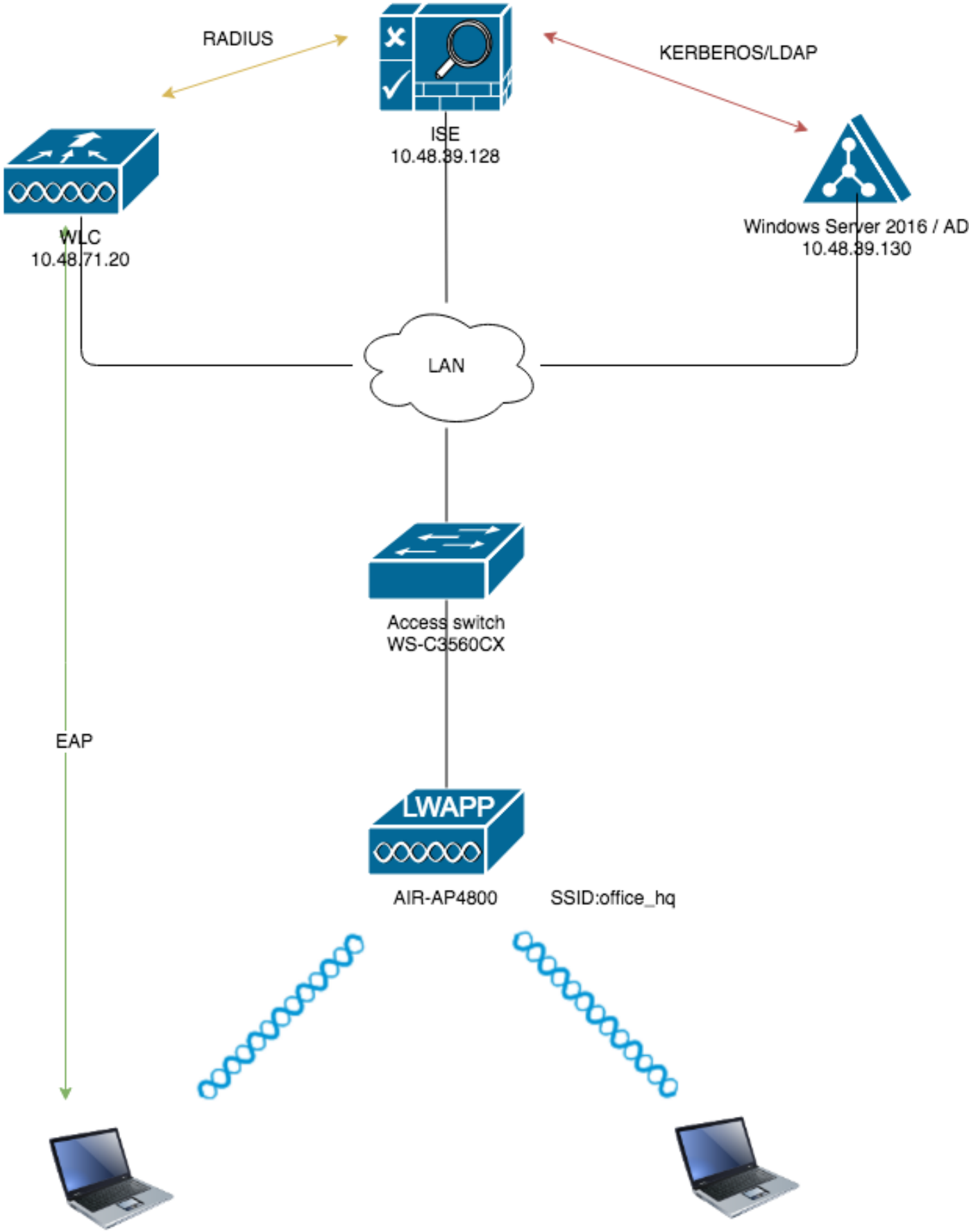
O ID da VLAN tem 12 bits e tem um valor entre 1 e 4094, inclusive. Como Tunnel-Private- Group-ID é do tipo string, conforme definido em RFC2868 para uso com IEEE 802.1X, o valor inteiro da ID da VLAN é codificado como uma string. Quando estes atributos de túnel são enviados, é necessário preencher o campo Tag.

Como observado no RFC 2868, seção 3.1: o campo Tag tem um octeto de comprimento e tem a intenção de fornecer um meio de agrupar atributos no mesmo pacote que se referem ao mesmo túnel. Os valores válidos para este campo são de 0x01 a 0x1F, inclusive. Se o campo Tag não for utilizado, ele deve ser zero (0x00). Consulte na RFC 2868 mais informações sobre todos os atributos de RADIUS.

Configurar

Esta seção fornece as informações necessárias para configurar os recursos descritos no documento.

Diagrama de Rede

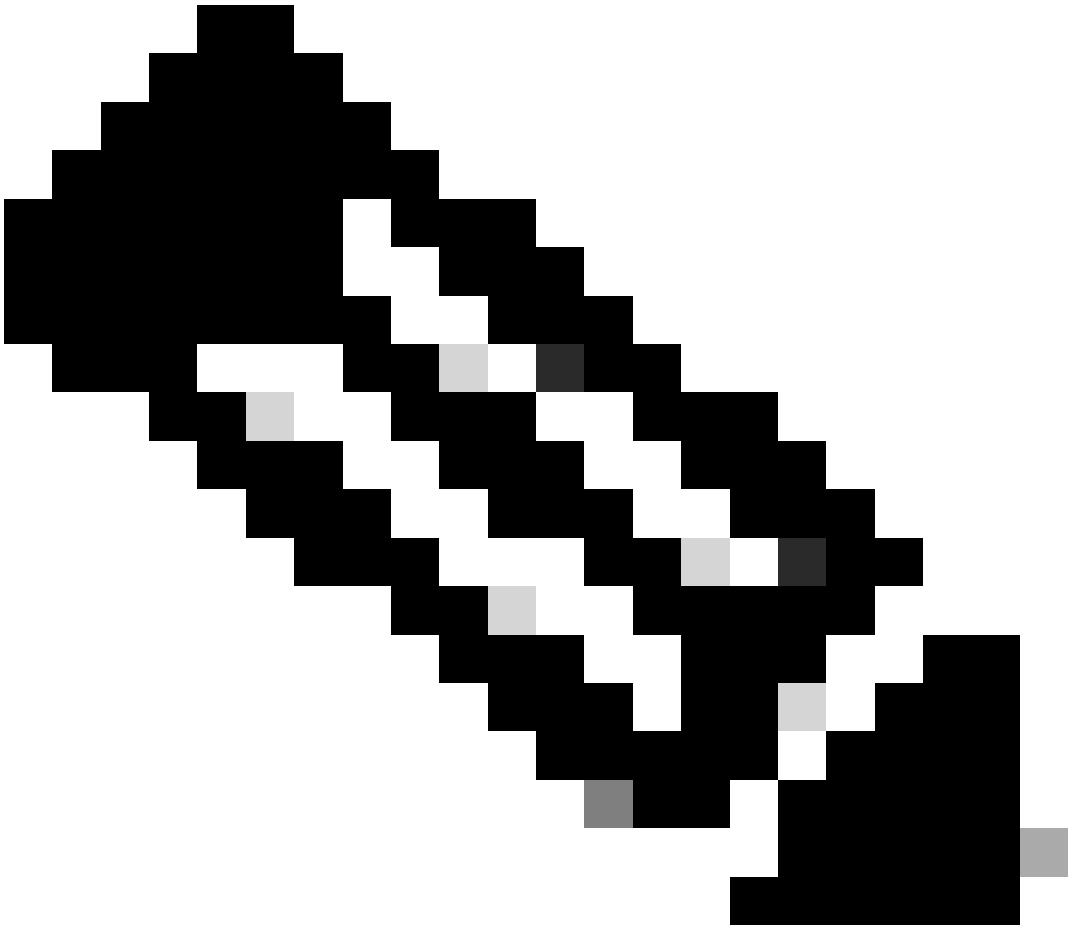


Configurações

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

- O endereço IP do servidor ISE (RADIUS) é 10.48.39.128.
- O endereço da interface do gerenciador de AP e gerenciamento do WLC é 10.48.71.20.
- O servidor DHCP reside na rede LAN e é configurado para os respectivos pools de clientes; ele não é mostrado no diagrama.
- VLAN1477 e VLAN1478 são usados em toda essa configuração. Os usuários do departamento Marketing são configurados para serem colocados na VLAN1477 e os usuários do departamento HR são configurados para serem colocados na VLAN1478 pelo servidor RADIUS quando ambos os usuários se conectam ao mesmo SSID — office_hq.

  VLAN1477: 192.168.77.0/24. Gateway: 192.168.77.1 VLAN1478: 192.168.78.0/24. Gateway: 192.168.78.1
- Este documento usa 802.1x com PEAP-mschapv2 como o mecanismo de segurança.



Observação: a Cisco recomenda que você use métodos de autenticação avançados, como a autenticação EAP-FAST e EAP-TLS, para proteger a WLAN.

Estas suposições são feitas antes de você executar esta configuração:

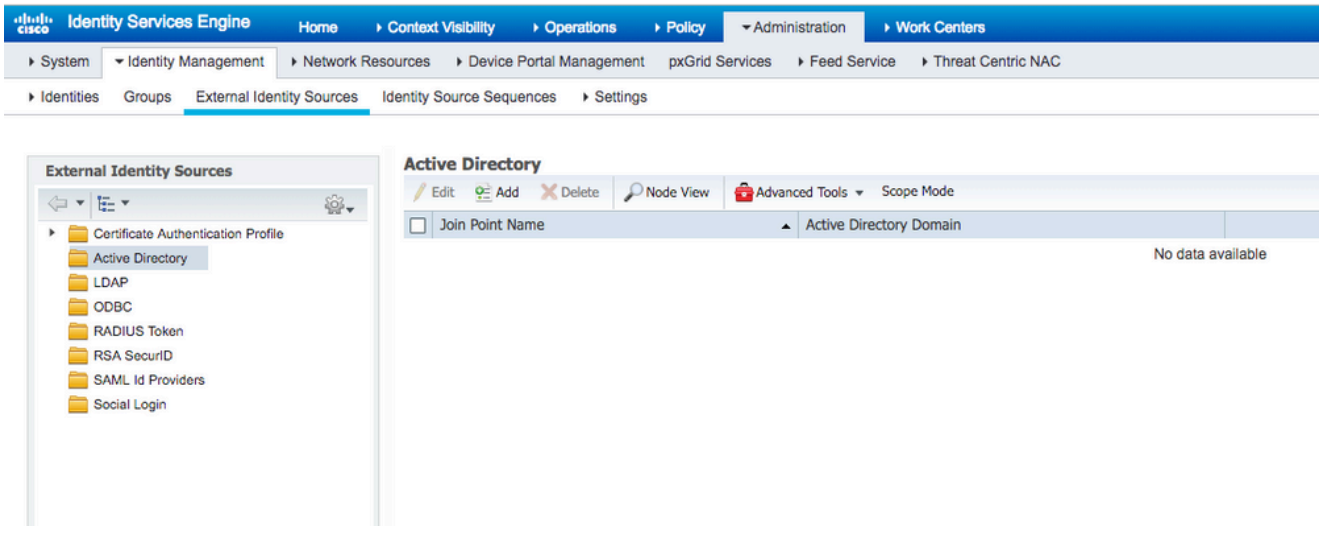
- O LAP já está registrado com o WLC
- O servidor DHCP recebe um escopo DHCP
- Existe conectividade de Camada 3 entre todos os dispositivos na rede
- O documento discute a configuração necessária no lado sem fio e supõe que a rede com fio está no lugar
- Os respectivos usuários e grupos são configurados no AD

