

BYOD sem fio com Identity Services Engine

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Topologia](#)

[Conventions](#)

[Visão geral de NAC e CoA do controlador de LAN sem fio](#)

[Fluxo de recursos de NAC e CoA do controlador de LAN sem fio](#)

[Visão geral do perfil do ISE](#)

[Criar usuários de identidade interna](#)

[Adicionar controlador de LAN sem fio ao ISE](#)

[Configurar o ISE para autenticação sem fio](#)

[Controlador de LAN sem fio Bootstrap](#)

[Conectando a WLC a uma rede](#)

[Adicionar servidores de autenticação \(ISE\) ao WLC](#)

[Criar interface dinâmica de funcionário da WLC](#)

[Criar interface dinâmica de convidado WLC](#)

[Adicionar WLAN 802.1x](#)

[Testar interfaces dinâmicas de WLC](#)

[Autenticação sem fio para iOS \(iPhone/iPad\)](#)

[Adicionar ACL de redirecionamento de postura à WLC](#)

[Ativar testes de criação de perfil no ISE](#)

[Ativar políticas de perfil do ISE para dispositivos](#)

[Perfil de autorização do ISE para redirecionamento de descoberta de postura](#)

[Criar perfil de autorização do ISE para funcionário](#)

[Criar Perfil de Autorização do ISE para Contratante](#)

[Política de autorização para postura/criação de perfis de dispositivos](#)

[Testando a Política de Correção de Postura](#)

[Política de autorização para acesso diferenciado](#)

[Testando o CoA para acesso diferenciado](#)

[WLAN Convidada da WLC](#)

[Testando a WLAN de Convidado e o Portal de Convidado](#)

[Acesso para convidados patrocinado pelo ISE Wireless](#)

[Patrocinando Convidado](#)

[Testando o acesso ao portal de convidados](#)

[Configuração do certificado](#)

[Integração com o Active Directory do Windows 2008](#)

[Adicionar Grupos do Ative Directory](#)

[Adicionar sequência de origem de identidade](#)

[Acesso de convidado patrocinado pelo ISE Wireless com AD integrado](#)

[Configurar o SPAN no Switch](#)

[Referência: autenticação sem fio para Apple MAC OS X](#)

[Referência: Wireless Authentication for Microsoft Windows XP \(Autenticação sem fio do Microsoft Windows XP\)](#)

[Referência: Wireless Authentication for Microsoft Windows 7 \(Autenticação sem fio para Microsoft Windows 7\)](#)

[Informações Relacionadas](#)

Introduction

O Cisco Identity Services Engine (ISE) é o servidor de políticas de última geração da Cisco que fornece infraestrutura de autenticação e autorização para a solução Cisco TrustSec. Ele também fornece dois outros serviços essenciais:

- O primeiro serviço é fornecer uma maneira de criar um perfil do tipo de dispositivo de endpoint automaticamente com base nos atributos que o Cisco ISE recebe de várias fontes de informação. Esse serviço (chamado Profiler) fornece funções equivalentes às oferecidas anteriormente pela Cisco com o dispositivo Cisco NAC Profiler.
- Outro serviço importante que o Cisco ISE fornece é verificar a conformidade do endpoint; por exemplo, a instalação do software AV/AS e sua validade do arquivo de definição (conhecida como Postura). Anteriormente, a Cisco oferecia essa função de postura exata apenas com o Cisco NAC Appliance.

O Cisco ISE fornece um nível equivalente de funcionalidade e está integrado aos mecanismos de autenticação 802.1X.

O Cisco ISE integrado com controladores de LAN sem fio (WLCs) pode fornecer mecanismos de criação de perfil de dispositivos móveis, como Apple iDevices (iPhone, iPad e iPod), smartphones baseados em Android e outros. Para usuários de 802.1X, o Cisco ISE pode fornecer o mesmo nível de serviços, como criação de perfis e verificação de postura. Os serviços convidados no Cisco ISE também podem ser integrados com o Cisco WLC, redirecionando as solicitações de autenticação da Web para o Cisco ISE para autenticação.

Este documento apresenta a solução sem fio para BYOD (Bring Your Own Device), como o fornecimento de acesso diferenciado com base em endpoints conhecidos e na política do usuário. Este documento não fornece a solução completa de BYOD, mas serve para demonstrar um caso de uso simples de acesso dinâmico. Outros exemplos de configuração incluem o uso do portal do patrocinador do ISE, onde um usuário privilegiado pode patrocinar um convidado para provisionamento de acesso sem fio para convidado.

Prerequisites

Requirements

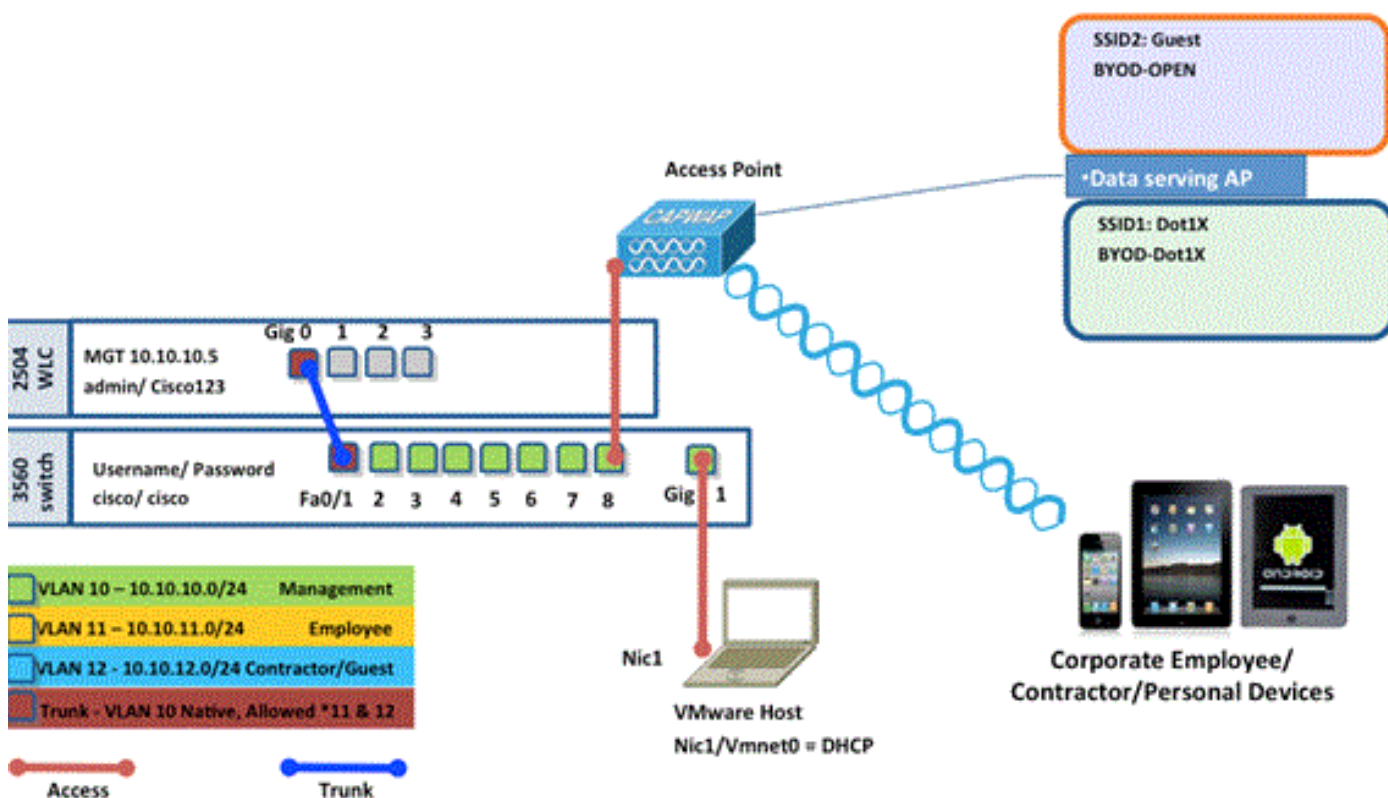
Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Cisco Wireless LAN Controller 2504 ou 2106 com a versão de software 7.2.103
- Catalyst 3560 - 8 portas
- WLC 2504
- Identity Services Engine 1.0MR (versão da imagem do servidor VMware)
- Windows 2008 Server (imagem VMware) — 512 MB, disco de 20 GB
Diretório ativo
DNS
DHCP
Serviços de certificado

Topologia



Name	IP Address	Credential
Vmware Host	10.10.10.2	(Machine used to host the ISE 1.0 MR vmware server files)
Identity Service Engine	10.10.10.70	admin/ default1A
Active Directory/ DNS/ DHCP/ CA Server	10.10.10.10	(Machine used to host Active Directory/ DNS/ DHCP/ CA Server)

Conventions

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

Visão geral de NAC e CoA do controlador de LAN sem fio

Essa configuração permite que a WLC procure os pares de AV de redirecionamento de URL

provenientes do servidor RADIUS ISE. Isso ocorre apenas em uma WLAN vinculada a uma interface com a configuração RADIUS NAC ativada. Quando o par Cisco AV para redirecionamento de URL é recebido, o cliente é colocado no estado POSTURE_REQD. Isso é basicamente o mesmo que o estado WEBAUTH_REQD internamente no controlador.

Quando o servidor ISE RADIUS considera que o cliente está em conformidade com a postura, ele emite uma ReAuth de CoA. O Session_ID é usado para vinculá-lo. Com esse novo AuthC (re-Auth), ele não envia os Pares de AV de Redirecionamento de URL. Como não há pares AV de redirecionamento de URL, a WLC sabe que o cliente não exige mais Posture.

Se a configuração RADIUS NAC não estiver habilitada, a WLC ignorará os VSAs de Redirecionamento de URL.

CoA-ReAuth: habilitado com a Configuração RFC 3576. O recurso ReAuth foi adicionado aos comandos CoA existentes que eram suportados anteriormente.

A configuração RADIUS NAC é mutuamente exclusiva desse recurso, embora seja necessária para que o CoA funcione.

ACL de pré-postura: quando um cliente está no estado POSTURE_REQ, o comportamento padrão da WLC é bloquear todo o tráfego, exceto DHCP/DNS. A ACL de pré-postura (que é chamada no par AV da acl de redirecionamento de url) é aplicada ao cliente e o que é permitido nessa ACL é o que o cliente pode alcançar.

Substituição de ACL vs. VLAN de pré-autenticação: uma VLAN de quarentena ou de autorização diferente da VLAN de acesso não é suportada no 7.0MR1. Se você definir uma VLAN a partir do Servidor de políticas, ela será a VLAN para toda a sessão. Nenhuma alteração de VLAN é necessária após a primeira AuthZ.

[Fluxo de recursos de NAC e CoA do controlador de LAN sem fio](#)

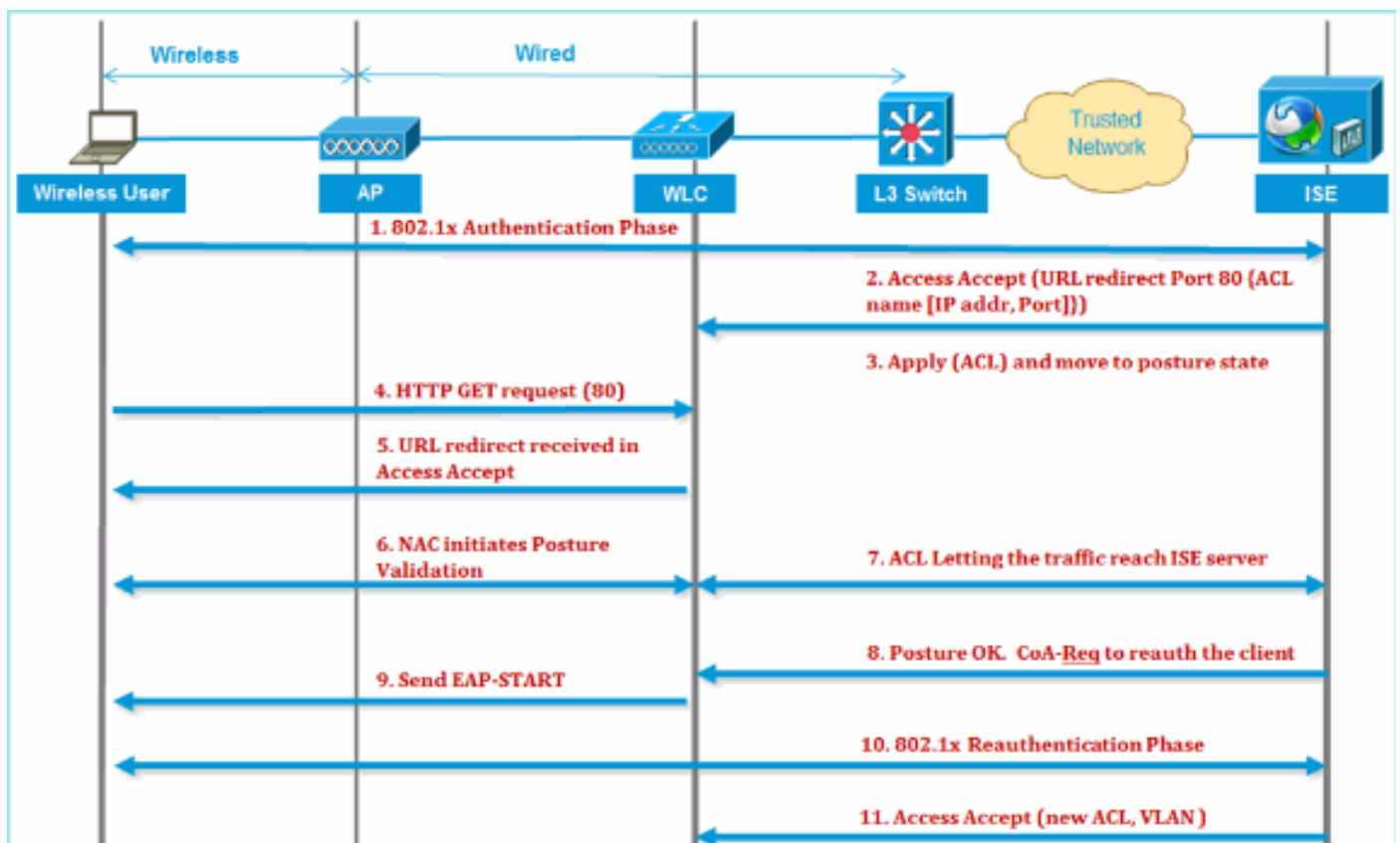
A [figura](#) abaixo fornece detalhes da troca de mensagens quando o cliente é autenticado no servidor de back-end e na validação da postura do NAC.

1. O cliente autentica usando a autenticação dot1x.
2. RADIUS Access Accept transporta o URL redirecionado para a porta 80 e ACLs de pré-autorização que incluem a permissão de endereços IP e portas ou VLAN de quarentena.
3. O cliente será redirecionado para a URL fornecida em aceitação de acesso e colocado em um novo estado até que a validação da postura seja feita. O cliente nesse estado se comunica com o servidor ISE e valida a si mesmo em relação às políticas configuradas no servidor ISE NAC.
4. O agente NAC no cliente inicia a validação da postura (tráfego para a porta 80): o agente envia a solicitação de descoberta HTTP para a porta 80, que é redirecionada pelo controlador para a URL fornecida na aceitação de acesso. O ISE sabe que o cliente está tentando alcançar e responde diretamente ao cliente. Dessa forma, o cliente aprende sobre o IP do servidor ISE e, a partir de agora, ele fala diretamente com o servidor ISE.
5. A WLC permite esse tráfego porque a ACL está configurada para permitir esse tráfego. Em caso de substituição de VLAN, o tráfego é ligado para que chegue ao servidor ISE.
6. Quando o cliente ISE concluir a avaliação, um RADIUS CoA-Req com serviço de reautenticação será enviado para a WLC. Isso inicia a reautenticação do cliente (enviando

EAP-START). Depois que a reautenticação for bem-sucedida, o ISE enviará a aceitação de acesso com uma nova ACL (se houver) e nenhum redirecionamento de URL ou VLAN de acesso.

7. A WLC tem suporte para CoA-Req e Disconnect-Req conforme RFC 3576. A WLC precisa suportar CoA-Req para o serviço de reautenticação, de acordo com o RFC 5176.
8. Em vez de ACLs para download, as ACLs pré-configuradas são usadas na WLC. O servidor ISE envia apenas o nome da ACL, que já está configurada no controlador.
9. Esse design deve funcionar para casos de VLAN e ACL. Em caso de substituição de VLAN, apenas redirecionamos a porta 80 que é redirecionada e permite (bridge) o resto do tráfego na VLAN de quarentena. Para a ACL, a ACL de pré-autenticação recebida na aceitação de acesso é aplicada.

Esta figura fornece uma representação visual desse fluxo de recursos:



Visão geral do perfil do ISE

O serviço de criação de perfis do Cisco ISE oferece a funcionalidade para descobrir, localizar e determinar os recursos de todos os endpoints conectados à rede, independentemente dos tipos de dispositivo, a fim de garantir e manter o acesso apropriado à rede da empresa. Ele coleta principalmente um atributo ou um conjunto de atributos de todos os endpoints em sua rede e os classifica de acordo com seus perfis.

O profiler é composto destes componentes:

- O sensor contém várias sondas. Os testes capturam pacotes de rede consultando dispositivos de acesso à rede e encaminham os atributos e seus valores de atributo que são coletados dos pontos finais para o analisador.
- Um analisador avalia os endpoints usando as políticas configuradas e os grupos de

identidade para corresponder aos atributos e seus valores de atributo coletados, o que classifica os endpoints para o grupo especificado e armazena os endpoints com o perfil correspondente no banco de dados do Cisco ISE.

Para a detecção de dispositivos móveis, é recomendável usar uma combinação destas sondas para a identificação correta do dispositivo:

- RADIUS (ID da estação de chamada): fornece o endereço MAC (OUI)
- DHCP (nome do host): Nome do host - o nome do host padrão pode incluir o tipo de dispositivo; por exemplo: jsmith-ipad
- DNS (pesquisa de IP reverso): FQDN - o nome de host padrão pode incluir o tipo de dispositivo
- HTTP (User-Agent): detalhes sobre o tipo específico de dispositivo móvel

Neste exemplo de um iPad, o profiler captura as informações do navegador da Web do atributo Usuário-Agente, bem como outros atributos HTTP das mensagens de solicitação, e os adiciona à lista de atributos de endpoint.



Is the MAC Address
from Apple?



Does the Hostname
contain "iPad"?



Is the Safari Browser
on an iPad?



I am
certain it
is an iPad!

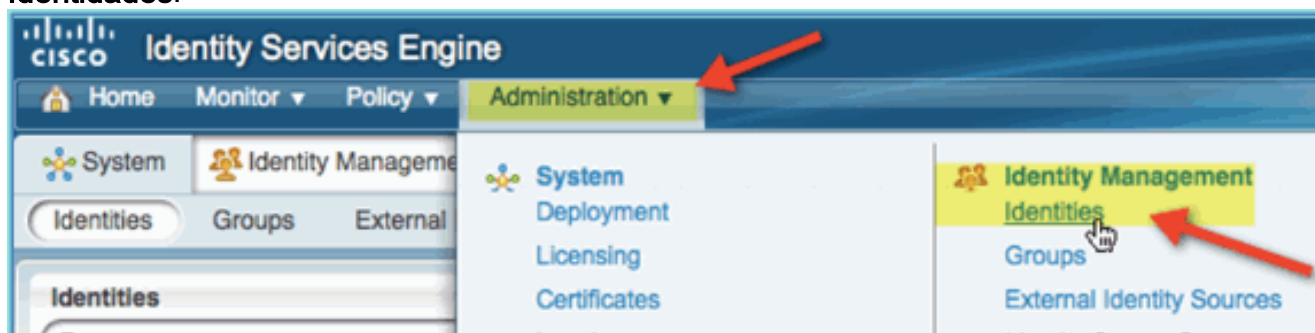
[Criar usuários de identidade interna](#)

O MS Ative Directory (AD) não é necessário para uma prova de conceito simples. O ISE pode ser usado como o único armazenamento de identidade, o que inclui diferenciar o acesso dos usuários para acesso e controle de política granular.

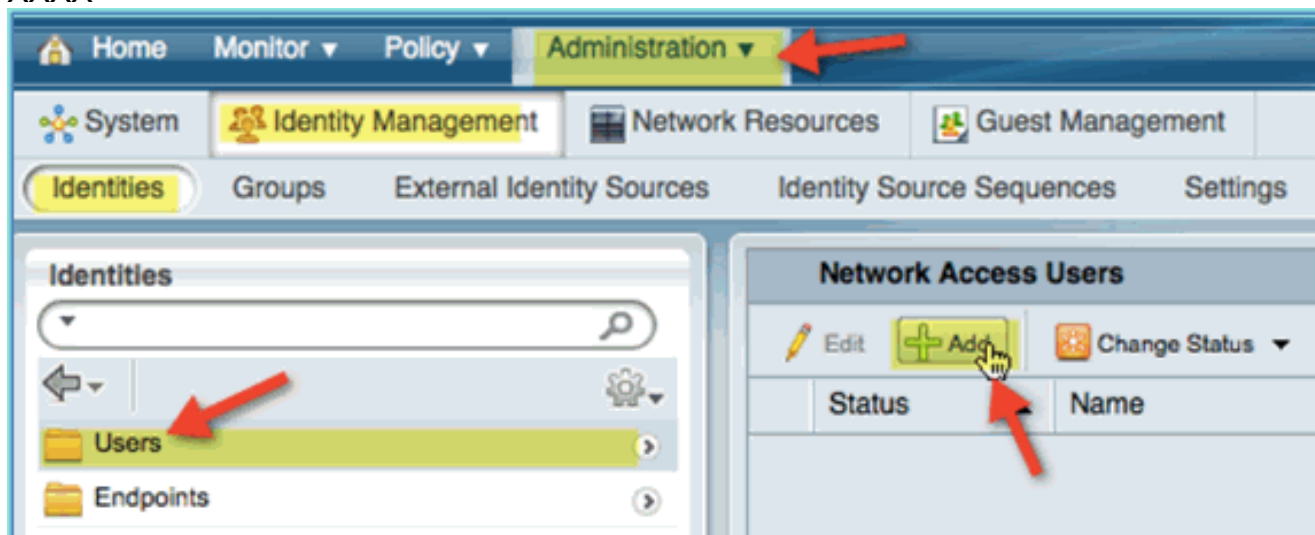
Na versão 1.0 do ISE, usando a integração do AD, o ISE pode usar grupos do AD em políticas de autorização. Se o armazenamento de usuário interno do ISE for usado (sem integração com o AD), os grupos não poderão ser usados em políticas em conjunto com grupos de identidade de dispositivo (bug identificado a ser resolvido no ISE 1.1). Portanto, somente usuários individuais podem ser diferenciados, como funcionários ou prestadores de serviços, quando usados além dos grupos de identidade do dispositivo.

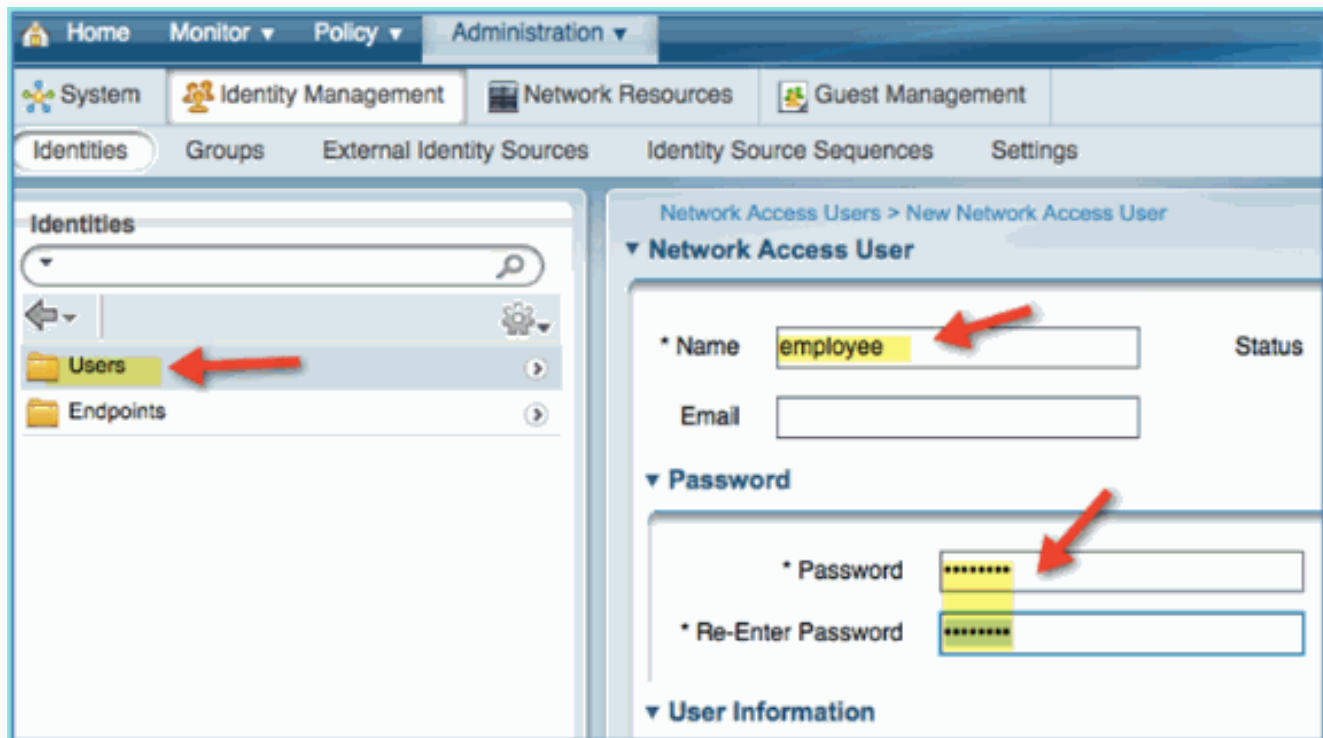
Conclua estes passos:

1. Abra uma janela do navegador para o endereço <https://ISEip>.
2. Navegue até **Administração > Gerenciamento de identidades > Identidades**.

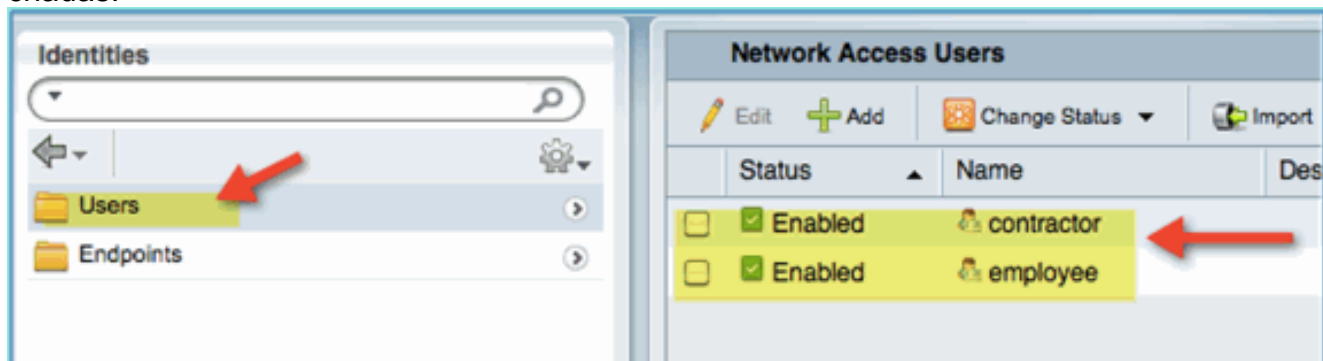


3. Selecione **Users** e clique em **Add** (Usuário de acesso à rede). Insira estes valores de usuário e atribua ao grupo de Funcionários: Nome: funcionário Senha: XXXX





4. Clique em Submit. Nome: contratante Senha: XXXX
5. Confirme se as duas contas foram criadas.



Adicionar controlador de LAN sem fio ao ISE

Qualquer dispositivo que inicie solicitações RADIUS para o ISE deve ter uma definição no ISE. Esses dispositivos de rede são definidos com base em seus endereços IP. As definições de dispositivo de rede do ISE podem especificar intervalos de endereços IP, permitindo assim que a definição represente vários dispositivos reais.

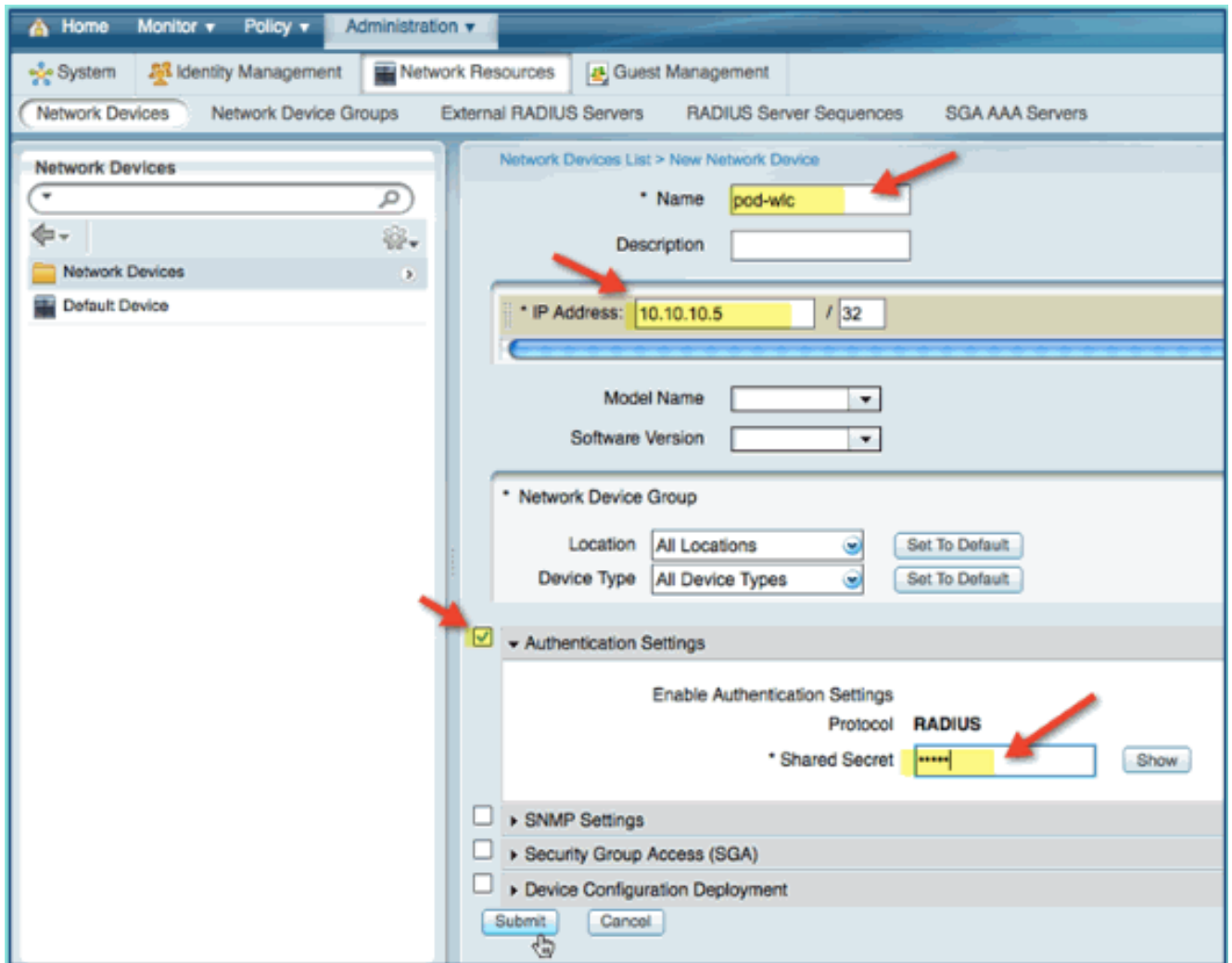
Além do que é necessário para a comunicação RADIUS, as definições do dispositivo de rede do ISE contêm configurações para outras comunicações do ISE/dispositivo, como SNMP e SSH.

Outro aspecto importante da definição de dispositivo de rede é o agrupamento apropriado de dispositivos para que esse agrupamento possa ser aproveitado na política de acesso à rede.

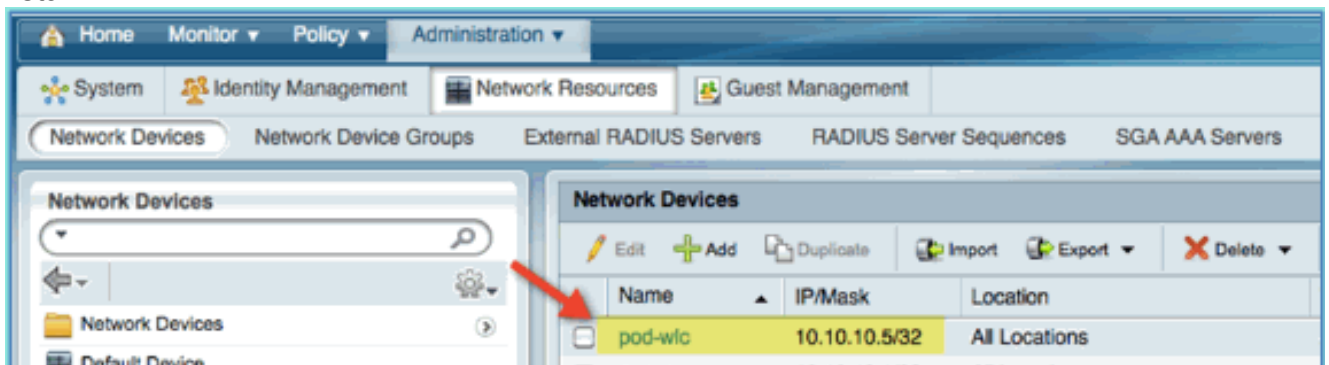
Neste exercício, as definições de dispositivo necessárias para seu laboratório são configuradas.

Conclua estes passos:

1. No ISE, vá para **Administração > Recursos de rede > Dispositivos de rede**.



2. Em Dispositivos de rede, clique em **Adicionar**. Insira o endereço IP, verifique a máscara e a configuração de autenticação e digite 'cisco' para segredo compartilhado.
3. Salve a entrada da WLC e confirme o controlador na lista.



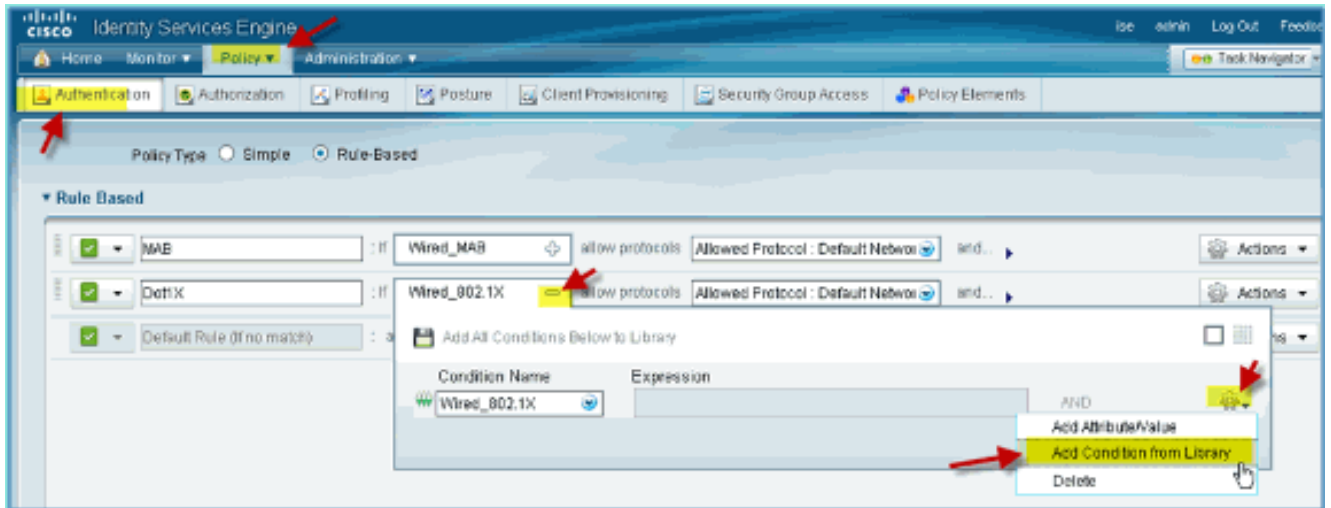
[Configurar o ISE para autenticação sem fio](#)

O ISE precisa ser configurado para autenticar clientes sem fio 802.1x e para usar o Active Directory como o armazenamento de identidade.

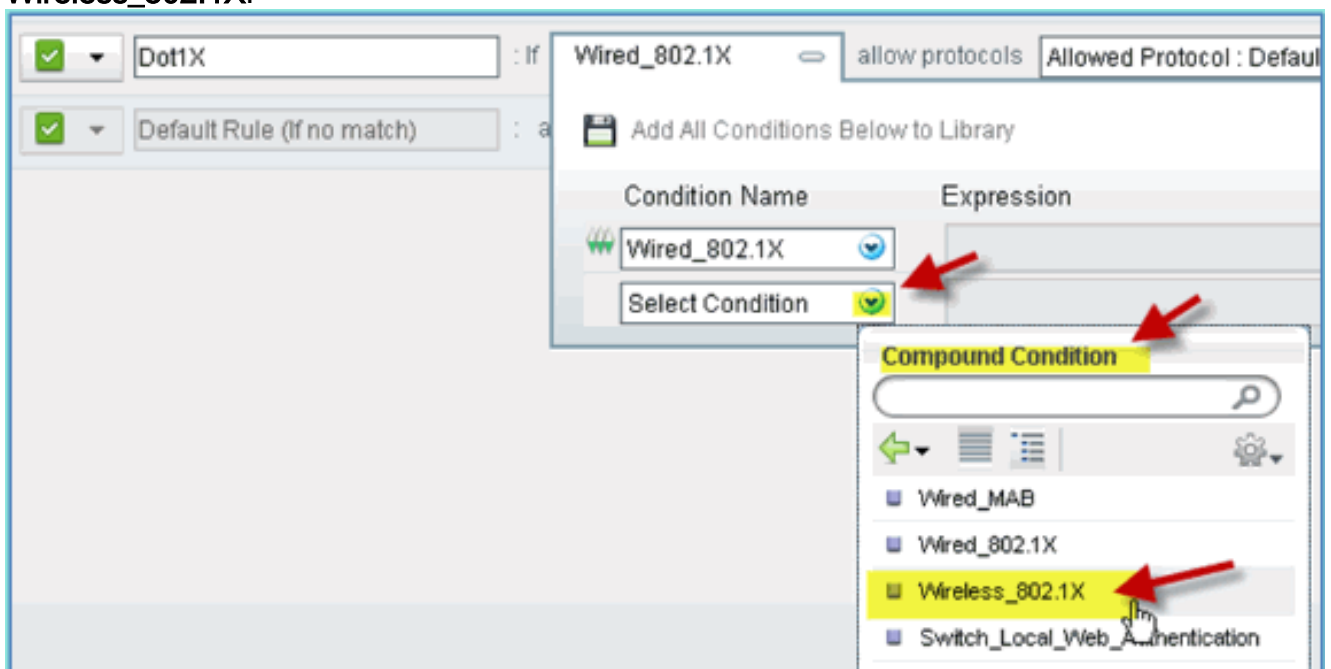
Conclua estes passos:

1. No ISE, navegue para **Política > Autenticação**.
2. Clique para expandir Dot1x > Wired_802.1X (-).
3. Clique no ícone de engrenagem para **Adicionar condição da**

biblioteca.

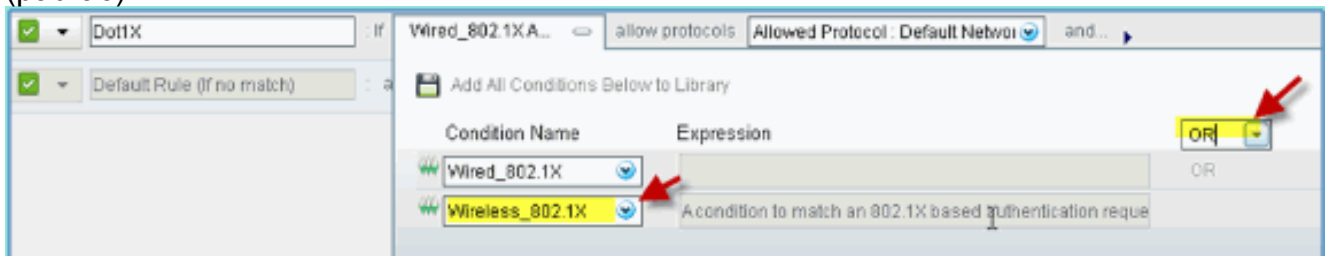


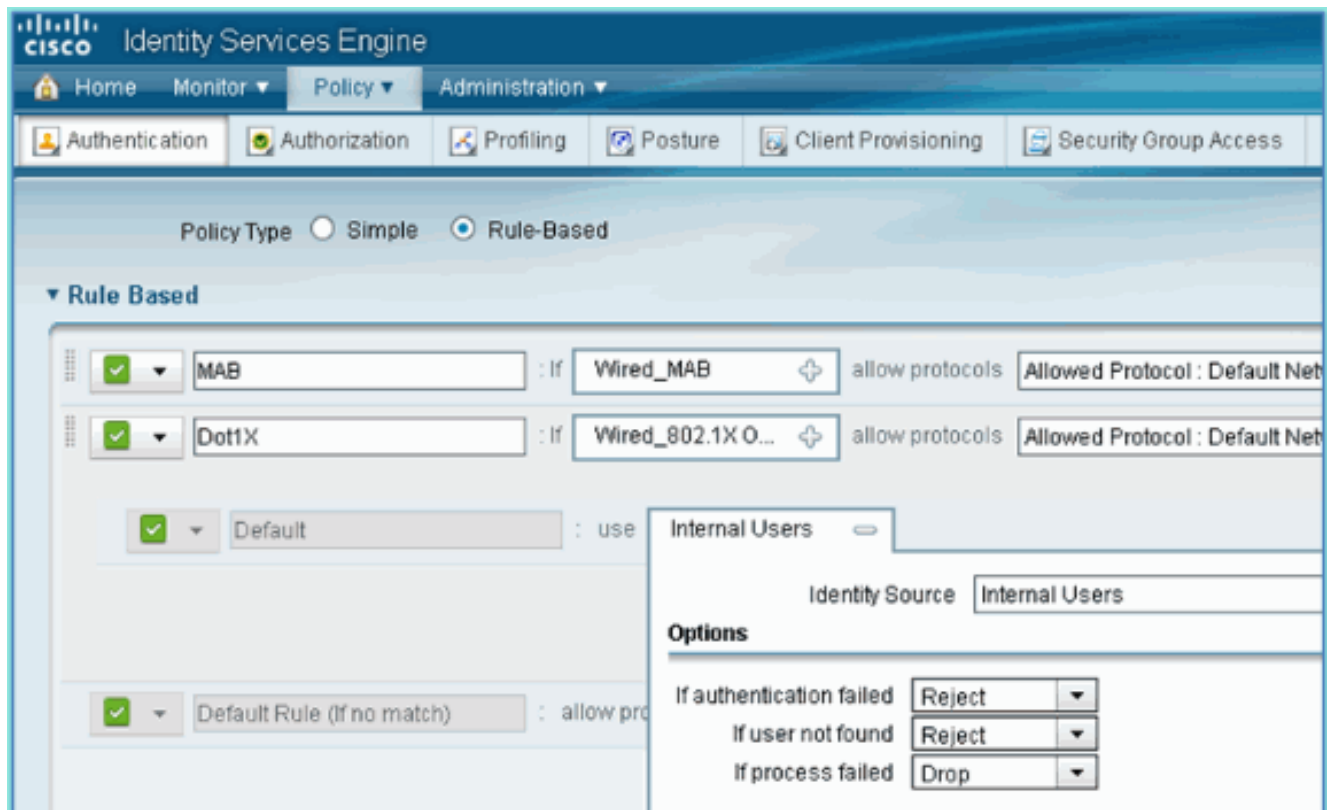
4. Na lista suspensa de seleção de condições, escolha **Condição composta** > **Wireless_802.1X**.