Para realizar a atribuição de VLAN dinâmica com WLCs baseadas no mapeamento de grupo ISE para AD, estas etapas devem ser executadas:

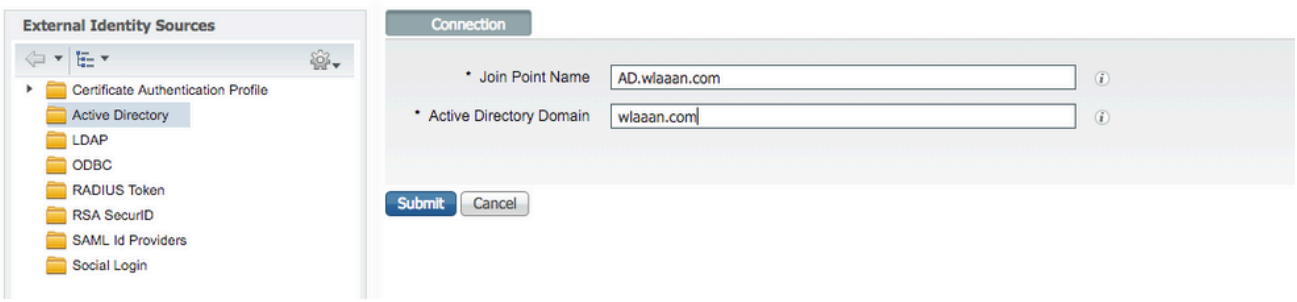
1. Integração de ISE para AD e configuração de políticas de autenticação e autorização para usuários no ISE.
2. Configuração da WLC para dar suporte à autenticação dot1x e à substituição de AAA para o SSID 'office_hq'.
3. Configuração do suplicante do cliente final.

Integração de ISE para AD e configuração de políticas de autenticação e autorização para usuários no ISE

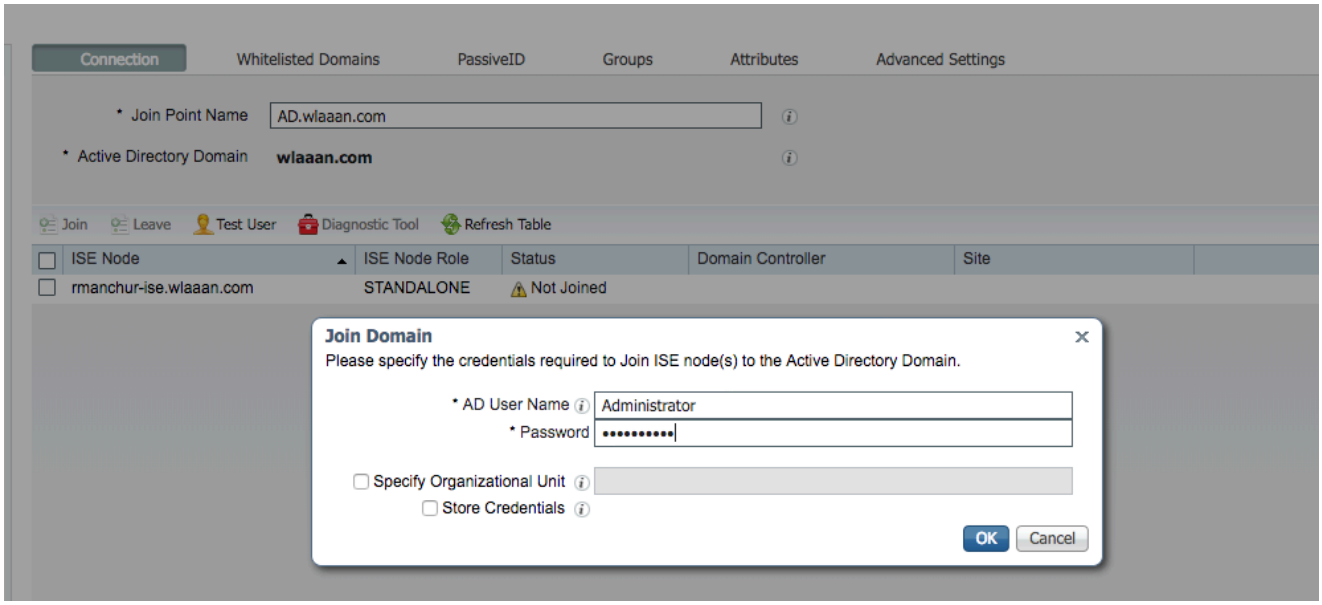
1. Faça login na interface de interface de usuário da Web do ISE usando uma conta admin.
2. Navegue até Administration > Identity management > External Identity Sources > Active directory.



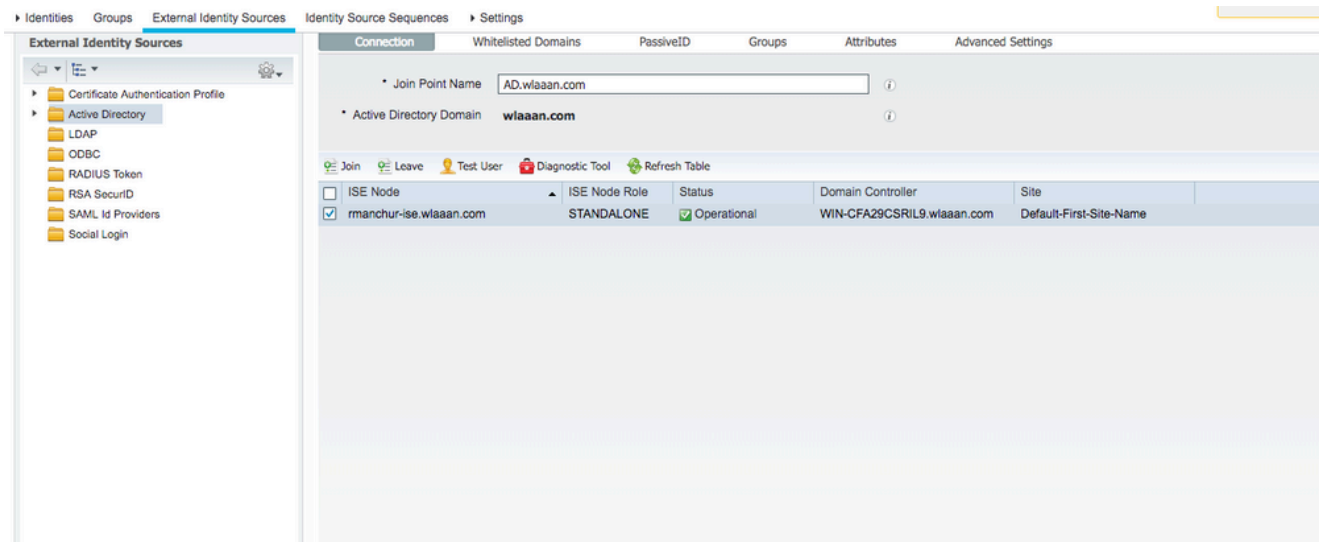
3. Clique em Adicionar e insira o nome do domínio e o nome do armazenamento de identidade nas configurações de Nome do ponto de ingresso do Ative Diretory. No exemplo, o ISE é registrado no domíniowlaaan.come joinpoint é especificado comoAD.wlaaan.com- nome localmente significativo para ISE.



4. Uma janela pop-up será aberta depois queSubmito botão for pressionado perguntando se você deseja ingressar no ISE para o AD imediatamente. PressioneYese forneça as credenciais de usuário do Ative Diretory com direitos de administrador para adicionar um novo host ao domínio.



5. Depois desse ponto, você deve ter o ISE registrado com êxito no AD.



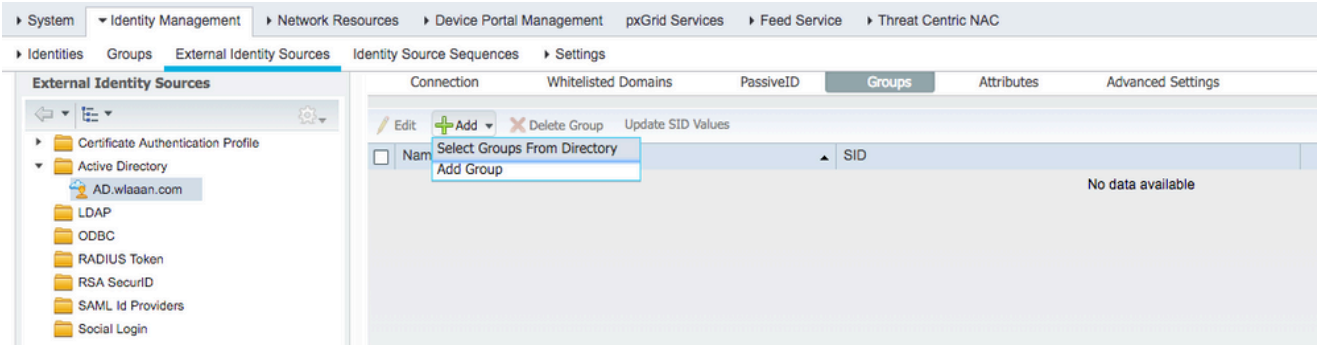
Caso tenha algum problema com o processo de registro, você pode usar oDiagnostic Tool para

executar os testes necessários para a conectividade do AD.