5. Defina a condição Express como **OR**.

6. Expanda a opção após permitir protocolos e aceite o padrão Usuários internos (padrão).





7. Deixe todo o resto como padrão. Clique em **Save** para concluir as etapas.

Controlador de LAN sem fio Bootstrap

Conectando a WLC a uma rede

Um guia de implantação do Cisco 2500 Wireless LAN Controller também está disponível no [Guia de implantação do Cisco 2500 Series Wireless Controller](#).

Configurar o controlador usando o assistente de inicialização

```
(Cisco Controller)
Welcome to the Cisco Wizard Configuration Tool Use the '-' character to backup
Would you like to terminate autoinstall? [yes]: yes AUTO-INSTALL: process terminated
-- no configuration loaded System Name [Cisco_d9:24:44] (31 characters max):
ISE-Podx Enter Administrative User Name (24 characters max): admin
Enter Administrative Password
(3 to 24 characters): Cisco123
Re-enter Administrative Password: Cisco123
Management Interface IP Address: 10.10.10.5
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.10.10.1
Management Interface VLAN Identifier (0 = untagged): 0
Management Interface Port Num [1 to 4]: 1
Management Interface DHCP Server IP Address: 10.10.10.10
Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: ISE
Network Name (SSID): PODx
Configure DHCP Bridging Mode [yes][NO]: no
Allow Static IP Addresses [YES][no]: no
Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.
```

Enter Country Code list (enter 'help' for a list of countries) [US]: US

Enable 802.11b Network [YES][no]: yes

Enable 802.11a Network [YES][no]: yes

Enable 802.11g Network [YES][no]: yes

Enable Auto-RF [YES][no]: yes

Configure a NTP server now? [YES][no]: no

Configure the ntp system time now? [YES][no]: yes

Enter the date in MM/DD/YY format: mm/dd/yy

Enter the time in HH:MM:SS format: hh:mm:ss

Configuration correct? If yes, system will save it and reset. [yes][NO]: yes

Configuration saved!

Resetting system with new configuration...

Restarting system.

Configuração do Switch Vizinho

O controlador está conectado à porta Ethernet no switch vizinho (Fast Ethernet 1). A porta do switch vizinho está configurada como um tronco 802.1Q e permite todas as VLANs no tronco. A VLAN 10 nativa permite que a interface de gerenciamento da WLC seja conectada.

A configuração da porta do switch 802.1Q é a seguinte:

```
switchport
switchport trunk encapsulation dot1q
switchport trunk native VLAN 10
switchport mode trunk
end
```

[Adicionar servidores de autenticação \(ISE\) ao WLC](#)

O ISE precisa ser adicionado à WLC para habilitar o 802.1X e o recurso de CoA para endpoints sem fio.

Conclua estes passos:

1. Abra um navegador e conecte-se à WLC do pod (usando o HTTP seguro) > <https://wlc>.
2. Navegue até **Segurança > Autenticação > Novo**.

MONITOR WLANS CONTROLLER WIRELESS **SECURITY** MANAGEMENT COMMANDS HELP FEEDBACK

RADIUS Authentication Servers > New

Server Index (Priority) 1

Server IP Address 10.10.10.70

Shared Secret Format ASCII

Shared Secret *****

Confirm Shared Secret *****

Key Wrap (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

Port Number 1812

Server Status Enabled

Support for RFC 3576 Enabled

Server Timeout 2 seconds

Network User Enable

Management Enable

IPSec Enable

3. Insira estes valores:Endereço IP do servidor: 10.10.10.70 (verifique a atribuição)Segredo compartilhado: ciscoSuporte para RFC 3576 (CoA): habilitado (padrão)Todo o resto: Padrão
4. Clique em **Aplicar** para continuar.
5. Selecione **Contabilidade RADIUS > adicionar NOVO**.

CISCO

MONITOR WLANS CONTROLLER WIRELESS **SECURITY** MANAGEMENT

Security RADIUS Accounting Servers > New

AAA

- General
- RADIUS
 - Authentication
 - Accounting**
 - Fallback
- TACACS+
- LDAP
- Local Net Users
- MAC Filtering
- Disabled Clients
- User Login Policies
- AP Policies
- Password Policies
- Local EAP
- Priority Order
- Certificate

Server Index (Priority) 2

Server IP Address 10.10.10.70

Shared Secret Format ASCII

Shared Secret *****

Confirm Shared Secret *****

Port Number 1813

Server Status Enabled

Server Timeout 2 seconds

Network User Enable

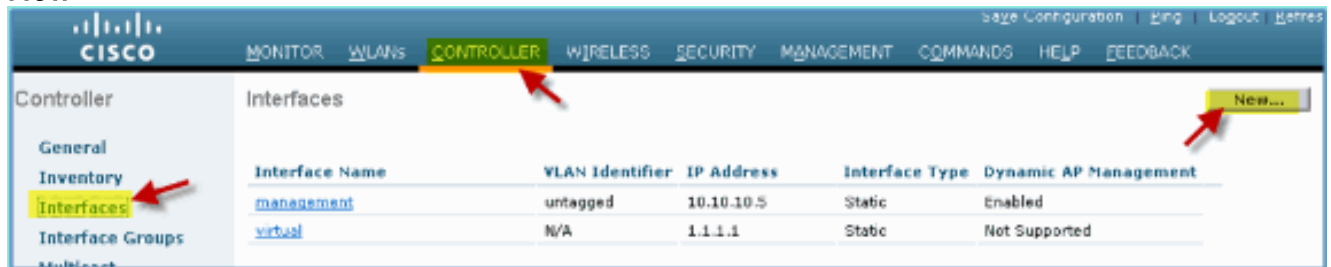
IPSec Enable

6. Insira estes valores:Endereço IP do servidor: 10.10.10.70Segredo compartilhado: ciscoTodo o resto: Padrão
7. Clique em **Apply** e salve a configuração da WLC.

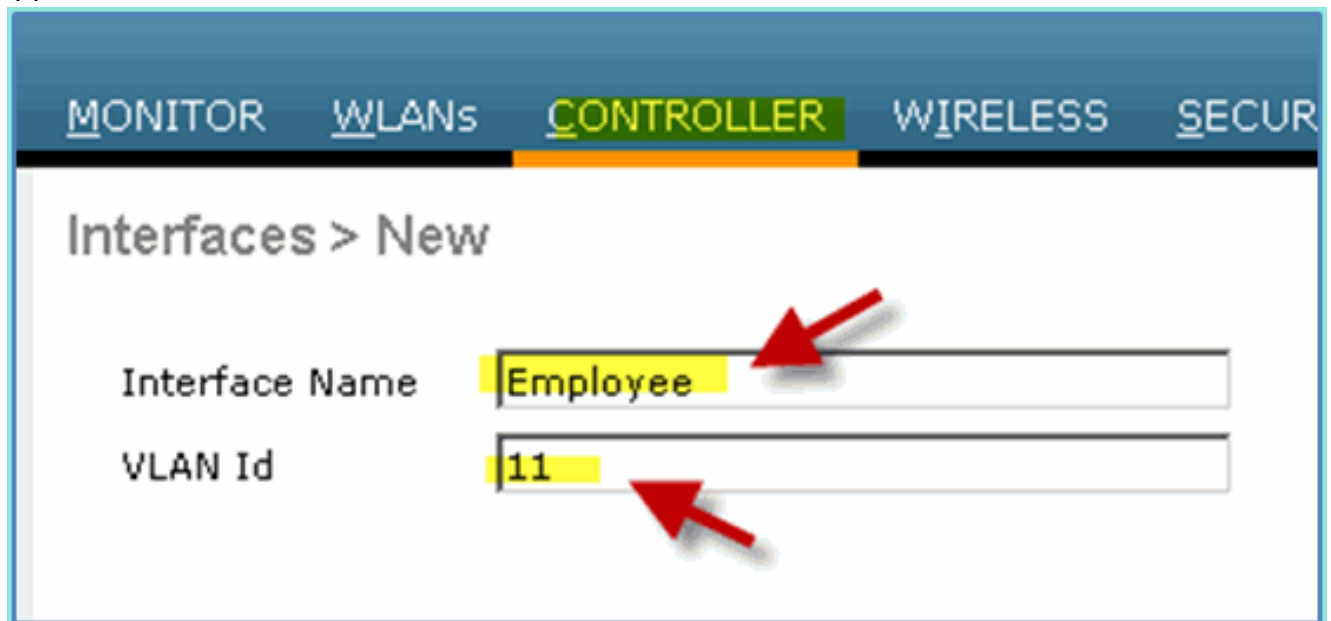
[Criar interface dinâmica de funcionário da WLC](#)

Conclua estes passos para adicionar uma nova interface dinâmica para a WLC e mapeá-la para a VLAN do funcionário:

1. Na WLC, navegue até **Controller > Interfaces**. Em seguida, clique em **New**.



2. Na WLC, navegue até **Controller > Interfaces**. Digite o seguinte: Nome da Interface: Funcionário ID da VLAN:
11



3. Informe o seguinte para a interface do Funcionário: Número da porta: 1 Identificador de VLAN: 11 Endereço IP: 10.10.11.5 Máscara de rede: 255.255.255.0 Gateway: 10.10.11.1 DHCP: 10.10.10.10

Configuration

Quarantine

Quarantine Vlan Id

Physical Information

Port Number

Backup Port

Active Port

Enable Dynamic AP Management

Interface Address

VLAN Identifier

IP Address

Netmask

Gateway

DHCP Information

Primary DHCP Server

Secondary DHCP Server

4. Confirme se a nova interface dinâmica de funcionário foi criada.

CISCO

MONITOR WLANs **CONTROLLER** WIRELESS SECURITY MANAGEMENT COMMUNITY

Controller

General

Inventory

Interfaces

Interface Groups

Multicast

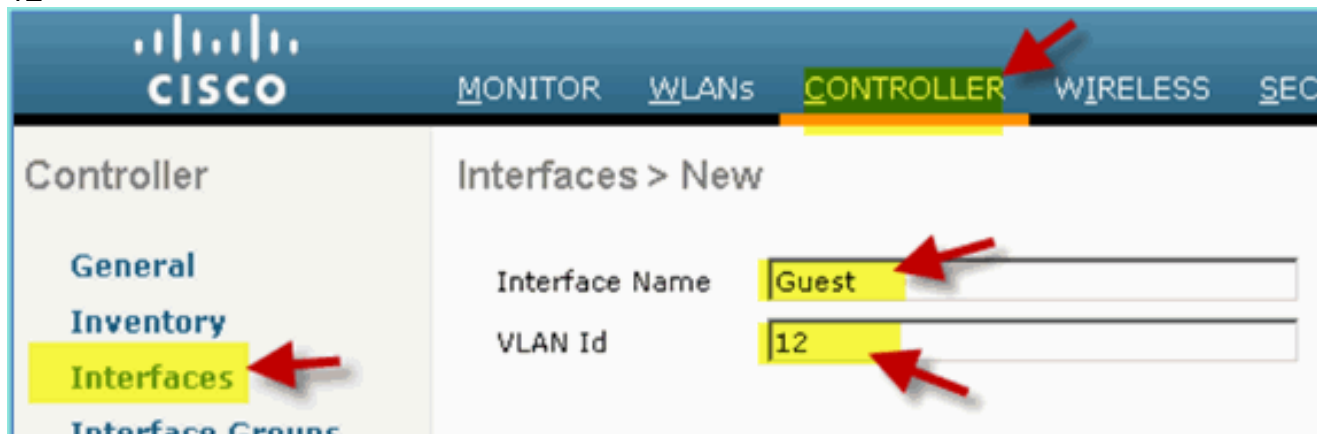
Interfaces

Interface Name	VLAN Identifier	IP Address	Interface Type
employee	11	10.10.11.5	Dynamic
management	untagged	10.10.10.5	Static
virtual	N/A	1.1.1.1	Static

Criar interface dinâmica de convidado WLC

Conclua estes passos para adicionar uma nova interface dinâmica para a WLC e mapeá-la para a VLAN Convidada:

1. Na WLC, navegue até **Controller > Interfaces**. Em seguida, clique em **New**.
2. Na WLC, navegue até **Controller > Interfaces**. Digite o seguinte: Nome da interface: Convidado ID da VLAN:
12



3. Insira estes para a interface de convidado: Número da porta: 1 Identificador de VLAN: 12 Endereço IP: 10.10.12.5 Máscara de rede: 255.255.255.0 Gateway: 10.10.12.1 DHCP: 10.10.10.10

Configuration

Quarantine
Quarantine Vlan Id

Physical Information

Port Number
Backup Port
Active Port
Enable Dynamic AP Management

Interface Address

VLAN Identifier
IP Address
Netmask
Gateway

DHCP Information

Primary DHCP Server
Secondary DHCP Server

Access Control List

ACL Name

Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.

4. Confirme se a interface de convidado foi adicionada.

Interface Name	VLAN Identifier	IP Address	Interface Type
employee	11	10.10.11.5	Dynamic
guest	12	10.10.12.5	Dynamic
management	untagged	10.10.10.5	Static
virtual	N/A	1.1.1.1	Static

Adicionar WLAN 802.1x

A partir do bootstrap inicial da WLC, pode ter sido criada uma WLAN padrão. Em caso afirmativo, modifique-a ou crie uma nova WLAN para suportar a autenticação 802.1X sem fio, conforme instruído no guia.

Conclua estes passos:

1. Na WLC, navegue até **WLAN > Create New**.



2. Para a WLAN, insira o seguinte: Nome do perfil: pod1xSSID: Igual



3. Para a guia Configurações de WLAN > Geral, use o seguinte: Política de rádio: tudoInterface/grupo: gerenciamentoTodo o resto: padrão

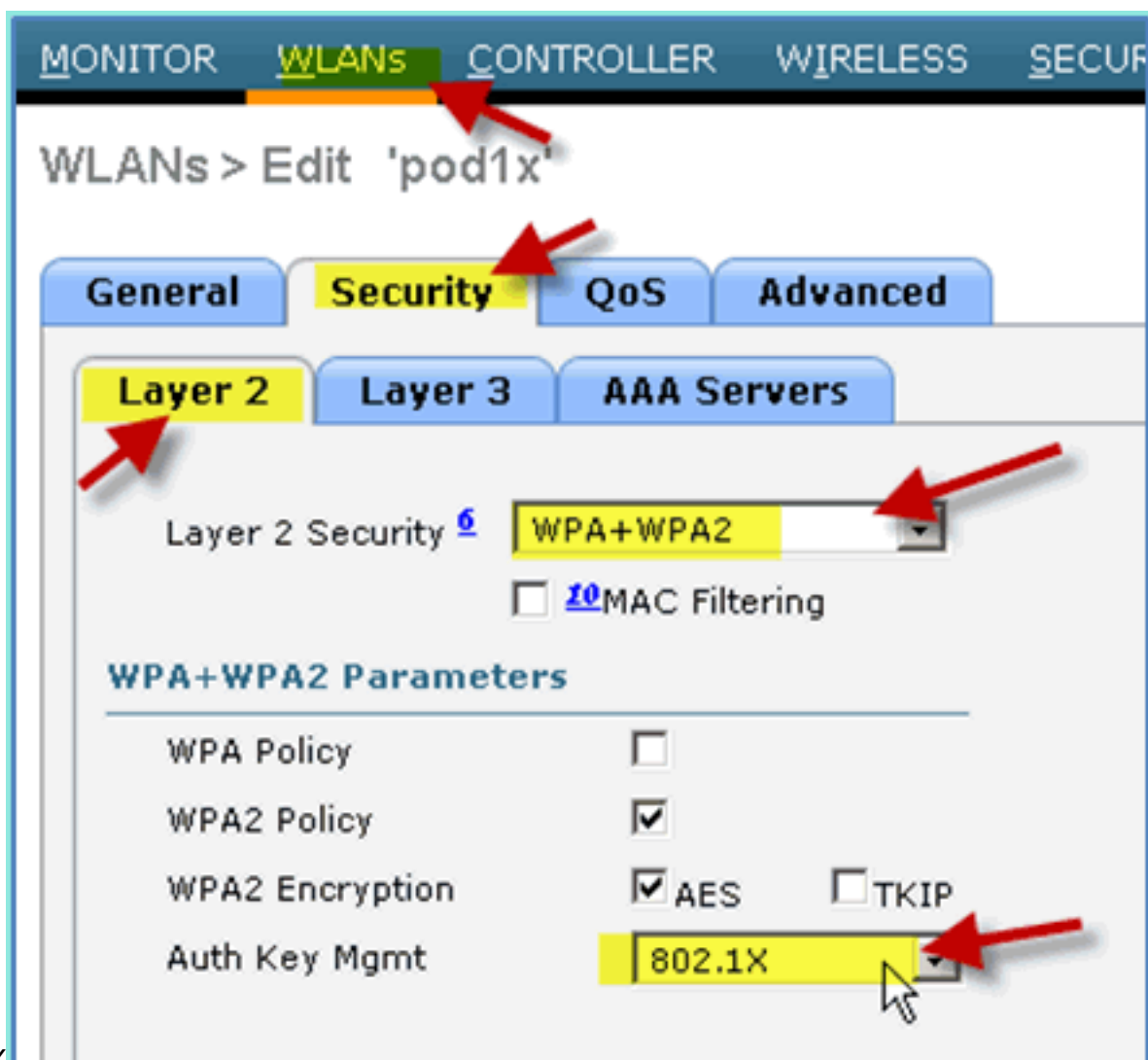
MONITOR WLANS CONTROLLER WIRELESS SECURITY

WLANs > Edit 'pod1x'

General Security QoS Advanced

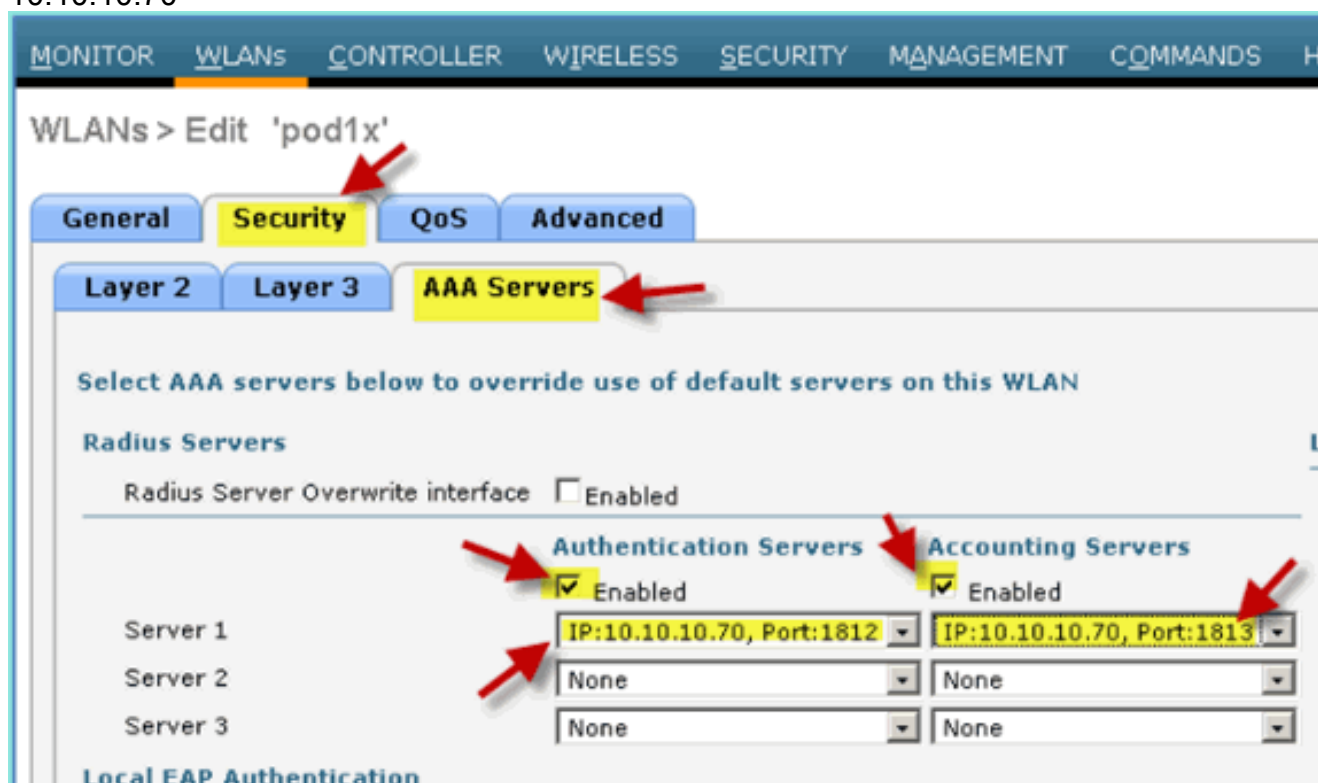
Profile Name	pod1x
Type	WLAN
SSID	pod1x
Status	<input type="checkbox"/> Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab w
Radio Policy	All
Interface/Interface Group(G)	management
Multicast Vlan Feature	<input type="checkbox"/> Enabled
Broadcast SSID	<input checked="" type="checkbox"/> Enabled

4. Para a guia WLAN > Security > Layer 2, defina o seguinte: Segurança de Camada 2: WPA+WPA2 Política / Criptografia WPA2: Habilitada / AES Gerenciamento de chave de autenticação:



802.1X

5. Para a guia WLAN > Security > AAA Servers, defina o seguinte: Radio Server Overwrite Interface: Disabled (Interface de substituição do servidor de rádio: desativada) Servidores de Autenticação/Contabilização: Habilitados Servidor 1: 10.10.10.70



6. Para a guia WLAN > Advanced, defina o seguinte: Allow AAA Override: Enabled (Permitir substituição de AAA) Estado do NAC: Radius NAC (selecionado)

The screenshot shows the 'WLANs > Edit 'pod1x'' configuration page. The 'Advanced' tab is selected and highlighted in yellow. A red arrow points to the 'Advanced' tab. Below the tabs, the 'Allow AAA Override' option is checked and set to 'Enabled', with a red arrow pointing to it. The 'NAC State' dropdown menu is set to 'Radius NAC', also with a red arrow pointing to it. Other visible options include Coverage Hole Detection (Enabled), Enable Session Timeout (1800), Aironet IE (Enabled), Diagnostic Channel (Disabled), IPv6 Enable (Disabled), Override Interface ACL (None), P2P Blocking Action (Disabled), Client Exclusion (Enabled, 60), Maximum Allowed Clients (0), and Static IP Tunneling (Disabled). On the right side, there are sections for DHCP, Management Frame Protection (MFP), DTIM Period, and NAC. The NAC section shows 'NAC State' set to 'Radius NAC'.

7. Volte para a guia WLAN > General > Enable WLAN (WLAN > guia Geral > Ativar WLAN) (caixa de seleção).

WLANs > Edit 'pod1x'

General Security QoS Advanced

Profile Name	pod1x
Type	WLAN
SSID	pod1x
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab)
Radio Policy	All
Interface/Interface Group(G)	management
Multicast Vlan Feature	<input type="checkbox"/> Enabled
Broadcast SSID	<input checked="" type="checkbox"/> Enabled

Testar interfaces dinâmicas de WLC

Você precisa verificar rapidamente se há interfaces válidas para funcionários e convidados. Use qualquer dispositivo para associar-se à WLAN e, em seguida, altere a atribuição da interface WLAN.

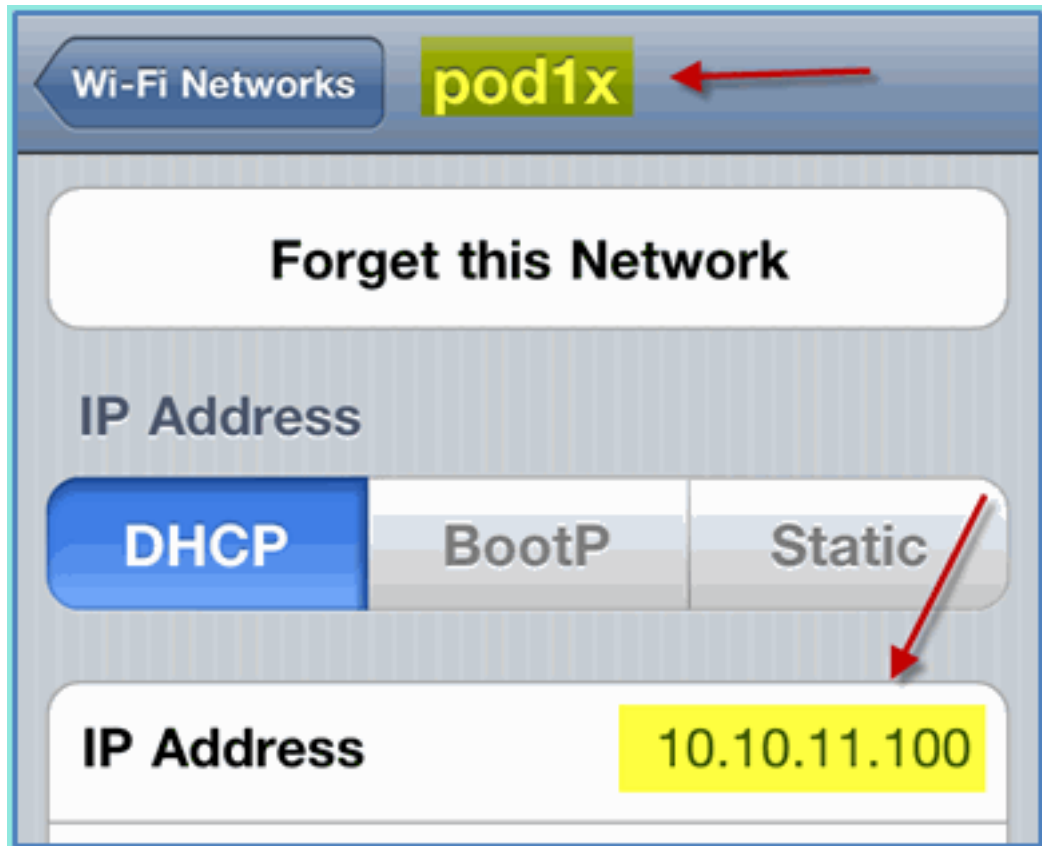
1. Na WLC, navegue até **WLAN > WLANs**. Clique para editar o SSID seguro criado no exercício anterior.
2. Altere a Interface/Grupo de interface para **Funcionário** e clique em **Aplicar**.

The screenshot displays the Cisco configuration interface for WLANs. At the top, the navigation menu includes MONITOR, WLANs (highlighted), CONTROLLER, WIRELESS, and SECURITY. The main content area is titled 'WLANs > Edit 'pod1x''. On the left, a sidebar shows 'WLANs' and 'Advanced' options, with 'WLANs' selected. The main configuration area has tabs for 'General', 'Security', 'QoS', and 'Advanced', with 'General' active. The configuration details are as follows:

Profile Name	pod1x
Type	WLAN
SSID	pod1x
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security to
Radio Policy	All
Interface/Interface Group(G)	management employee guest management
Multicast Vlan Feature	<input type="checkbox"/> Enabled
Broadcast SSID	<input checked="" type="checkbox"/> Enabled

Red arrows point to the 'WLANs' menu item, the 'WLANs' sidebar item, the 'General' tab, and the 'employee' option in the 'Interface/Interface Group(G)' dropdown menu.

3. Se configurado corretamente, um dispositivo recebe um endereço IP da VLAN do funcionário (10.10.11.0/24). Este exemplo mostra um dispositivo iOS que obtém um novo



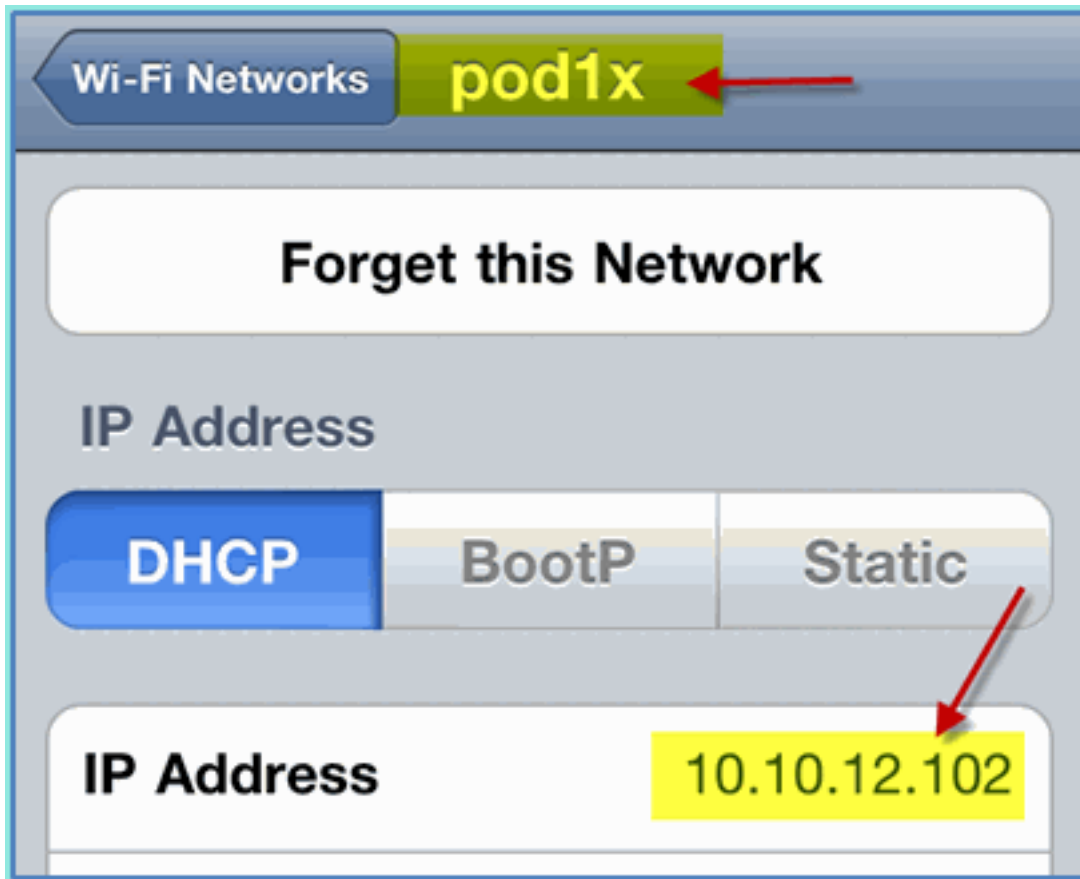
endereço IP.

4. Depois que a interface anterior tiver sido confirmada, altere a atribuição da interface WLAN para **Guest** e clique em **Apply**.

The screenshot displays the Cisco WLAN configuration page. At the top, the Cisco logo is on the left, and navigation tabs for 'MONITOR', 'WLANs', 'CONTROLLER', and 'WIRELESS' are on the right. The 'WLANs' tab is selected. On the left sidebar, a tree view shows 'WLANs' expanded, with 'WLANs' and 'Advanced' sub-items. The main content area is titled 'WLANs > Edit 'pod1x''. Below this title are four tabs: 'General' (selected), 'Security', 'QoS', and 'Advanced'. The 'General' tab contains the following configuration details:

Profile Name	pod1x
Type	WLAN
SSID	pod1x
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under se
Radio Policy	All
Interface/Interface Group(G)	quest
Multicast Vlan Feature	quest
Broadcast SSID	<input checked="" type="checkbox"/> Enabled

5. Se configurado corretamente, um dispositivo recebe um endereço IP da VLAN convidada (10.10.12.0/24). Este exemplo mostra um dispositivo iOS que obtém um novo endereço



IP.

6. **IMPORTANTE:** Altere a atribuição da Interface de volta para o gerenciamento original.
7. Clique em **Apply** e salve a configuração para a WLC.

[Autenticação sem fio para iOS \(iPhone/iPad\)](#)

Associe à WLC através de um SSID autenticado um usuário INTERNO (ou integrado, usuário do AD) usando um dispositivo iOS, como um iPhone, iPad ou iPod. Ignore essas etapas se não for aplicável.

1. No dispositivo iOS, vá para as configurações de WLAN. Ative o WIFI e selecione o SSID habilitado para 802.1X criado na seção anterior.
2. Forneça estas informações para conectar: Nome de usuário: funcionário (interno - Funcionário) ou contratado (interno - Contratante) Senha:



XXXX

3. Clique para aceitar o certificado



ISE.

4. Confirme se o dispositivo iOS está obtendo um endereço IP da interface de gerenciamento



(VLAN10).

5. Em WLC > Monitor > Clients, verifique as informações de endpoint incluindo uso, estado e tipo de EAP.

The screenshot displays the Cisco ISE Monitor interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', and 'WIRELESS'. The left sidebar shows a menu with 'Monitor' selected, and sub-items like 'Summary', 'Access Points', 'Cisco CleanAir', 'Statistics', 'CDP', 'Rogues', 'Clients', and 'Multicast'. The main content area is titled 'Clients > Detail' and is divided into two sections: 'Client Properties' and 'Security Information'.

Client Properties

MAC Address	5c:59:48:40:82:8d
IP Address	10.10.10.102
Client Type	Regular
User Name	aduser
Port Number	1
Interface	management
Mobility Peer IP Address	N/A
Policy Manager State	RUN
Management Frame Protection	No

Security Information

Security Policy Completed	Yes
Policy Type	RSN (WPA2)
Encryption Cipher	CCMP (AES)
EAP Type	PEAP
SNMP NAC State	Access
Radius NAC State	RUN
AAA Override ACL Name	none



6. Da mesma forma, as informações do cliente podem ser fornecidas pela página ISE > Monitorar > Autenticação.

CISCO Identity Services Engine

Home Monitor Policy Administration

Authentications Alarms Reports Troubleshoot

Add or Remove Columns Refresh

Time	Status	Details	Username	Endpoint ID	Network Device	Authorization Profiles	Ident
Jul 13,11 04:39:36.573 PM	✓		aduser	5C:59:48:40:82:8D	WLC	PermitAccess	
Jul 13,11 04:38:46.285 PM	✓		aduser	5C:59:48:40:82:8D	WLC	PermitAccess	

7. Clique no ícone **Details** para fazer o drill-down para obter informações detalhadas da sessão.

CISCO Identity Services Engine

Showing Page 1 of 1 | First Prev

AAA Protocol > RADIUS Authentication Detail

RADIUS Audit Session ID : 0a0a0a050000000d4e1e2a45
 AAA session ID : ise/99967658/11
 Date : July 13,2011

Generated on July 13, 2011 4:41:11 PM PDT

Authentication Summary	
Logged At:	July 13,2011 4:39:36.573 PM
RADIUS Status:	Authentication succeeded
NAS Failure:	
Username:	<u>aduser</u>
MAC/IP Address:	<u>5C:59:48:40:82:8D</u>
Network Device:	<u>WLC : 10.10.10.5 :</u>
Allowed Protocol:	<u>Default Network Access</u>
Identity Store:	AD1
Authorization Profiles:	PermitAccess
SGA Security Group:	
Authentication Protocol :	PEAP(EAP-MSCHAPv2)

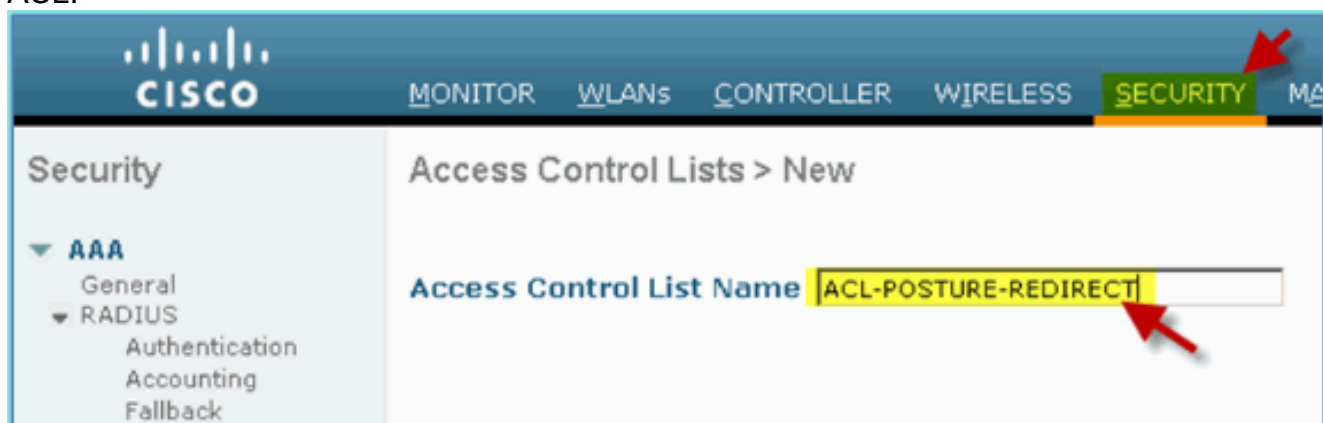
Adicionar ACL de redirecionamento de postura à WLC

A ACL de redirecionamento de postura é configurada na WLC, onde o ISE usará para restringir a postura do cliente. Efetivamente e no mínimo, a ACL permite o tráfego entre o ISE. Regras opcionais podem ser adicionadas nessa ACL, se necessário.

1. Navegue para **WLC > Security > Access Control Lists > Access Control Lists**. Clique em **New**.



2. Forneça um nome (ACL-POSTURE-REDIRECT) para a ACL.



3. Clique em **Add New Rule** para a nova ACL. Defina os seguintes valores para a sequência ACL #1. Clique em **Apply** quando terminar. Fonte: Qualquer Destino: Endereço IP 10.10.10.70, 255.255.255.255 Protocolo: Qualquer Ação: Permitir

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

Access Control Lists > Rules > Edit

Sequence:

Source:

Destination: IP Address: Netmask:

Protocol:

DSCP:

Direction:

Action:

4. A sequência de confirmação foi adicionada.

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	10.10.10.70 / 255.255.255.255	Any	Any	Any	Any	Any	0

5. Clique em **Adicionar nova regra**. Defina os seguintes valores para a sequência ACL #2. Clique em **Apply** quando terminar. Origem: Endereço IP 10.10.10.70, 255.255.255.255 Destino: qualquer um Protocolo: Qualquer Ação: Permitir

Sequence:

Source: IP Address: Netmask:

Destination:

Protocol:

DSCP:

Direction:

Action:

6. A sequência de confirmação foi adicionada.

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
<u>1</u>	Permit	0.0.0.0 /	10.10.10.70 /	Any	Any	Any	Any	Any
		0.0.0.0	255.255.255.255					
<u>2</u>	Permit	10.10.10.70 /	0.0.0.0 /	Any	Any	Any	Any	Any
		255.255.255.255	0.0.0.0					

7. Defina os seguintes valores para a sequência ACL #3. Clique em **Apply** quando terminar. Fonte: Qualquer Destino: qualquer um Protocolo: UDP Porta de origem: DNS Porta de destino: qualquer uma Ação:

The screenshot shows a configuration interface for an ACL rule. Red arrows point to the following fields:

- Sequence:** 3
- Source:** Any
- Destination:** Any
- Protocol:** UDP
- Source Port:** DNS
- Destination Port:** Any
- DSCP:** Any
- Direction:** Any
- Action:** Permit

Permitir

8. A sequência de confirmação foi adicionada.

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
<u>1</u>	Permit	0.0.0.0 /	10.10.10.70 /	Any	Any	Any	Any	Any
		0.0.0.0	255.255.255.255					
<u>2</u>	Permit	10.10.10.70 /	0.0.0.0 /	Any	Any	Any	Any	Any
		255.255.255.255	0.0.0.0					
<u>3</u>	Permit	0.0.0.0 /	0.0.0.0 /	UDP	DNS	Any	Any	Any
		0.0.0.0	0.0.0.0					

9. Clique em **Adicionar nova regra**. Defina os seguintes valores para a sequência ACL #4.

Clique em **Apply** quando terminar. Fonte: Qualquer Destino: qualquer um Protocolo: UDP Porta de origem: Qualquer Porta de destino: DNS Ação: Permitir

The image shows a configuration interface for a firewall rule. The fields and their values are as follows:

- Sequence:** 4
- Source:** Any
- Destination:** Any
- Protocol:** UDP
- Source Port:** Any
- Destination Port:** DNS
- DSCP:** Any
- Direction:** Any
- Action:** Permit

10. A sequência de confirmação foi adicionada.

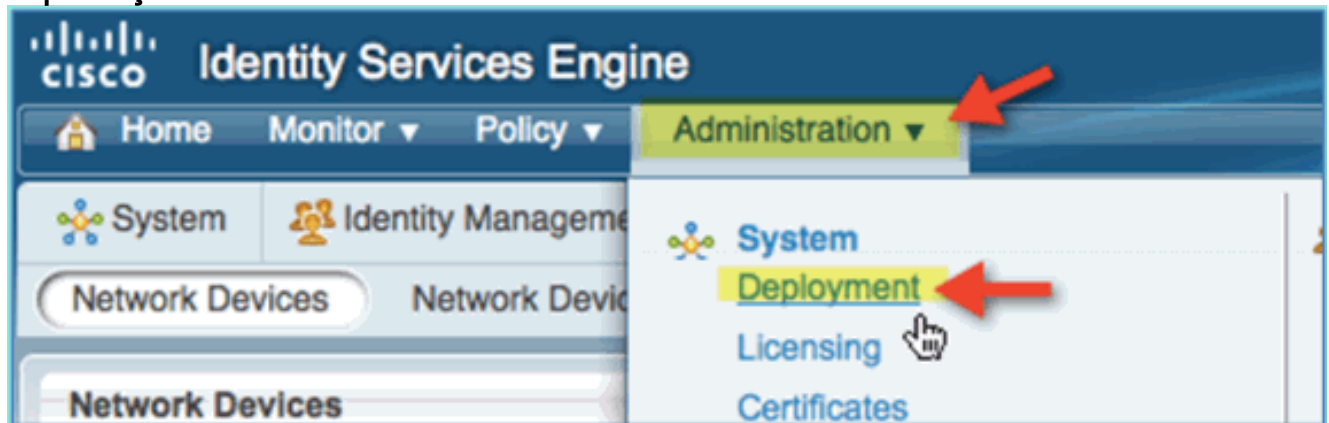
Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
1	Permit	0.0.0.0 /	10.10.10.70 /	Any	Any	Any	Any	Any
2	Permit	0.0.0.0 /	255.255.255.255 /	Any	Any	Any	Any	Any
3	Permit	10.10.10.70 /	0.0.0.0 /	Any	Any	Any	Any	Any
3	Permit	255.255.255.255 /	0.0.0.0 /	UDP	DNS	Any	Any	Any
4	Permit	0.0.0.0 /	0.0.0.0 /	UDP	Any	DNS	Any	Any

11. Salve a configuração atual da WLC.

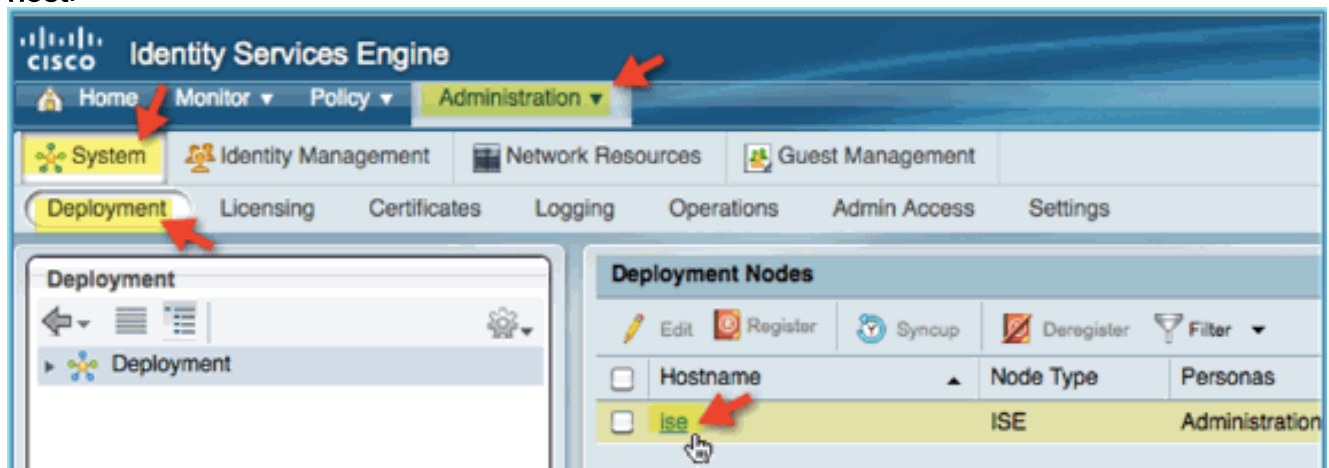
Ativar testes de criação de perfil no ISE

O ISE precisa ser configurado como testes para criar perfis de endpoints com eficiência. Por padrão, essas opções estão desativadas. Esta seção mostra como configurar o ISE para ser testadores.

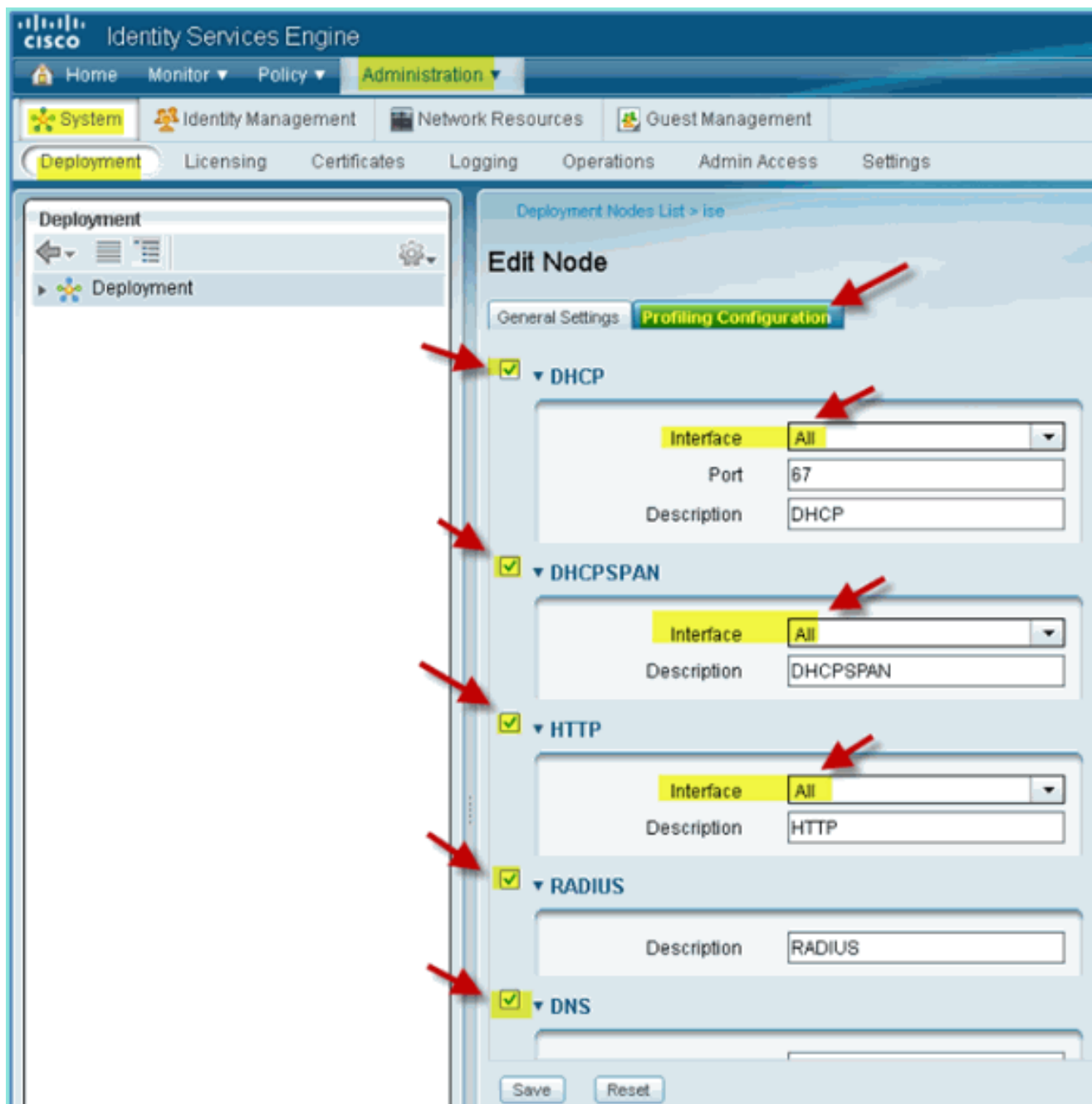
1. No gerenciamento do ISE, navegue até **Administração > Sistema > Implantação**.



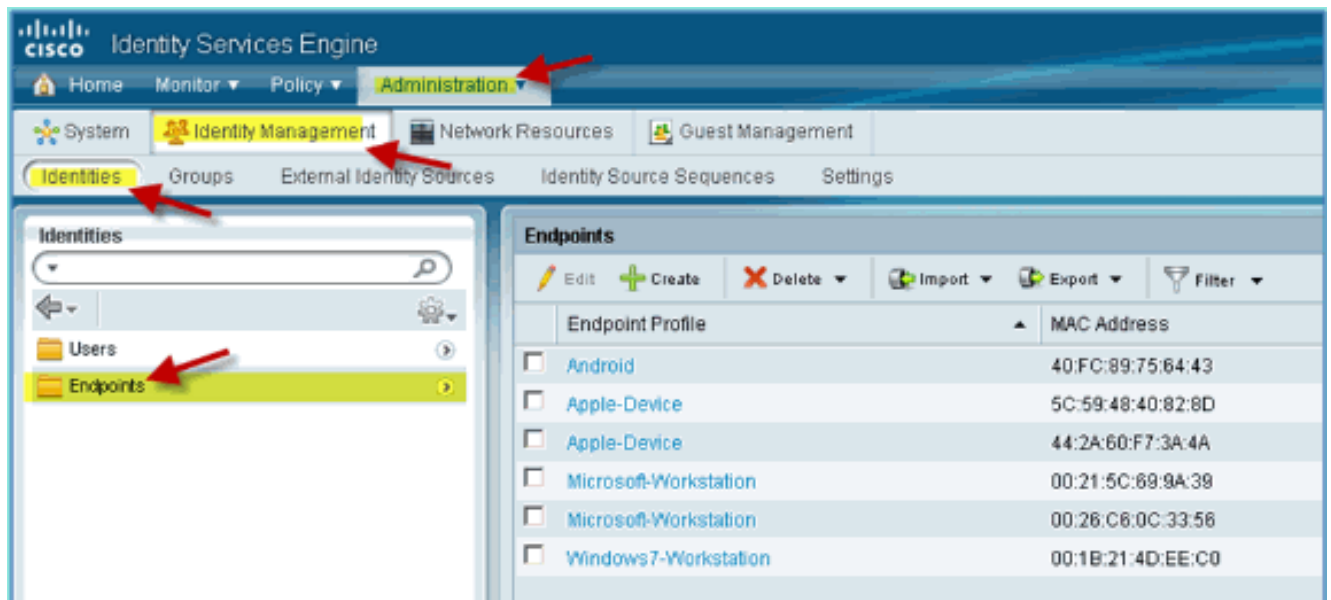
2. Escolha **ISE**. Clique em **Edit ISE host**.



3. Na página Editar nó, selecione a Configuração de criação de perfil e configure o seguinte: DHCP: Enabled, All (ou default) (Habilitado, Todos [ou padrão]) DHCPSPAN: Habilitado, Todos (ou padrão) HTTP: Habilitado, Todos (ou padrão) RADIUS: habilitado, N/DDNS: Habilitado, N/D



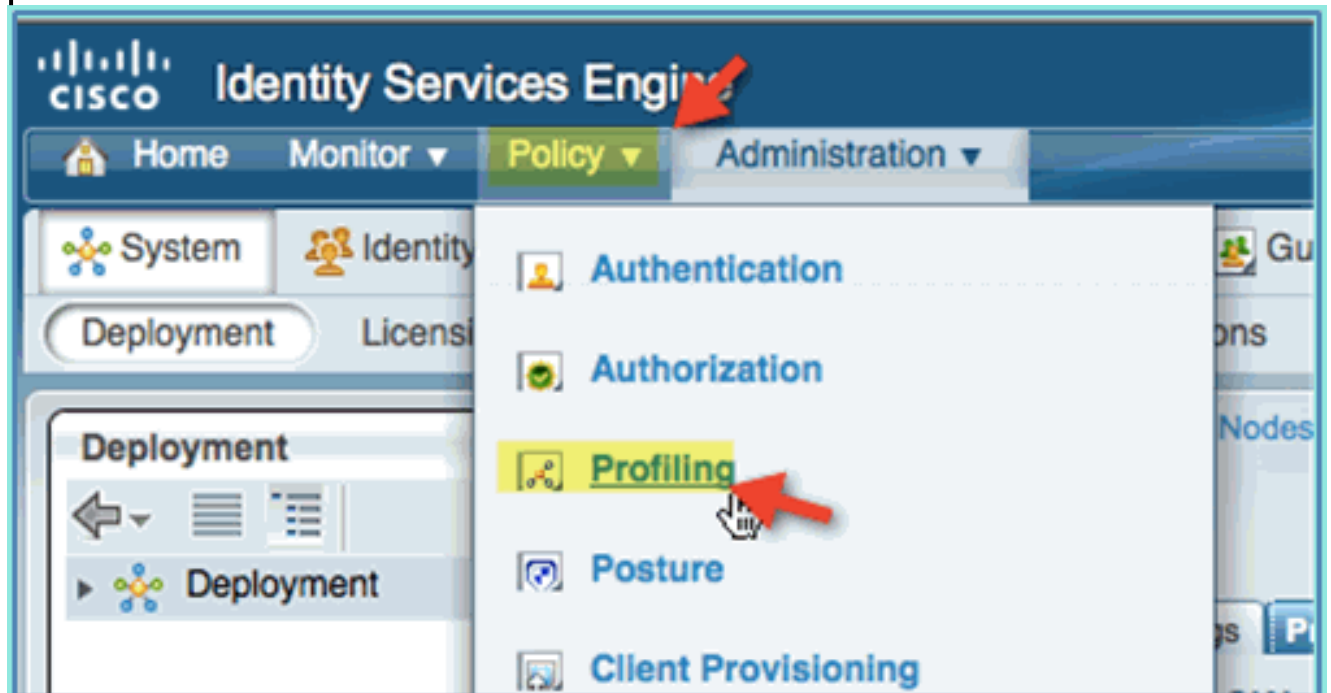
4. Reassocie os dispositivos (iPhone/iPads/Droids/Mac, etc.).
5. Confirme as identidades do ponto de extremidade do ISE. Navegue até **Administração > Gerenciamento de identidades > Identidades**. Clique em Endpoints para listar o que foi perfilado. **Observação:** a criação de perfil inicial é a partir de testes RADIUS.



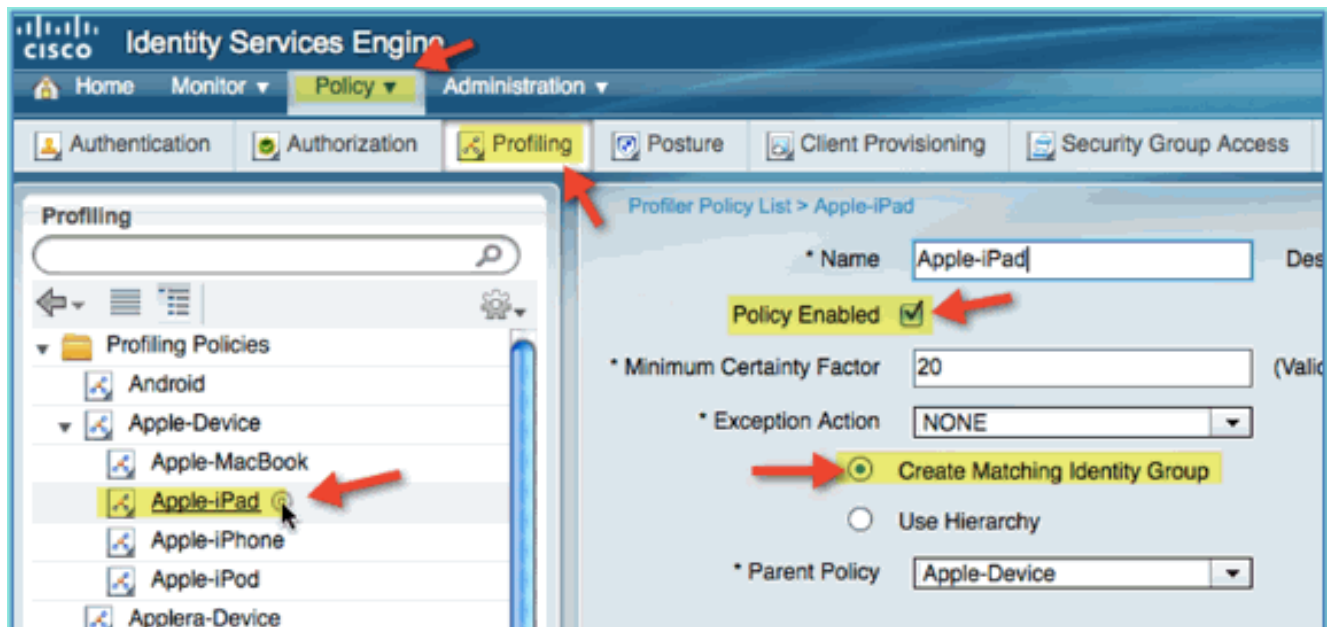
Ativar políticas de perfil do ISE para dispositivos

O ISE fornece uma biblioteca de vários perfis de endpoint prontos para uso. Conclua estas etapas para ativar perfis para dispositivos:

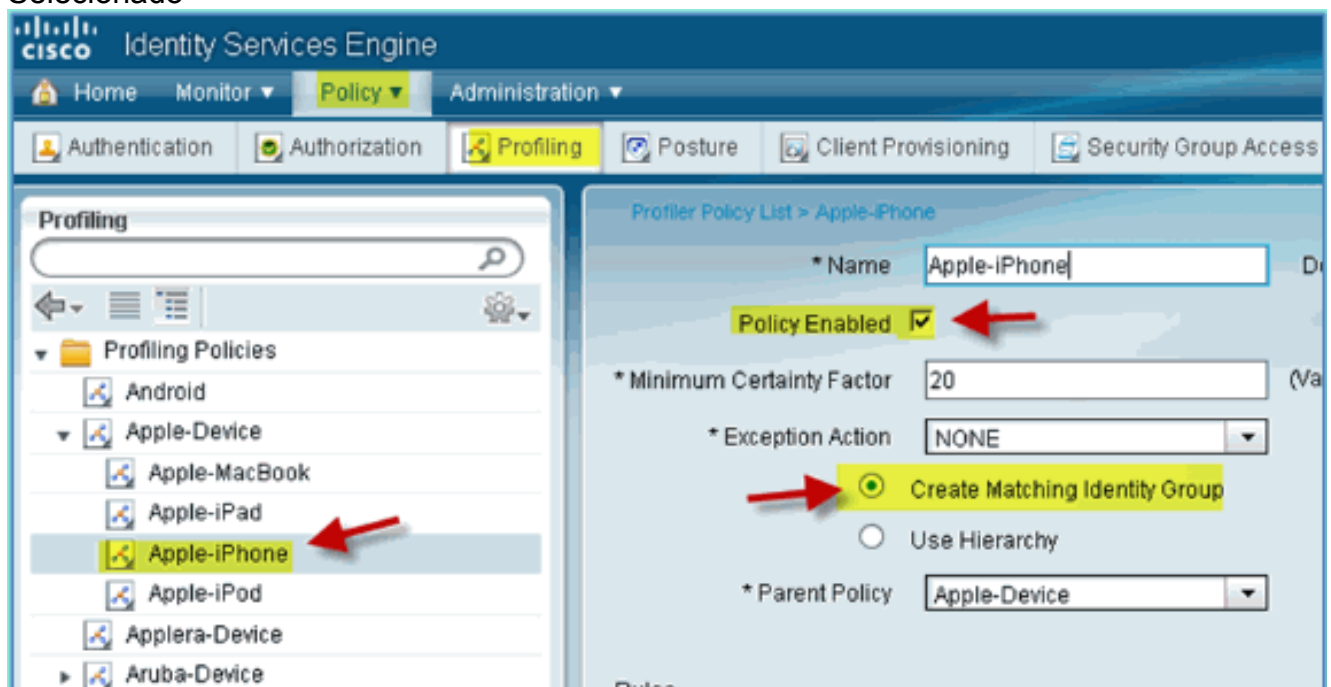
1. No ISE, navegue para **Política > Criação de perfil**.



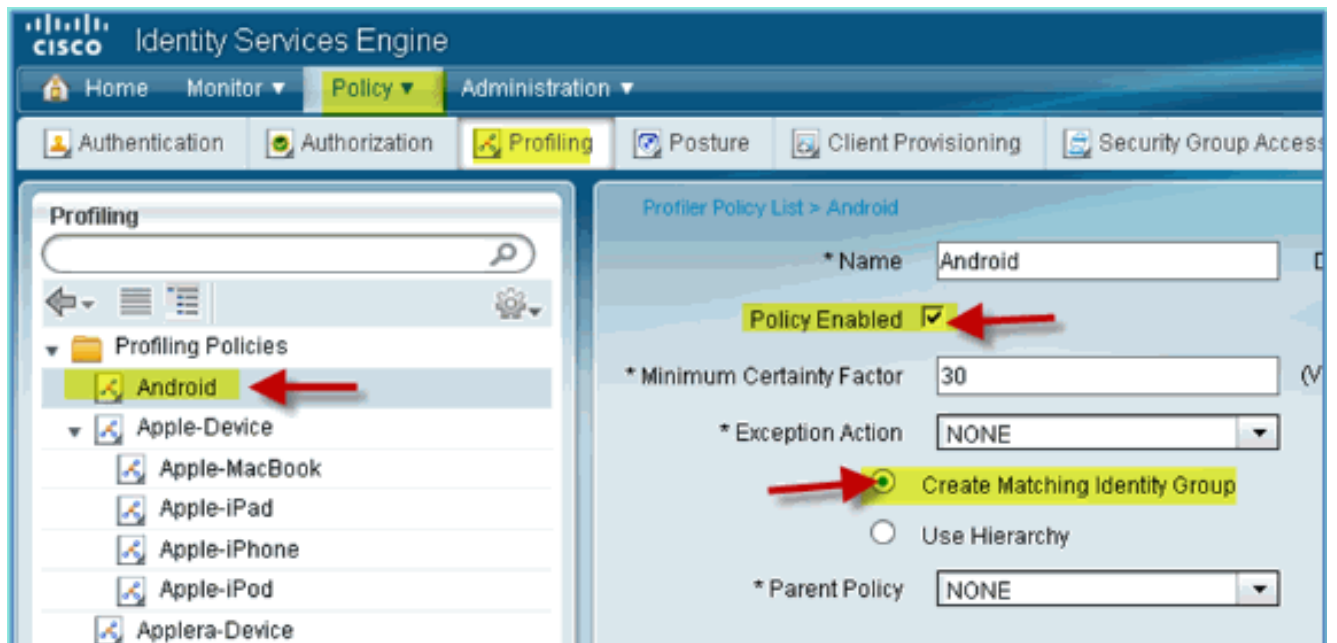
2. No painel esquerdo, expanda **Profiling Policies**.
3. Clique em **Apple Device > Apple iPad** e defina o seguinte: Política habilitada: habilitada
Criar Grupo de Identidades Correspondente:
Selecionado



4. Clique em **Apple Device > Apple iPhone**, defina o seguinte: Política habilitada: habilitada Criar Grupo de Identidades Correspondente: Selecionado



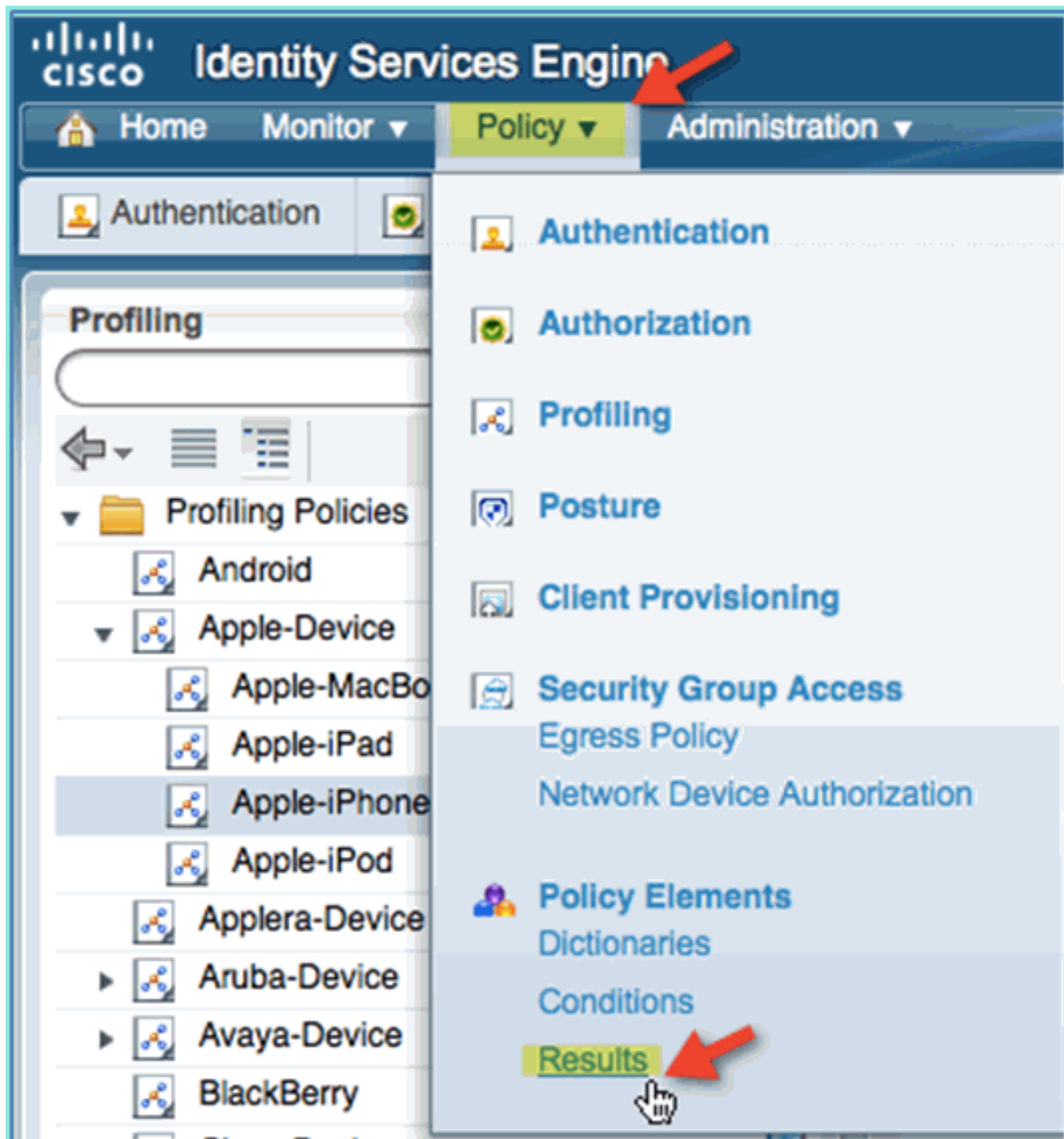
5. Clique em **Android**, defina o seguinte: Política habilitada: habilitada Criar Grupo de Identidades Correspondente: Selecionado



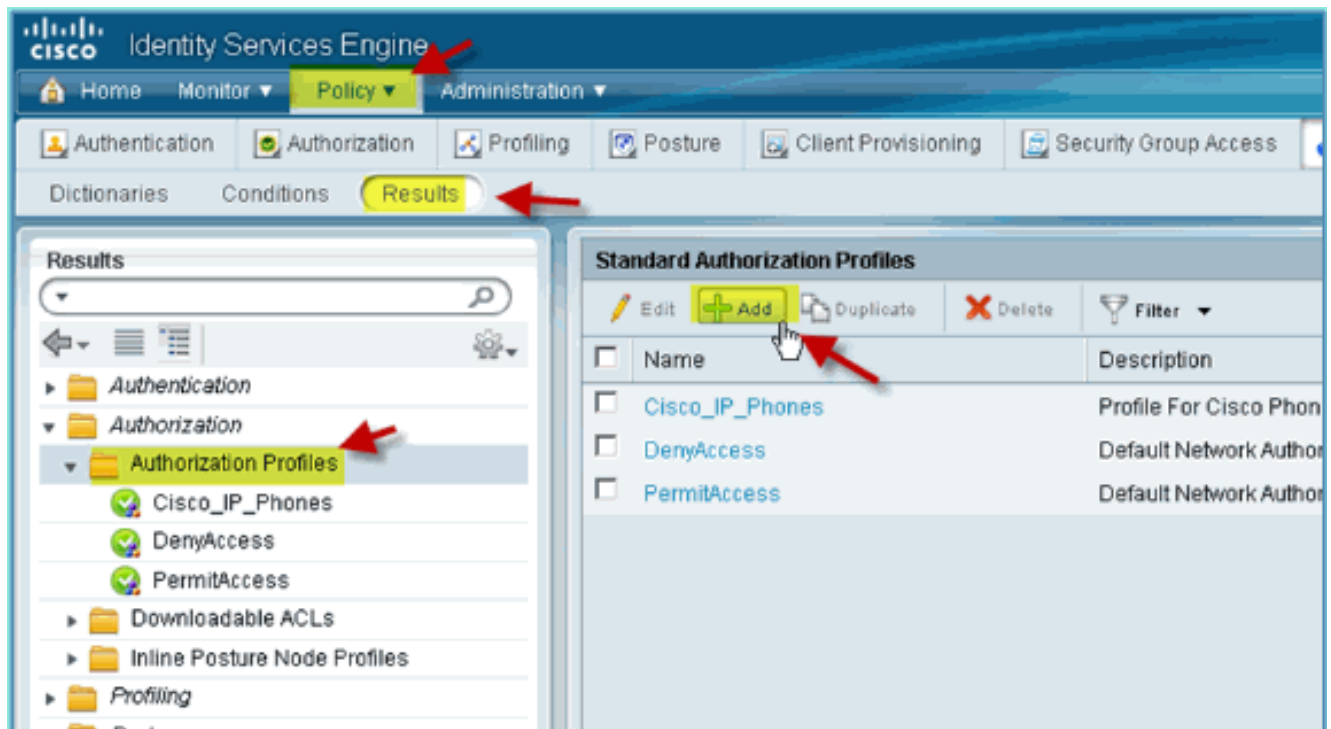
[Perfil de autorização do ISE para redirecionamento de descoberta de postura](#)

Conclua estas etapas para configurar um redirecionamento de postura de política de autorização que permita que novos dispositivos sejam redirecionados para o ISE para detecção e criação de perfil adequados:

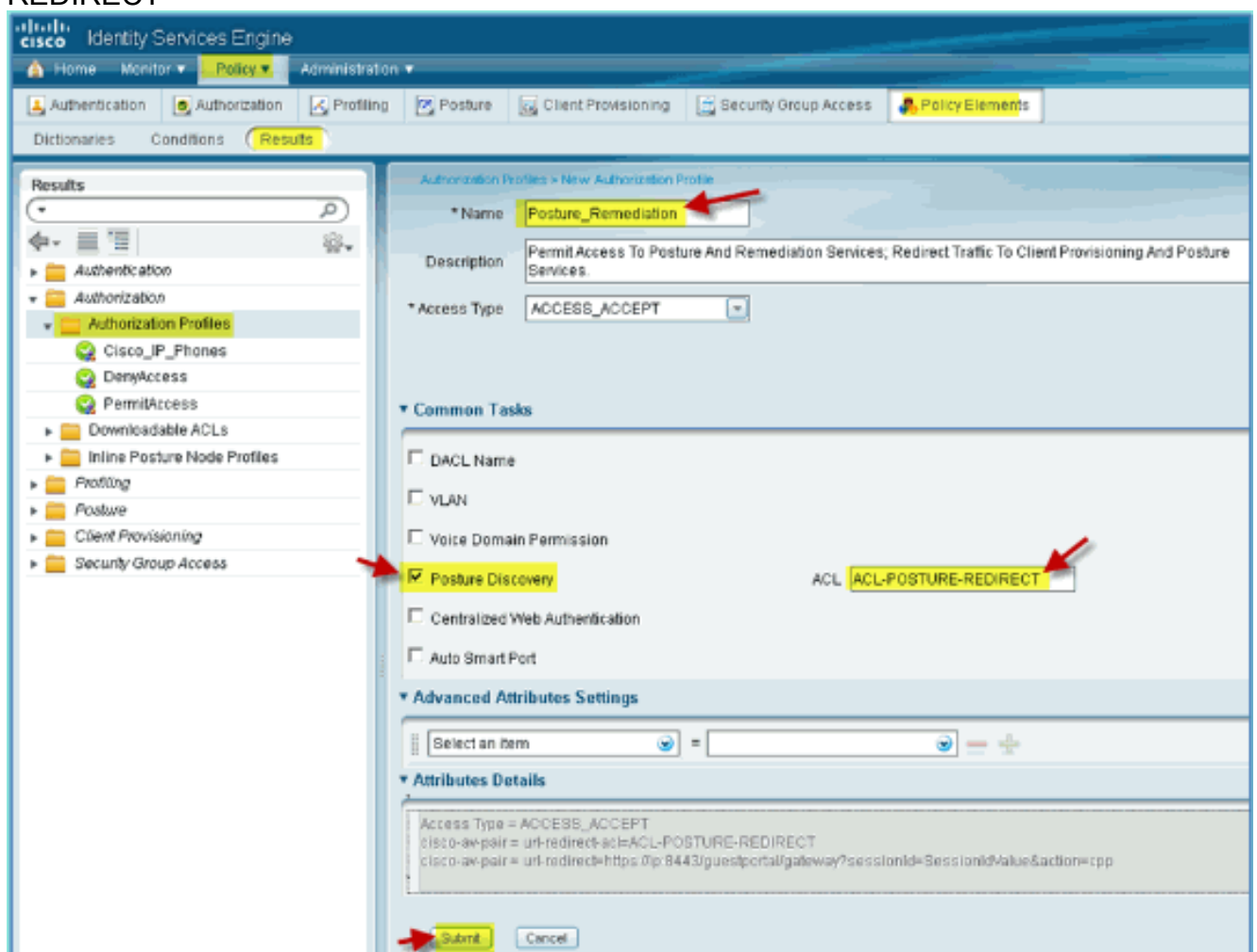
1. No ISE, navegue até **Policy > Policy Elements > Results**.



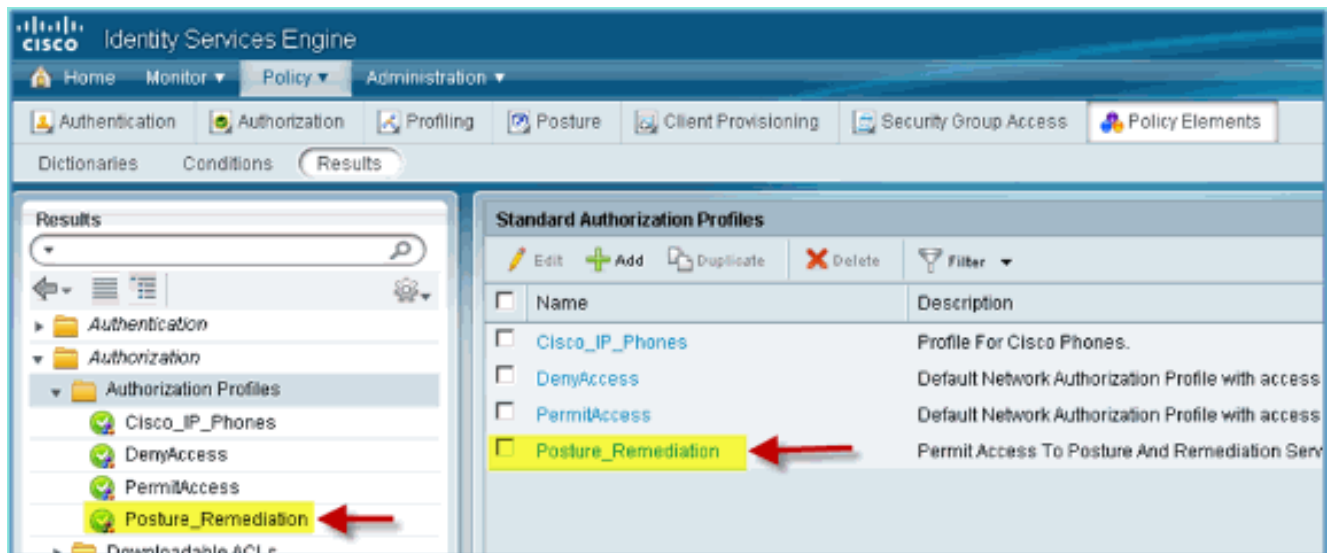
2. Expanda **Authorization**. Clique em **Perfis de autorização** (painel esquerdo) e clique em **Adicionar**.



3. Crie o perfil de autorização com o seguinte: Nome: Posture_Remediation Tipo de acesso: Access_Accept Ferramentas comuns: Descoberta de postura, Habilidade de descoberta de postura, ACL-POSTURE-REDIRECT



4. Clique em **Enviar** para concluir esta tarefa.
5. Confirme se o novo perfil de autorização foi adicionado.

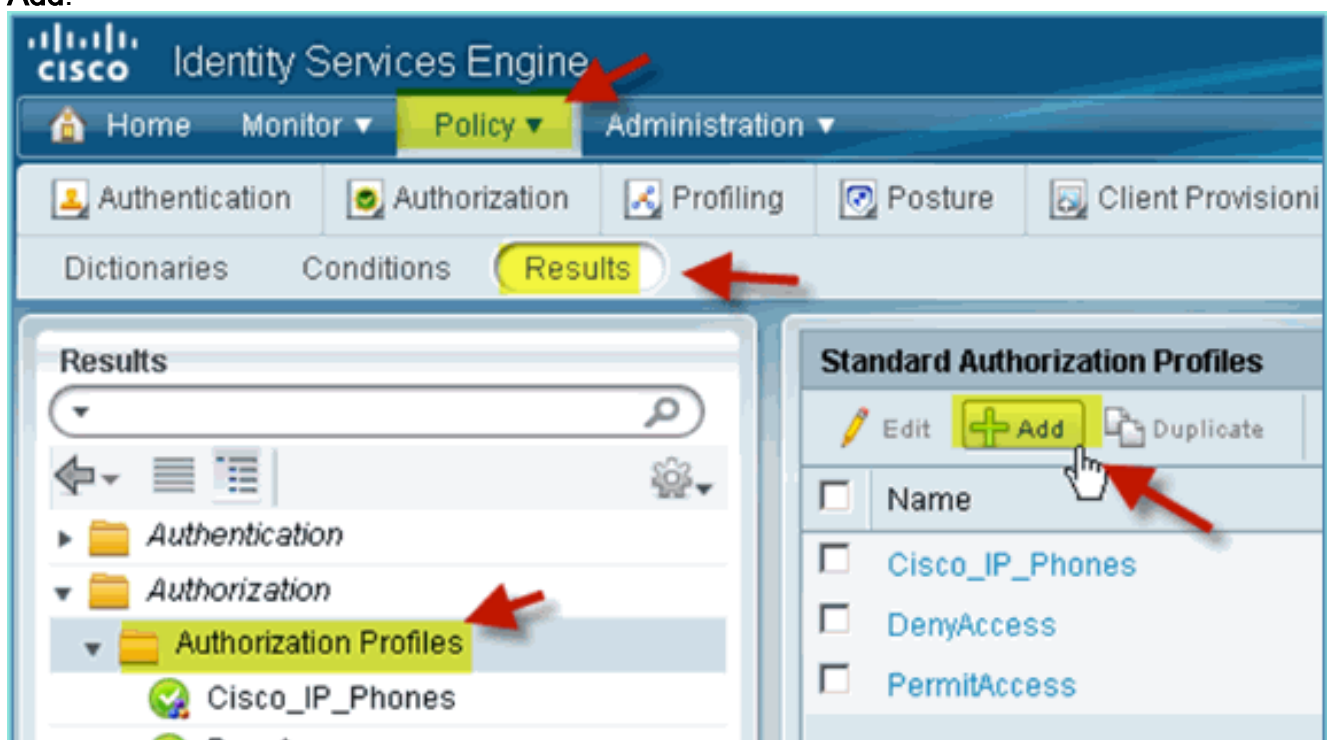


Criar perfil de autorização do ISE para funcionário

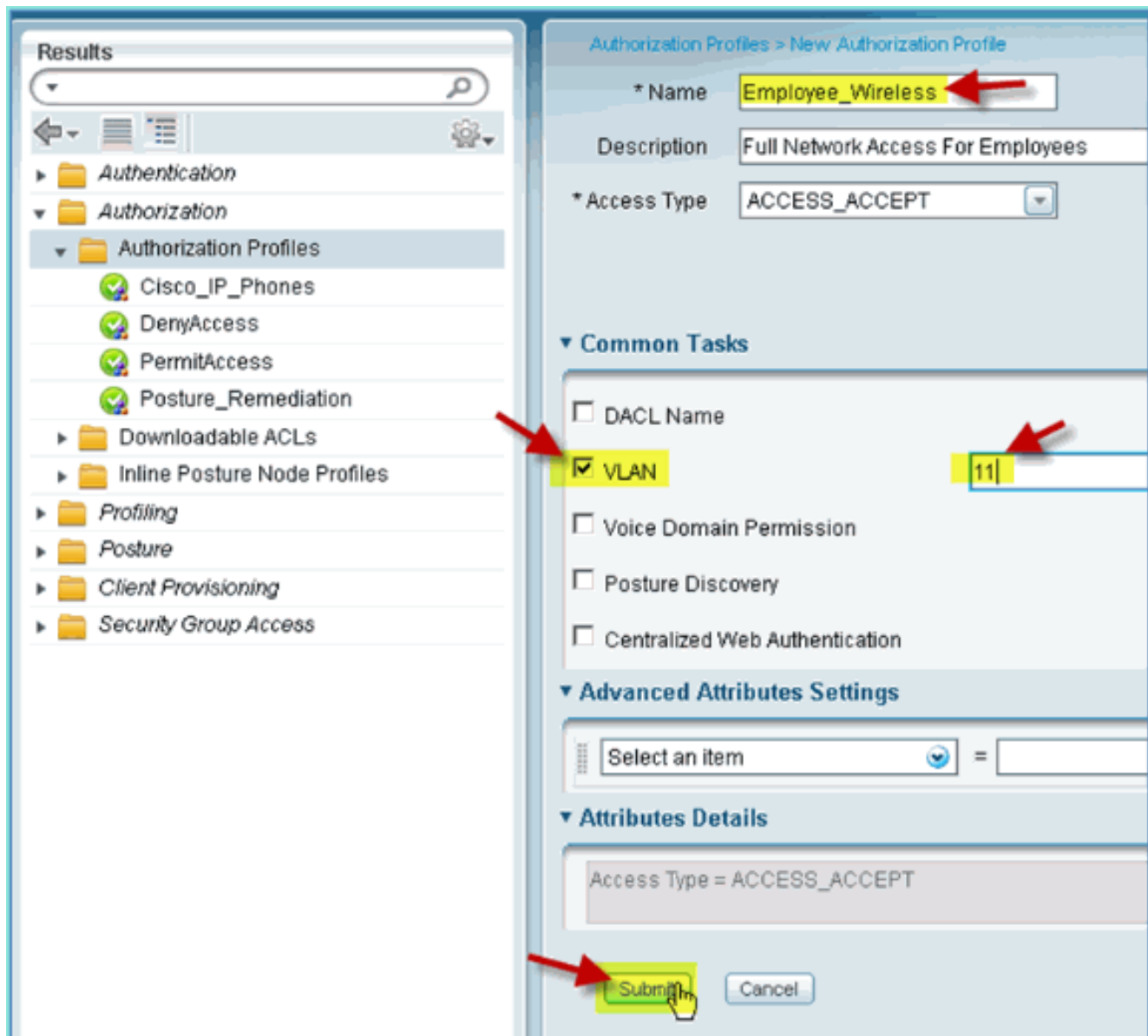
Adicionar um perfil de autorização para um funcionário permite que o ISE autorize e permita o acesso com os atributos atribuídos. A VLAN 11 do funcionário é atribuída neste caso.

Conclua estes passos:

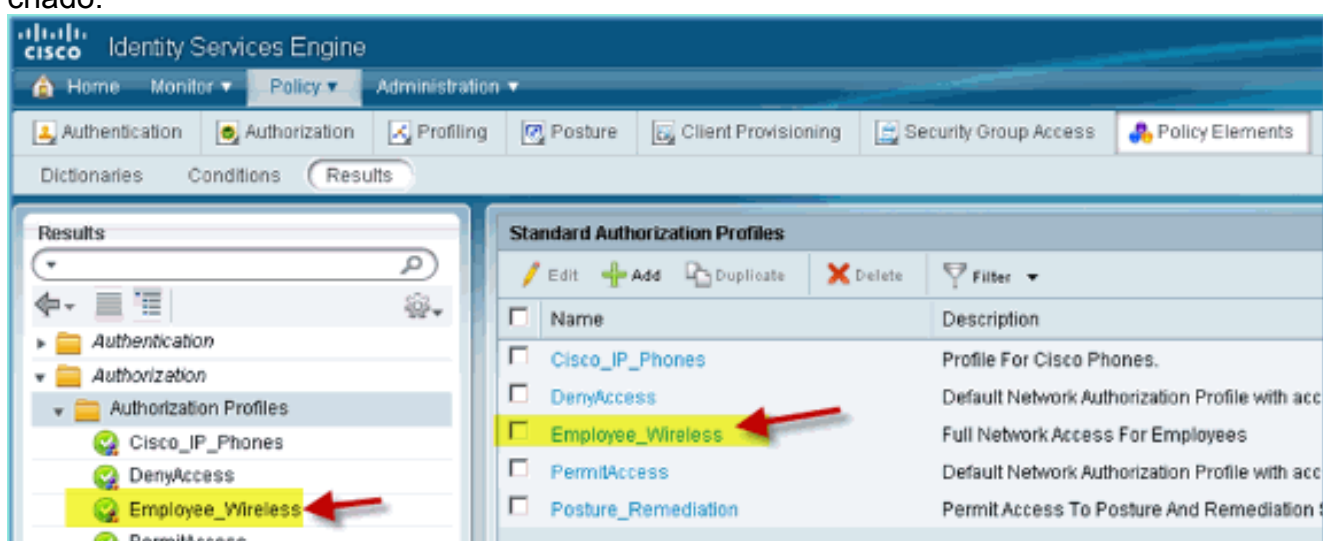
1. No ISE, navegue até **Política > Resultados**. Expanda **Authorization**, em seguida, clique em **Authorization Profiles** e clique em **Add**.