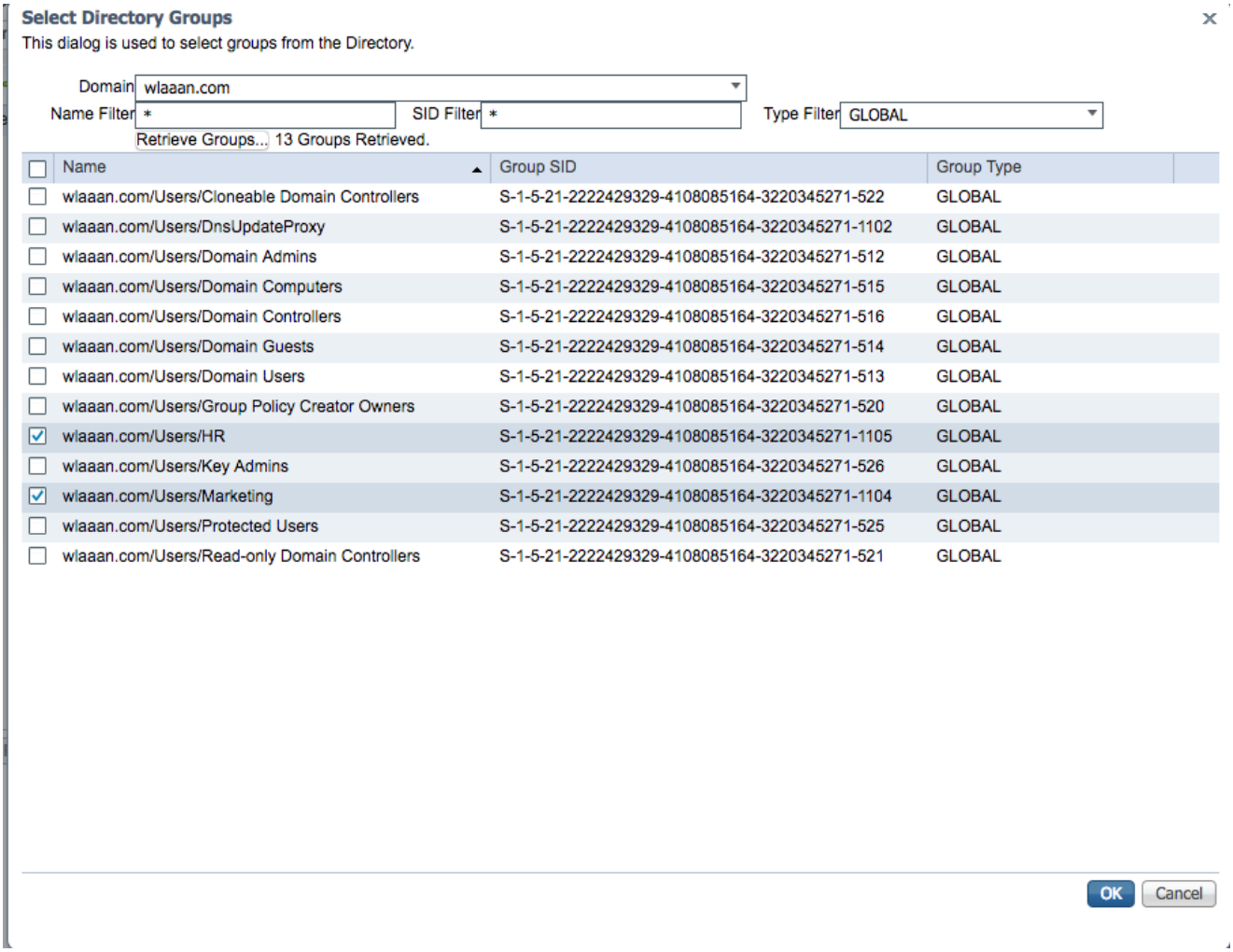
6. Você deve recuperar grupos para os Ative Directories que são usados para atribuir os respectivos perfis de autorização. Navegue atéAdministration > Identity management > External Identity Sources > Active directory >

> Groups

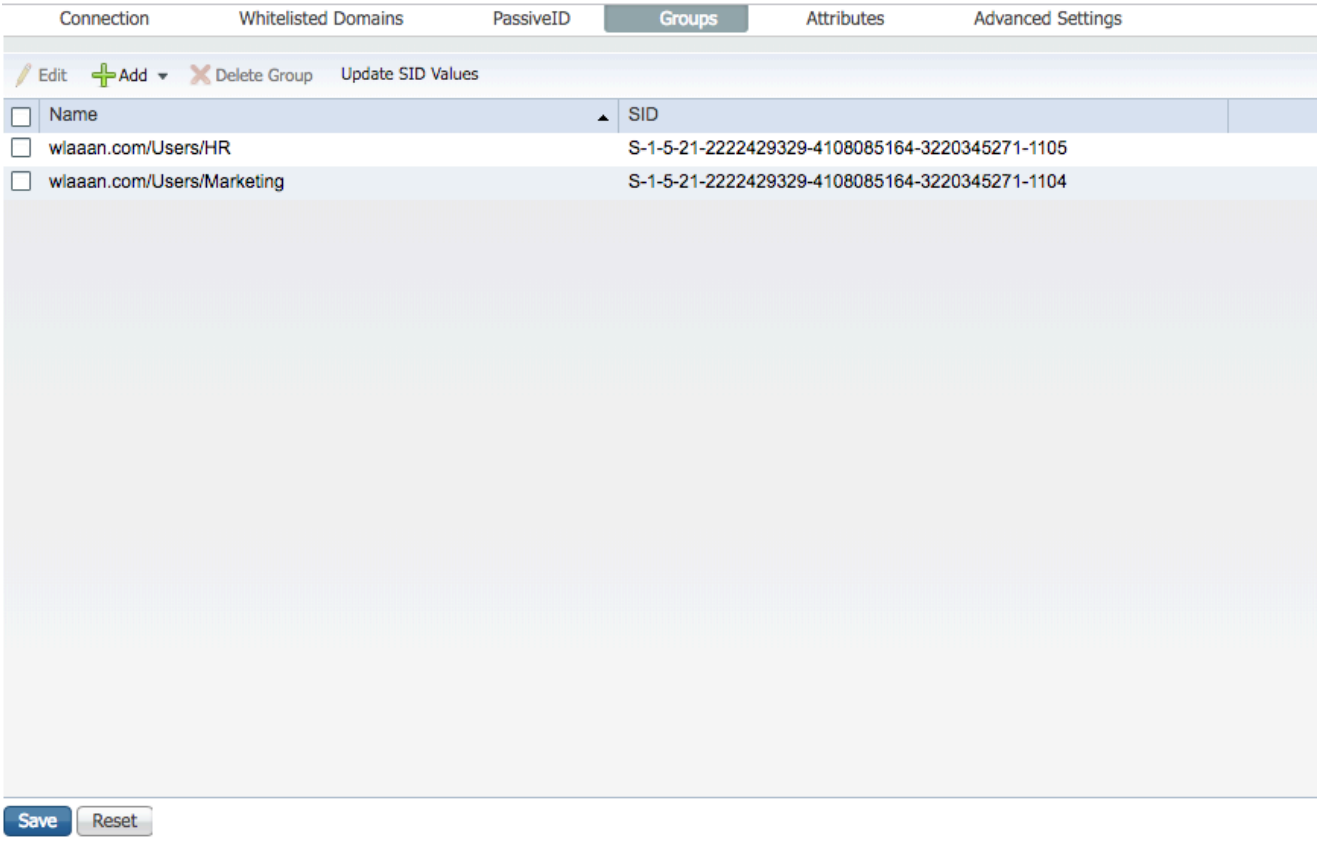
, clique emAdde escolhaSelect Groups from Active Directory.



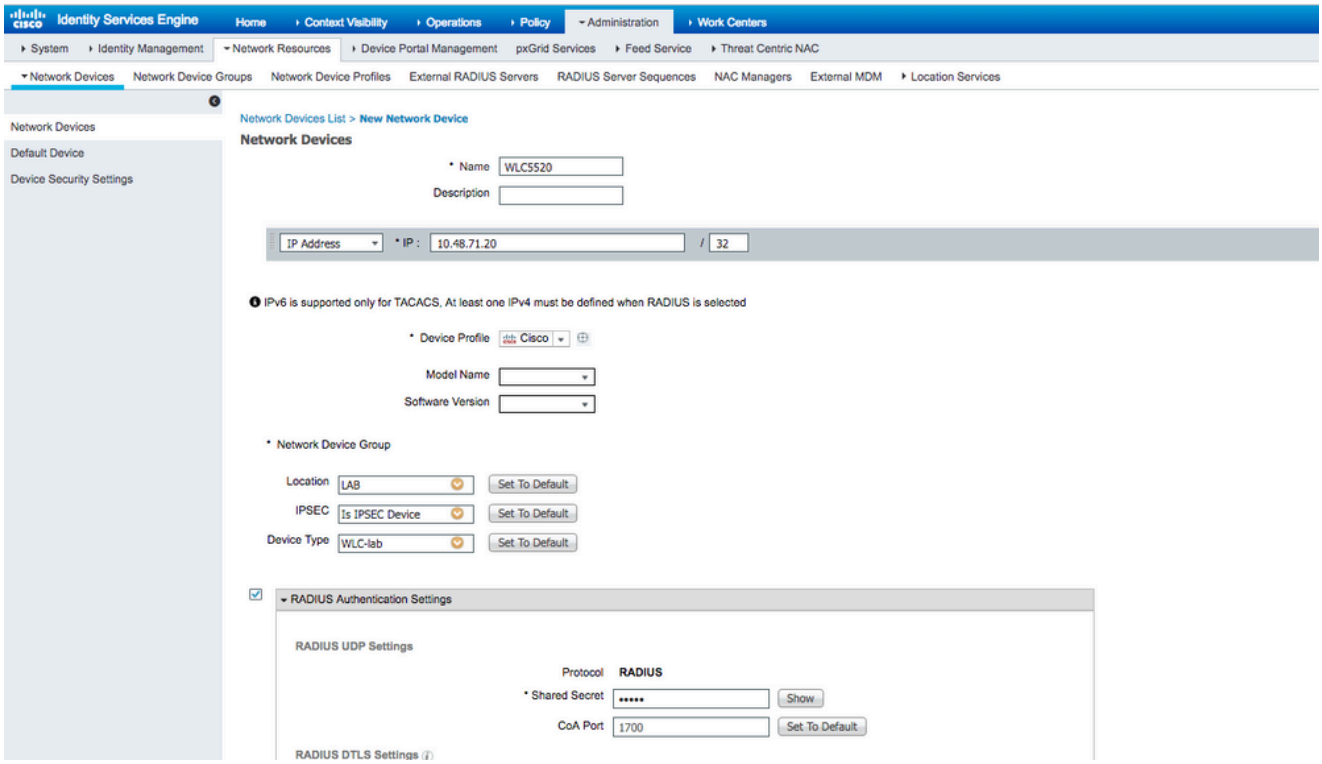
7. Uma nova janela pop-up é aberta, na qual você pode especificar um filtro para recuperar grupos específicos ou recuperar todos os grupos do AD.
   Escolha os respectivos grupos na lista de grupos do AD e pressioneOK.



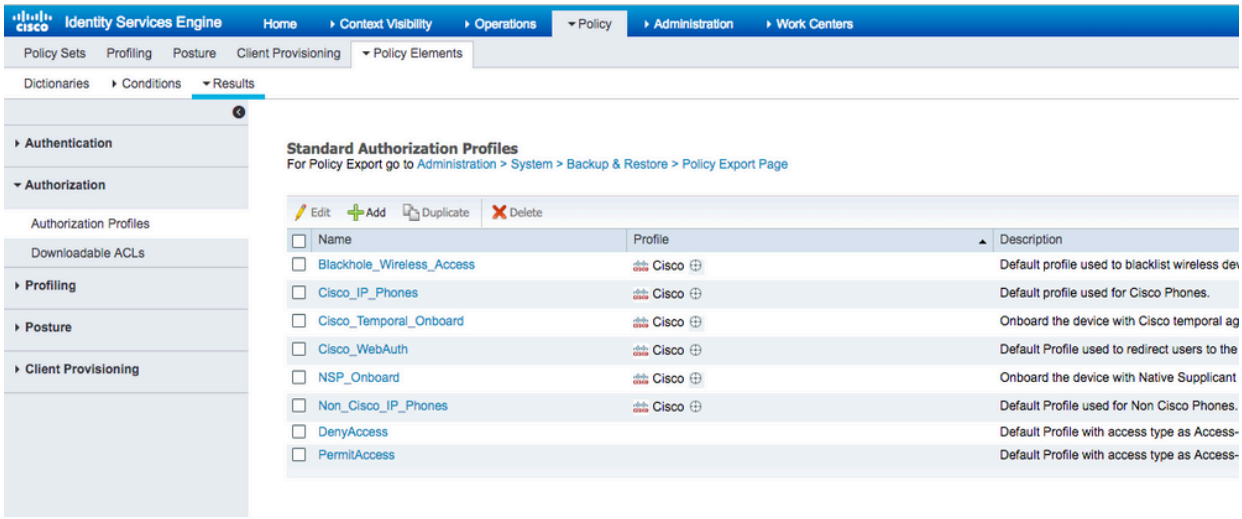
8. Os respectivos grupos são adicionados ao ISE e podem ser salvos. PressioneSave.



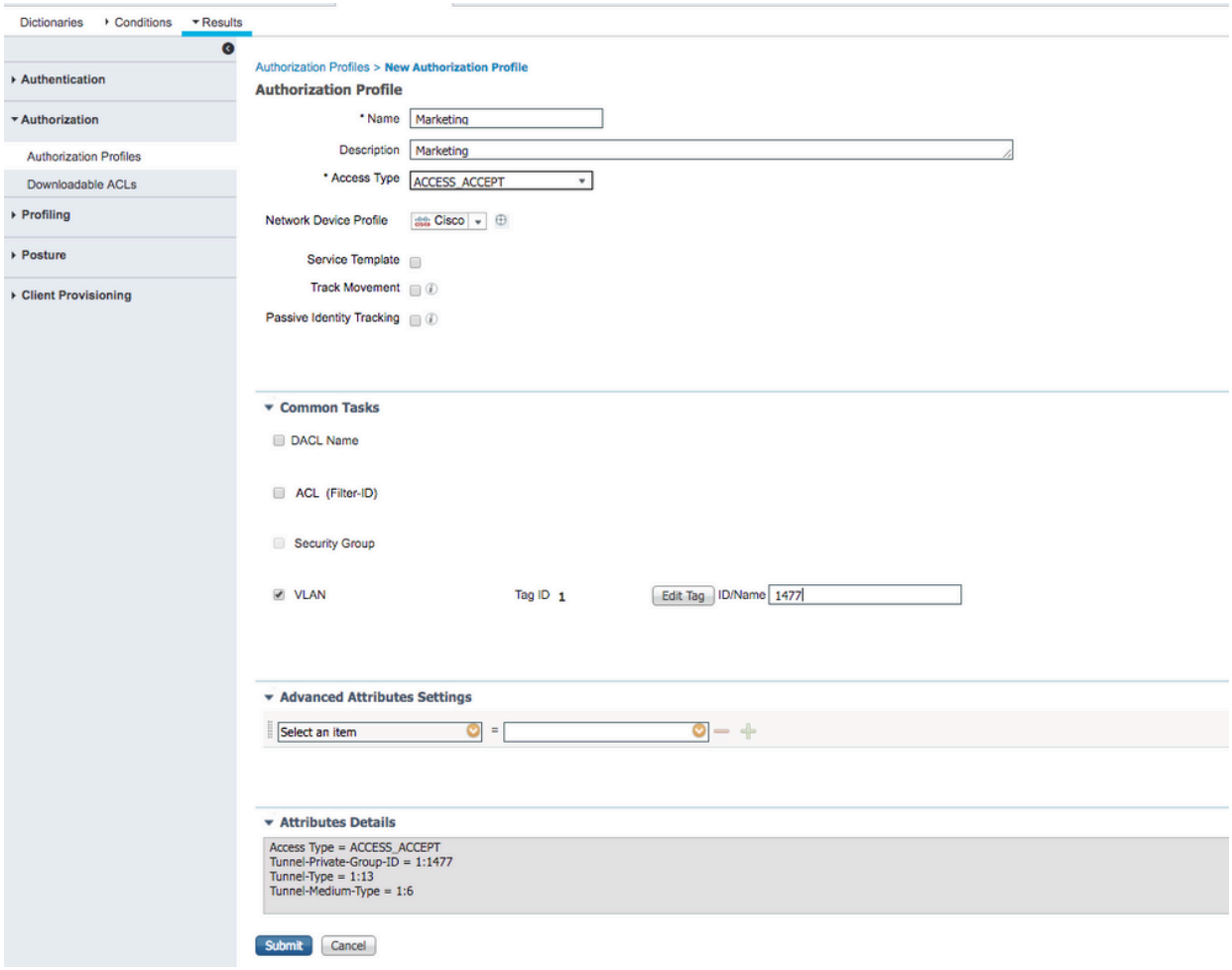
9. Adicione a WLC à lista de dispositivos de rede do ISE - navegue atéAdministration > Network Resources > Network Devicese pressioneAdd.
   Conclua a configuração, fornecendo o endereço IP de gerenciamento da WLC e o segredo compartilhado RADIUS entre a WLC e o ISE.



10. Agora, depois de ter ingressado no ISE para o AD e adicionado a WLC à lista de dispositivos, você pode iniciar a configuração de políticas de autenticação e autorização para usuários.
    - Crie um perfil de autorização para atribuir usuários de Marketing à VLAN1477 e do grupo de RH à VLAN1478.
      Navegue atéPolicy > Policy Elements > Results > Authorization > Authorization profilese clique no botãoAddpara criar um novo perfil.

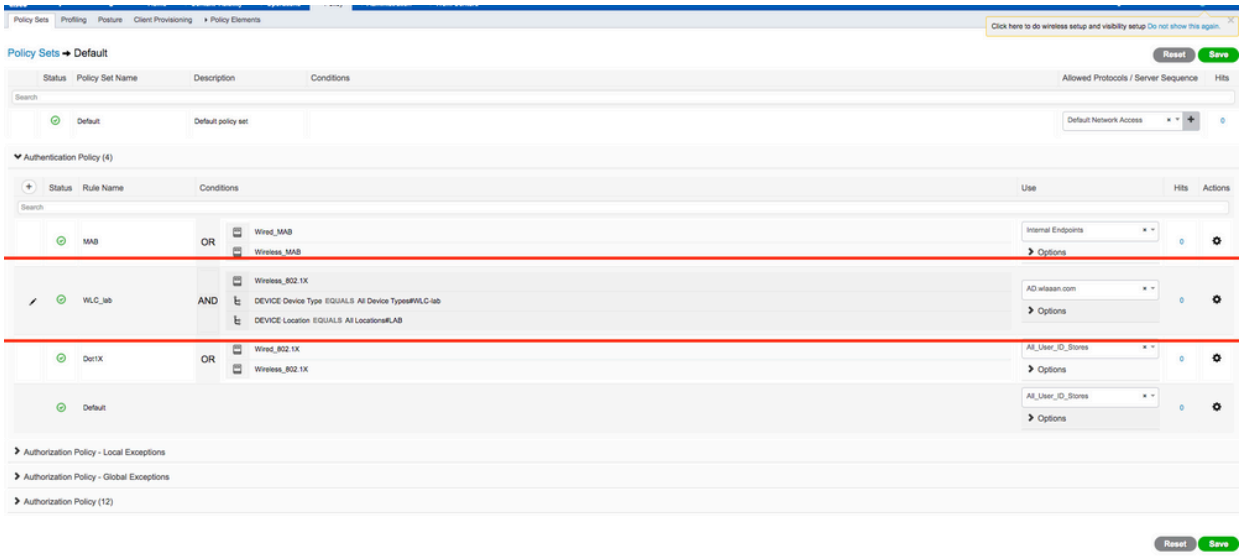


    - Conclua a configuração do perfil de autorização com informações de VLAN para o respectivo grupo; o exemplo mostraMarketingas definições de configuração do grupo.

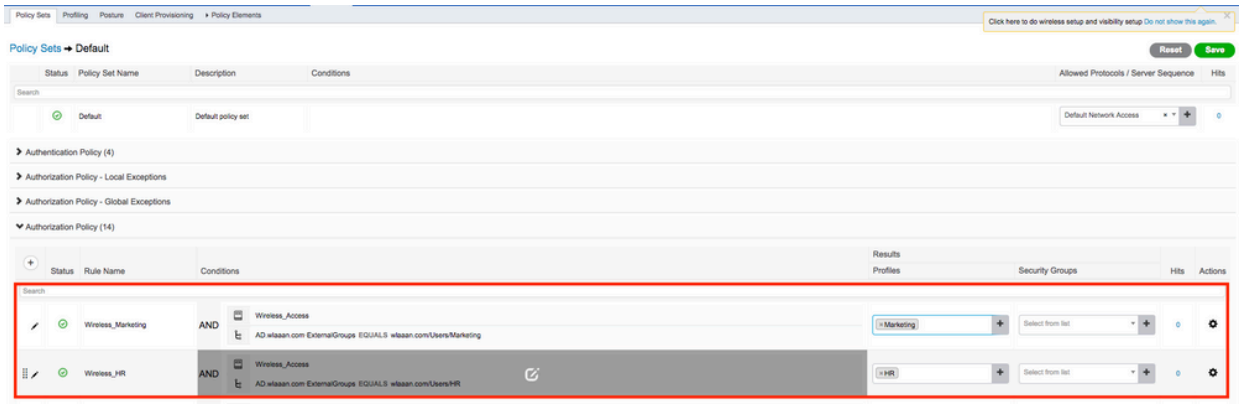


Uma configuração semelhante deve ser feita para outros grupos e os respectivos atributos de marca de VLAN devem ser configurados.

- Depois que os perfis de autorização forem configurados, você poderá definir políticas de autenticação para usuários sem fio. Isso pode ser feito configurando`Custom`ou modificando o conjunto`Default`de políticas. Neste exemplo, o conjunto de políticas padrão é modificado. Navegue até`Policy > Policy Sets > Default`. Por padrão, para o tipo de`dot1x`autenticação, o ISE usará`All_User_ID_Stores`, embora funcione mesmo com as configurações padrão atuais, já que AD faz parte da lista de origem de identidade de `All_User_ID_Stores`, este exemplo usa uma regra mais específica`WLC_lab`para esse controlador de LAB respectivo e usa AD como a única origem para autenticação.