2. Informe o seguinte para o perfil de autorização do Funcionário: Nome: Employee_WirelessTarefas comuns:VLAN, HabilidadeVLAN, subvalor 11
3. Clique em **Enviar** para concluir esta tarefa.



4. Confirme se o novo perfil de autorização de funcionário foi criado.

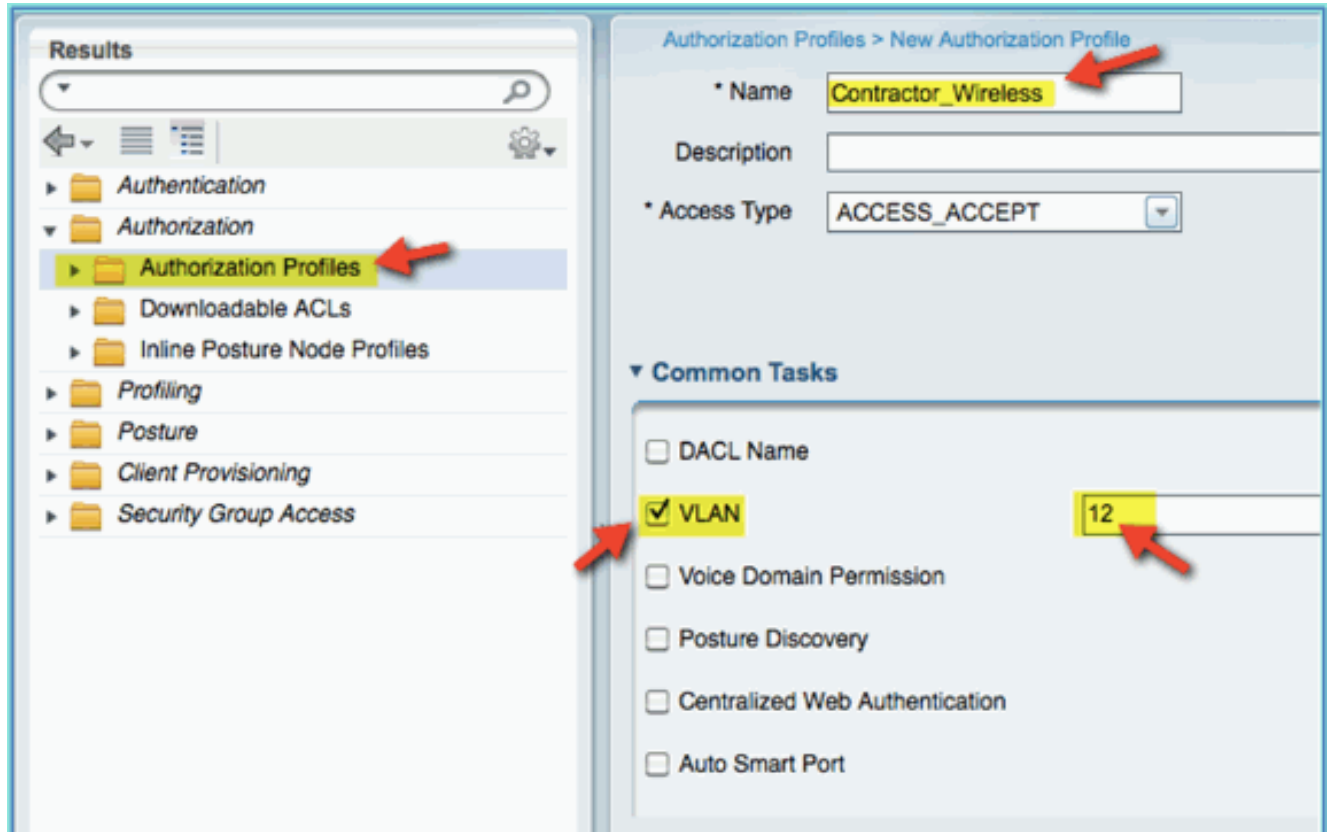


Criar Perfil de Autorização do ISE para Contratante

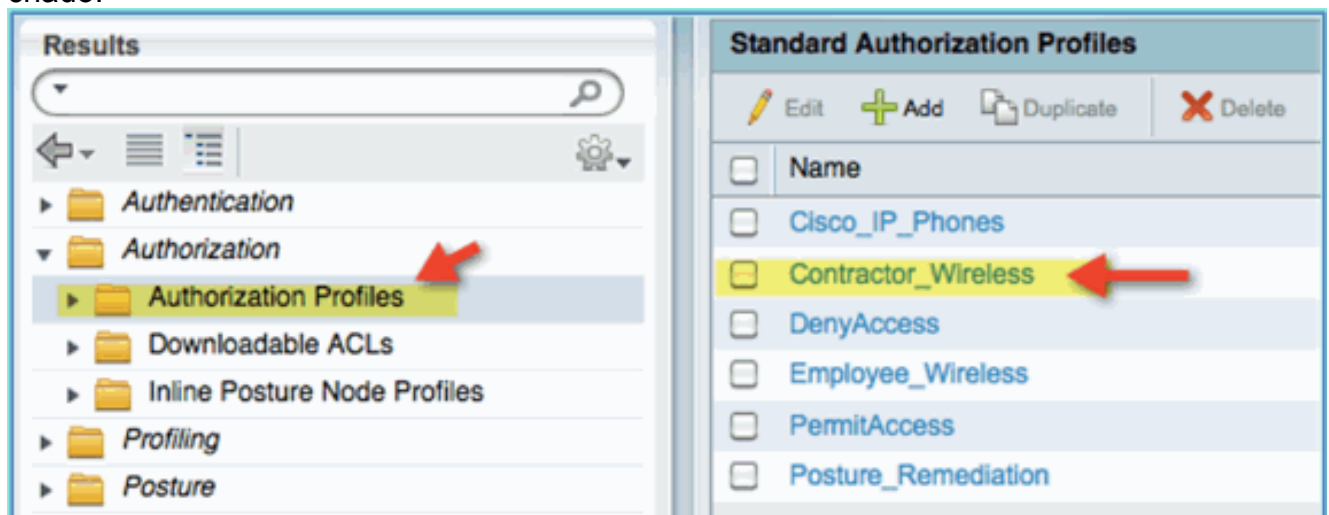
Adicionar um perfil de autorização para um contratante permite que o ISE autorize e permita o acesso com os atributos atribuídos. A contratada VLAN 12 é atribuída neste caso.

Conclua estes passos:

1. No ISE, navegue até **Política > Resultados**. Expanda **Authorization**, em seguida, clique em **Authorization Profiles** e clique em **Add**.
2. Informe o seguinte para o perfil de autorização do Funcionário:Nome: Employee_WirelessTarefas comuns:VLAN, HabilitadoVLAN, subvalor 12



3. Clique em **Enviar** para concluir esta tarefa.
4. Confirme se o perfil de autorização do Contratante foi criado.



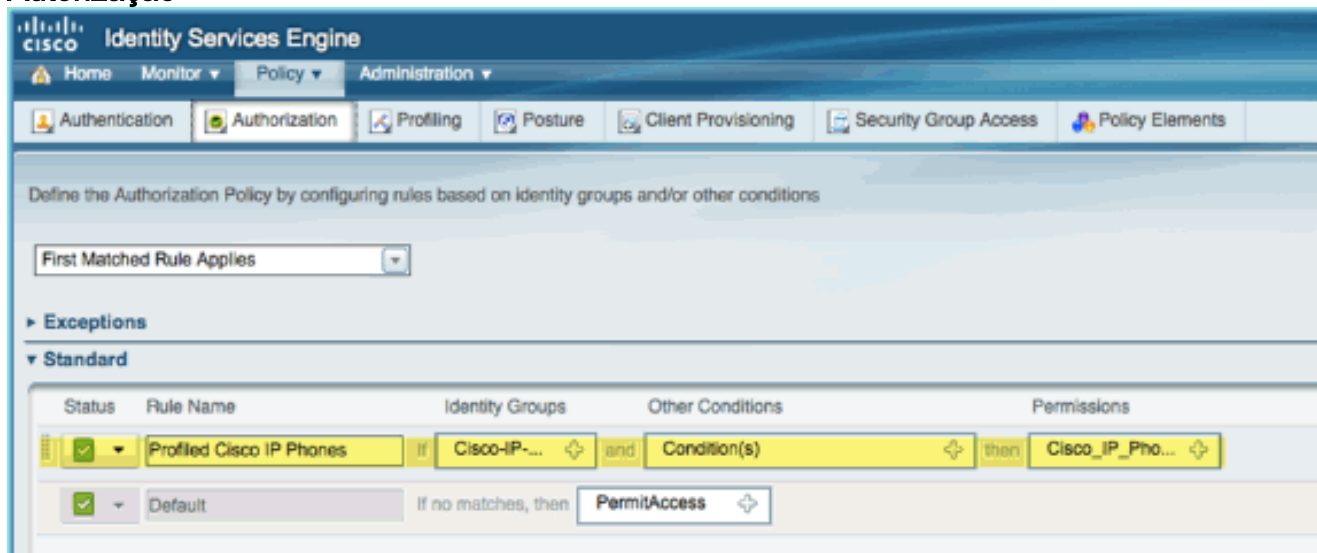
Política de autorização para postura/criação de perfis de dispositivos

Pouco se sabe sobre um novo dispositivo quando ele entra pela primeira vez na rede, um

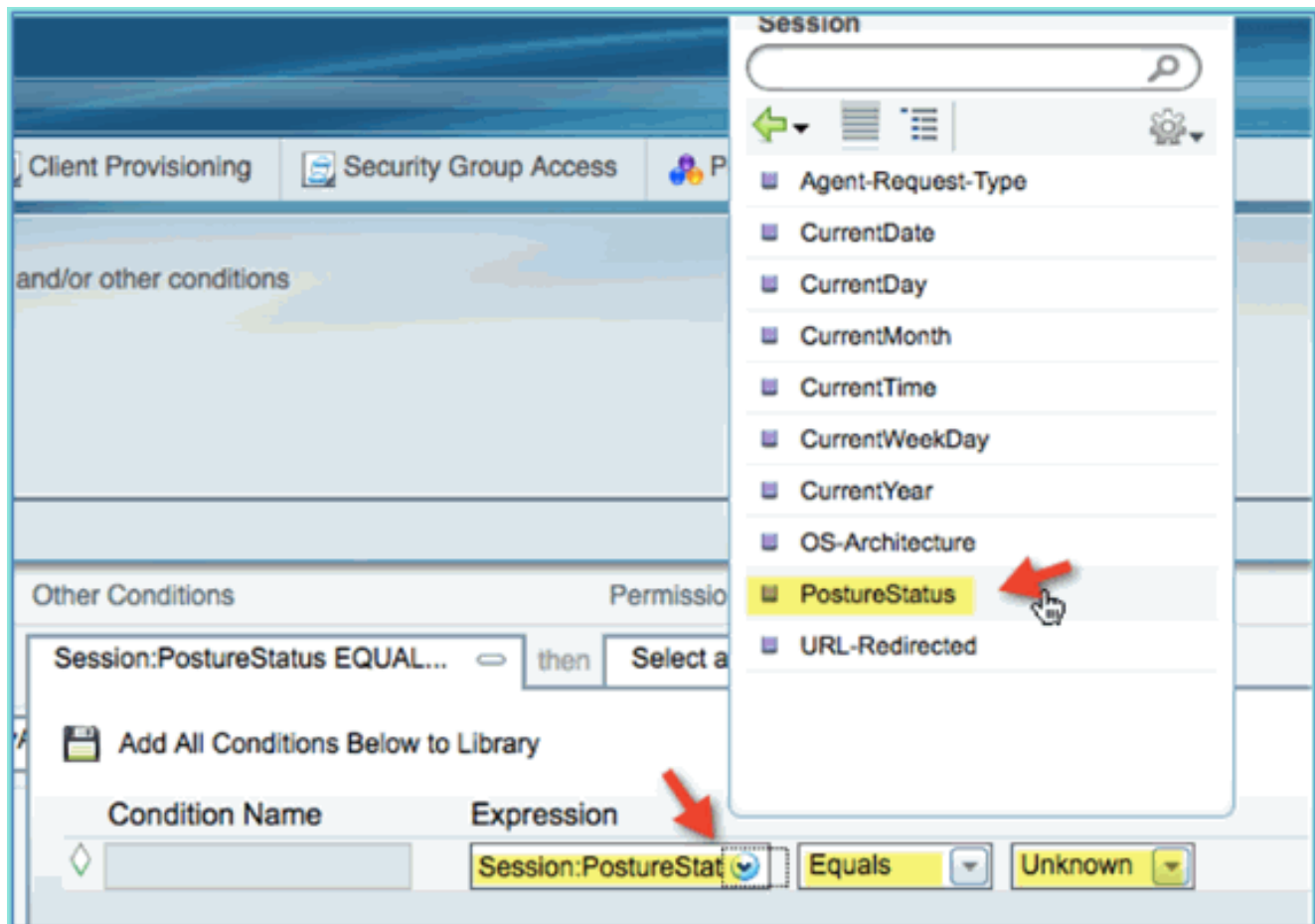
administrador criará a política apropriada para permitir que terminais desconhecidos sejam identificados antes de permitir o acesso. Neste exercício, a política de autorização será criada para que um novo dispositivo seja redirecionado para o ISE para avaliação de postura (para dispositivos móveis são sem agente, portanto, somente a criação de perfil é relevante); os endpoints serão redirecionados para o portal cativo do ISE e identificados.

Conclua estes passos:

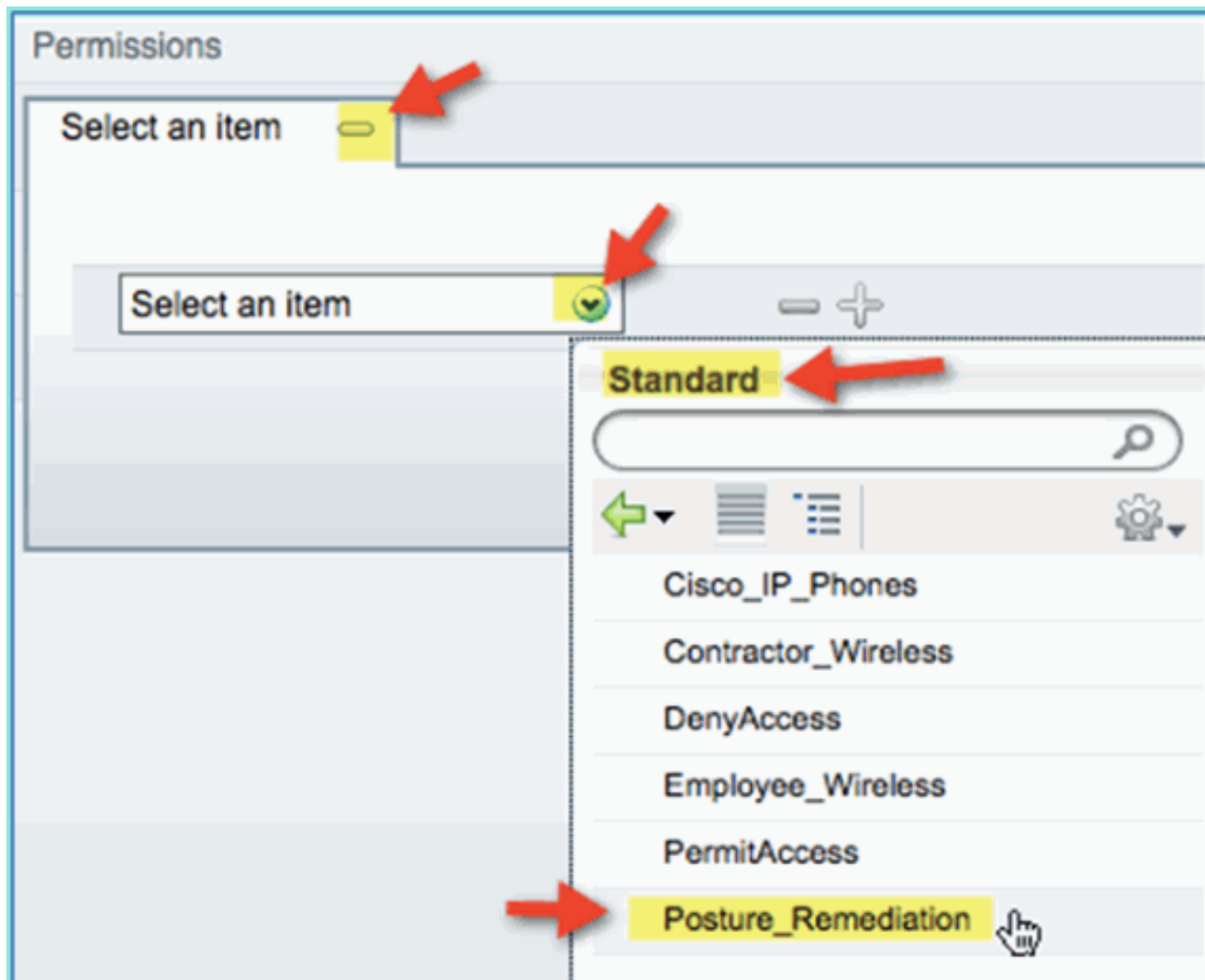
1. No ISE, navegue até **Política > Autorização**.



2. Existe uma política para os telefones IP da Cisco com perfil. Isto é pronto para uso. Editar como uma política de postura.
3. Insira os seguintes valores para esta política: Nome da regra: Posture_Remediation Grupos de Identidade: Qualquer Outras Condições > Criar Nova: Sessão (Avançada) > PostureStatus Status da postura > Iguais: Desconhecido



4. Defina o seguinte para permissões: Permissões > Padrão:
Posture_Remediation



5. Click **Save**. **Observação:** como alternativa, os elementos de política personalizada podem ser criados para adicionar facilidade de uso.

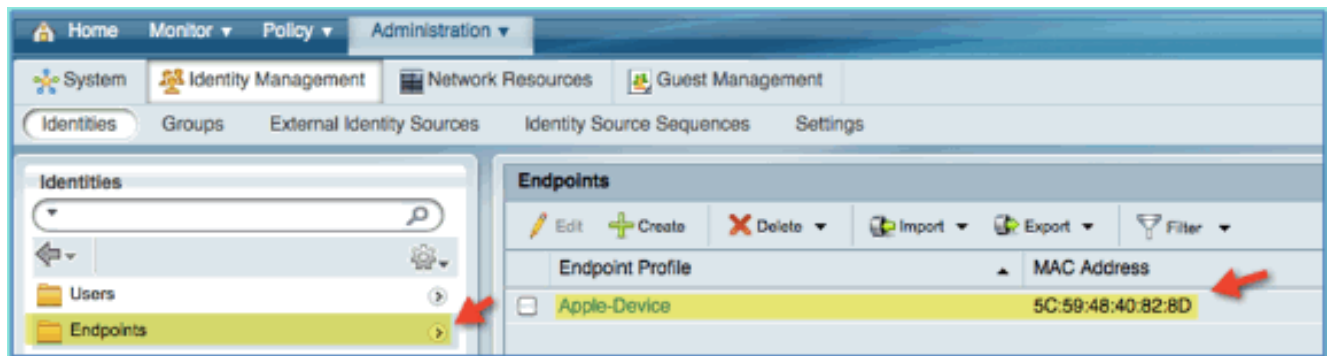
[Testando a Política de Correção de Postura](#)

Uma demonstração simples pode ser realizada para mostrar que o ISE está definindo corretamente o perfil de um novo dispositivo com base na política de postura.

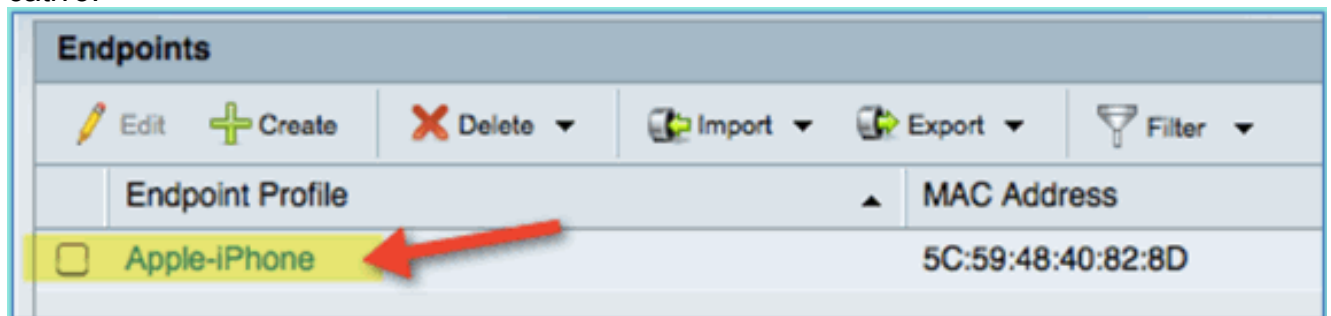
1. No ISE, navegue até **Administração > Gerenciamento de identidades > Identidades**.



2. Clique em **Endpoints**. Associe e conecte um dispositivo (um iPhone neste exemplo).



3. Atualize a lista de endpoints. Observe quais informações são fornecidas.
4. No dispositivo de endpoint, navegue até:URL: http://www (ou 10.10.10.10)O dispositivo é redirecionado. Aceite qualquer prompt para certificados.
5. Depois que o dispositivo móvel for completamente redirecionado, no ISE, atualize a lista Endpoints novamente. Observe o que mudou. O endpoint anterior (por exemplo, Apple-Device) deveria ter sido alterado para "Apple-iPhone"etc. O motivo é que o testador HTTP obtém efetivamente informações de agente de usuário, como parte do processo de redirecionamento para o portal cativo.

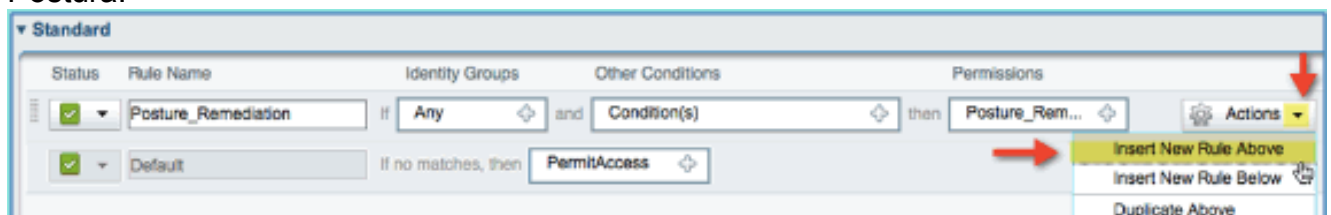


Política de autorização para acesso diferenciado

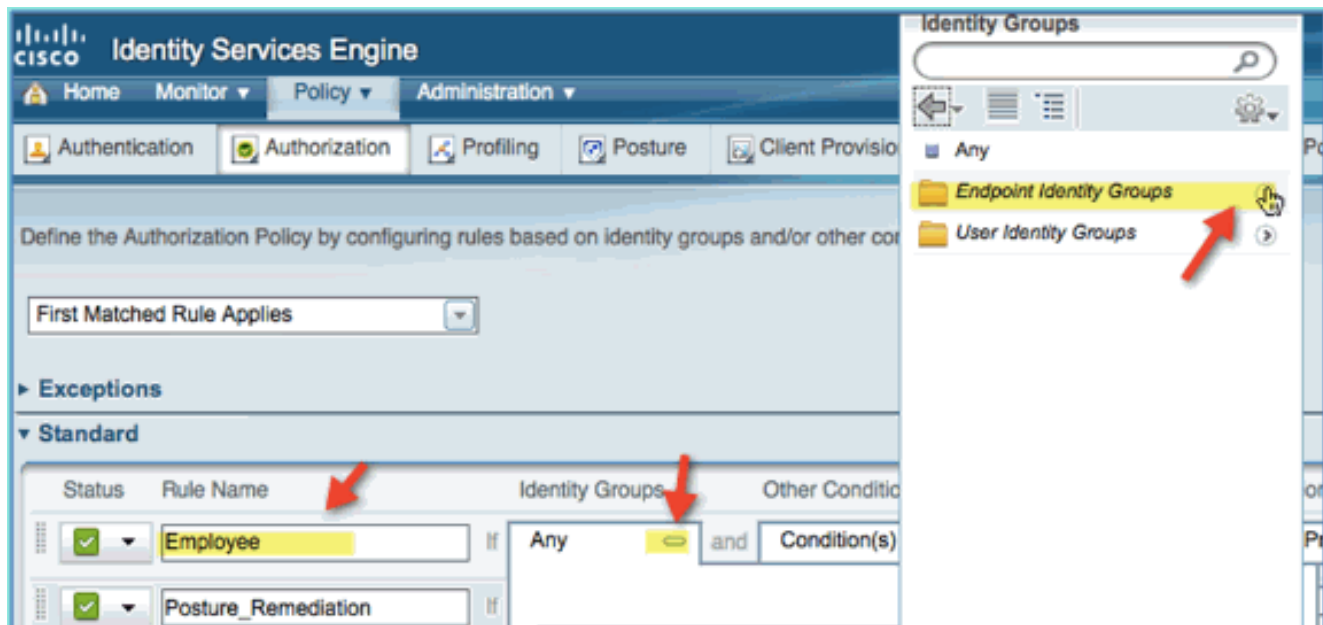
Depois de testar com sucesso a autorização de postura, continue a criar políticas para suportar o acesso diferenciado para o Funcionário e Contratante com dispositivos conhecidos e atribuição de VLAN diferente específica para a função do usuário (neste cenário, Funcionário e Contratante).

Conclua estes passos:

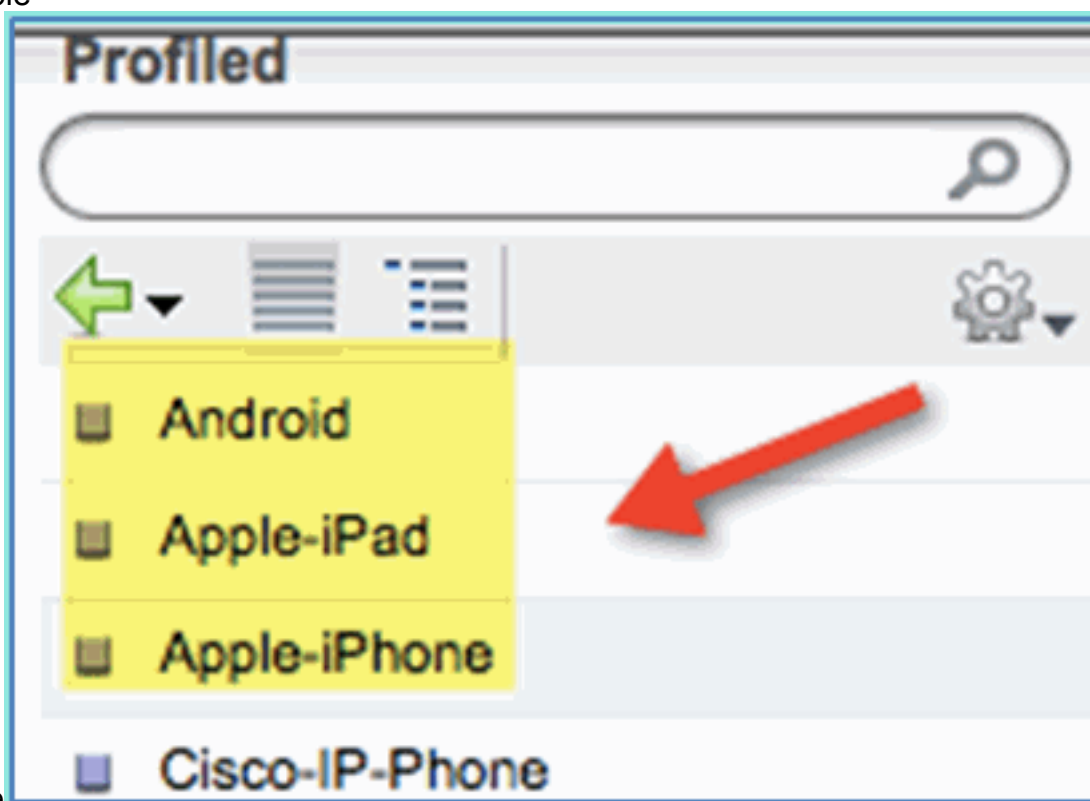
1. Navegue até ISE > Política > Autorização.
2. Adicionar/Inserir uma nova regra acima da política/linha de Correção de Postura.



3. Insira os seguintes valores para esta política:Nome da Regra: FuncionárioGrupos de Identidade (expandir): Grupos de Identidade de Ponto Final

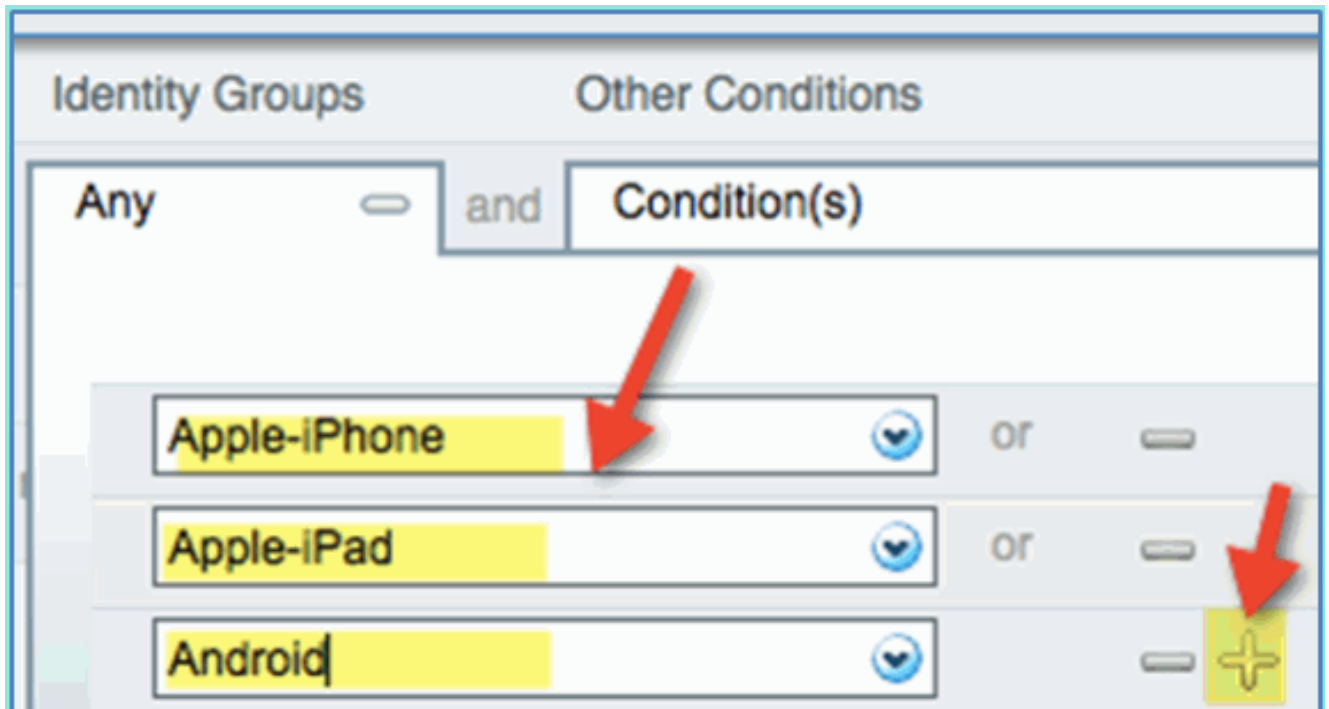


Grupos de Identidade de Ponto de Extremidade: Com Perfil
 Com perfil: Android, Apple-iPad ou Apple-

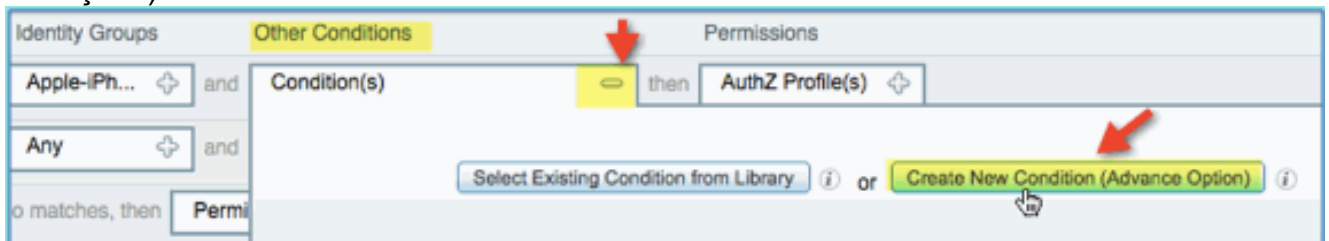


iPhone

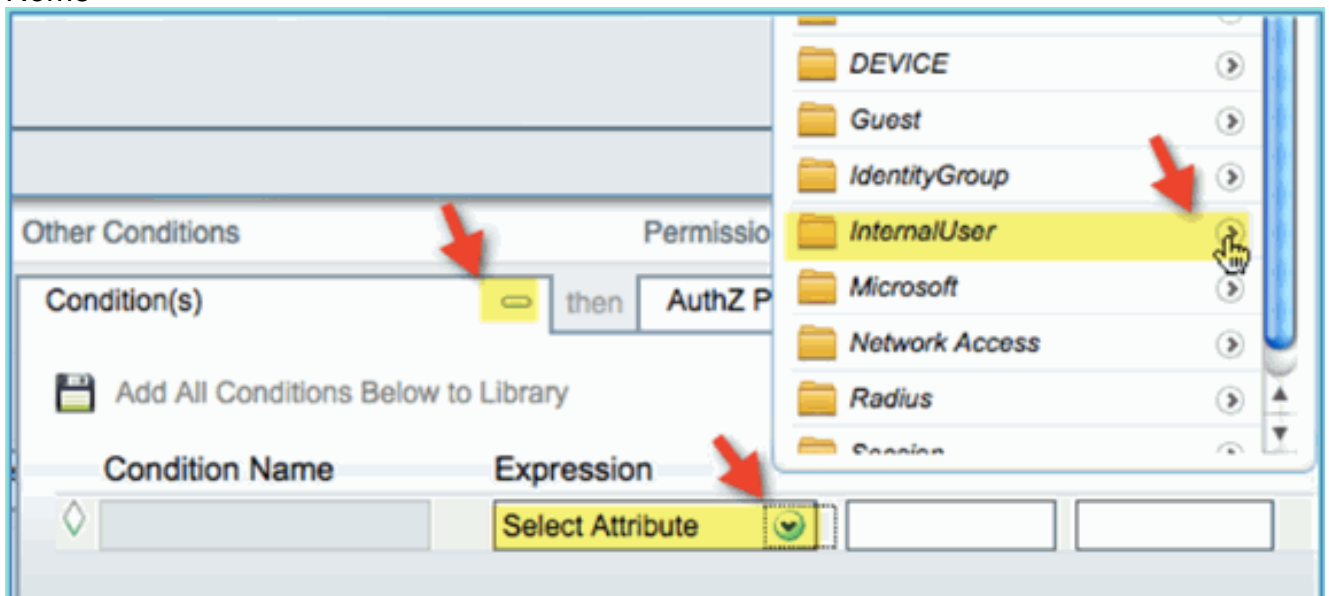
- Para especificar tipos de dispositivos adicionais, clique em + e adicione mais dispositivos (se necessário): Grupos de Identidade de Ponto de Extremidade: Com Perfil
 Com perfil: Android, Apple-iPad ou Apple-iPhone



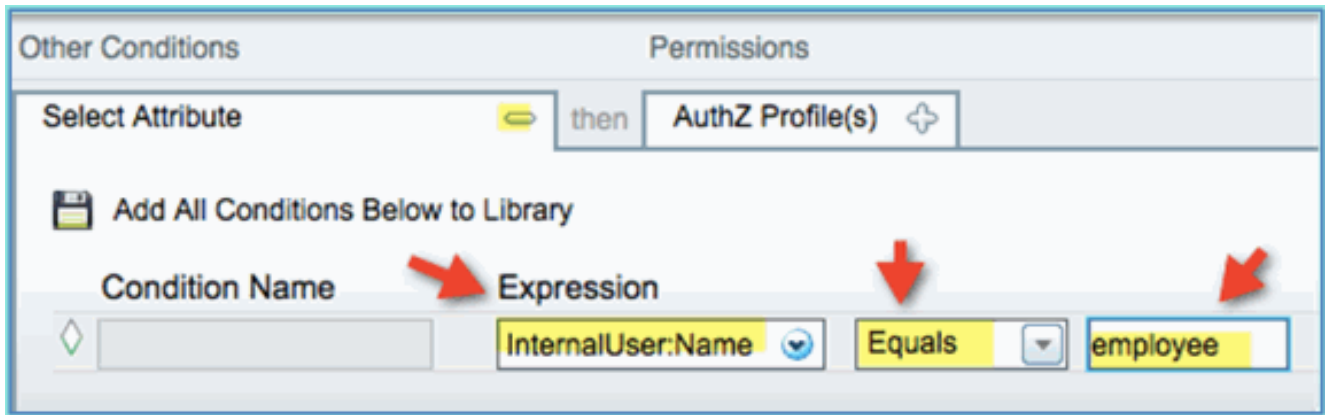
5. Especifique os seguintes valores de Permissões para esta política: Outras Condições (expandir): Criar Nova Condição (Opção Avançada)



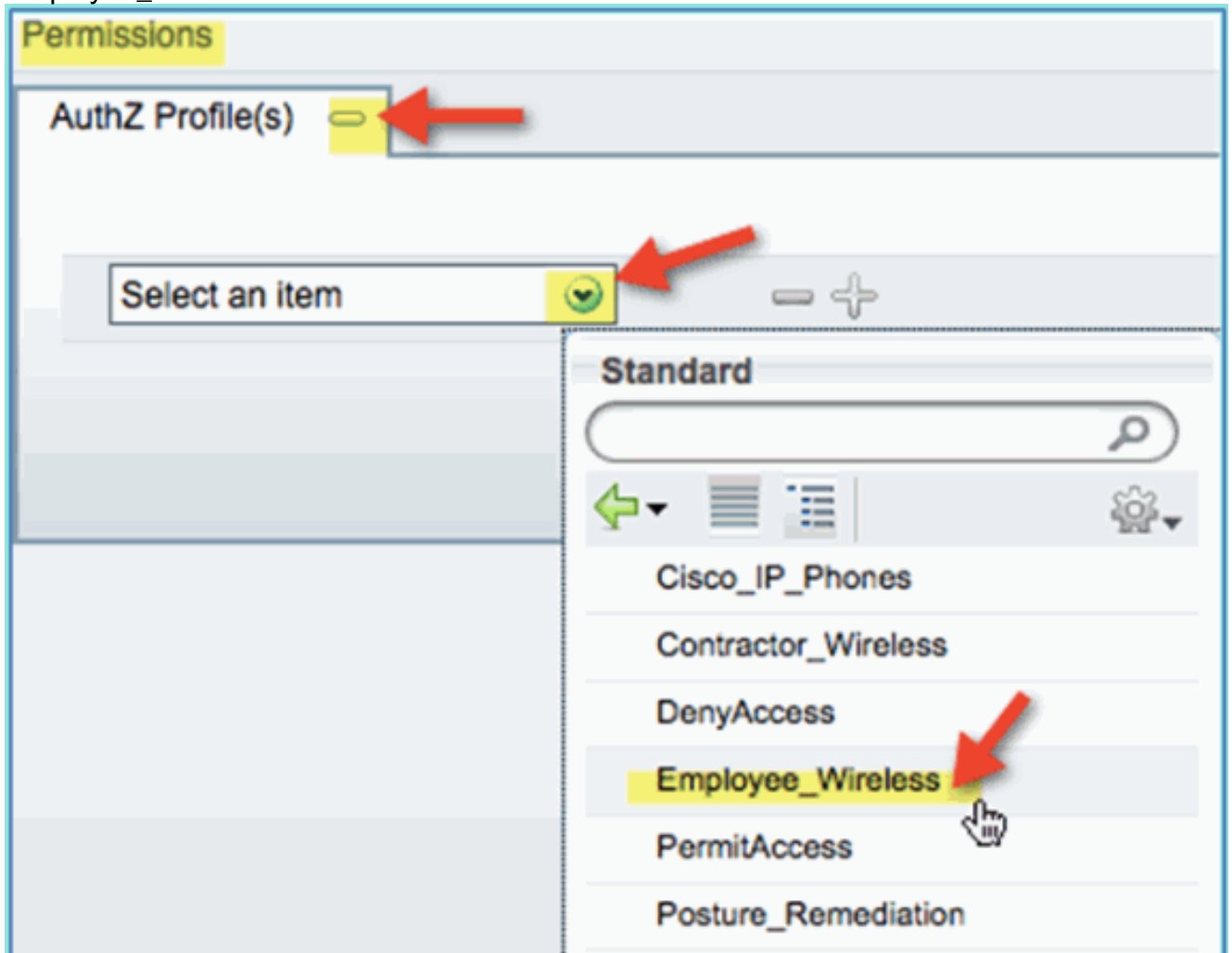
Condição > Expressão (na lista): InternalUser > Nome



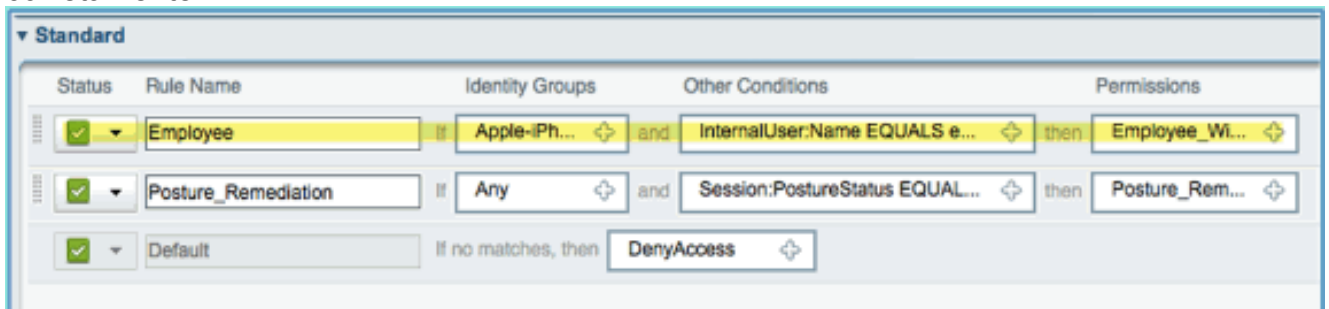
Usuário interno > Nome:
funcionário



6. Adicionar uma condição para Sessão de postura Compatível:Permissões > Perfis > Padrão: Employee_Wireless

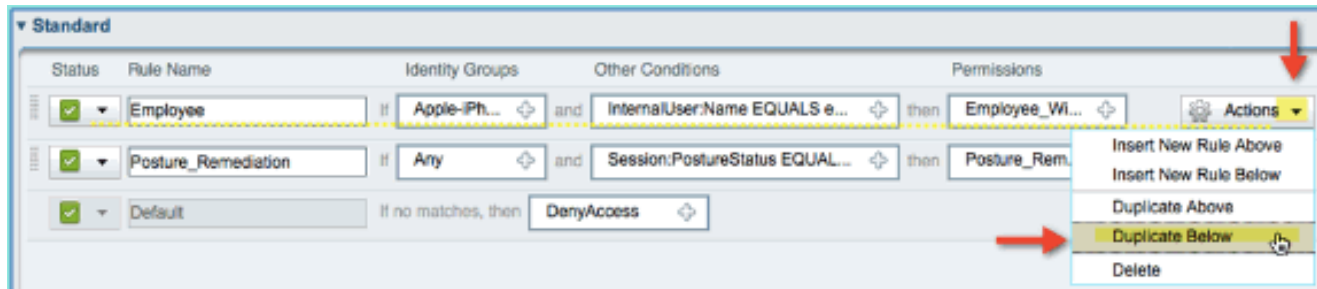


7. Click **Save**. Confirme se a política foi adicionada corretamente.

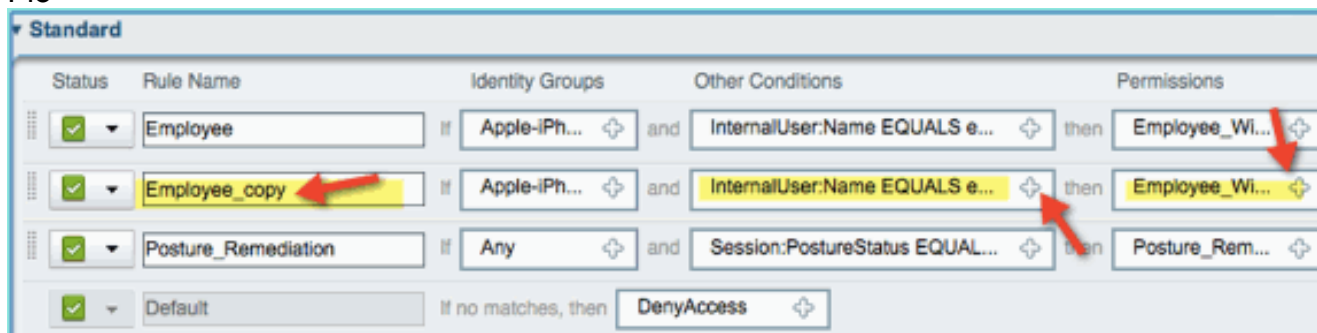


8. Continue adicionando a política Contratante. Neste documento, a política anterior é duplicada para agilizar o processo (ou você pode configurar manualmente para uma boa

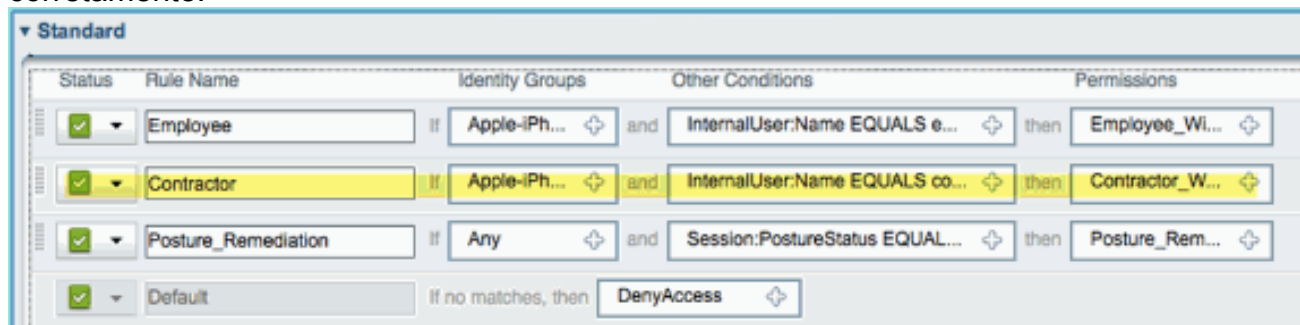
prática). Em Política de funcionários > Ações, clique em **Duplicar** abaixo.