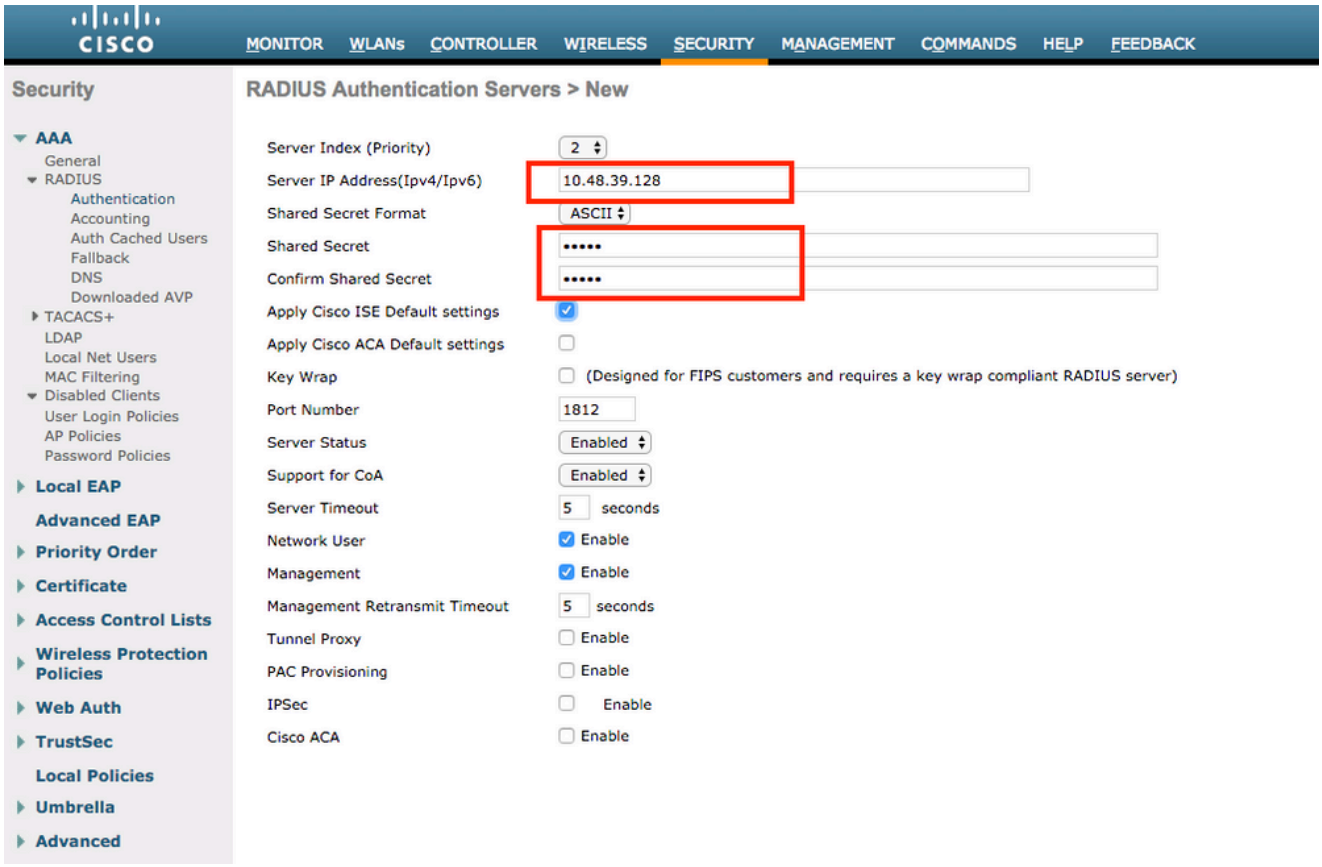


- Agora você deve criar políticas de autorização para usuários que atribuem respectivos perfis de autorização com base na associação de grupo. Navegue atéAuthorization policya seção e crie políticas para atender a esse requisito.

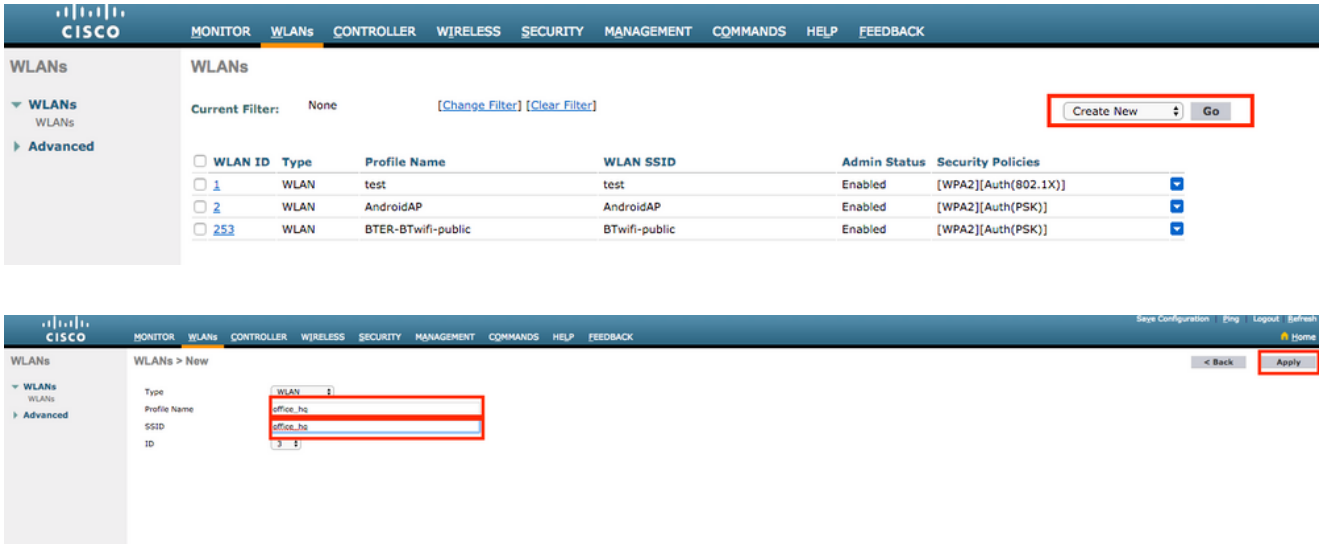


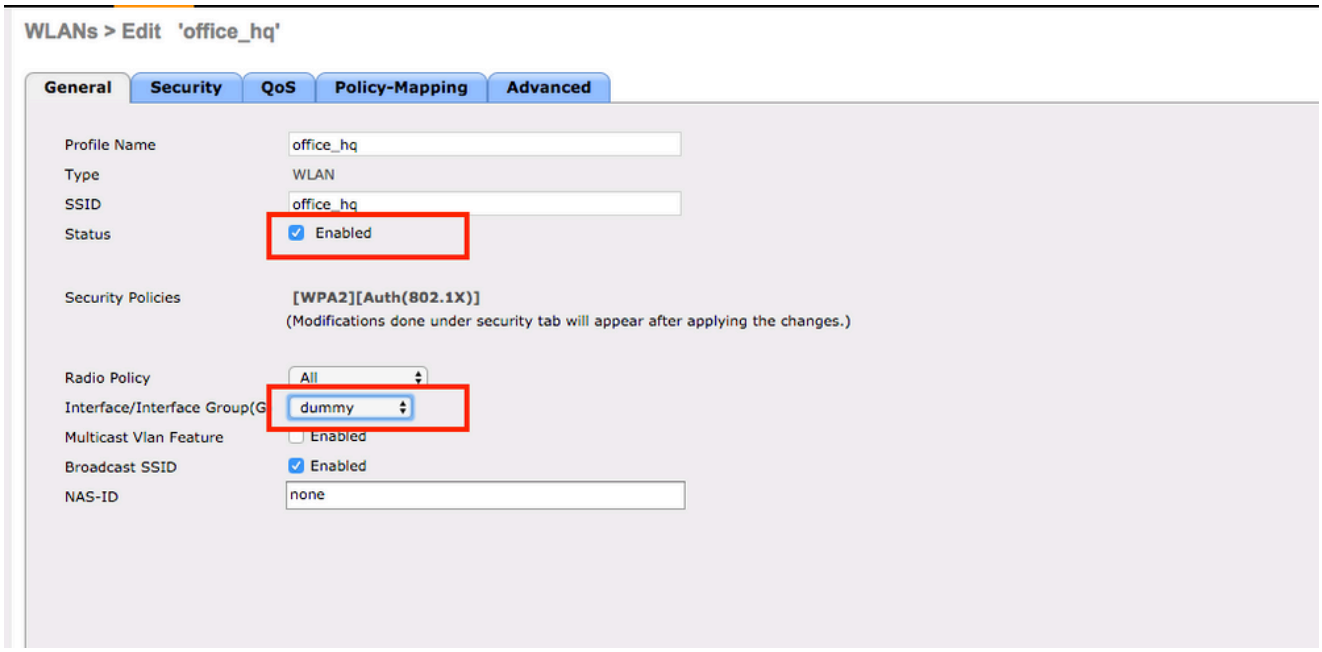
Configuração de WLC para suportar autenticação dot1x e substituição de AAA para SSID 'office_hq'

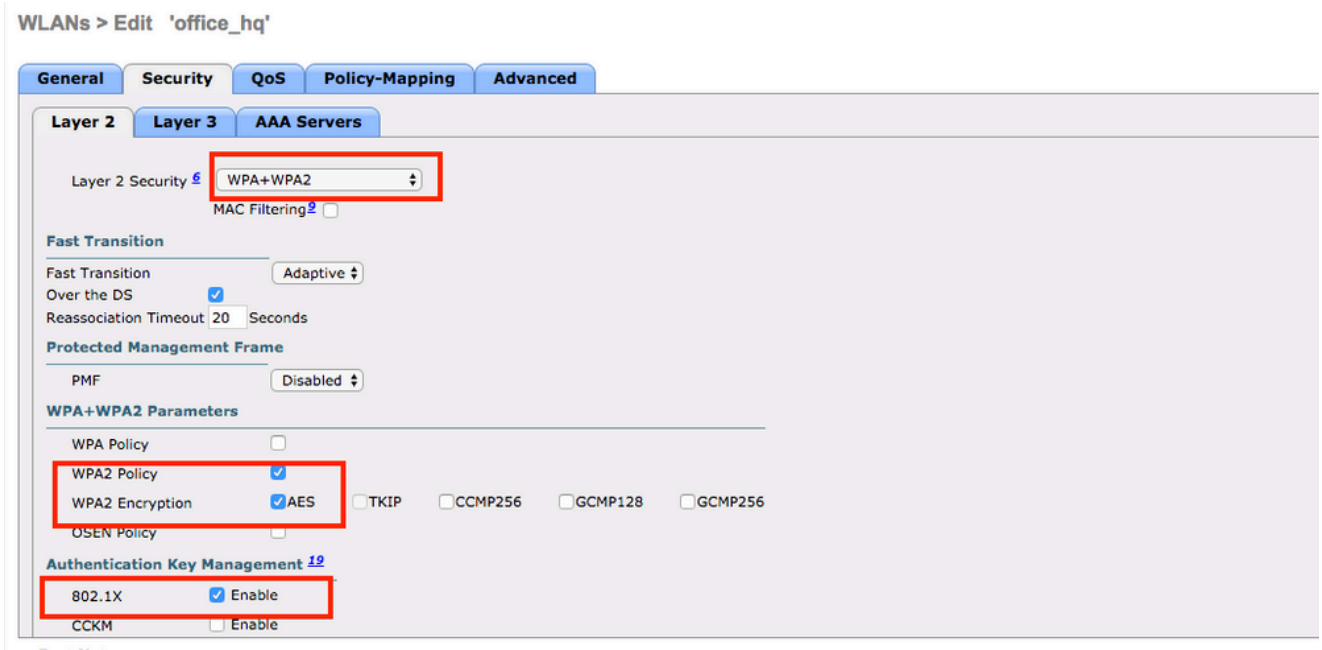
1. Configure o ISE como um servidor de autenticação RADIUS no WLC. Navegue até aSecurity > AAA > RADIUS > Authenticationseção na interface da interface de usuário da Web e forneça o endereço IP do ISE e as informações de segredo compartilhado.

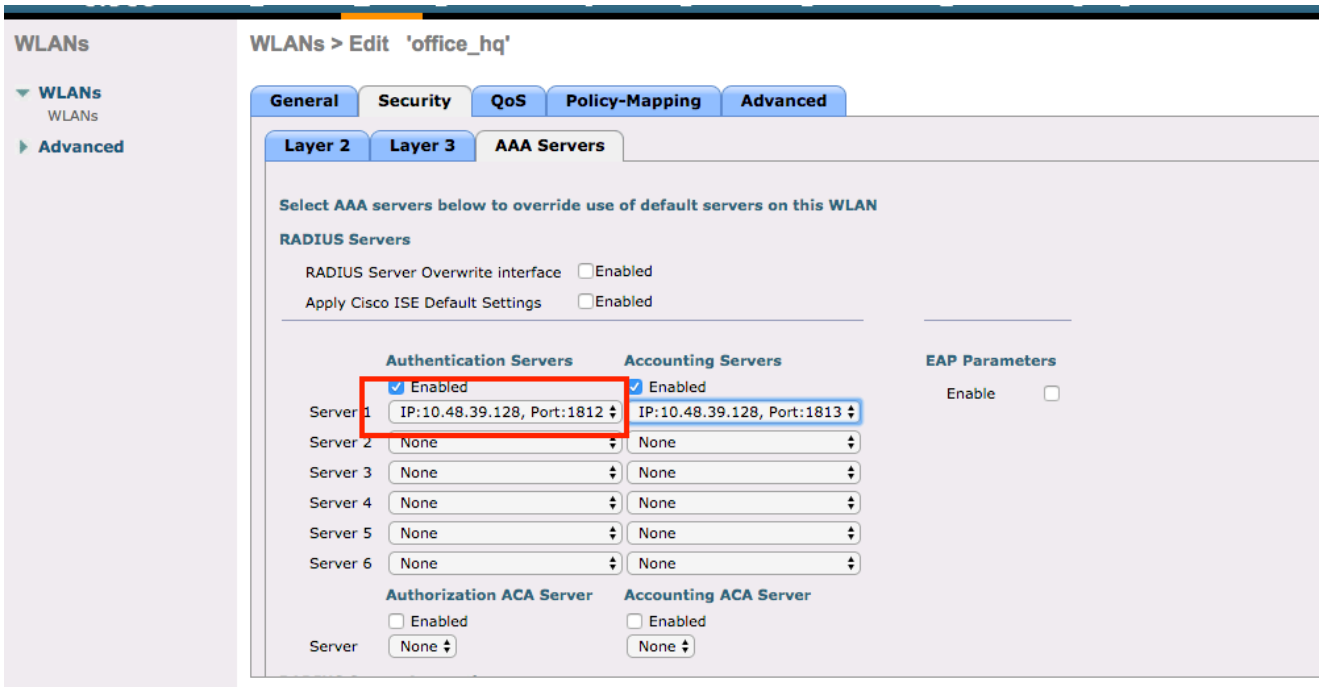


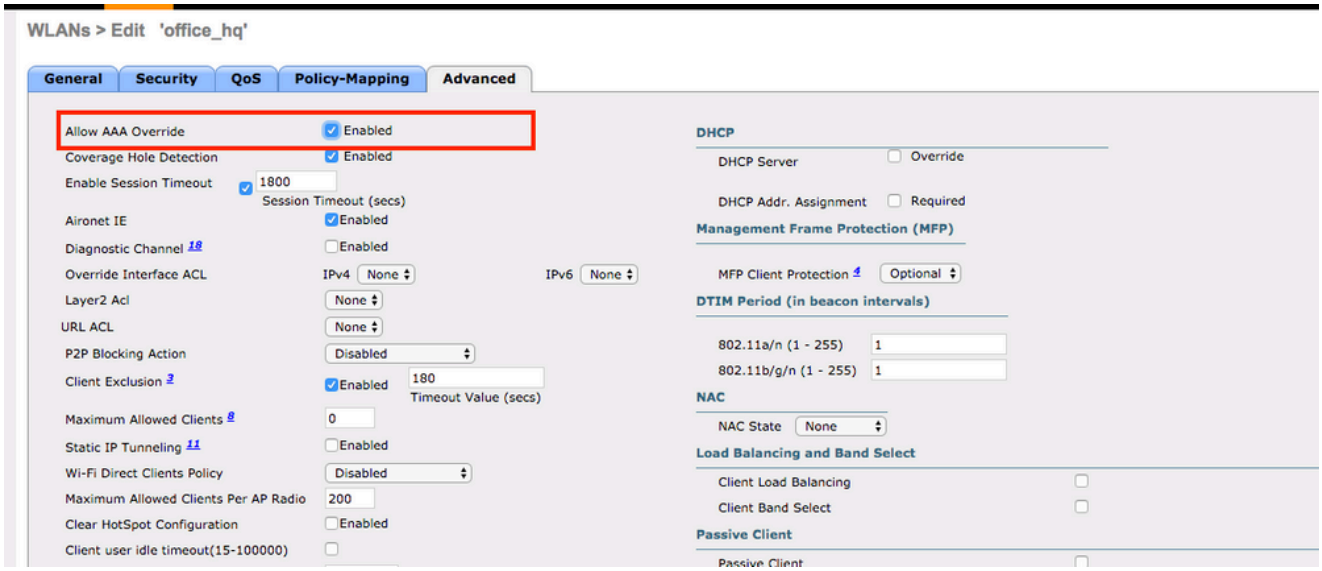
2. Configure o SSIDoffice_hqna seçãoWLANsna WLC; este exemplo configura o SSID comWPA2/AES+dot1xe substituição de AAA. A interfaceDummyé escolhida para a WLAN, já que a VLAN apropriada é atribuída através do RADIUS de qualquer forma. Essa interface fictícia deve ser criada na WLC e receber um endereço IP, mas o endereço IP não precisa ser válido e a VLAN na qual ele é colocado não pode ser criada no switch de uplink para que, se nenhuma VLAN estiver sendo atribuída, o cliente não possa ir a lugar algum.



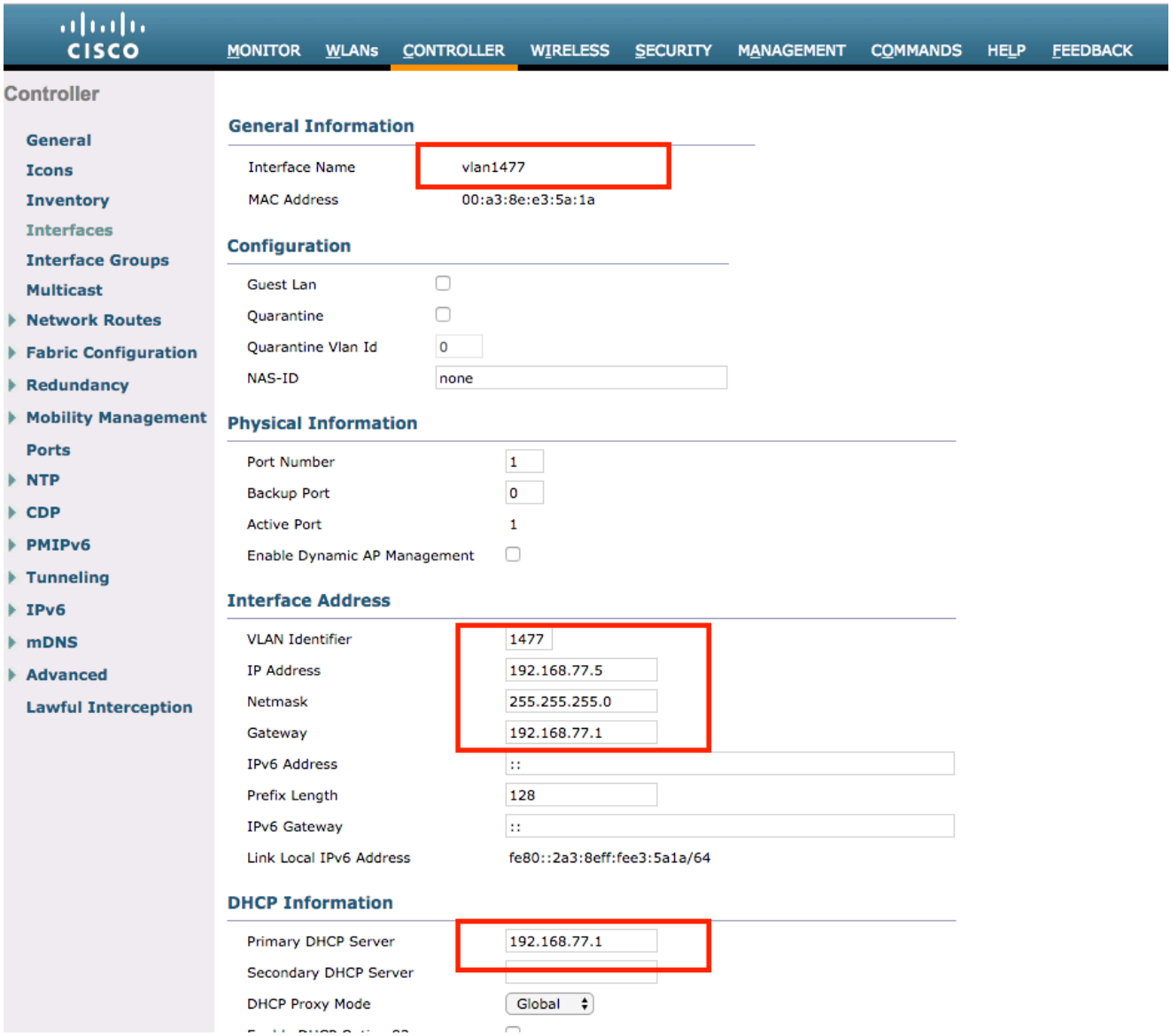

WLANs > Edit 'office_hq'
General
Security
QoS
Policy-Mapping
Advanced
Profile Name
office_hq
Type
WLAN
SSID
office_hq
Status
Enabled
Security Policies
[WPA2][Auth(802.1X)]
(Modifications done under security tab will appear after applying the changes.)
Radio Policy
All
Interface/Interface Group(G
dummy
Multicast Vlan Feature
Enabled
Broadcast SSID
Enabled
NAS-ID
none


WLANs > Edit 'office_hq'
General
Security
QoS
Policy-Mapping
Advanced
Layer 2
Layer 3
AAA Servers
Layer 2 Security
WPA+WPA2
MAC Filtering
Fast Transition
Fast Transition
Adaptive
Over the DS
Reassociation Timeout
20
Seconds
Protected Management Frame
PMF
Disabled
WPA+WPA2 Parameters
WPA Policy
WPA2 Policy
WPA2 Encryption
AES
TKIP
CCMP256
GCMP128
GCMP256
OSEN Policy
Authentication Key Management
802.1X
Enable
CCKM
Enable





3. Você também deve criar interfaces dinâmicas no WLC para VLANs de usuário. Navegue até o menu daController > InterfacesIU. A WLC só poderá honrar a atribuição de VLAN recebida via AAA se tiver uma interface dinâmica nessa VLAN.