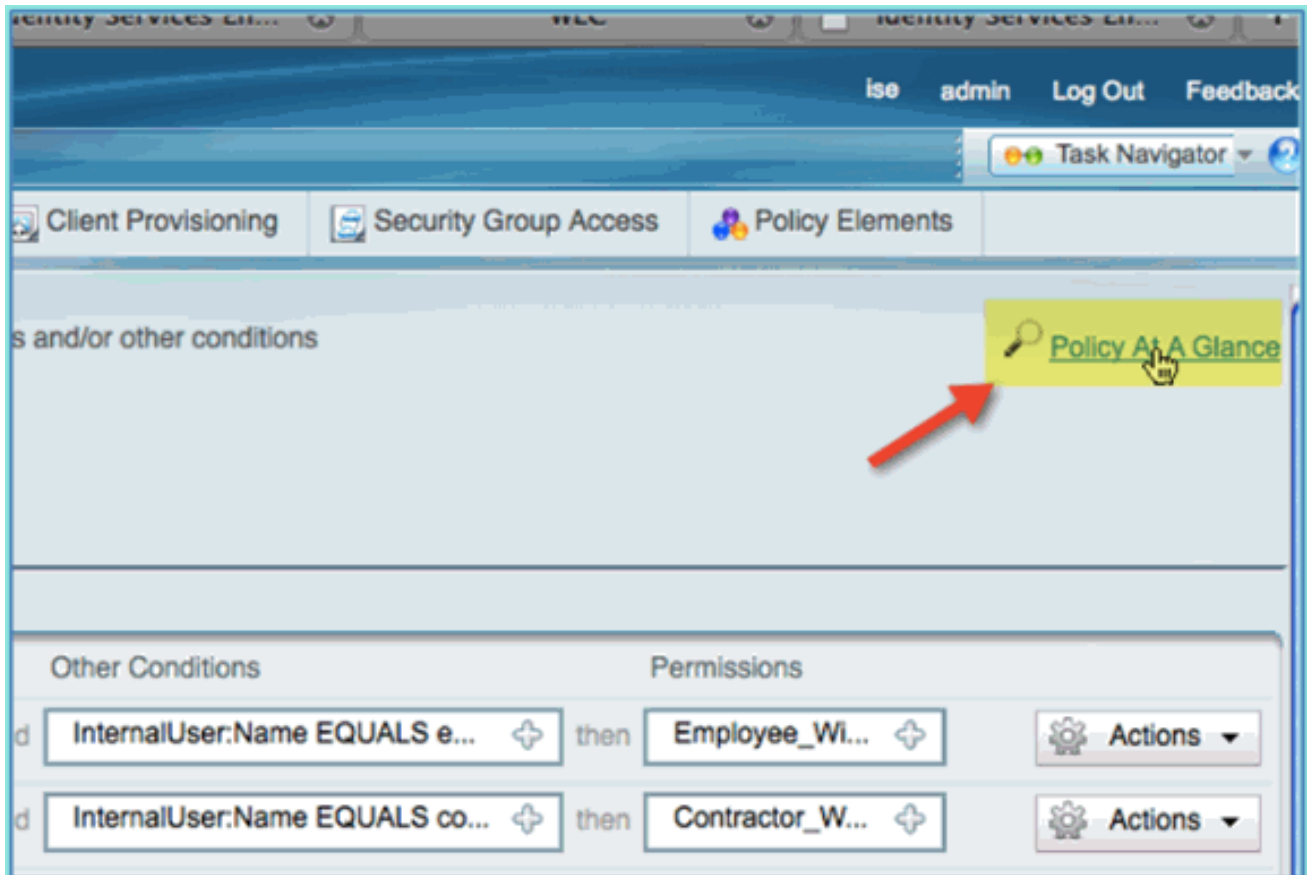
9. Edite os seguintes campos para esta política (cópia duplicada): Nome da Regra: ContratanteOutras Condições > Usuário Interno > Nome: contratantePermissões: Contratante_Sem Fio



10. Click **Save**. Confirme se a cópia duplicada anterior (ou a nova política) está configurada corretamente.



11. Para visualizar as diretivas, clique em **Policy-at-a-Glance**.



A visão geral da política oferece uma visão resumida consolidada e fácil de ver as políticas.

Authorization Policy At A Glance				
First Matched Rule Applies				
Exceptions				
Status	Rule Name	Identity Groups	Other Conditions	Permissions
No data available				
Standard				
Status	Rule Name	Identity Groups	Other Conditions	Permissions
<input checked="" type="checkbox"/> Enabled	Employee	Android OR Apple-iPad OR Apple-iphone	InternalUser.Name EQUALS employee	Employee_Wireless
<input checked="" type="checkbox"/> Enabled	Contractor	Android OR Apple-iPad OR Apple-iphone	InternalUser.Name EQUALS contractor	Contractor_Wireless
<input checked="" type="checkbox"/> Enabled	Posture_Remediation	Any	Session:PostureStatus EQUALS Unknown	Posture_Remediation
<input checked="" type="checkbox"/> Enabled	Default	Any		DenyAccess

Testando o CoA para acesso diferenciado

Com os perfis de autorização e as políticas preparadas para diferenciar o acesso, é hora de testar. Com uma única WLAN segura, uma VLAN de funcionário será atribuída a um funcionário e uma contratada será para a VLAN da contratada. Um iPhone/iPad da Apple é usado nos próximos exemplos.

Conclua estes passos:

1. Conecte-se à WLAN segura (POD1x) com o dispositivo móvel e use estas credenciais: Nome de usuário: funcionário Senha: XXXXX



2. Clique em **Ingressar**. Confirme se a VLAN 11 (VLAN do funcionário) foi atribuída ao funcionário.



3. Clique em **Forget this Network**. Confirme clicando em



Ignorar.

4. Vá para a WLC e remova as conexões de clientes existentes (se o mesmo foi usado nas etapas anteriores). Navegue até **Monitor > Clients > MAC address** e clique em **Remove**.

Monitor

Clients

Summary

Current Filter

▶ Access Points

▶ Cisco CleanAir

▶ Statistics

▶ CDP

▶ Rogues

Clients

Multicast

Client MAC Addr

[44:2a:60:f7:3a:4a](#)

[5c:59:48:40:82:8d](#)

Status	Auth	Port	WGB
--------	------	------	-----

Associated	Yes	1	No
------------	-----	---	----

Associated	No	1	
------------	----	---	--

LinkTest

Disable

Remove

802.11aTSM

802.11b/gTSM

5. Outra maneira segura de limpar sessões anteriores do cliente é desabilitar/habilitar a WLAN. Vá para **WLC > WLANs > WLAN** e clique na WLAN para editar. Desmarque **Enabled** > **Apply** (para desativar). Marque a caixa de seleção **Enabled** > **Apply** (para reativar).



6. Volte para o dispositivo móvel. Conecte-se novamente à mesma WLAN com estas credenciais: Nome de usuário: contratante Senha:

Enter the password for "pod1x"

Cancel **Enter Password**

Username contractor ←

Password ●●●●●●●● | ←

Mode Automatic >

1 2 3 4 5 6 7 8 9 0

XXXX

7. Clique em **Ingressar**. Confirme se a VLAN 12 (VLAN do Contratante/convidado) foi atribuída ao usuário contratado.



8. Você pode observar a exibição do registro em tempo real do ISE em **ISE > Monitorar > Autorizações**. Você deve ver usuários individuais (funcionário, contratado) obterem perfis de autorização diferenciados (Employee_Wireless vs Contractor_Wireless) em VLANs diferentes.

Time	Status	Details	Username	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles
Aug 02,11 03:40:18.331 PM	✓	🔒	employee	5C:59:48:40:82:8D		wlc		Employee_Wireless
Aug 02,11 03:36:33.663 PM	✓	🔒	contractor	5C:59:48:40:82:8D		wlc		Contractor_Wireless

[WLAN Convidada da WLC](#)

Conclua estes passos para adicionar uma WLAN de convidado para permitir que os convidados

acessem o Portal de Convidado do Patrocinador do ISE:

1. Na WLC, navegue até **WLANS > WLANS > Add New**.
2. Digite o seguinte para a nova WLAN de convidado: Nome do perfil: pod1guestSSID: pod1convidado



3. Clique em Apply.
4. Digite o seguinte na guia Guest WLAN > General: Status: Desabilitado Interface/grupo de interface: convidado

MONITOR **WLANs** CONTROLLER WIRELESS SECUR

WLANs > Edit 'pod1guest'

General Security QoS Advanced

Profile Name pod1guest

Type WLAN

SSID pod1guest

Status Enabled

Security Policies [WPA2][Auth(802.1X)]
(Modifications done under security)

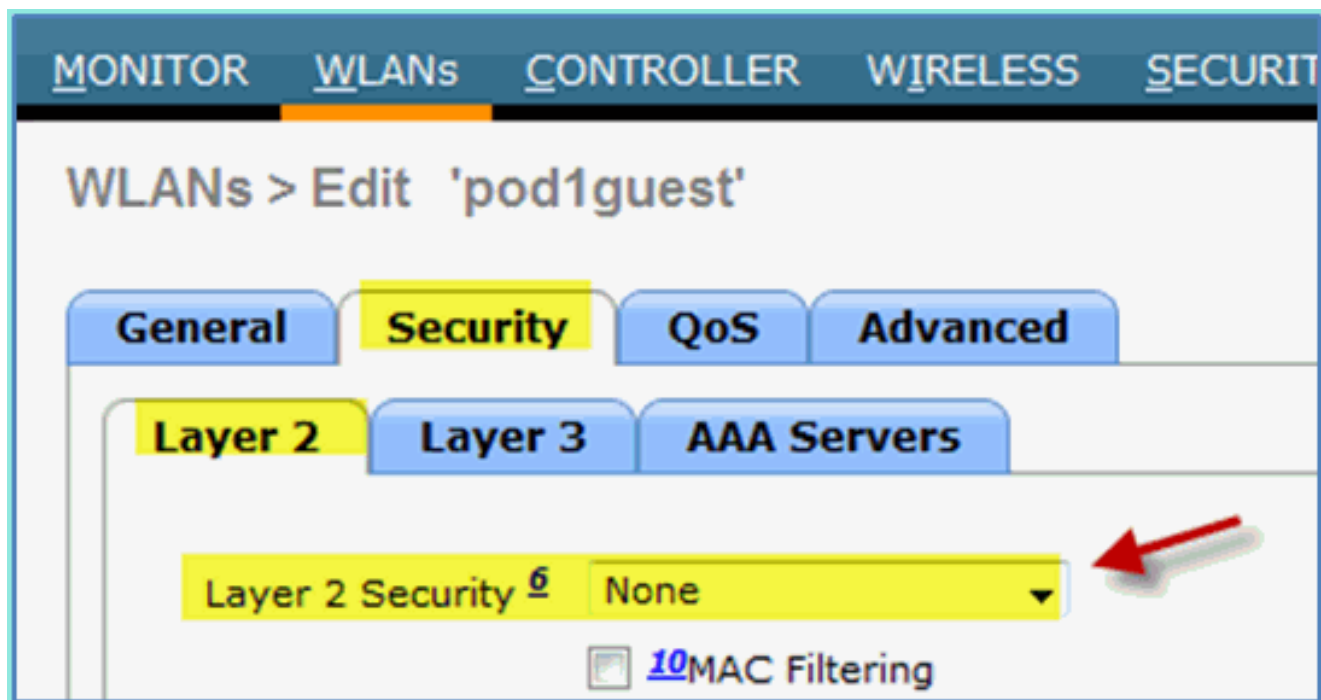
Radio Policy All

Interface/Interface Group(G) **guest**

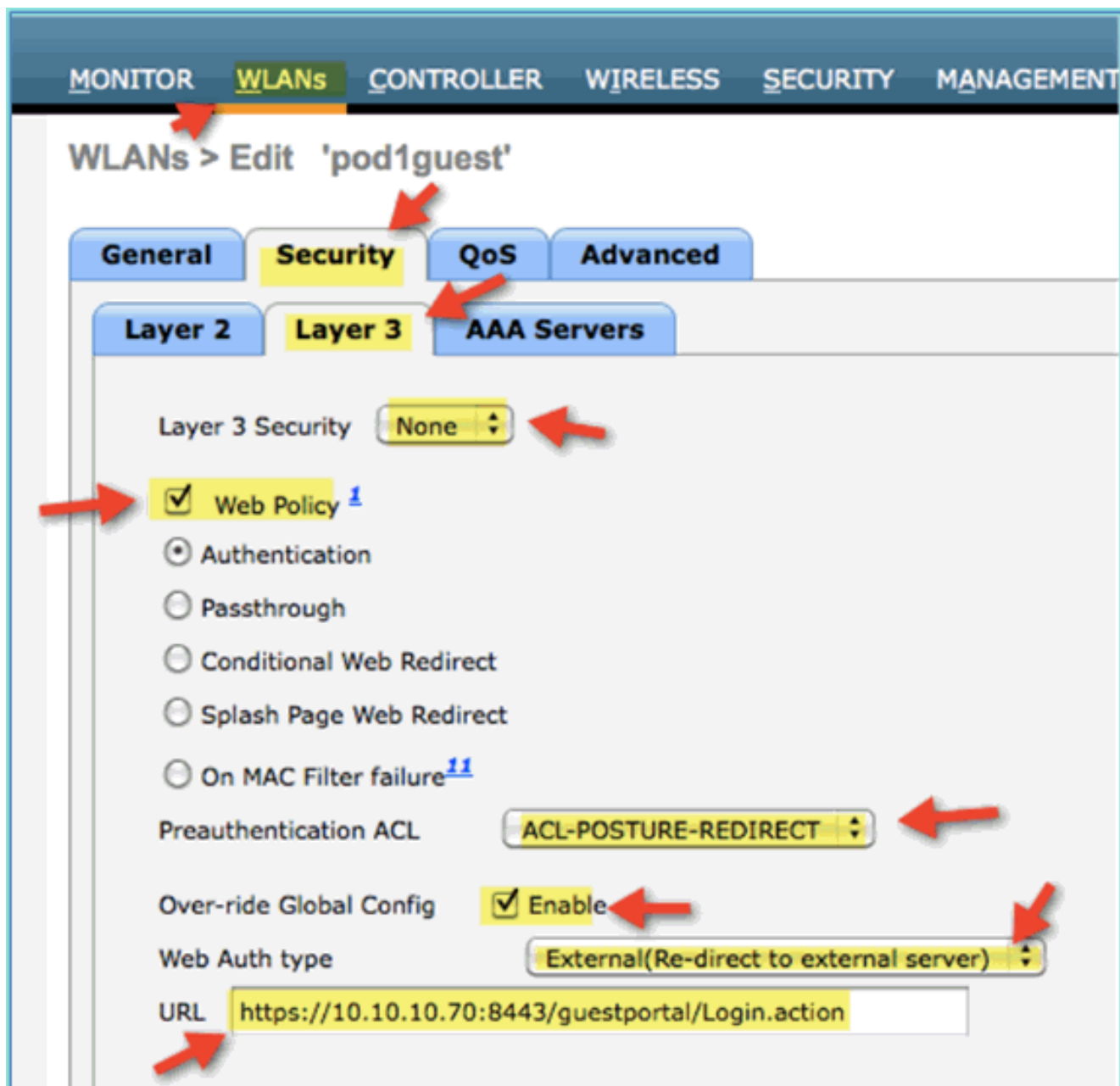
Multicast Vlan Feature Enabled

Broadcast SSID Enabled

5. Navegue para convidado WLAN > Security > Layer2 e digite o seguinte:Segurança de Camada 2:
Nenhuma



6. Navegue até a guia guest WLAN > Security > Layer3 e insira o seguinte: Segurança da camada 3: nenhuma Política da Web: Habilitada Subvalor da Política da Web: Autenticação ACL de pré-autenticação: ACL-POSTURE-REDIRECT Tipo de Autenticação da Web: Externa (Redirecionar para servidor externo) URL: <https://10.10.10.70:8443/guestportal/Login.action>



7. Clique em Apply.

8. Certifique-se de salvar a configuração da WLC.

Testando a WLAN de Convidado e o Portal de Convidado

Agora, você pode testar a configuração da WLAN convidada. Ele deve redirecionar os convidados para o portal de convidados do ISE.

Conclua estes passos:

1. Em um dispositivo iOS, como um iPhone, navegue até **Wi-Fi Networks > Enable**. Em seguida, selecione a rede de convidado

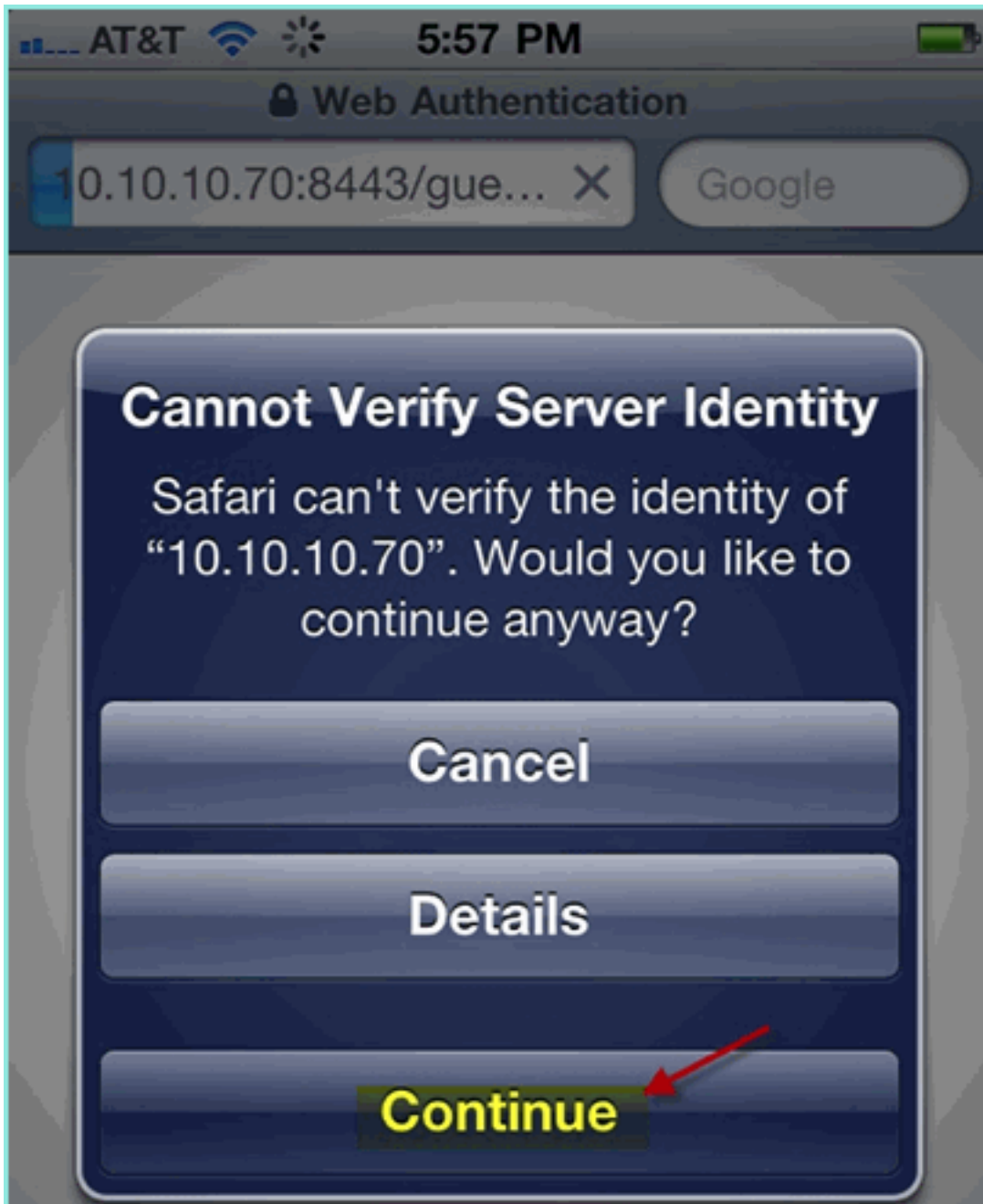


POD.

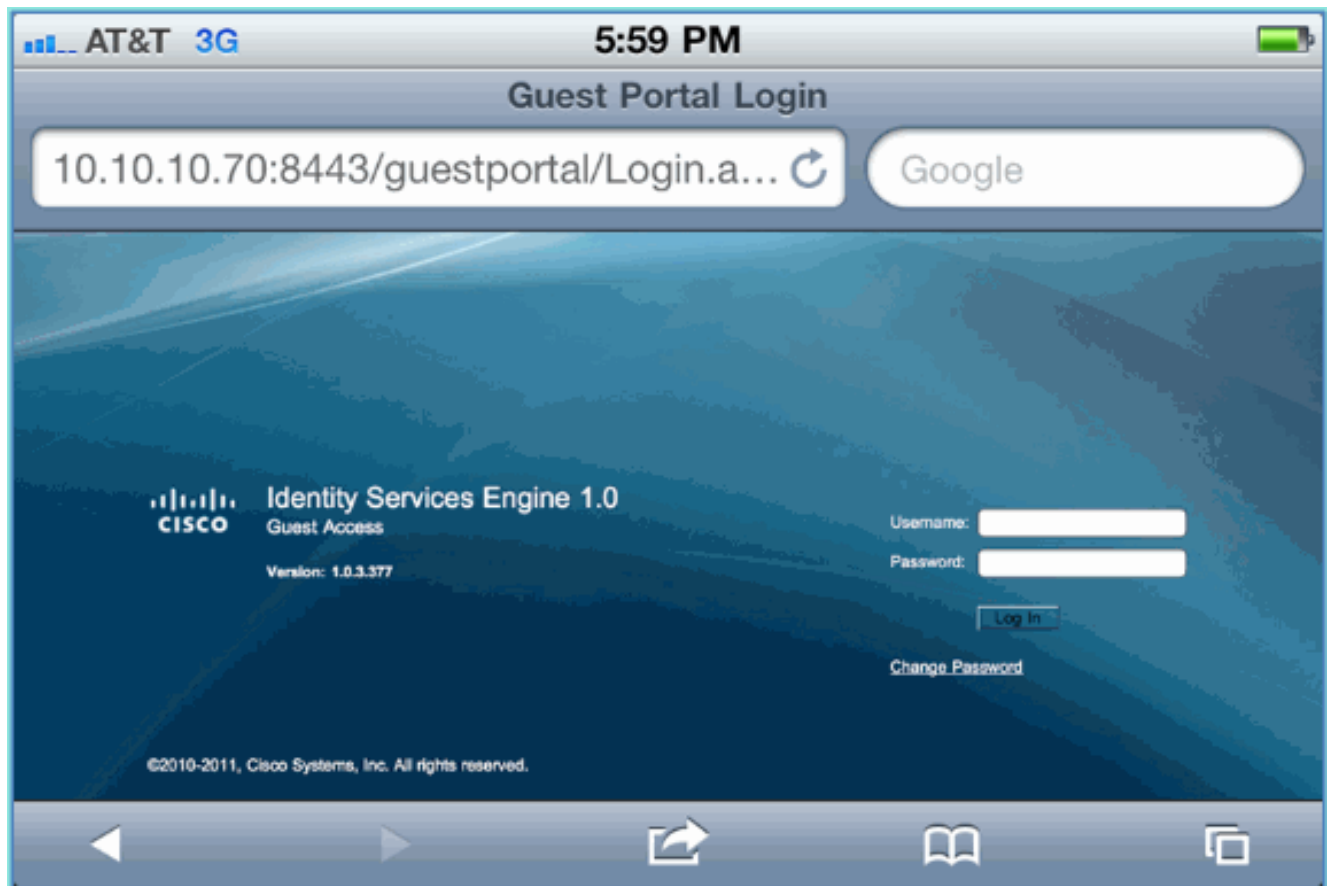
2. Seu dispositivo iOS deve mostrar um endereço IP válido da VLAN convidada (10.10.12.0/24).



3. Abra o navegador Safari e conecte-se a:URL: <http://10.10.10.10>Um redirecionamento de Autenticação da Web é exibido.
4. Clique em **Continuar** até chegar à página Portal do convidado do



ISE. A próxima captura de tela de exemplo mostra o dispositivo iOS em um Login no Portal de Convidado. Isso confirma que a configuração correta para o Portal de convidado WLAN e ISE está ativa.

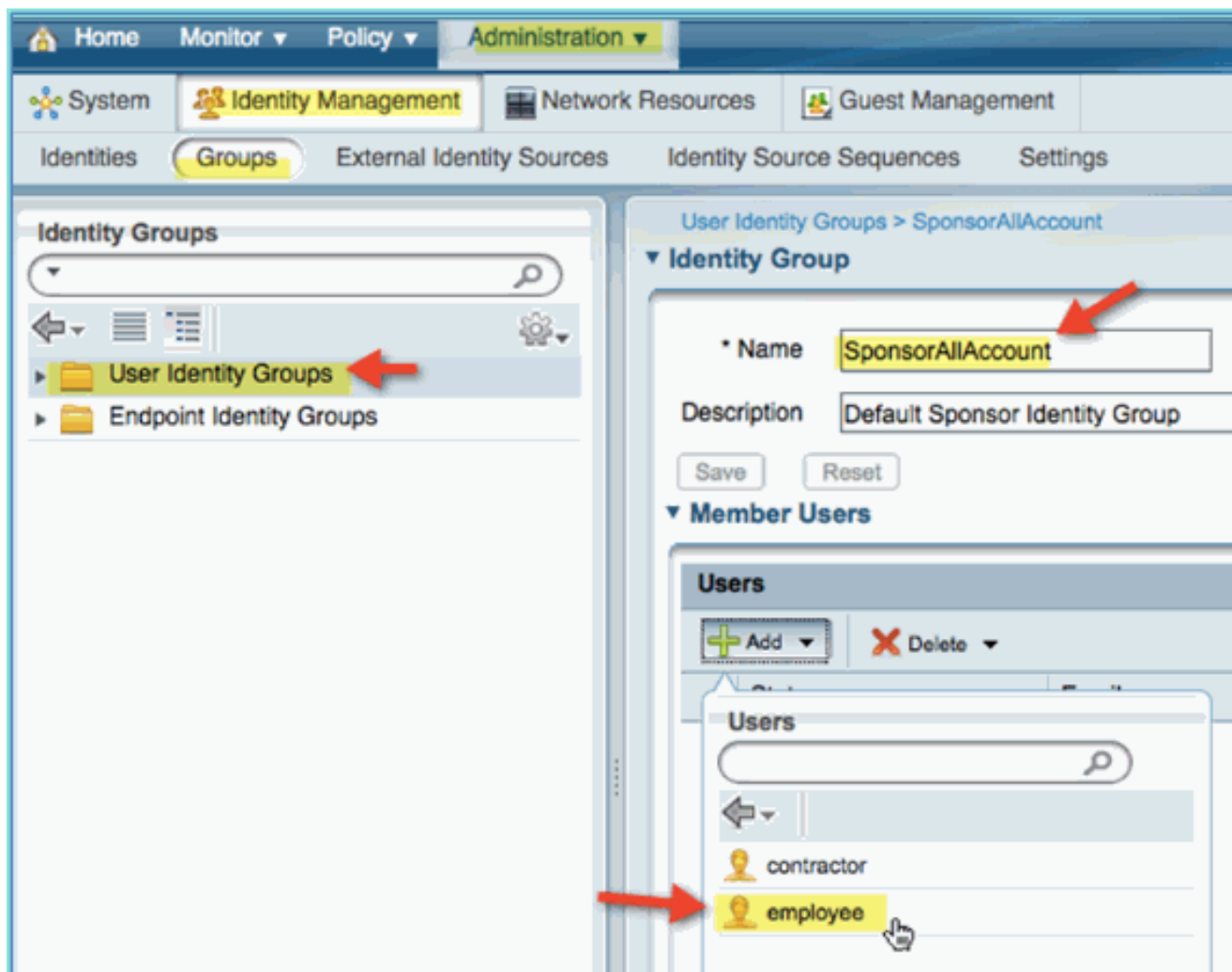


[Acesso para convidados patrocinado pelo ISE Wireless](#)

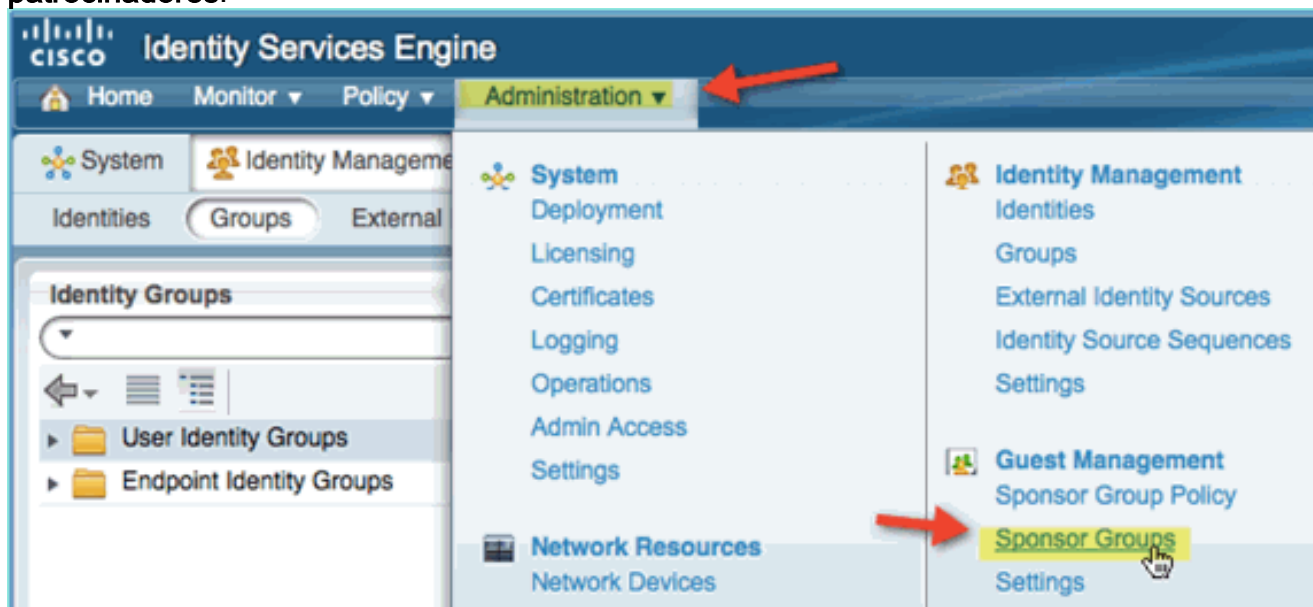
O ISE pode ser configurado para permitir que os convidados sejam patrocinados. Nesse caso, você configurará as políticas de convidado do ISE para permitir que usuários de domínio interno ou do AD (se integrados) patrocinem o acesso de convidado. Você também configurará o ISE para permitir que os patrocinadores vejam a senha do convidado (opcional), o que é útil para este laboratório.

Conclua estes passos:

1. Adicione o usuário funcionário ao grupo SponsorAllAccount. Há diferentes maneiras de fazer isso: ir diretamente para o grupo ou editar o usuário e atribuir o grupo. Para este exemplo, navegue para **Administração > Gerenciamento de identidade > Grupos > Grupos de identidade de usuário**. Em seguida, clique em **SponsorAllAccount** e adicione o usuário do funcionário.



2. Navegue até **Administração > Gerenciamento de convidados > Grupos de patrocinadores**.



3. Clique em **Edit** e escolha **SponsorAllAccounts**.





CISCO Identity Services Engine

Home Monitor Policy Administration

System Identity Management Network Resources Guest Management

Sponsor Group Policy **Sponsor Groups** Settings

Guest Sponsor Groups

 Edit  Add  Delete  Filter

<input type="checkbox"/>	Sponsor Group Name	Description
<input checked="" type="checkbox"/>	SponsorAllAccounts	Default SponsorGroup
<input type="checkbox"/>	SponsorGroupGrpAccounts	Default SponsorGroup

4. Selecione Níveis de Autorização e defina o seguinte: Exibir Senha do Convidado:
Sim

Cisco Identity Services Engine Administration console. The breadcrumb trail is "Sponsor Group List > SponsorAllAccounts". The "Authorization Levels" tab is selected. A red arrow points to the "View Guest Password" dropdown menu, which is currently set to "Yes" and is highlighted in yellow. Another red arrow points to the "Sponsor Groups" breadcrumb. Other settings include "Allow Login", "Create Accounts", "Create Bulk Accounts", "Create Random Accounts", "Import CSV", "Send Email", "Send SMS", "Allow Printing Guest Details", "View/Edit Accounts", and "Suspend/Reinstate Accounts". At the bottom, there are "Save" and "Reset" buttons.

5. Clique em **Salvar** para concluir esta tarefa.

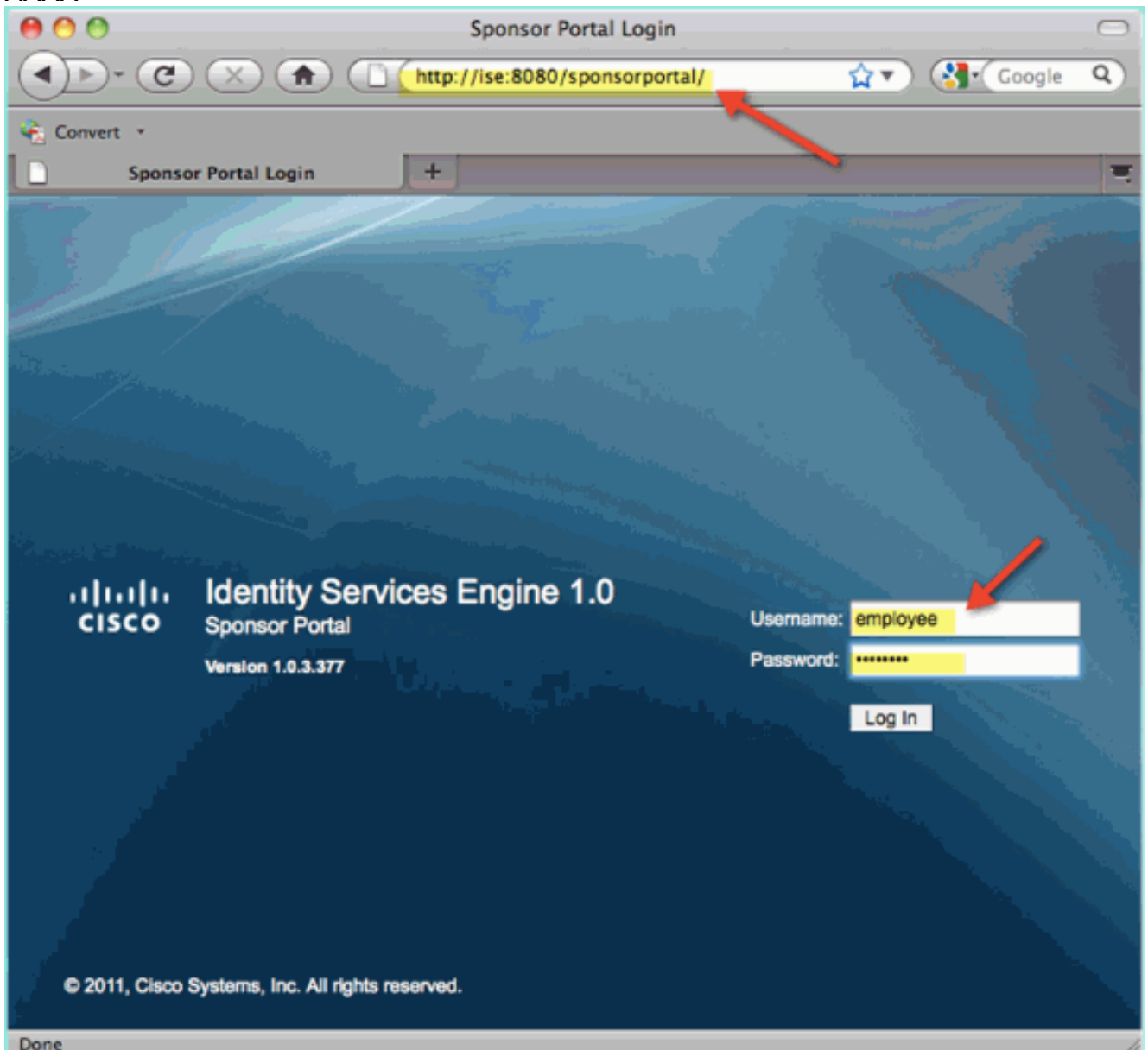
Patrocinando Convidado

Anteriormente, você configurou a política de convidado e os grupos apropriados para permitir que o usuário de domínio do AD patrocine convidados temporários. Em seguida, você acessará o Portal do Patrocinador e criará um acesso de convidado temporário.

Conclua estes passos:

1. Em um navegador, navegue até um destes URLs: <http://<ip>:8080/sponsorportal/> ou <https://<ip>:8443/sponsorportal/>. Em seguida, faça login com o seguinte: Nome de usuário: aduser (Active Directory), employee (Usuário interno) Senha:

XXXX



2. Na página Patrocinador, clique em **Criar conta única de usuário convidado**.

CISCO Sponsor Portal

▼ Sponsor

- Home
- Settings Customization

▼ Account Management

- View Guest Accounts
- Create Multiple Accounts

Sponsor Portal: Getting Started

[View All Guest User Accounts](#)

[Create Single Guest User Account](#)

[Create Multiple Guest User Accounts](#)

3. Para um convidado temporário, adicione o seguinte:
- Nome: obrigatório (por exemplo, Sam)
 - Sobrenome: obrigatório (por exemplo, Jones)
 - Função do grupo: Convidado
 - Perfil de Tempo: DefaultOneHour
 - Fuso horário: Qualquer/Padrão

Sponsor Portal

Account Management > [View All Guest Accounts](#) > Create Guest Account

Create Guest Account

First Name:

Last Name:

Email Address:

Phone Number:

Company:

Optional Data 1:

Optional Data 2:

Optional Data 3:

Optional Data 4:

Optional Data 5:

Group Role:

Time Profile:

Timezone:

⚙ = Required fields

4. Clique em Submit.
5. Uma conta de convidado é criada com base em sua entrada anterior. Observe que a senha é visível (do exercício anterior), ao contrário dos *** de hash.
6. Deixe essa janela aberta mostrando o Nome de Usuário e a Senha do convidado. Você os usará para testar o Login no Portal do Convidado (a seguir).