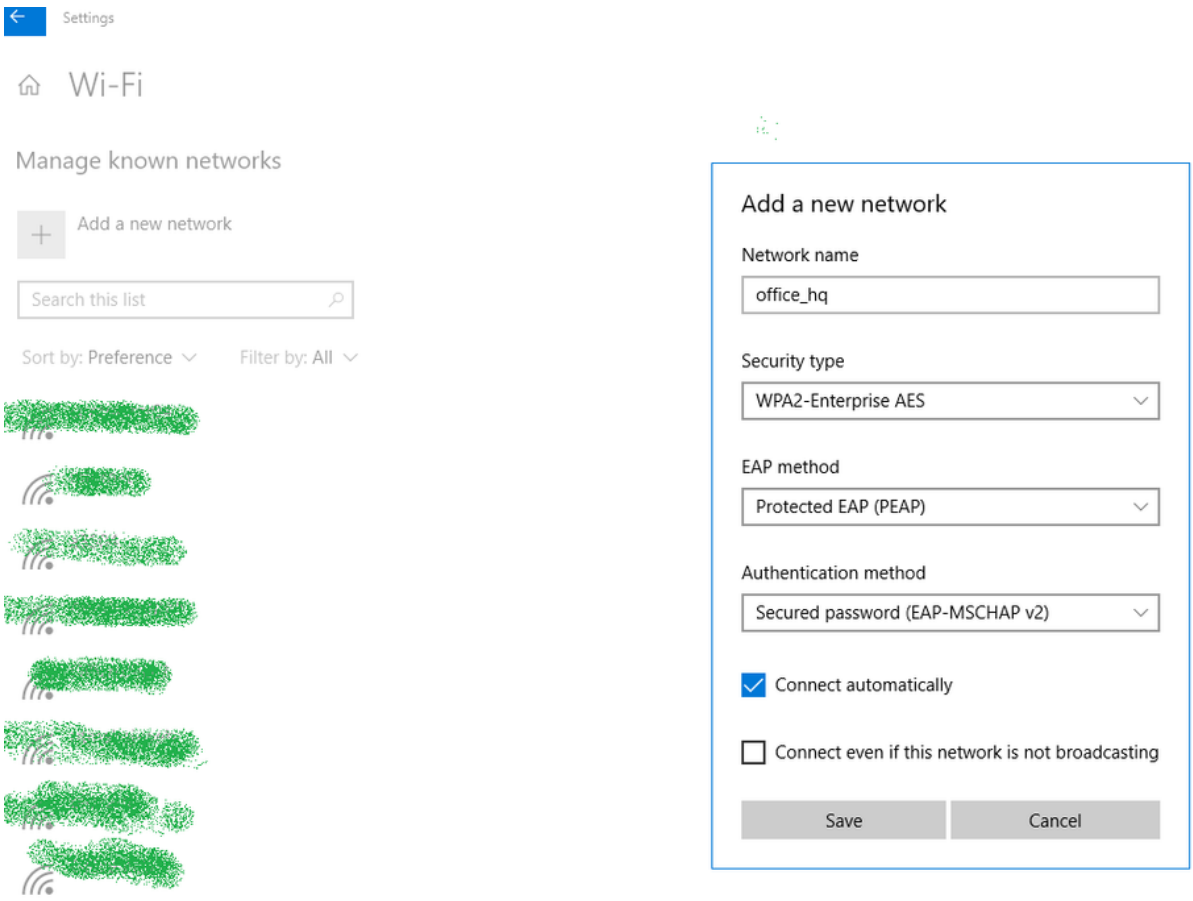
Verificar

Use o suplicante nativo do Windows 10 e o NAM do Anyconnect para testar conexões.

Como você está usando a autenticação EAP-PEAP e o ISE está usando um certificado autoassinado (SSC), você deve concordar com um aviso de certificado ou desabilitar a validação do certificado. Em um ambiente corporativo, você deve usar um certificado assinado e confiável no ISE e garantir que os dispositivos do usuário final tenham o certificado raiz apropriado instalado na lista CA confiável.

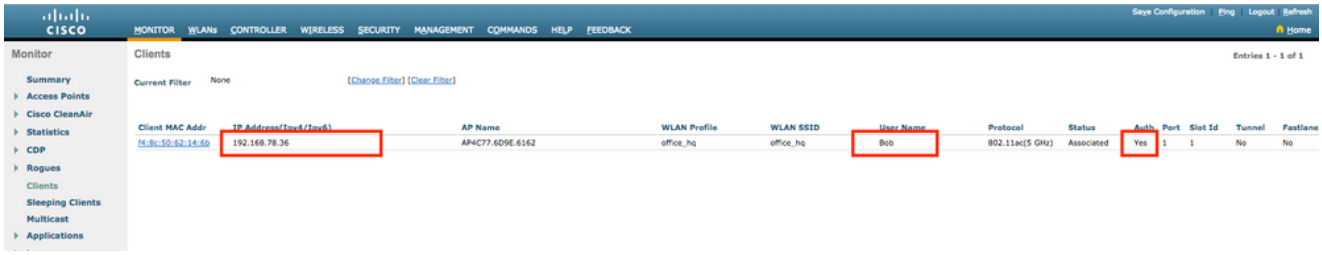
Testar conexão com o Windows 10 e suplicante nativo:

1. AbraNetwork & Internet settings > Wi-Fi > Manage known networkse crie um novo perfil de rede pressionando oAdd new networkbotão; preencha as informações necessárias.



2. Verifique o log de autenticação no ISE e verifique se o perfil correto está selecionado para o usuário.

3. Verifique a entrada do cliente na WLC e certifique-se de que ela esteja atribuída à VLAN correta e esteja no estado RUN.



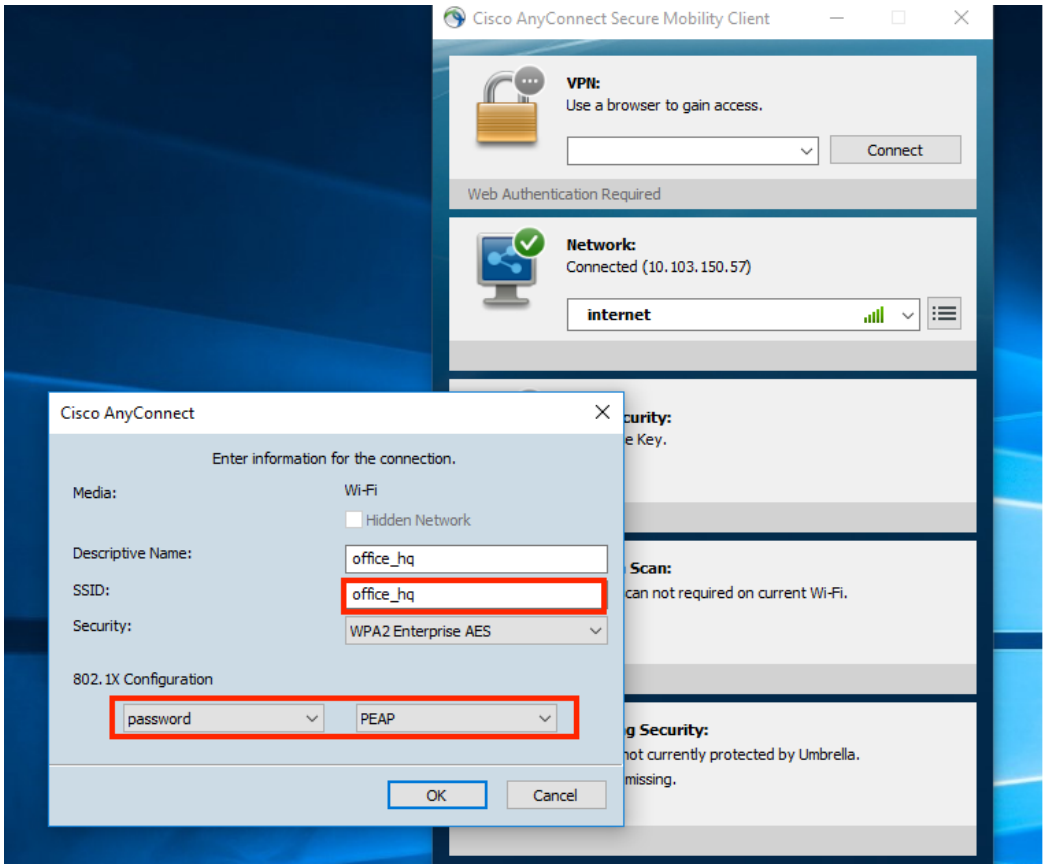
4. Na CLI da WLC, o status do cliente pode ser verificado com o`show client dertails` :

```
show client detail f4:8c:50:62:14:6b
Client MAC Address.............................. f4:8c:50:62:14:6b
Client Username ................................ Bob
```

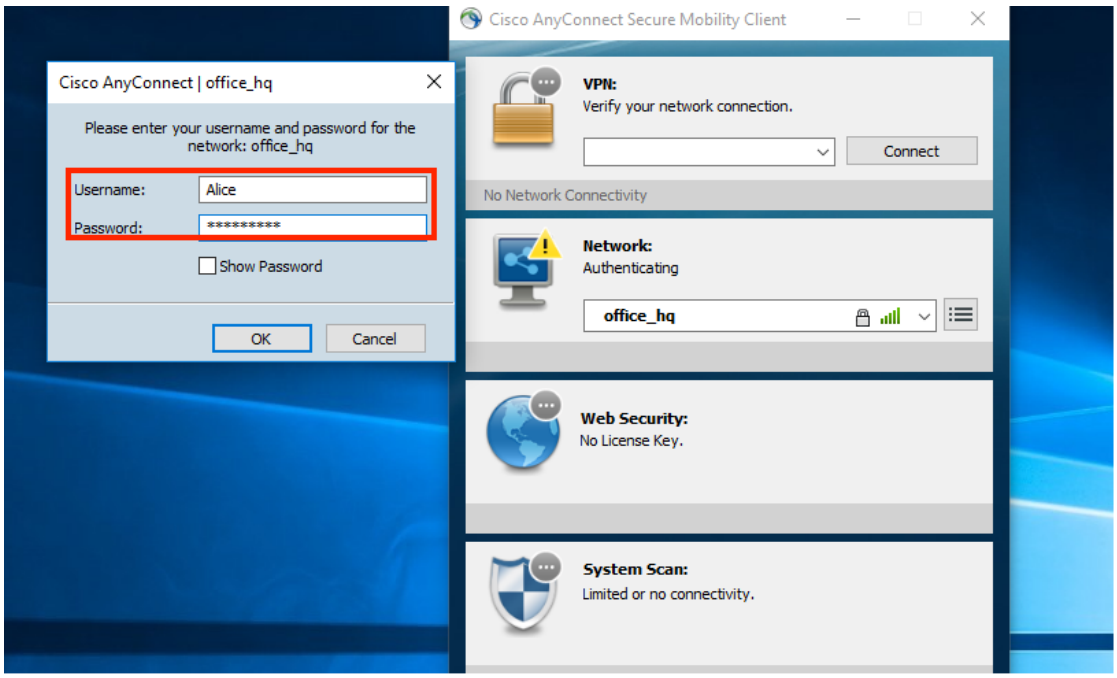
```
Client Webauth Username ..... N/A
Hostname: .....
Device Type: ..... Intel-Device
AP MAC Address..... 70:69:5a:51:4e:c0
AP Name..... AP4C77.6D9E.6162
AP radio slot Id..... 1
Client State..... Associated
User Authenticated by ..... RADIUS Server
Client User Group..... Bob
Client NAC OOB State..... Access
Wireless LAN Id..... 3
Wireless LAN Network Name (SSID)..... office_hq
Wireless LAN Profile Name..... office_hq
Hotspot (802.11u)..... Not Supported
Connected For ..... 242 secs
BSSID..... 70:69:5a:51:4e:cd
Channel..... 36
IP Address..... 192.168.78.36
Gateway Address..... 192.168.78.1
Netmask..... 255.255.255.0
...
Policy Manager State..... RUN
...
EAP Type..... PEAP
Interface..... vlan1478
VLAN..... 1478
Quarantine VLAN..... 0
Access VLAN..... 1478
```

Testar a conexão com o Windows 10 e o Anyconnect NAM:

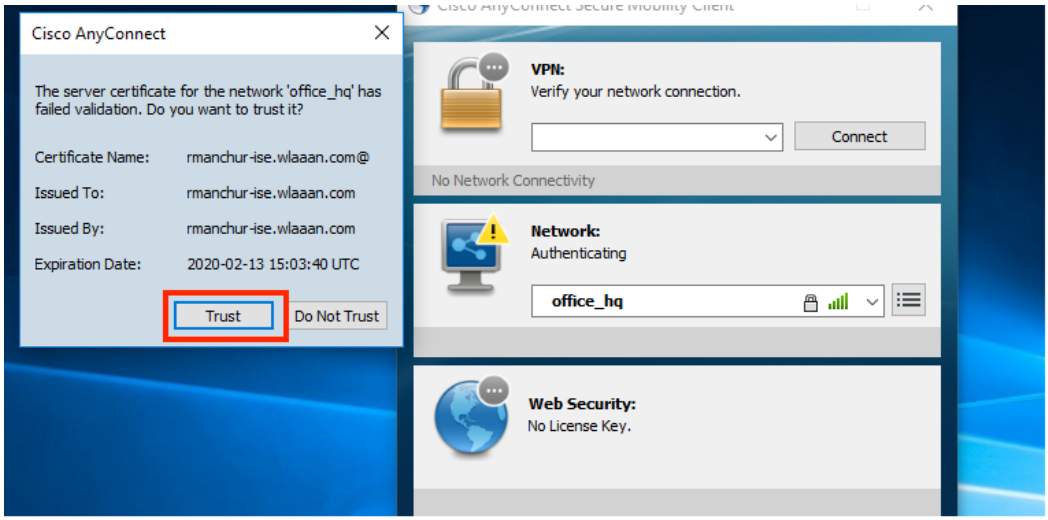
1. Escolha o SSID na lista de SSIDs disponíveis e o respectivo tipo de autenticação EAP (neste exemplo, PEAP) e o formulário de autenticação interna.



2. Forneça o nome de usuário e a senha para autenticação do usuário.

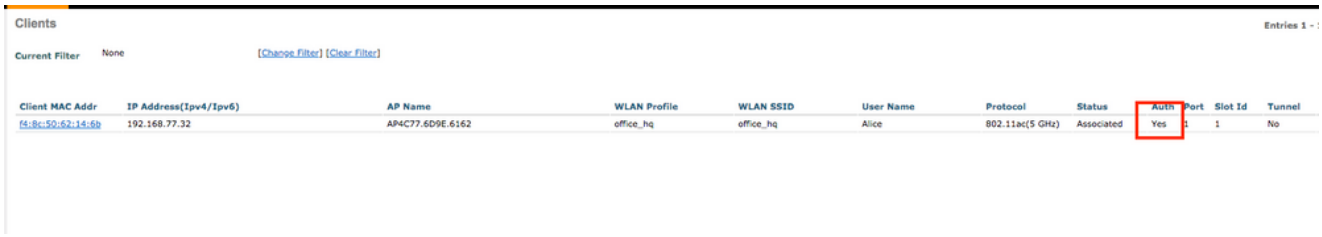


3. Como o ISE está enviando um SSC ao cliente, você deve escolher manualmente se confia no certificado (no ambiente de produção, é altamente recomendável instalar o certificado confiável no ISE).



4. Verifique os logs de autenticação no ISE e verifique se o perfil de autorização correto está selecionado para o usuário.

5. Verifique a entrada do cliente na WLC e certifique-se de que ela esteja atribuída à VLAN correta e esteja no estado RUN.



6. Na CLI da WLC, o status do cliente pode ser verificado com o`show client dertails` :

```
Client MAC Address.............................. f4:8c:50:62:14:6b
Client Username ................................ Alice
Client Webauth Username ........................ N/A
Hostname: ......................................
Device Type: ................................... Intel-Device
AP MAC Address.................................. 70:69:5a:51:4e:c0
AP Name......................................... AP4C77.6D9E.6162
AP radio slot Id................................ 1
```

```
Client State..................................... Associated
User Authenticated by ........................... RADIUS Server
Client User Group................................ Alice
Client NAC OOB State............................. Access
Wireless LAN Id.................................. 3
Wireless LAN Network Name (SSID)................. office_hq
Wireless LAN Profile Name........................ office_hq
Hotspot (802.11u)................................ Not Supported
Connected For ................................... 765 secs
BSSID............................................ 70:69:5a:51:4e:cd
Channel.......................................... 36
IP Address....................................... 192.168.77.32
Gateway Address.................................. 192.168.77.1
Netmask.......................................... 255.255.255.0
...
Policy Manager State............................. RUN
...
Policy Type...................................... WPA2
Authentication Key Management.................... 802.1x
Encryption Cipher................................ CCMP-128 (AES)
Protected Management Frame ...................... No
Management Frame Protection...................... No
EAP Type......................................... PEAP
Interface........................................ vlan1477
VLAN............................................. 1477
```

Troubleshooting

1. Use o`test aaa radius username`

   `password`

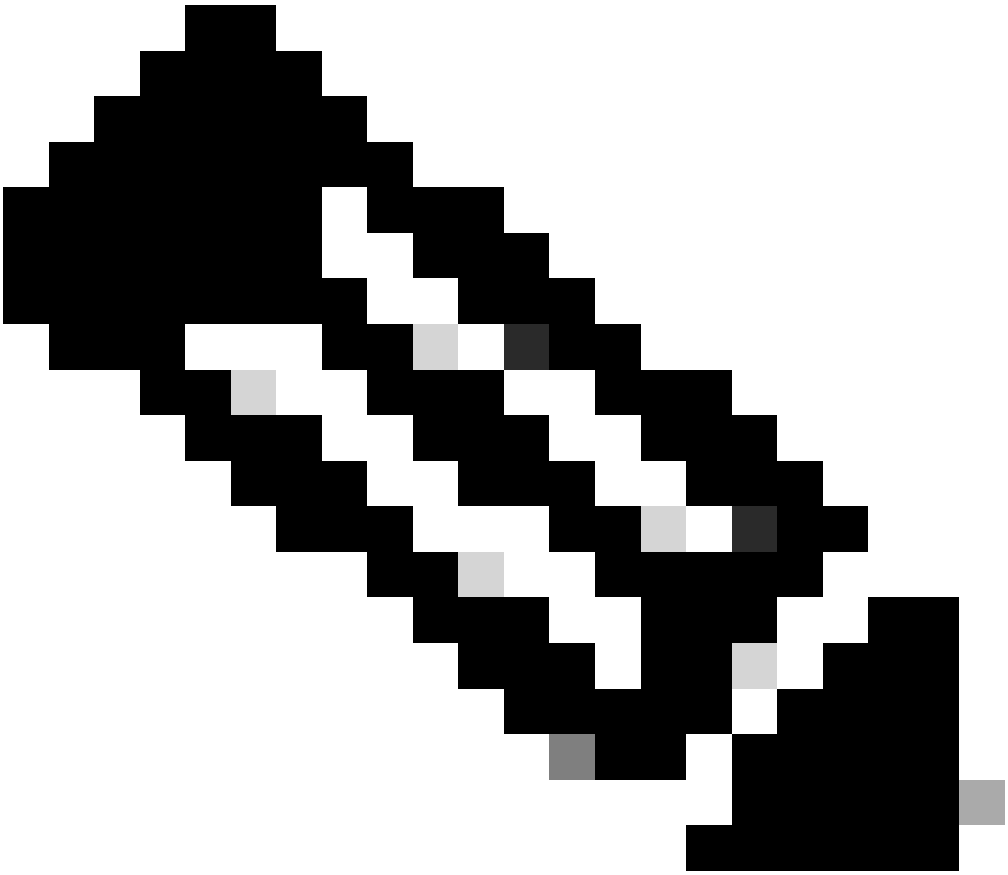
   `wlan-id`

   para testar a conexão RADIUS entre a WLC e o ISE e o`test aaa show radius`para mostrar os resultados.

```
test aaa radius username Alice password <removed> wlan-id 2

Radius Test Request
  Wlan-id.......................................... 2
  ApGroup Name..................................... none

  Attributes                    Values
  ----------                    ------
  User-Name                     Alice
  Called-Station-Id             00-00-00-00-00-00:AndroidAP
  Calling-Station-Id            00-11-22-33-44-55
  Nas-Port                      0x00000001 (1)
```

```
  Nas-Ip-Address                  10.48.71.20
  NAS-Identifier                  0x6e6f (28271)
  Airespace / WLAN-Identifier     0x00000002 (2)
  User-Password                   cisco!123
  Service-Type                    0x00000008 (8)
  Framed-MTU                      0x00000514 (1300)
  Nas-Port-Type                   0x00000013 (19)
  Cisco / Audit-Session-Id        1447300a0000003041d5665c
  Acct-Session-Id                 5c66d541/00:11:22:33:44:55/743


test radius auth request successfully sent. Execute 'test aaa show radius' for response

(Cisco Controller) >test aaa show radius

Radius Test Request
  Wlan-id..................................... 2
  ApGroup Name................................ none
Radius Test Response

Radius Server            Retry Status
-------------            ----- ------
10.48.39.128             1     Success

Authentication Response:
  Result Code: Success

  Attributes                      Values
  ----------                      ------
  User-Name                       Alice
  State                           ReauthSession:1447300a0000003041d5665c
  Class                           CACS:1447300a0000003041d5665c:rmanchur-ise/339603379/59
  Tunnel-Type                     0x0000000d (13)
  Tunnel-Medium-Type              0x00000006 (6)
  Tunnel-Group-Id                 0x000005c5 (1477)



(Cisco Controller) >
```

2. Use o debug client
   para solucionar problemas de conectividade do cliente sem fio.
3. Use odebug aaa all enablepara solucionar problemas de autenticação e autorização na WLC.



Observação: use esse comando apenas com o`debug mac addr`para limitar a saída com base no endereço MAC para o qual a depuração é feita.

4. Consulte os logs ao vivo do ISE e os logs de sessão para identificar problemas de falhas de autenticação e problemas de comunicação do AD.

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.