Successfully Created Guest Account **siam0002**

Username: **siam0002** ←

Password: **5_5g6d7Kx** ←

First Name: Sam ←

Last Name: iAm

Email Address:

Phone Number:

Company:

Status: AWAITING INITIAL LOGIN

Suspended: false

Optional Data 1:

Optional Data 2:

Optional Data 3:

Optional Data 4:

Optional Data 5:

Group Role: Guest

Time Profile: DefaultOneHour

Timezone: EST

Account Start Date: 2011-07-15 13:56:04 EST

Account Expiration Date: 2011-07-15 14:56:04 EST

Email

Print

Create Another Account

View All Accounts

Testando o acesso ao portal de convidados

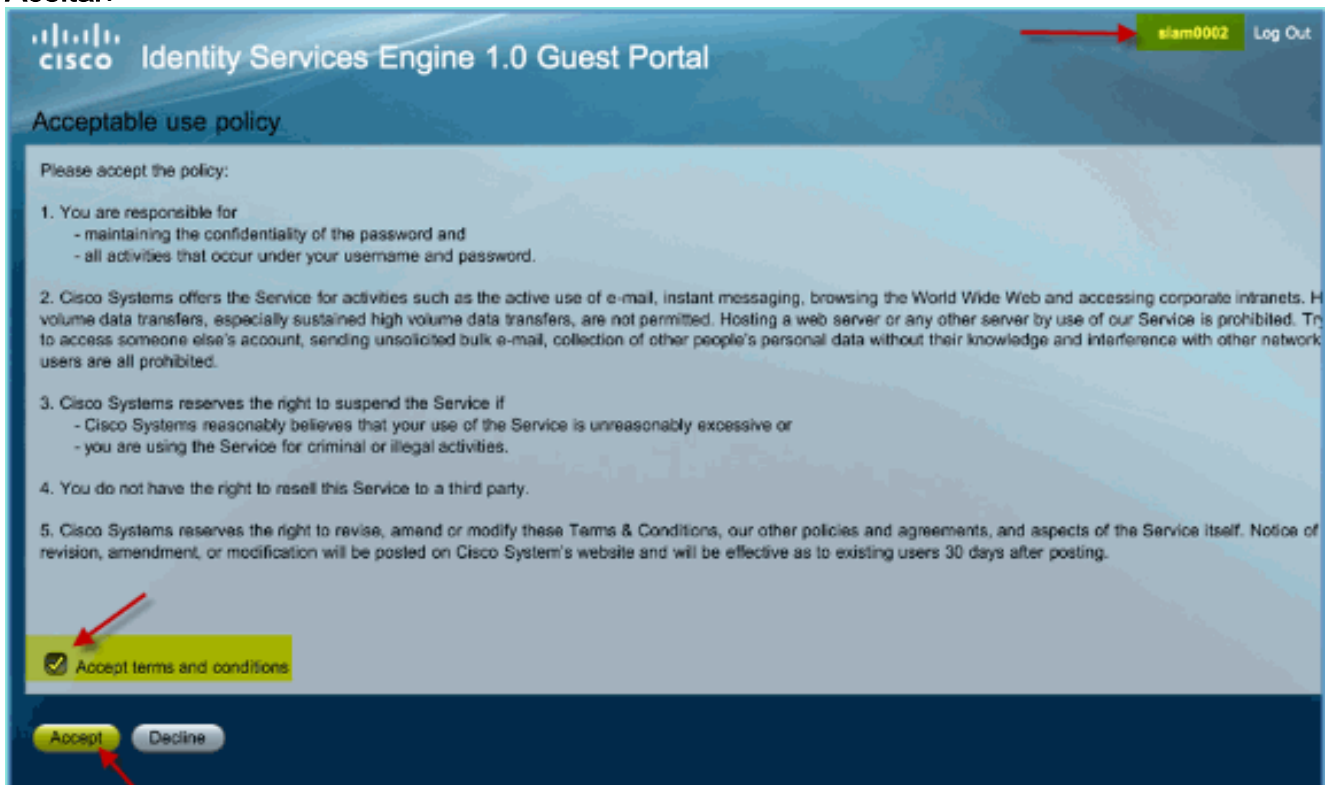
Com a nova conta de convidado criada por um usuário/patrocinador do AD, é hora de testar o acesso e o portal do convidado.

Conclua estes passos:

1. Em um dispositivo preferencial (neste caso, um iOS/iPad da Apple), conecte-se ao SSID de convidado do Pod e verifique o endereço IP/conectividade.
2. Use o navegador e tente navegar até <http://www.Você será redirecionado para a página Login no Portal do convidado>.



3. Faça login usando a conta de convidado criada no exercício anterior. Se a operação for bem-sucedida, a página Política de uso aceitável será exibida.
4. Marque **Aceitar termos e condições** e clique em **Aceitar**.



A URL original é concluída, e o ponto final tem acesso permitido como convidado.

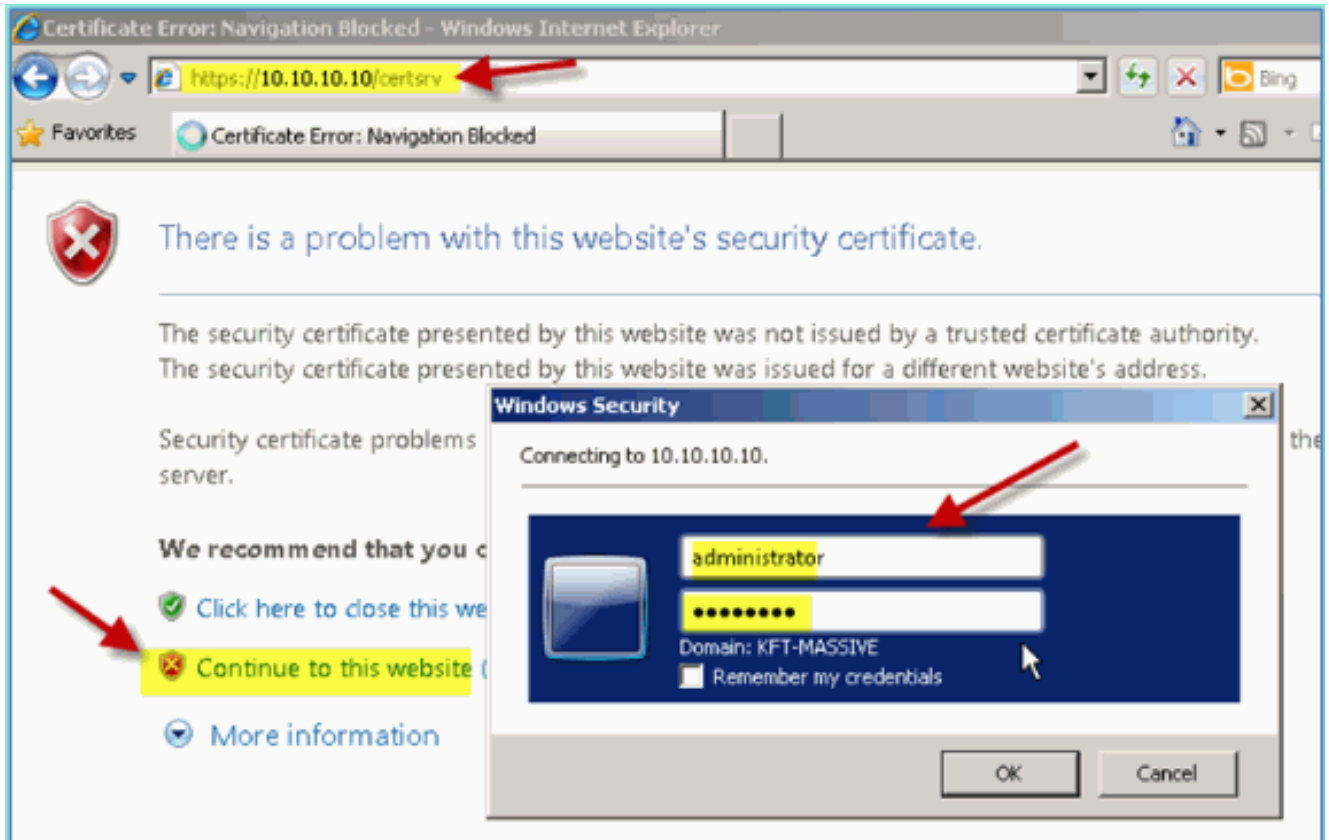
Configuração do certificado

Para proteger as comunicações com o ISE, determine se a comunicação está relacionada à autenticação ou ao gerenciamento do ISE. Por exemplo, para a configuração usando a IU da Web do ISE, os certificados X.509 e as cadeias confiáveis de certificados precisam ser configurados para permitir a criptografia assimétrica.

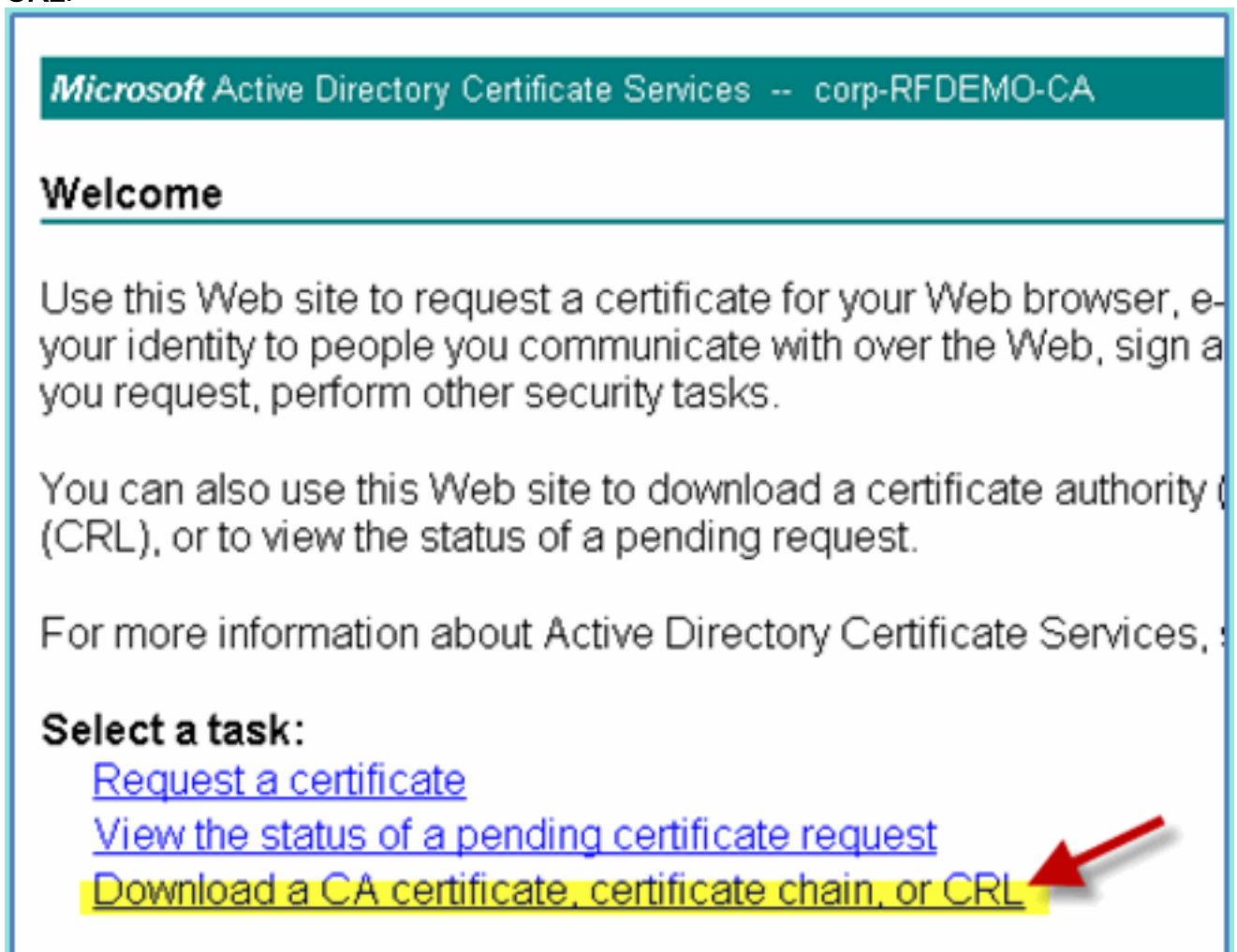
Conclua estes passos:

1. No PC conectado com fio, abra uma janela do navegador para <https://AD/certsrv>. **Observação:** use o HTTP seguro. **Observação:** use o Mozilla Firefox ou o MS Internet Explorer para acessar o ISE.
2. Efetue login como

administrator/Cisco123.



3. Clique em **Baixar um certificado de CA, uma cadeia de certificados ou um CRL**.



4. Clique em **Download CA certificate** e salve-o (observe o local de

Microsoft Active Directory Certificate Services -- corp-RFDEMO-CA

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, install the CA certificate on your computer.

To download a CA certificate, certificate chain, or CRL, select the type of file you want to download.

CA certificate:

Current [corp-RFDEMO-CA]

Encoding method:

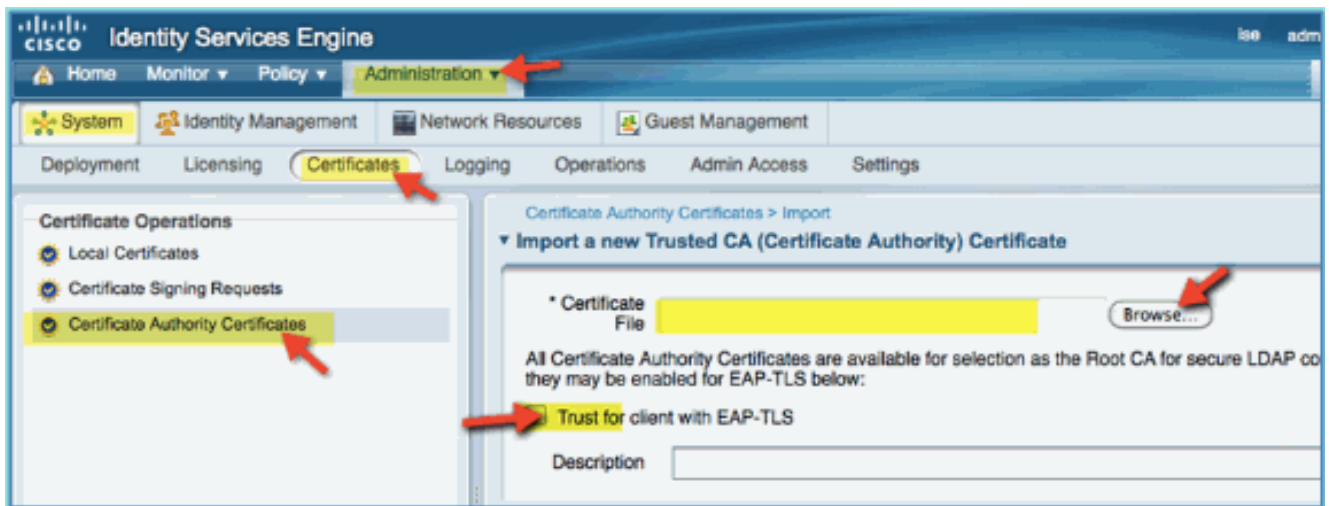
DER
 Base 64

[Download CA certificate](#)
[Download CA certificate chain](#)
[Download latest base CRL](#)
[Download latest delta CRL](#)

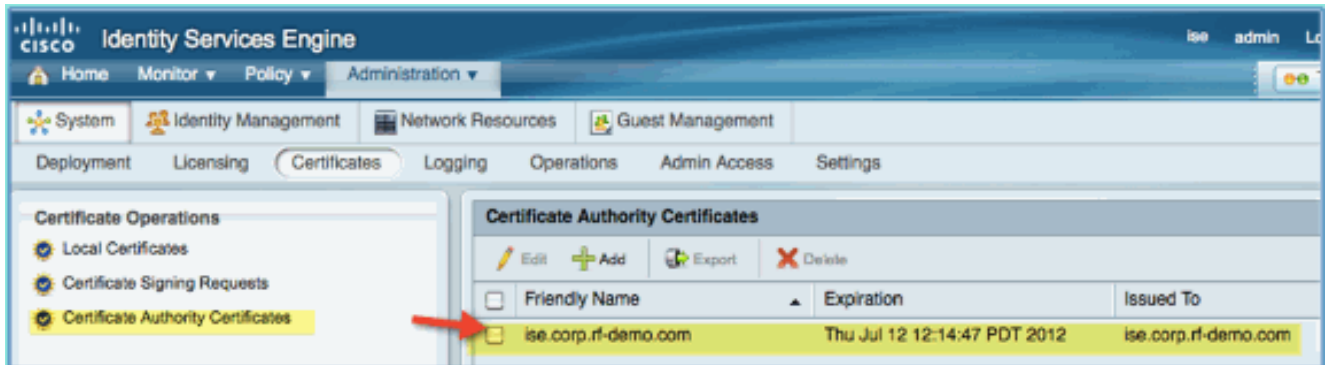
salvamento).

5. Abra uma janela do navegador em <https://<Pod-ISE>>.
6. Vá para **Administration > System > Certificates > Certificates Authority Certificates**.

7. Selecione a operação **Certificados de Autoridade de Certificação** e navegue até o certificado de CA baixado anteriormente.
8. Selecione **Confiança para cliente com EAP-TLS** e, em seguida, envie.

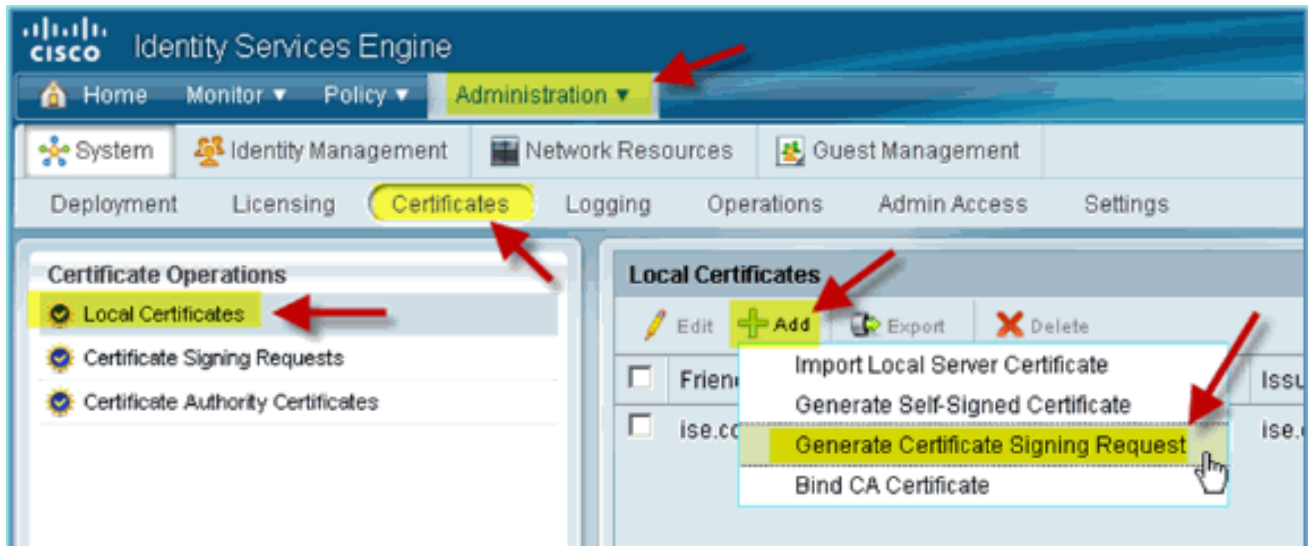


9. Confirme se a CA foi adicionada como confiável como CA raiz.



10. Em um navegador, vá para **Administration > System > Certificates > Certificates Authority Certificates**.

11. Clique em **Adicionar** e em **Gerar Solicitação de Assinatura de Certificado**.



12. Enviar estes valores: Assunto do certificado: CN=ise.corp.rf-demo.com
Comprimento da chave: 2048

Local Certificates > Generate Certificate Signing Request

▼ **Generate Certificate Signing Request**

Certificate

* Certificate Subject

* Key Length

Digest to Sign With SHA1

13. O ISE avisa que o CSR está disponível na página CSR. Click OK.



14. Selecione o CSR na página ISE CSR e clique em **Exportar**.
15. Salve o arquivo em qualquer local (por exemplo, Downloads, etc.)
16. O arquivo será salvo como *.pem.

Cisco Identity Services Engine Administration

System Identity Management Network Resources Guest Management

Deployment Licensing Certificates Logging Operations Admin Access Settings

Certificate Operations

- Local Certificates
- Certificate Signing Requests**
- Certificate Authority Certificates

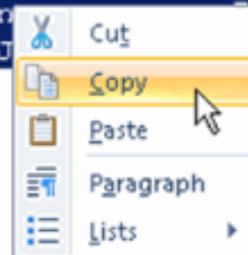
Certificate Signing Requests

Export Delete

<input checked="" type="checkbox"/>	Friendly Name	Certificate Subject	Key Length
<input checked="" type="checkbox"/>	ise.corp.rf-demo.com	CN=ise.corp.rf-demo.com	2048

17. Localize o arquivo CSR e edite com o Notepad/Wordpad/TextEdit.
18. Copie o conteúdo (Selecionar tudo > Copiar).

```
-----BEGIN CERTIFICATE REQUEST-----
MIICyTCCAAbECAQAwHzEdMBSGA1UEAxMUaXNlLmNvcnAucmYtZGVtby5jb20wggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDXaeWDSqfiI64K59dyRLm8JAxan
WYTaAJ68/Ke206ws/K3BFAFJQhndQQ0hYVmGcJLVN03pXtRln/q/HBuglLIItIvbe
86FADPq3kUNb48UHcdR9b5rUs7B8T5E6banZia6eHSXjIzX4f0U7mVOrzALeAPDK
HXU+/y/gleyNL6P8zC4bvi/SZXhZp1OvTQpi+8lh14M5ROChhbPUnB3EGVaIVRiN
wYn8Ojvejbtg//k0CItGARlG2IFbBbgUpkMVhDQqgixp3wrlm3hi9JXgffEI f4BO
sirLrhvMSuSNESnIVWYrRLz5Xt4dMct+bu08xaEYPqgoukYjxsA9gn0bRDMJAgMB
AAGgZTBjBqkqhkiG9w0BCQ4xVjBUMASGA1UdDwQEAWICrDAdBgNVHQ4EFgQU2jmj
715rSw0yVb/vlWAYkK/YBwkWewYDVR0lBAwwCgYIKwYBBQUHAWewEQYJYIZIAYb4
QgEBBAQDAgZAMA0GCSqGSIb3DQEBBQUAA4IBAQBz4YPO9sN7WF2Htg+48300mw9q
gA/MMZsTioEPekcunrm+ZFtlAXajB32uwHHi1lc9Rn93TgOWPFxKEX9E89fzSWDK
J4qsQM7KEYOpQt4bia07188Lm6BBTk9mRhiTBwSF3dx0tlzfgiHc72kjWvxsgg/c
k8a7LHYgkgLRYBnpu15RjQ7wWijArH8cK1OrVT42riz7vK0g0nkWRHF52uiu3AkP
LPKQ72N2XYIXfu0jdgOaJjmsk6T9nLABVYQ6n...KDJTHchcwx6I1k/
V5QYBOjTYHXIPG8/ned9z3M0iZd2sm4XNS2bJ...W1ZuB6drHg9
-----END CERTIFICATE REQUEST-----
```



19. Abra uma janela do navegador em <https://<Pod-AD>/certsrv>.
20. Clique em **Solicitar um certificado**.

Microsoft Active Directory Certificate Services -- corp-RFDEMO-CA

Welcome

Use this Web site to request a certificate for your Web browser to communicate with over the Web, sign and encrypt messages.

You can also use this Web site to download a certificate automatically for a pending request.

For more information about Active Directory Certificate Services, click the following link:

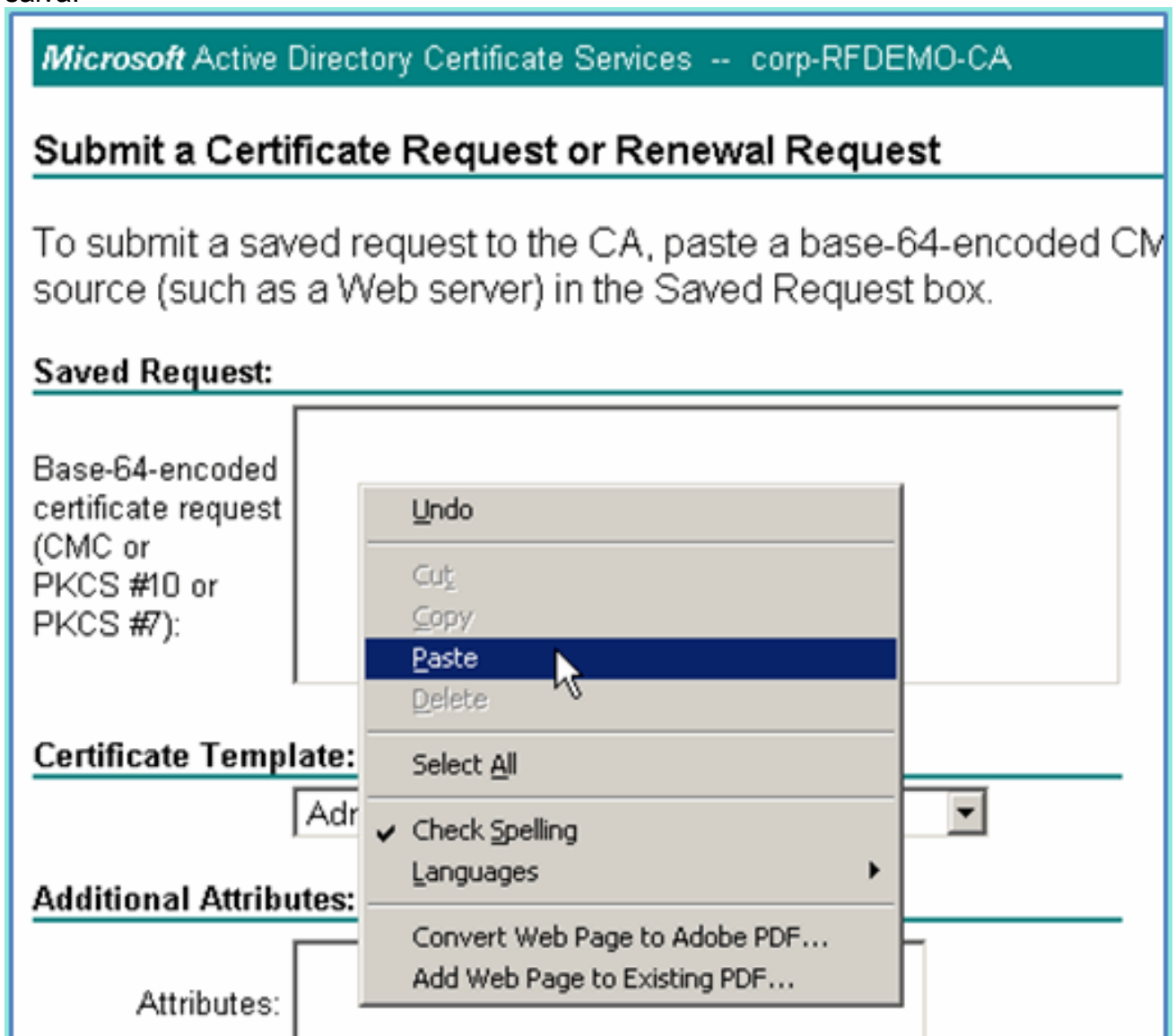
Select a task:

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

21. Clique em para enviar uma **solicitação de certificado avançada**.



22. Cole o conteúdo de CSR no campo de solicitação salva.



23. Selecione **Servidor Web** como o Modelo de certificado e clique em **Enviar**.

Microsoft Active Directory Certificate Services -- corp-RFDEMO-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
gA/MMZsTioEPekcunnm+ZFt1AXajB32uwHH11c9
J4qsQM7KEYOpQt4bia071S8Lm6BBTk9mRhiTBwSF
kSa7LHYgkgLRYBnpul5RjQ7wWijArH8cK1OrVT42
LPKQ72N2XYIXfu0jdgogaJjmsk6T9nLABVYQ6nKQx
V5QYBOjTYHXIPG8/ned9z3MOiZd2sm4XNS2bJfO/
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Web Server

Additional Attributes:

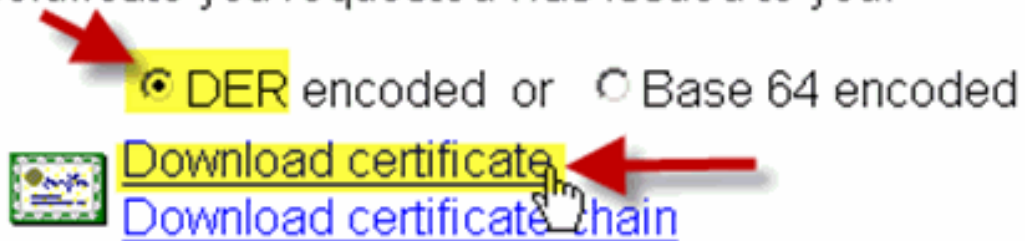
Attributes:

Submit >

24. Selecione **DER encoded** e clique em **Download certificate**.

Certificate Issued

The certificate you requested was issued to you.

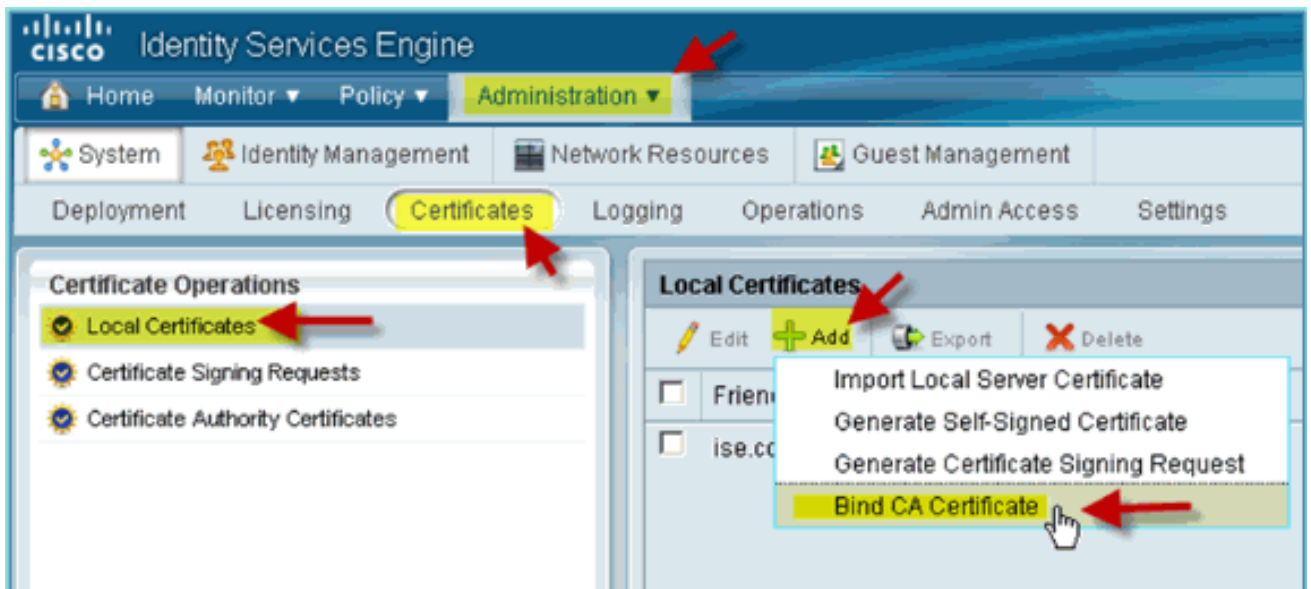


25. Salve o arquivo em um local conhecido (por exemplo, Downloads)

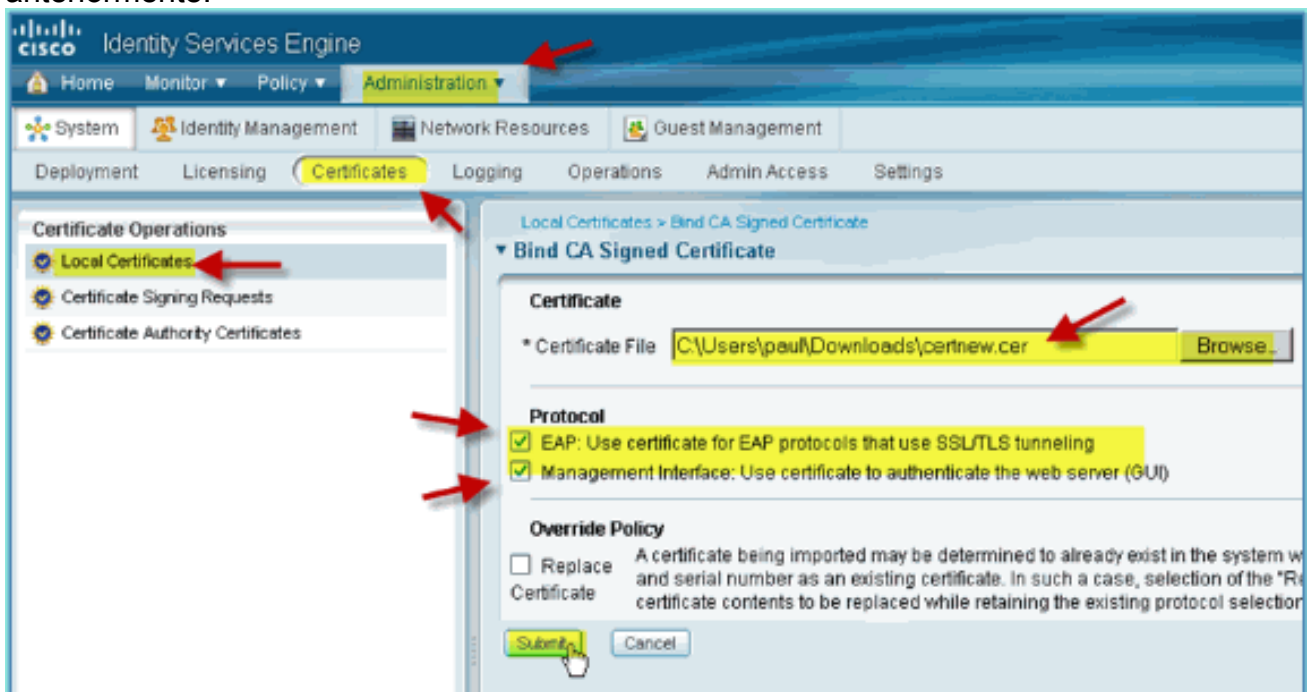
26. Vá para **Administration > System > Certificates > Certificates Authority Certificates**.



27. Clique em **Add > Bind CA Certificate**.

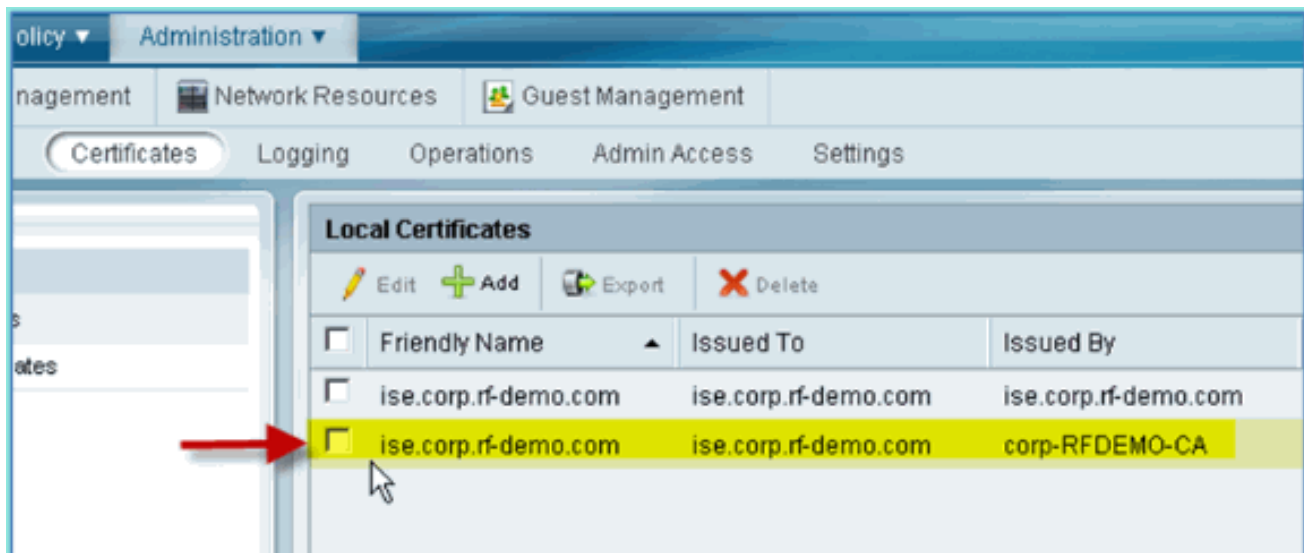


28. Navegue até o certificado CA baixado anteriormente.



29. Selecione Protocol EAP e Management Interface e clique em Submit.

30. Confirme se a CA foi adicionada como confiável como CA raiz.

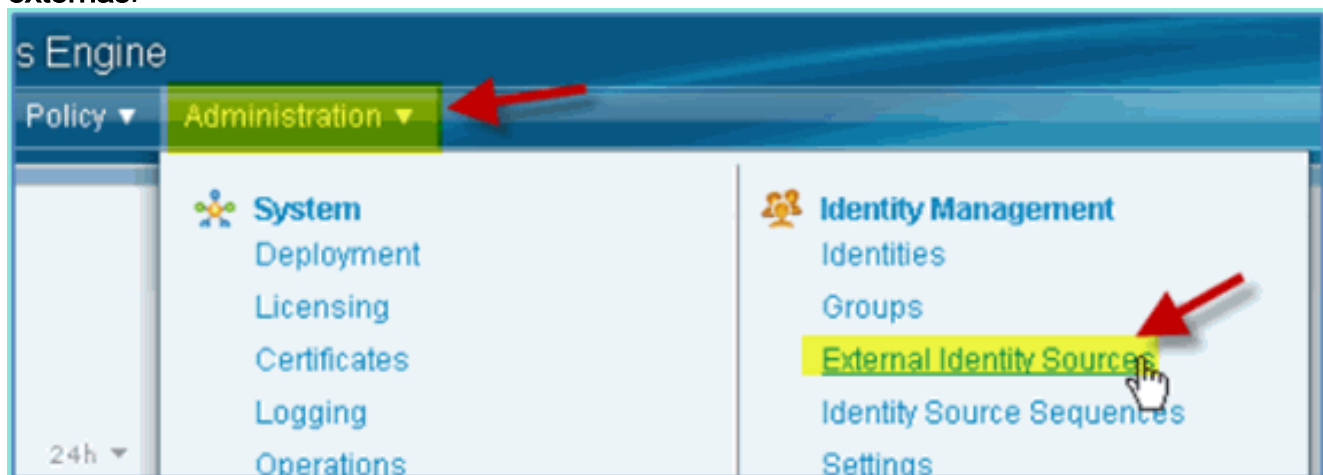


[Integração com o Ative Directory do Windows 2008](#)

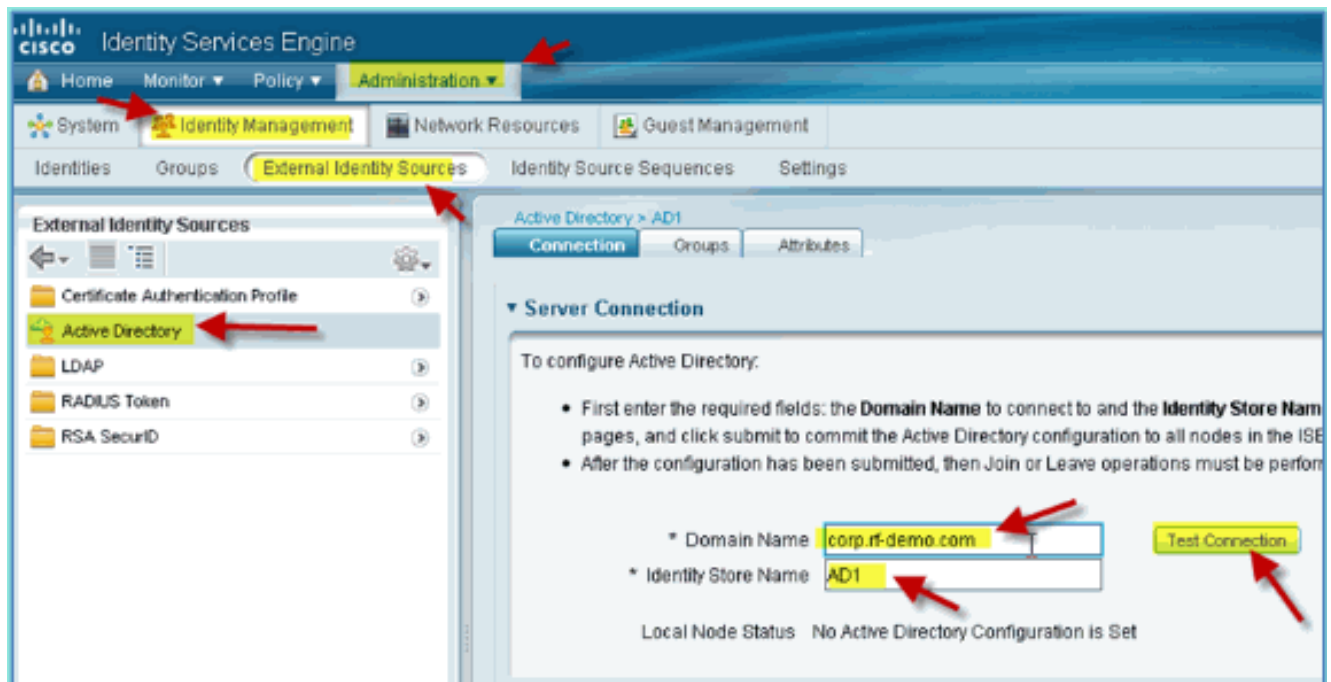
O ISE pode se comunicar diretamente com o Ative Directory (AD) para autenticação de usuário/máquina ou para recuperar informações de autorização dos atributos do usuário. Para se comunicar com o AD, o ISE deve estar "associado" a um domínio do AD. Neste exercício, você ingressará o ISE em um domínio do AD e confirmará se a comunicação do AD está funcionando corretamente.

Conclua estes passos:

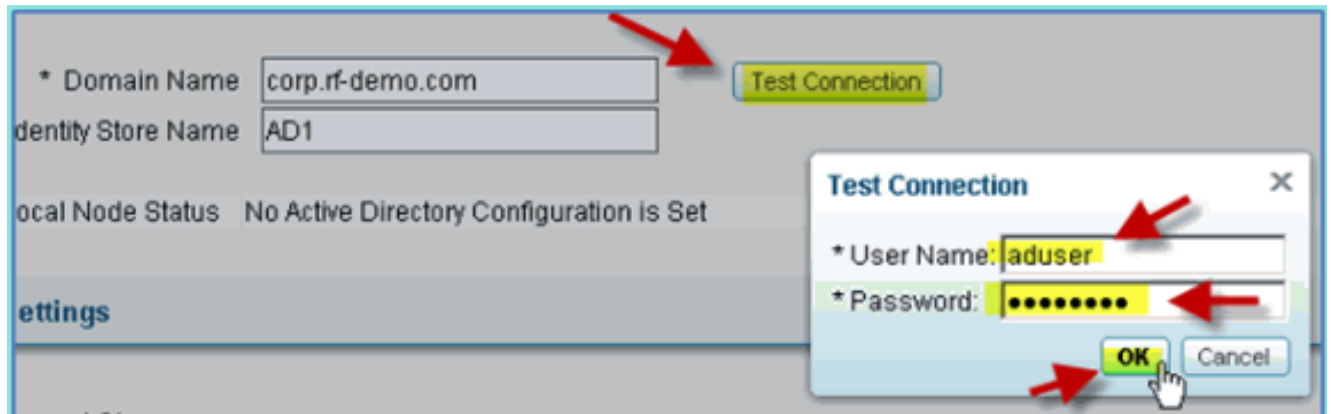
1. Para ingressar o ISE no domínio do AD, no ISE, vá para **Administração > Gerenciamento de identidade > Fontes de identidade externas**.



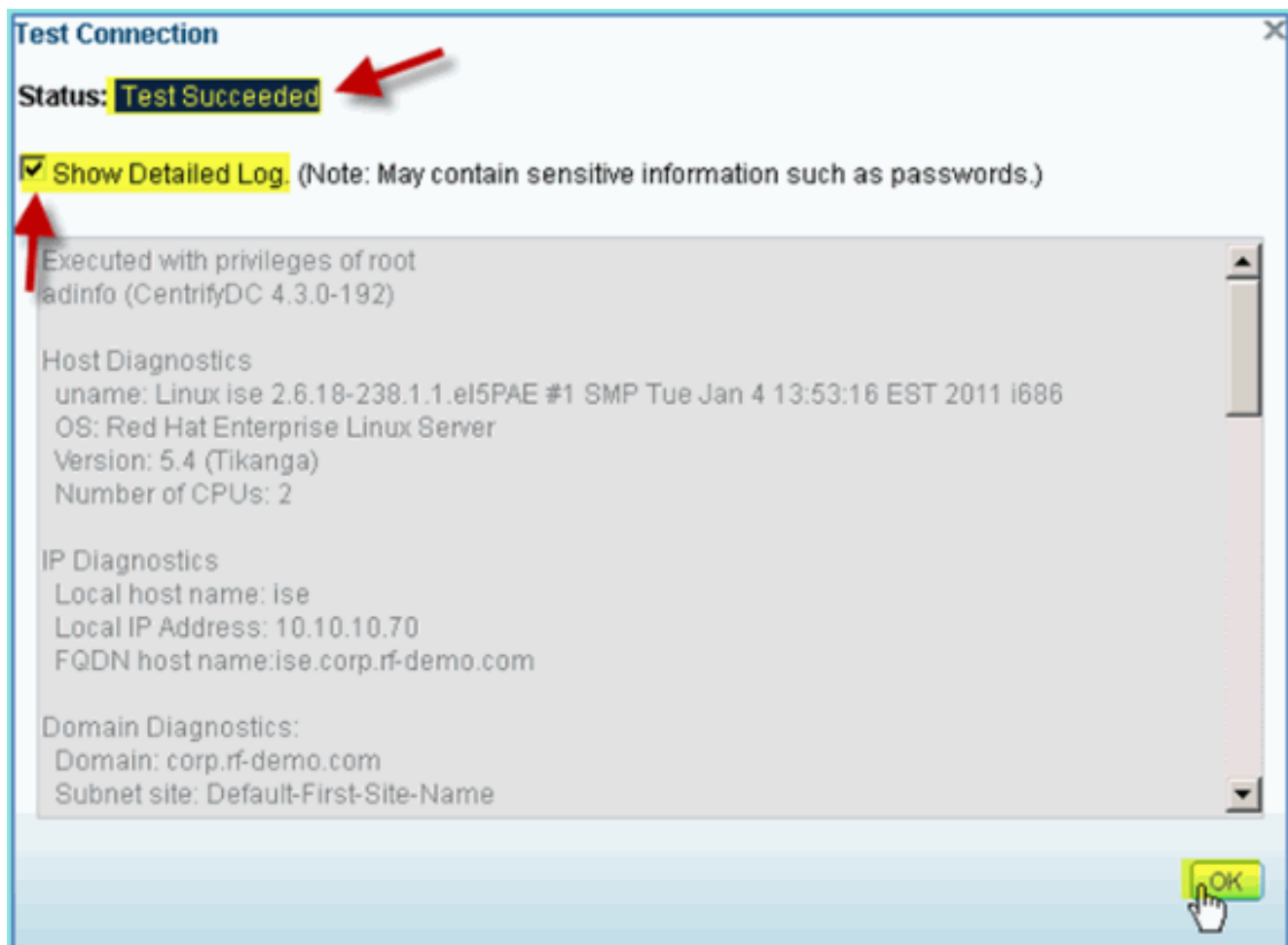
2. No painel esquerdo (Fontes de identidade externas), selecione **Ative Directory**.
3. No lado direito, selecione a guia **Connection** e insira o seguinte: Nome do domínio: corp.rf-demo.com Nome do Repositório de Identidades: AD1



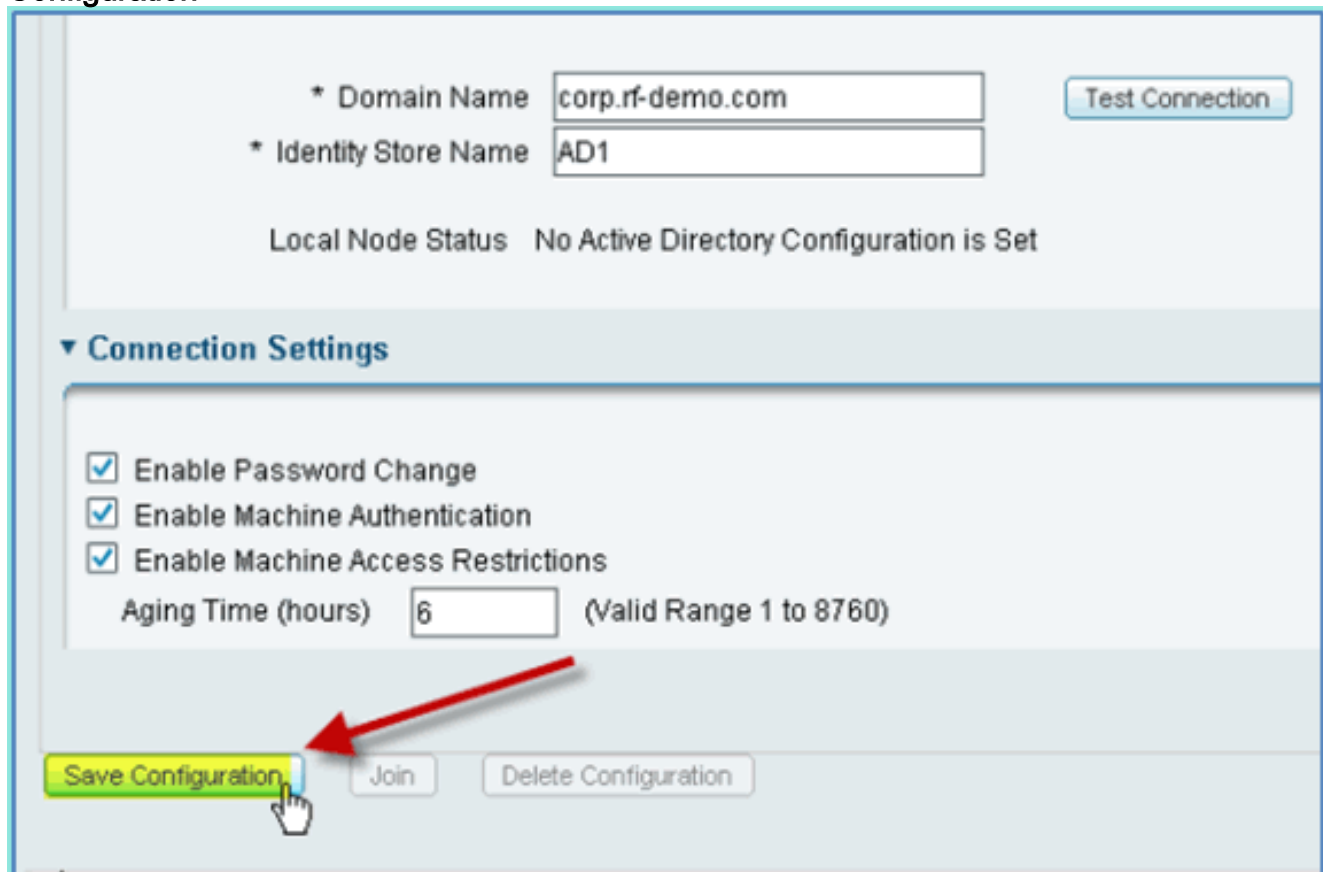
4. Clique em **Testar conexão**. Insira o nome de usuário do AD (aduser/Cisco123) e clique em **OK**.



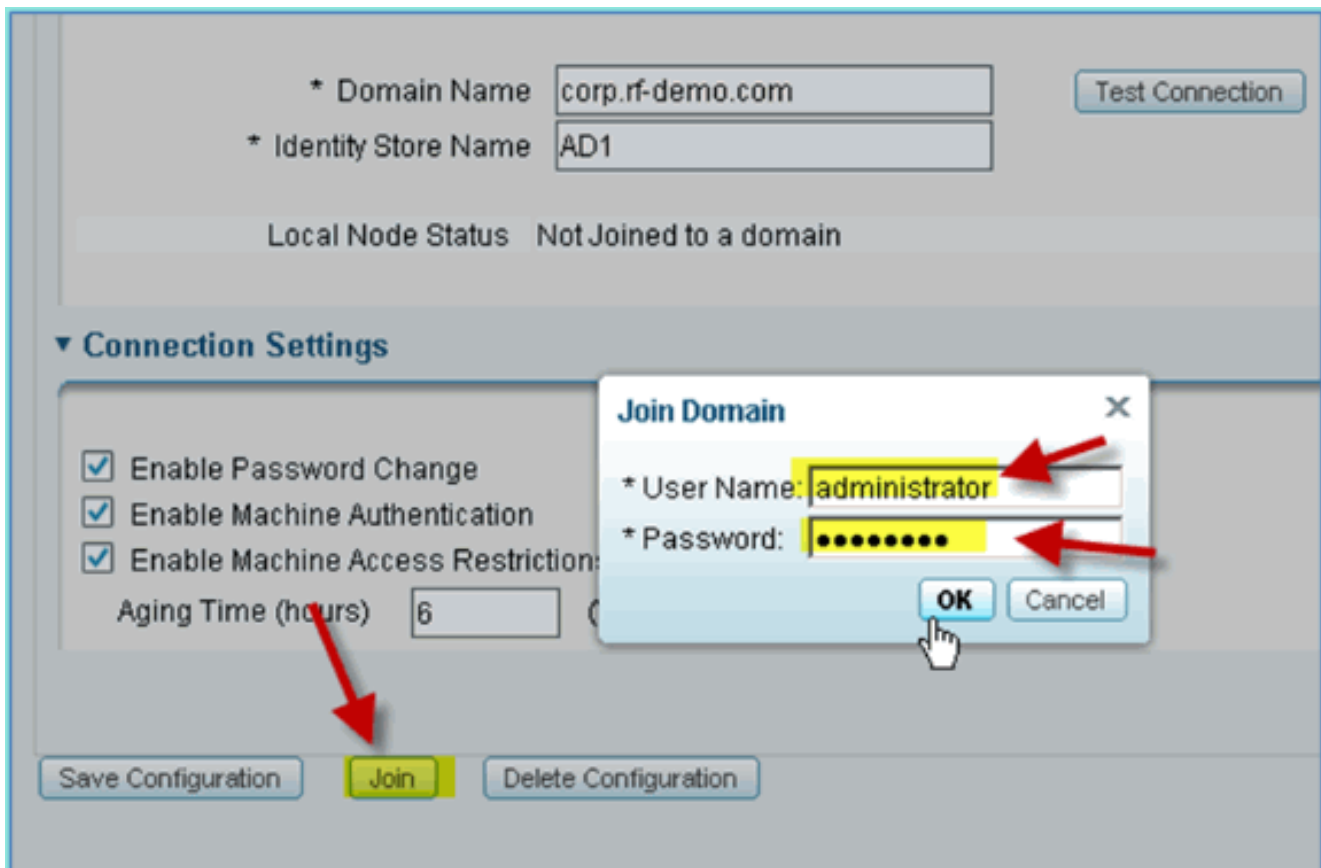
5. Confirme se o Status do teste mostra **Teste bem-sucedido**.
6. Selecione **Mostrar log detalhado** e observe os detalhes úteis para a solução de problemas. Clique em **OK** para continuar.



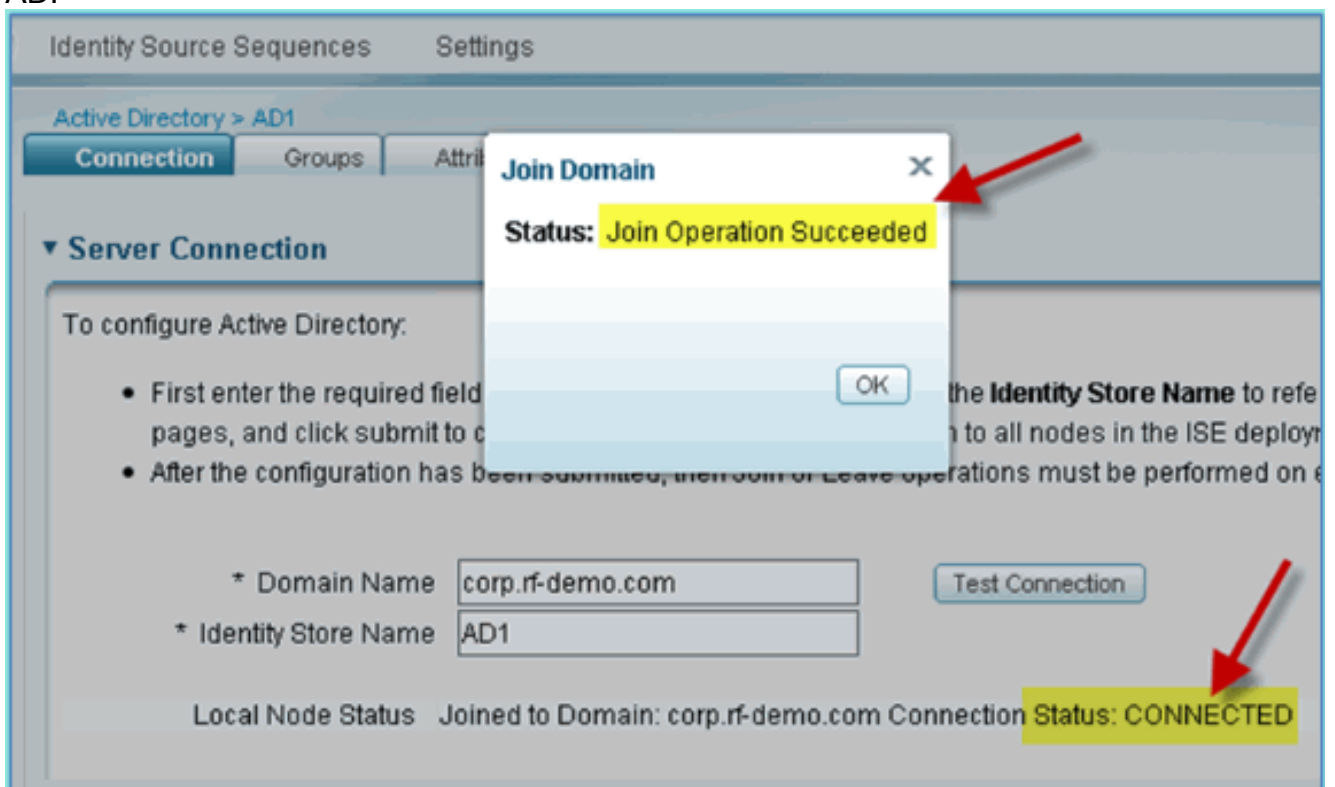
7. Clique em **Save Configuration**.



8. Clique em **Ingressar**. Insira o usuário do AD (administrador/Cisco123) e clique em **OK**.



9. Confirme se Join Operation Status (Status da operação de junção) mostra **Succeeded** e clique em **OK** para continuar. O Status da conexão do servidor mostra **CONNECTED**. Se esse Status mudar a qualquer momento, uma Conexão de teste ajudará a solucionar problemas com as operações do AD.



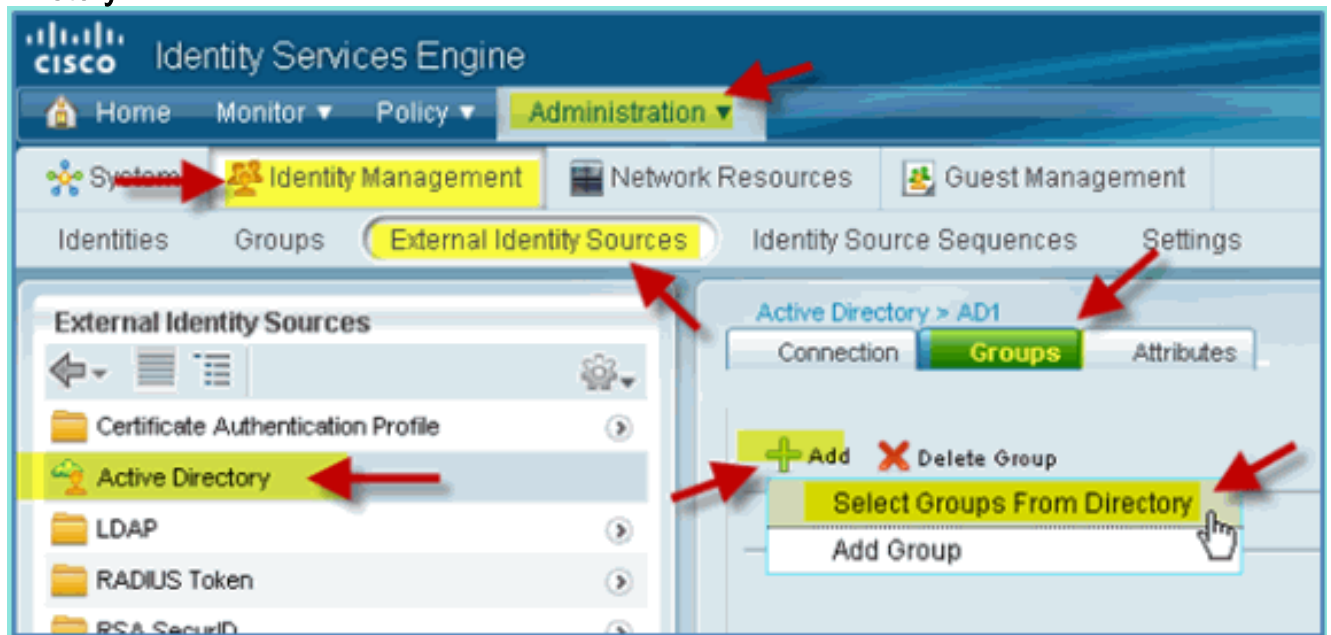
[Adicionar Grupos do Ative Diretory](#)

Quando grupos do AD são adicionados, é permitido um controle mais granular sobre as políticas do ISE. Por exemplo, os grupos do AD podem ser diferenciados por funções funcionais, como grupos de funcionários ou contratados, sem que o bug relacionado tenha sido detectado em exercícios anteriores do ISE 1.0, em que as políticas eram limitadas apenas aos usuários.

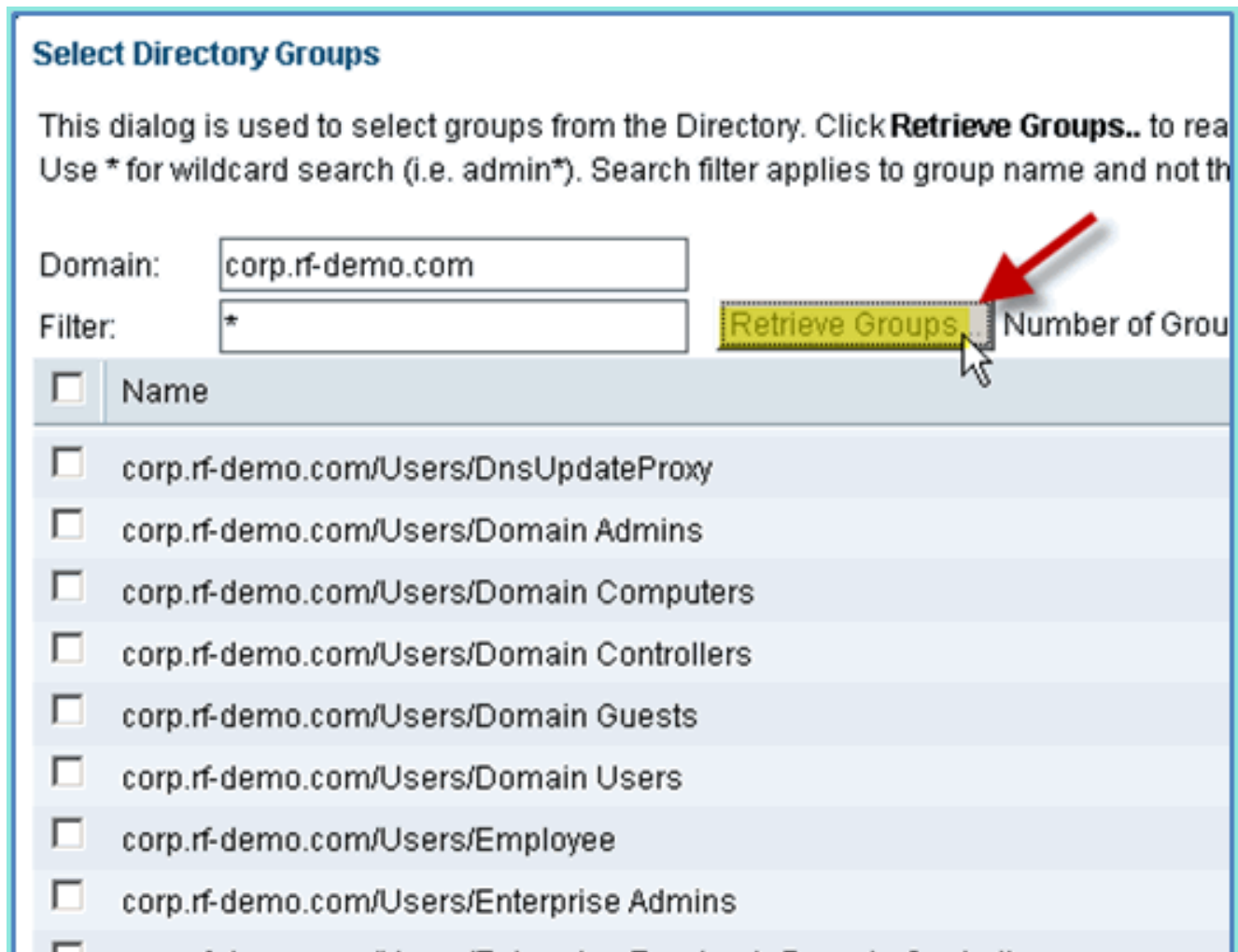
Neste laboratório, somente os Usuários do domínio e/ou o grupo Funcionário são usados.

Conclua estes passos:

1. No ISE, vá para **Administration > Identity Management > External Identity Sources**.
2. Selecione a guia **Active Directory > Groups**.
3. Clique em **+Add** e, em seguida, em **Select Groups From Directory**.



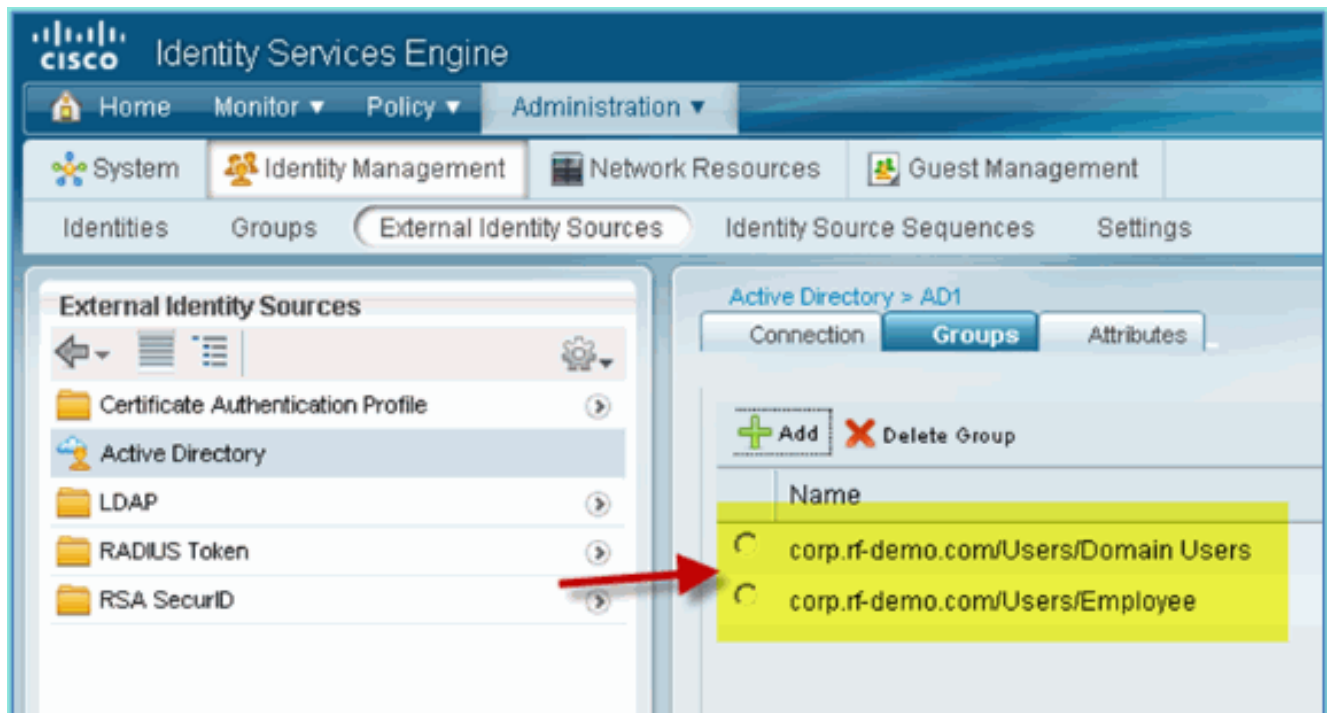
4. Na janela de acompanhamento (Selecionar grupos de diretórios), aceite os padrões para domínio (corp-rf-demo.com) e Filtro (*). Em seguida, clique em **Recuperar grupos**.



5. Selecione as caixas para os grupos **Usuários do domínio** e **Funcionário**. Clique em OK quando terminar.



6. Confirme se os grupos foram adicionados à lista.

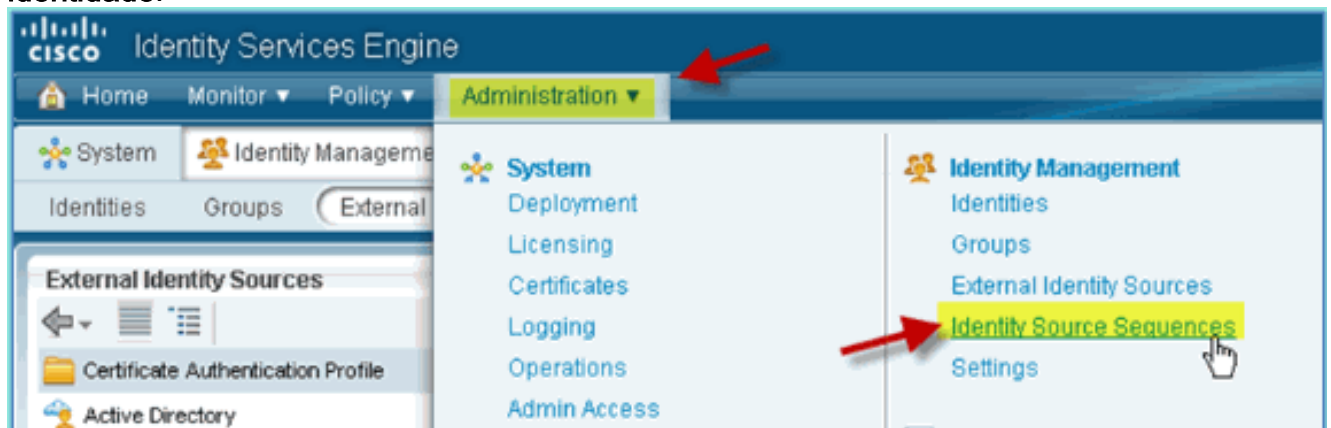


Adicionar sequência de origem de identidade

Por padrão, o ISE é definido para usar Usuários internos para armazenamento de autenticação. Se o AD for adicionado, uma ordem de prioridade de sequência poderá ser criada para incluir o AD que o ISE usará para verificar a autenticação.

Conclua estes passos:

1. No ISE, navegue até **Administração > Gerenciamento de identidades > Sequências de origem de identidade**.



2. Clique em **+Add** para adicionar uma nova sequência.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes 'Home', 'Monitor', 'Policy', and 'Administration'. Below this, there are tabs for 'System', 'Identity Management', 'Network Resources', and 'Guest Management'. The 'Identity Source Sequences' tab is selected. The main content area displays a table of Identity Source Sequences with columns for 'Name', 'Description', and 'Identity Stores'. The 'Add' button is highlighted with a red arrow.

Name	Description	Identity Stores
Guest_Portal_Sequence	A built-in Identity Sequence for the Guest Portal	Internal Users
Sponsor_Portal_Sequence	A built-in Identity Sequence for the Sponsor Portal	Internal Users

3. Insira o novo nome: **AD_Internal**. Adicione todas as origens disponíveis ao campo Selecionado. Em seguida, reordene conforme necessário para que AD1 seja movido para o início da lista. Clique em Submit.

Identities Groups External Identity Sources **Identity Source Sequences** Settings

Identity Source Sequences List > New Identity Source Sequence

▼ Identity Source Sequence

* Name

Description

▼ Certificate Based Authentication

Select Certificate Authentication Profile

▼ Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available	Selected
	AD1 Internal Users Internal Endpoints

▼ Advanced Search List Settings

Select the action to be performed if a selected identity store cannot be accessed for authentication

Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"

Treat as if the user was not found and proceed to the next store in the sequence

4. Confirme se a sequência foi adicionada à lista.

CISCO Identity Services Engine

Home Monitor Policy Administration

System Identity Management Network Resources Guest Management

Identities Groups External Identity Sources **Identity Source Sequences** Settings

Identity Source Sequences

Edit Add Duplicates Delete Filter

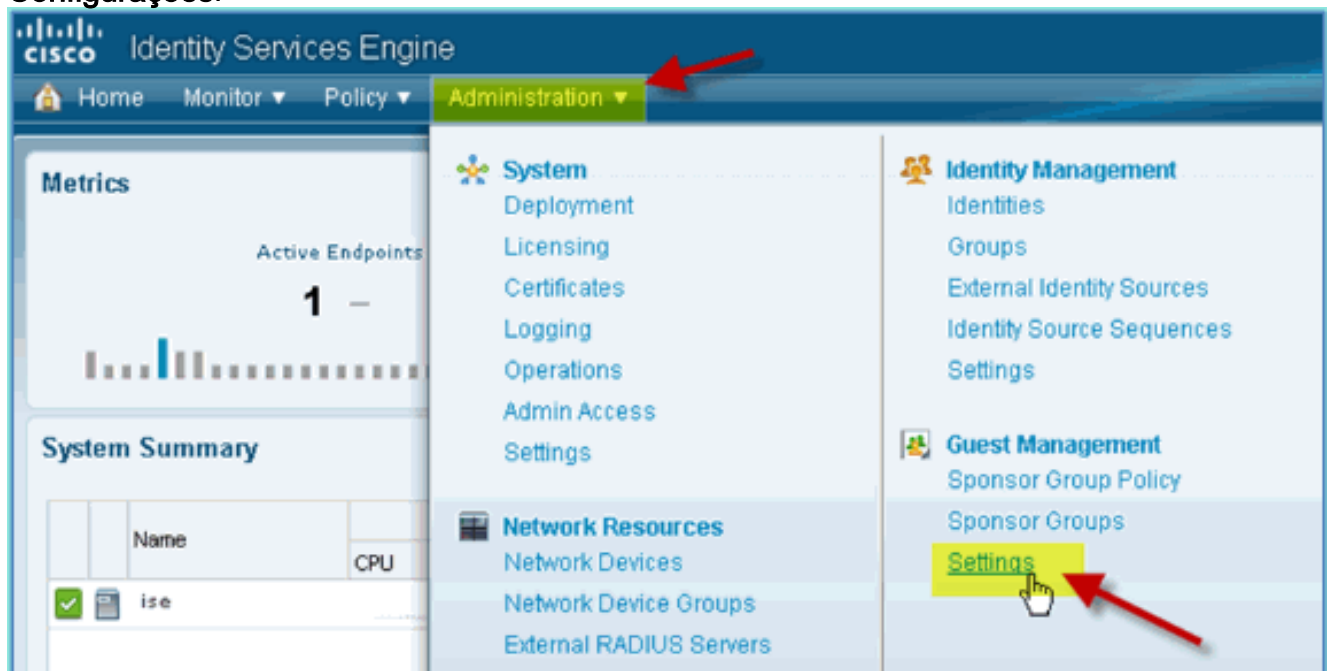
Name	Description	Identity Stores
AD_Internal		AD1, Internal Endpoints, Internal Users
Guest_Portal_Sequence	A built-in Identity Sequence for the Guest Portal	Internal Users
Sponsor_Portal_Sequence	A built-in Identity Sequence for the Sponsor Portal	Internal Users

Acesso de convidado patrocinado pelo ISE Wireless com AD integrado

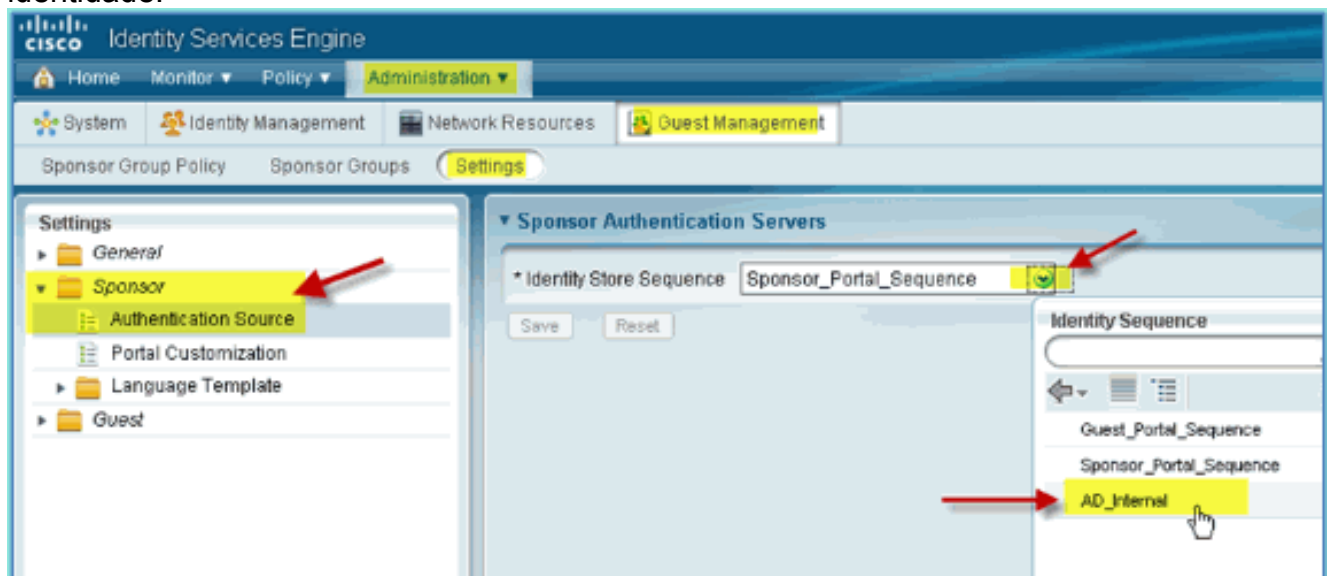
O ISE pode ser configurado para permitir que convidados sejam patrocinados com políticas para permitir que usuários de domínio do AD patrocinem o acesso de convidados.

Conclua estes passos:

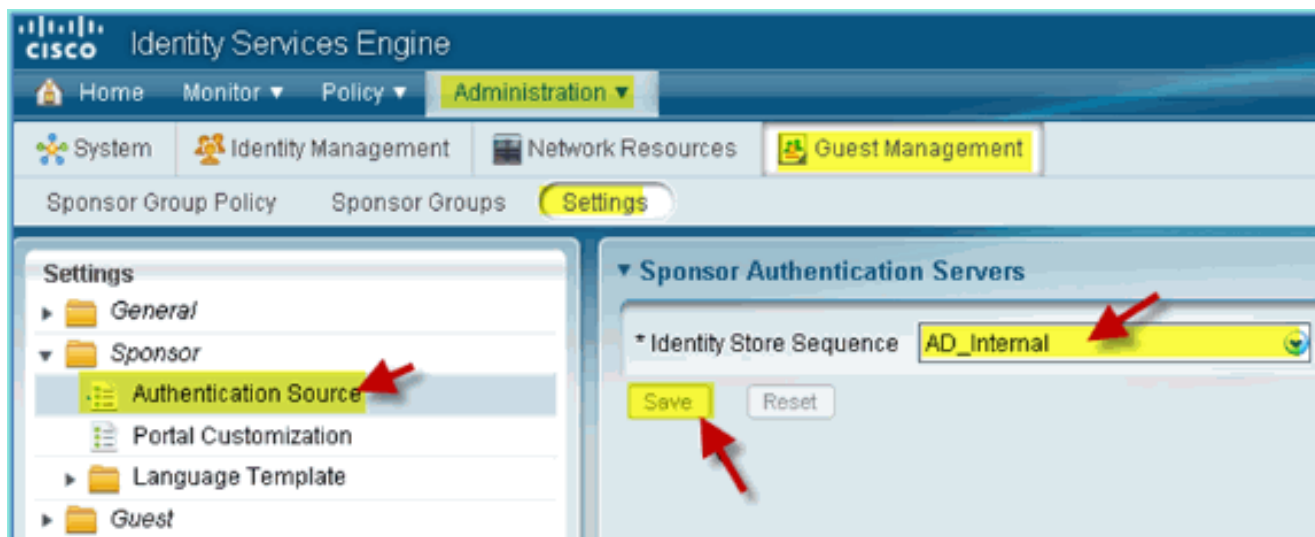
1. No ISE, navegue até **Administração > Gerenciamento de convidados > Configurações**.



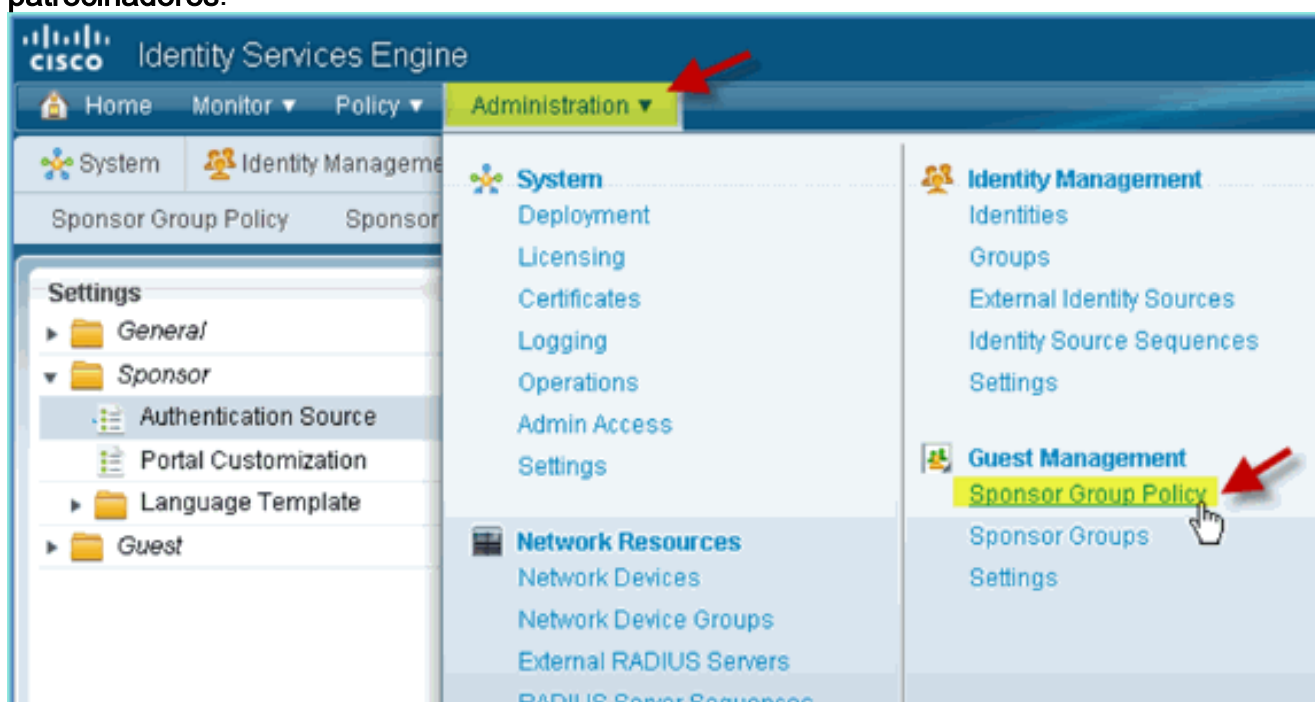
2. Expanda **Patrocinador** e clique em **Origem da autenticação**. Em seguida, selecione **AD_Internal** como Sequência de armazenamento de identidade.



3. Confirme **AD_Internal** como a Sequência do Repositório de Identidades. Click **Save**.



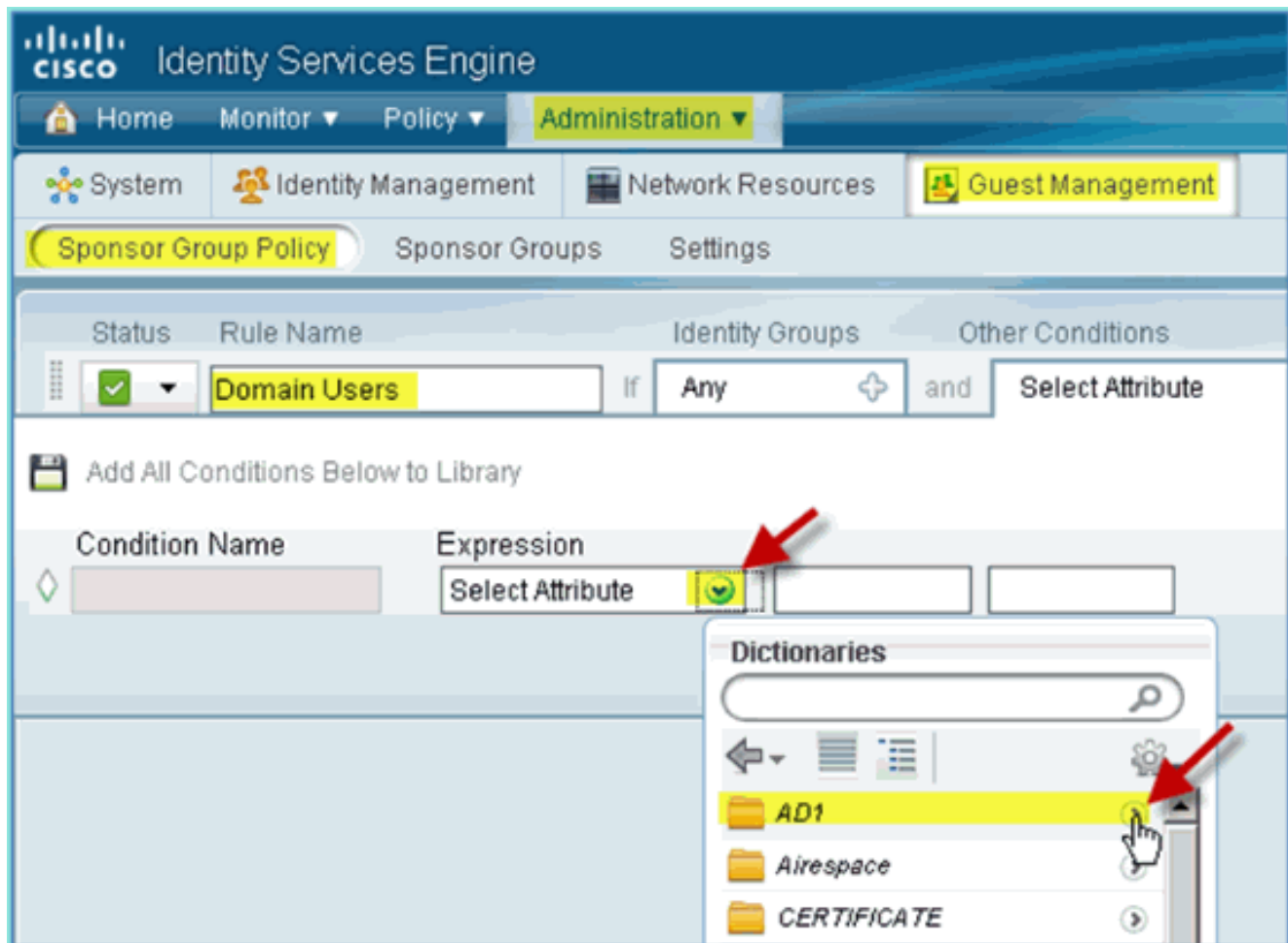
4. Navegue até Administração > Gerenciamento de convidados > Política de grupo de patrocinadores.



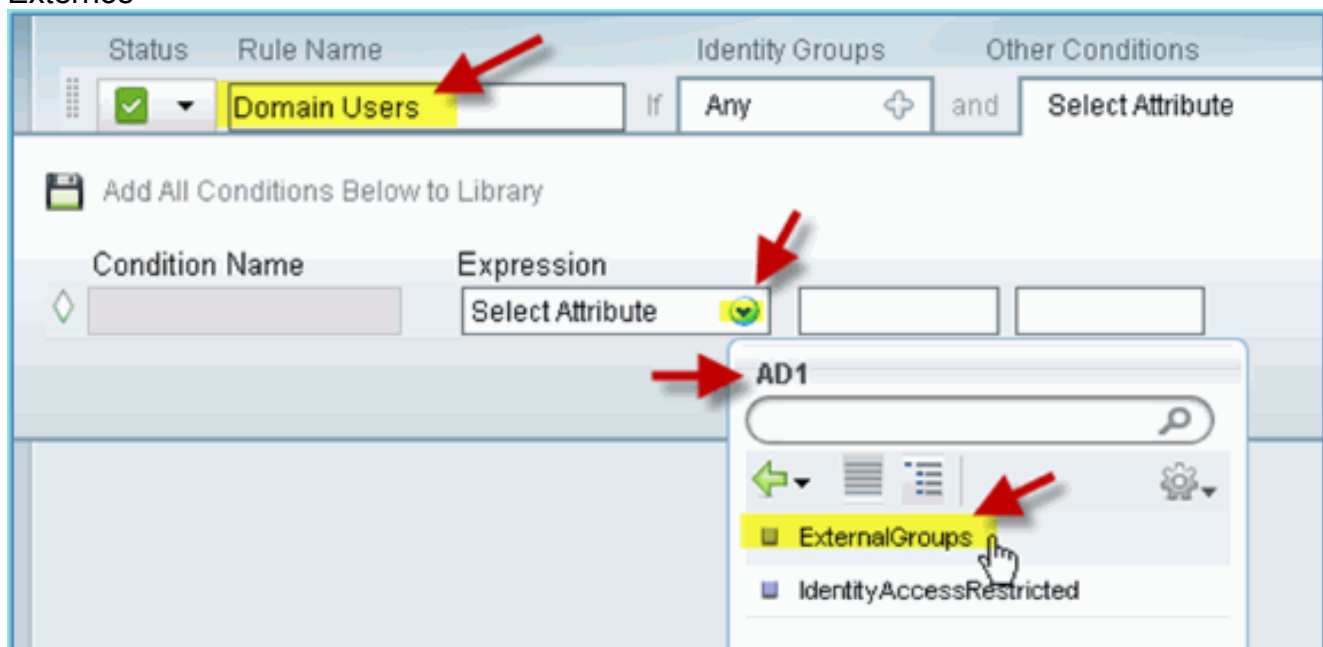
5. Inserir nova política Acima da primeira regra (clique no ícone Ações à direita).



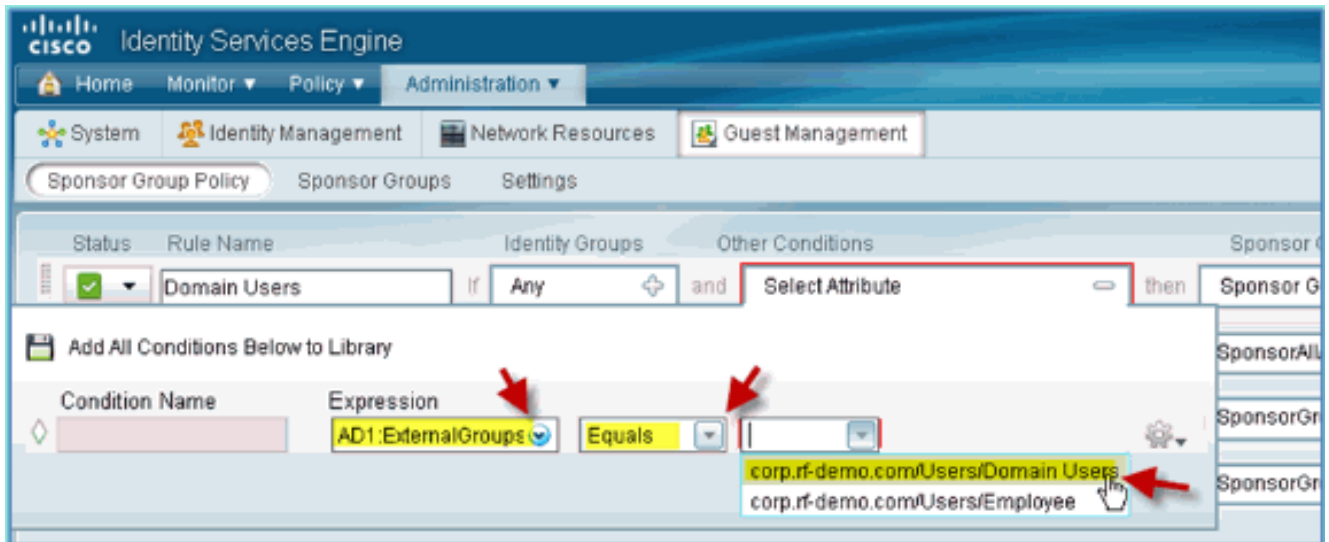
6. Para a nova Política de grupo do patrocinador, crie o seguinte: Nome da regra: Usuários do domínio Grupos de Identidade: Qualquer Outras condições: (Criar novo/avançado) > AD1



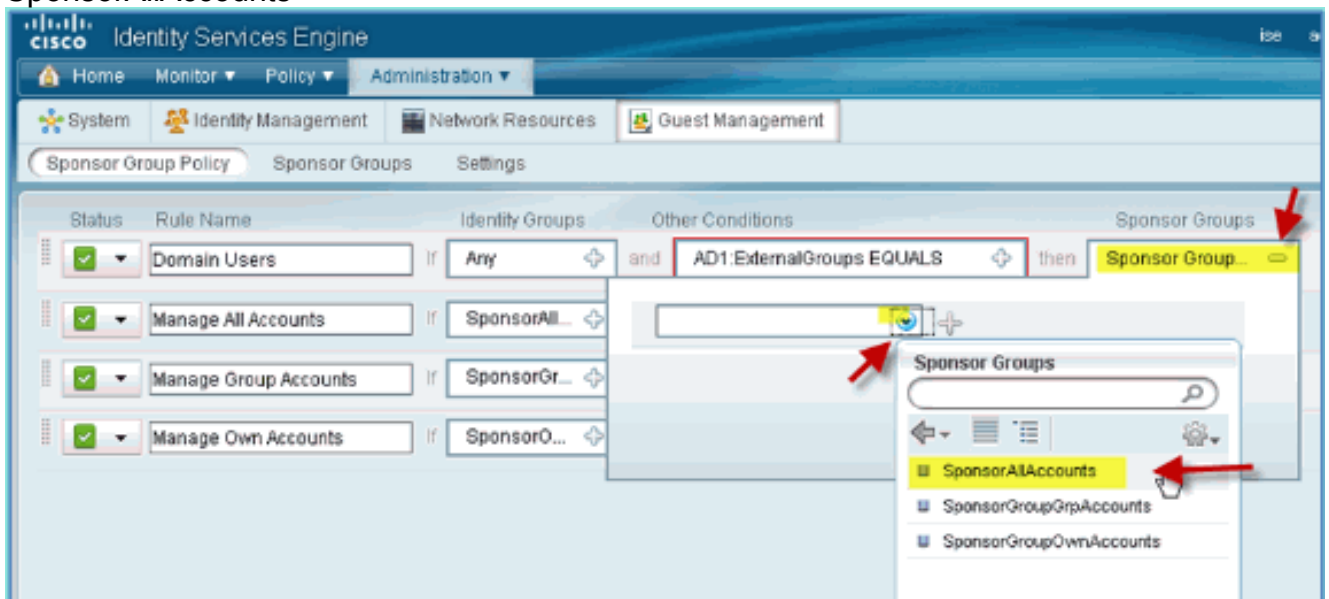
AD1: Grupos
Externos



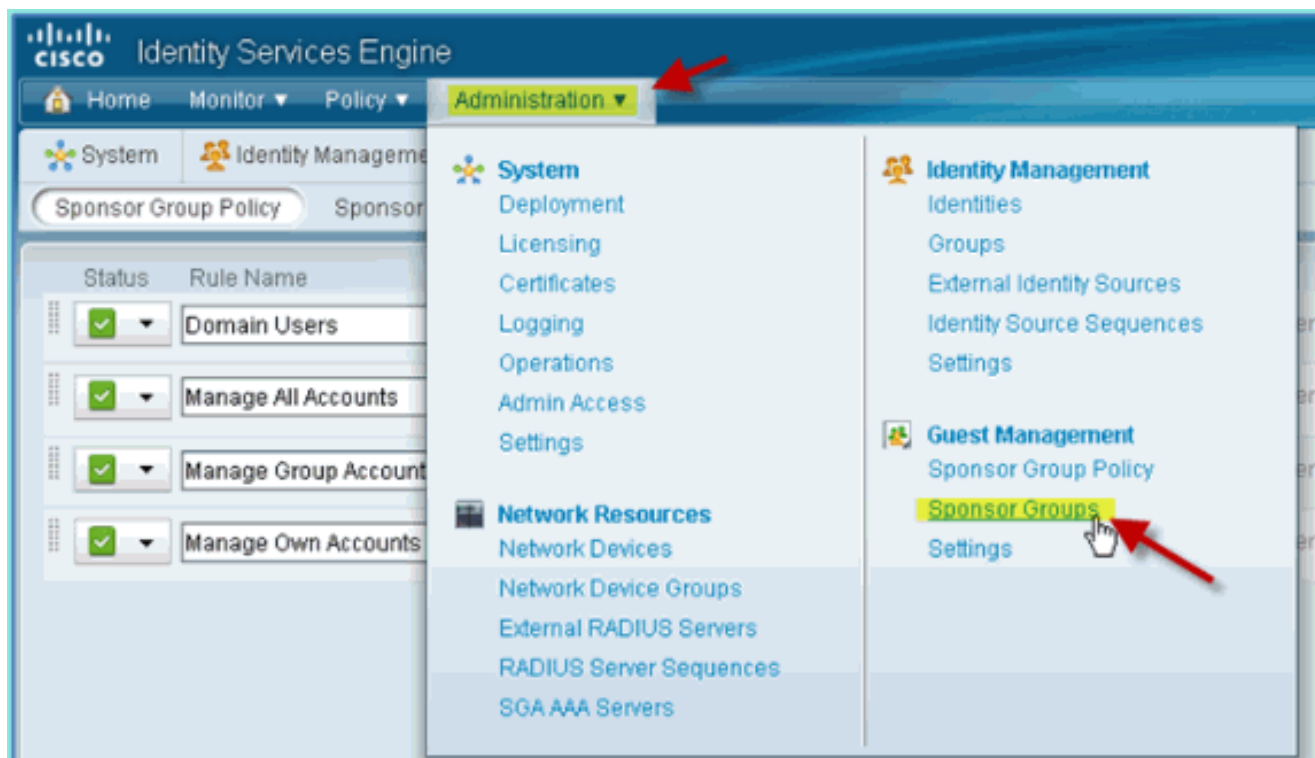
Grupos Externos do AD1 > Iguais > Usuários corp.rf-
demo.com/Users/Domain



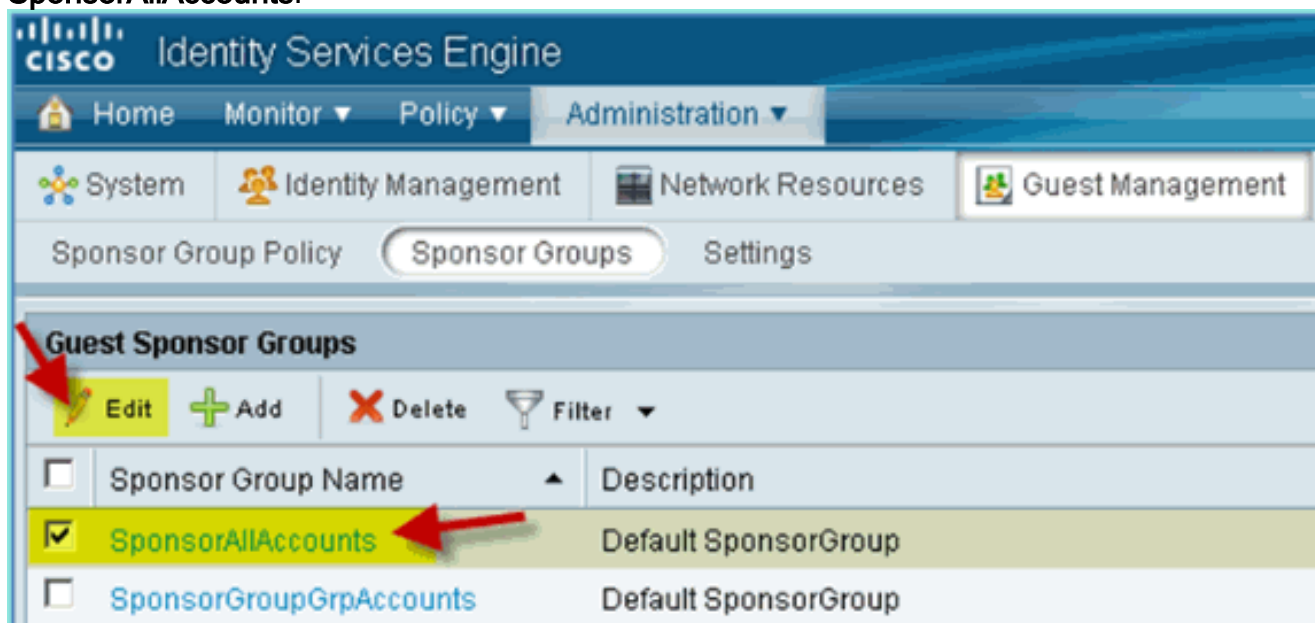
7. Em Grupos de patrocinadores, defina o seguinte: Grupos de patrocinadores: SponsorAllAccounts



8. Navegue até Administração > Gerenciamento de convidados > Grupos de patrocinadores.



9. Selezione Editar >
SponsorAllAccounts.



10. Selezione Níveis de Autorização e defina o seguinte: Exibir Senha do Convidado:
Sim

Identity Services Engine

Home Monitor Policy Administration

System Identity Management Network Resources Guest Management

Sponsor Group Policy Sponsor Groups Settings

Sponsor Group List > SponsorAllAccounts

General Authorization Levels Guest Roles Time Profiles

Allow Login	Yes
Create Accounts	Yes
Create Bulk Accounts	Yes
Create Random Accounts	Yes
Import CSV	Yes
Send Email	Yes
Send SMS	No
View Guest Password	Yes
Allow Printing Guest Details	Yes
View/Edit Accounts	All Accounts
Suspend/Reinstate Accounts	All Accounts
* Account Start Time	1 Days (Valid Range 1 to 999999999)
* Maximum Duration of Account	5 Days (Valid Range 1 to 999999999)

Save Reset

[Configurar o SPAN no Switch](#)

Configurar o SPAN - a interface de gerenciamento/sonda do ISE é L2 adjacente à interface de gerenciamento do WLC. O switch pode ser configurado para SPAN e outras interfaces, como VLANs de funcionários e convidados.

```
Podswitch(config)#monitor session 1 source vlan10 , 11 , 12
Podswitch(config)#monitor session 1 destination interface Fa0/8
ISE virtual probe interface.
```

[Referência: autenticação sem fio para Apple MAC OS X](#)

Associe-se à WLC através de um SSID autenticado como um usuário INTERNO (ou usuário AD

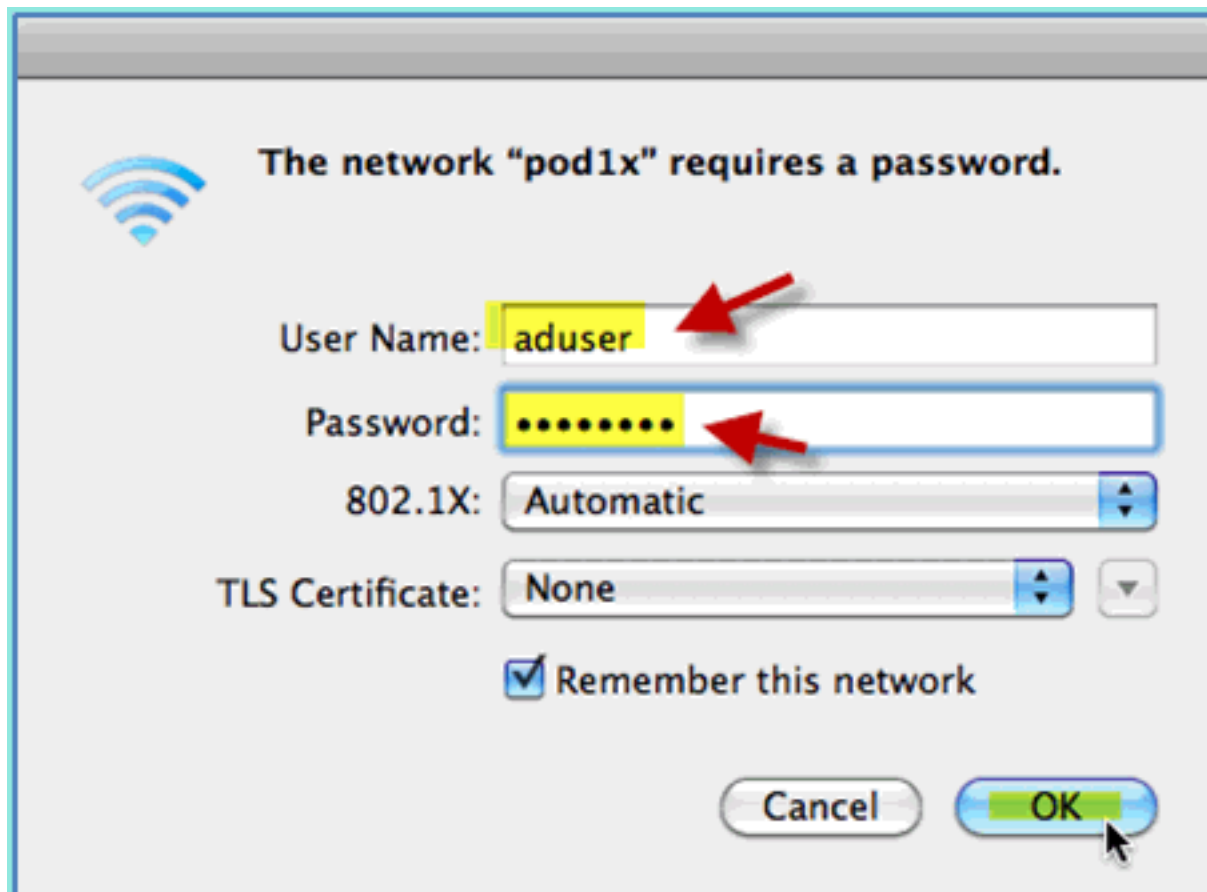
integrado) usando um laptop sem fio Apple Mac OS X. Ignorar se não aplicável.

1. Em um Mac, vá para as configurações de WLAN. Ative o WIFI, selecione e conecte-se ao SSID do POD habilitado para 802.1X criado no exercício



anterior.

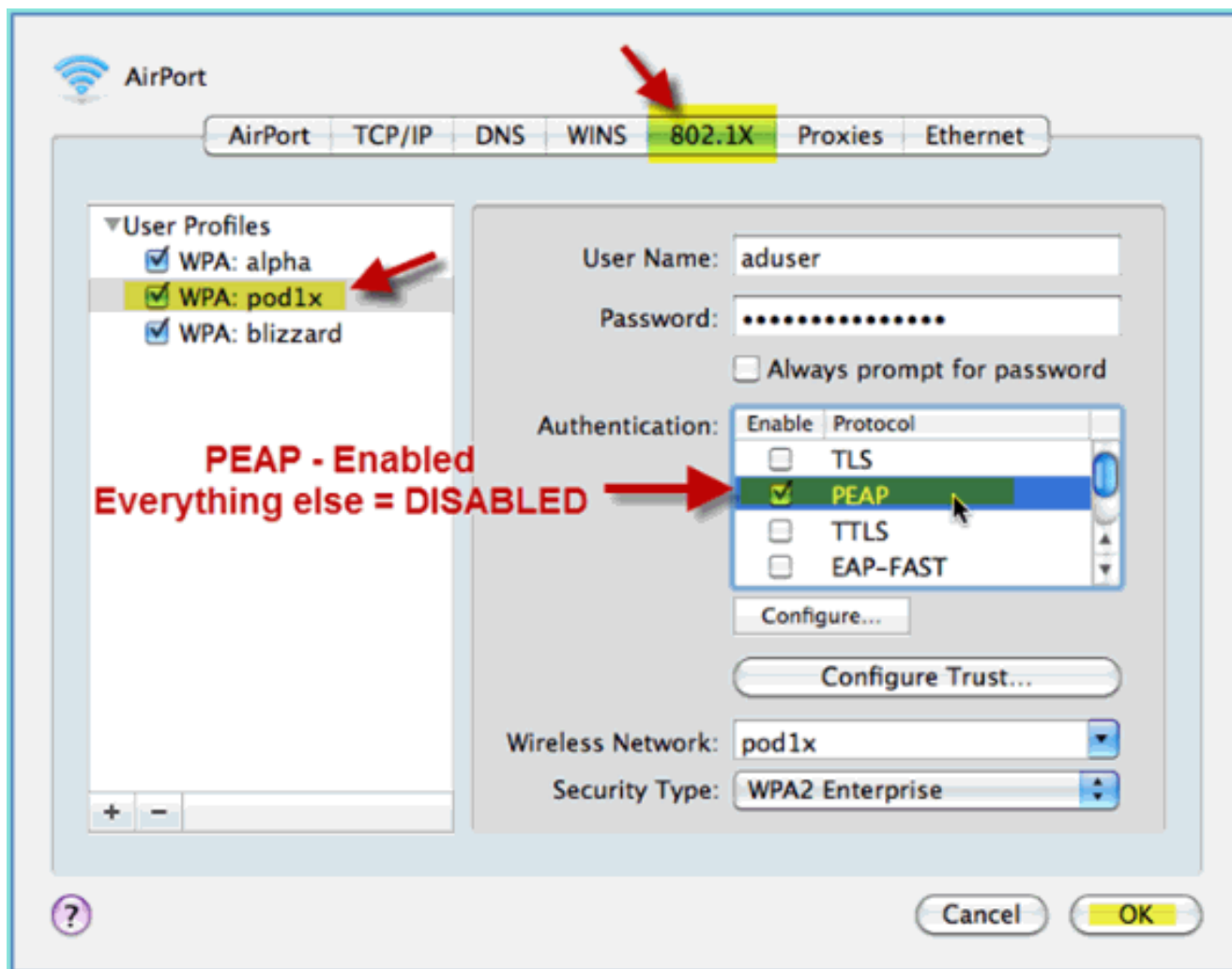
2. Forneça as seguintes informações para conexão: Nome de usuário: aduser (se estiver usando AD), employee (interno - Funcionário), contractor (interno - Contratante) Senha: XXXX802.1X: automático Certificado TLS: Nenhum



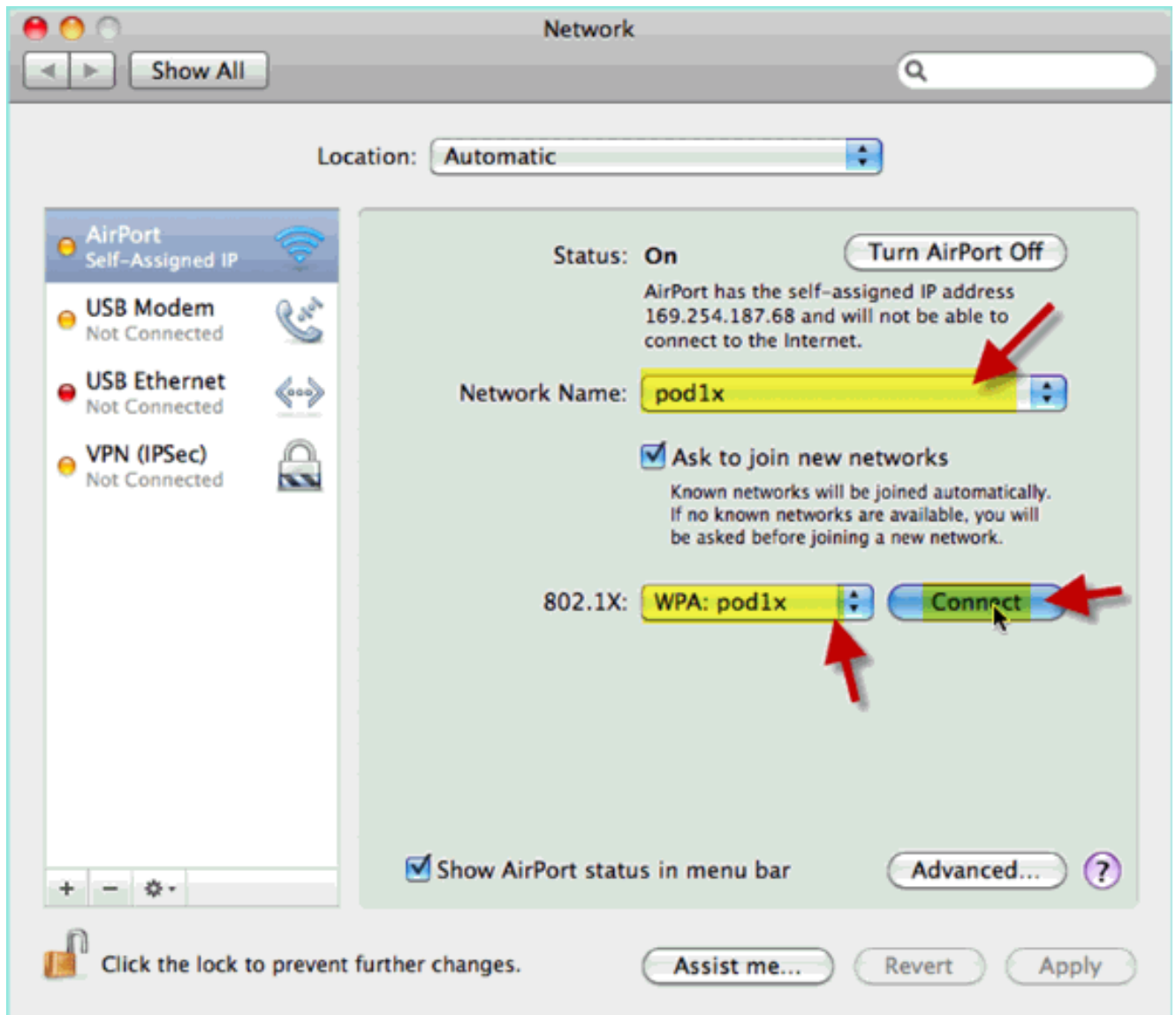
Neste momento, o laptop pode não estar conectado. Além disso, o ISE pode lançar um evento com falha da seguinte maneira:

```
Authentication failed :12514 EAP-TLS failed SSL/TLS handshake because of an unknown CA in the client certificates chain
```

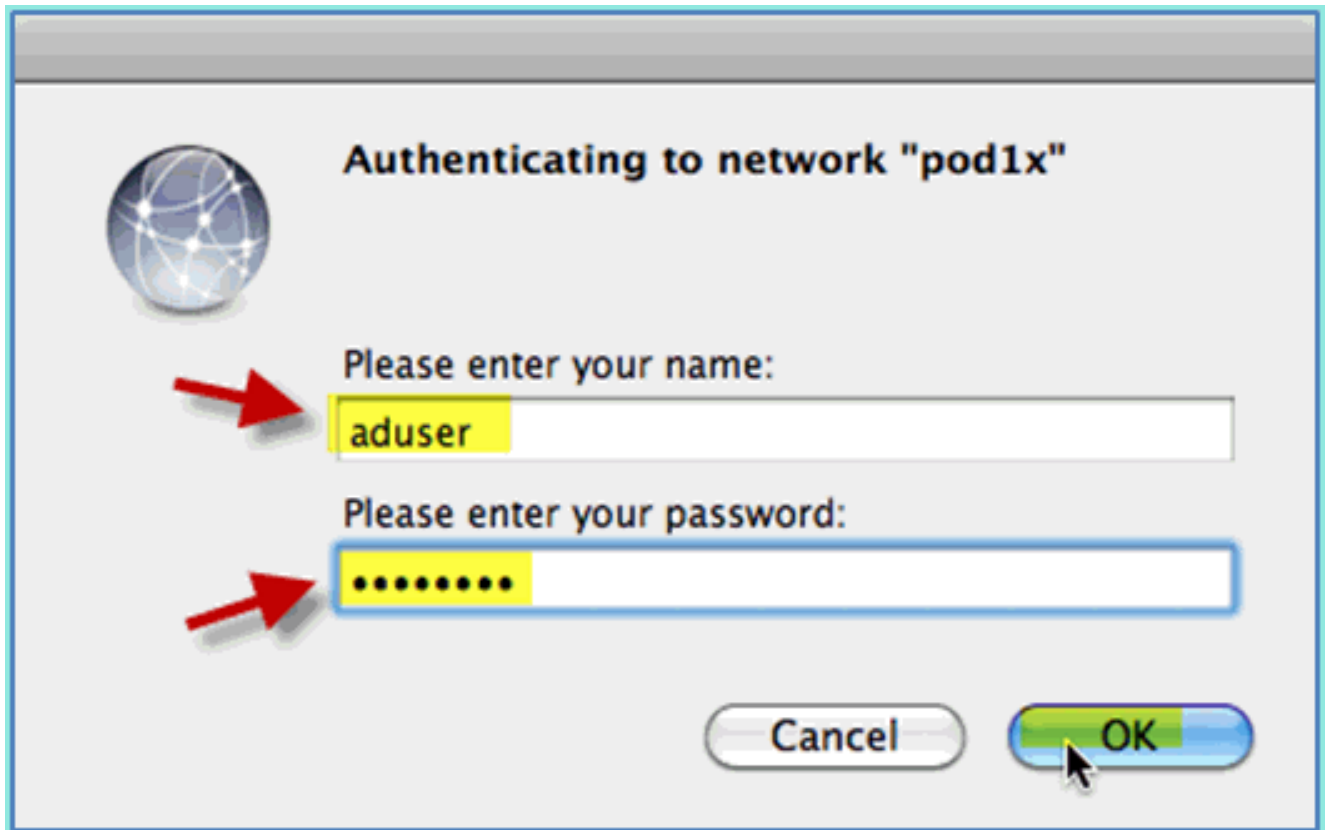
3. Vá para a configuração **Preferência do sistema > Rede > Aeroporto > 802.1X** e defina a nova Autenticação de perfil POD SSID/WPA como: TLS: Desabilitado PEAP: habilitado TTLS: Desabilitado EAP-FAST: desativado



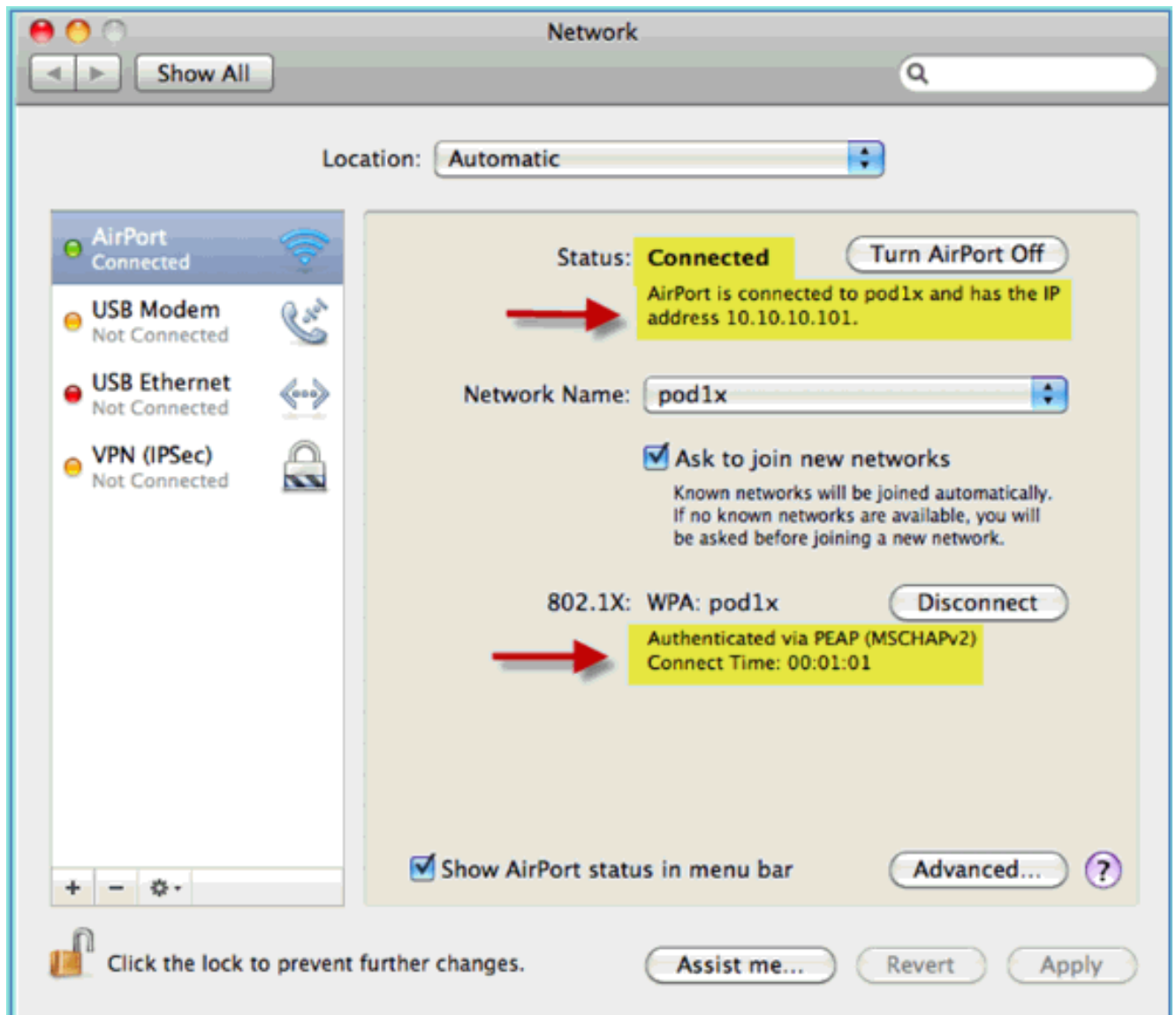
4. Clique em **OK** para continuar e permitir que a configuração seja salva.
5. Na tela Network, selecione o perfil SSID + 802.1X WPA apropriado e clique em **Connect**.



6. O sistema pode solicitar um nome de usuário e uma senha. Insira o usuário e a senha do AD (aduser/XXXX) e clique em OK.



O cliente deve mostrar **Connected** via PEAP com um endereço IP válido.

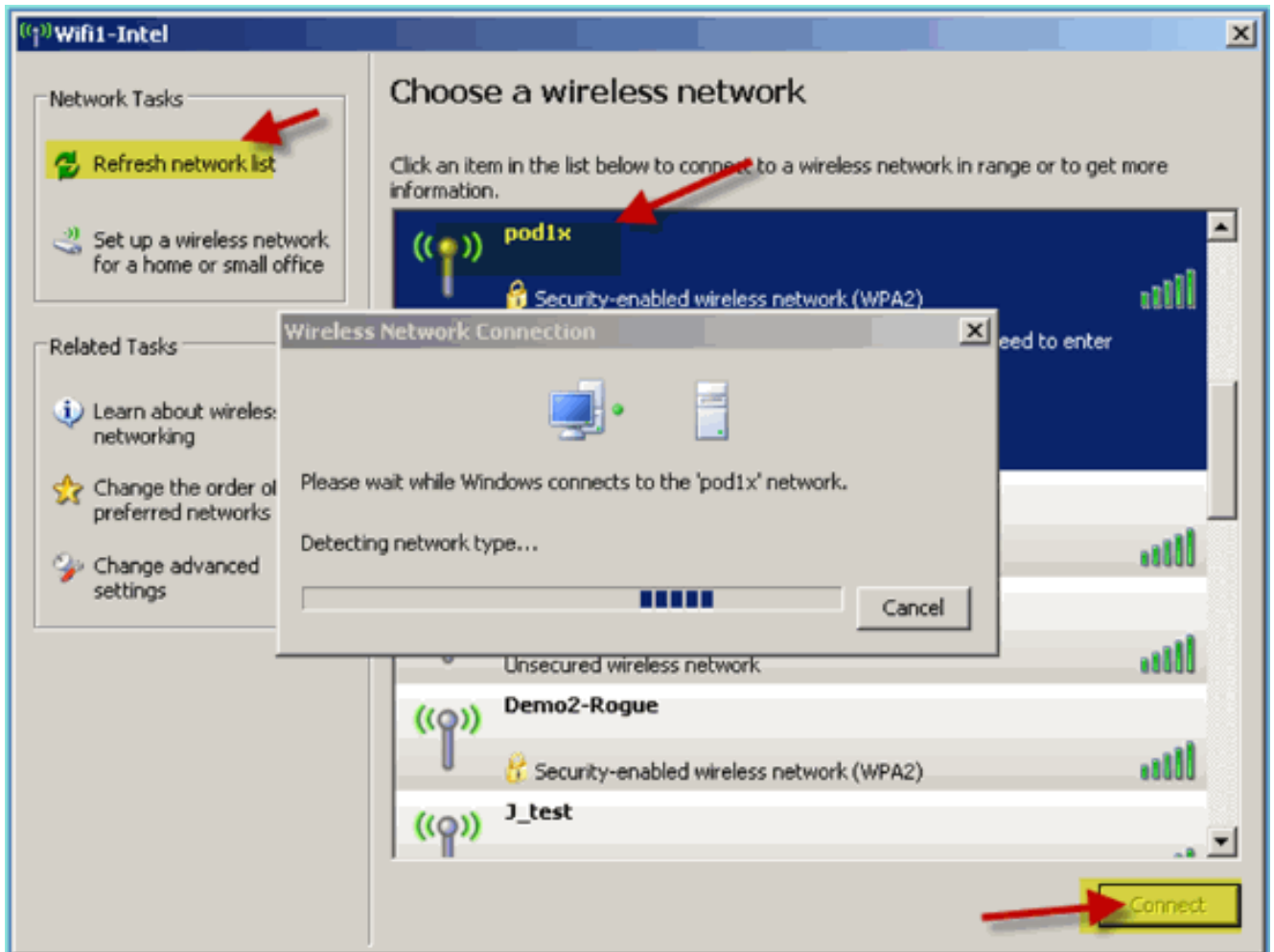


[Referência: Wireless Authentication for Microsoft Windows XP \(Autenticação sem fio do Microsoft Windows XP\)](#)

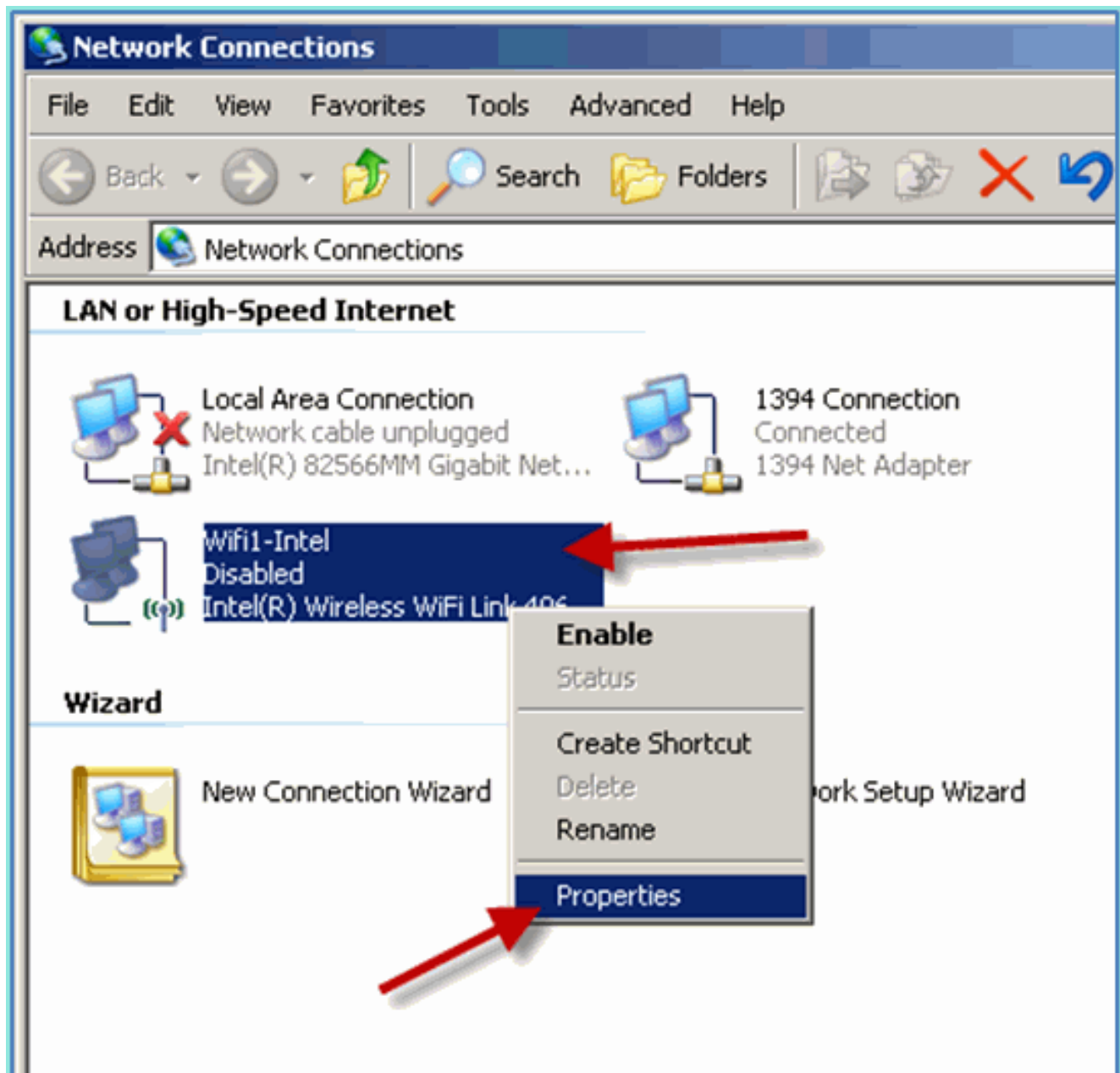
Associe-se à WLC através de um SSID autenticado como um usuário INTERNO (ou integrado, usuário do AD) usando um laptop sem fio com Windows XP. Ignorar se não aplicável.

Conclua estes passos:

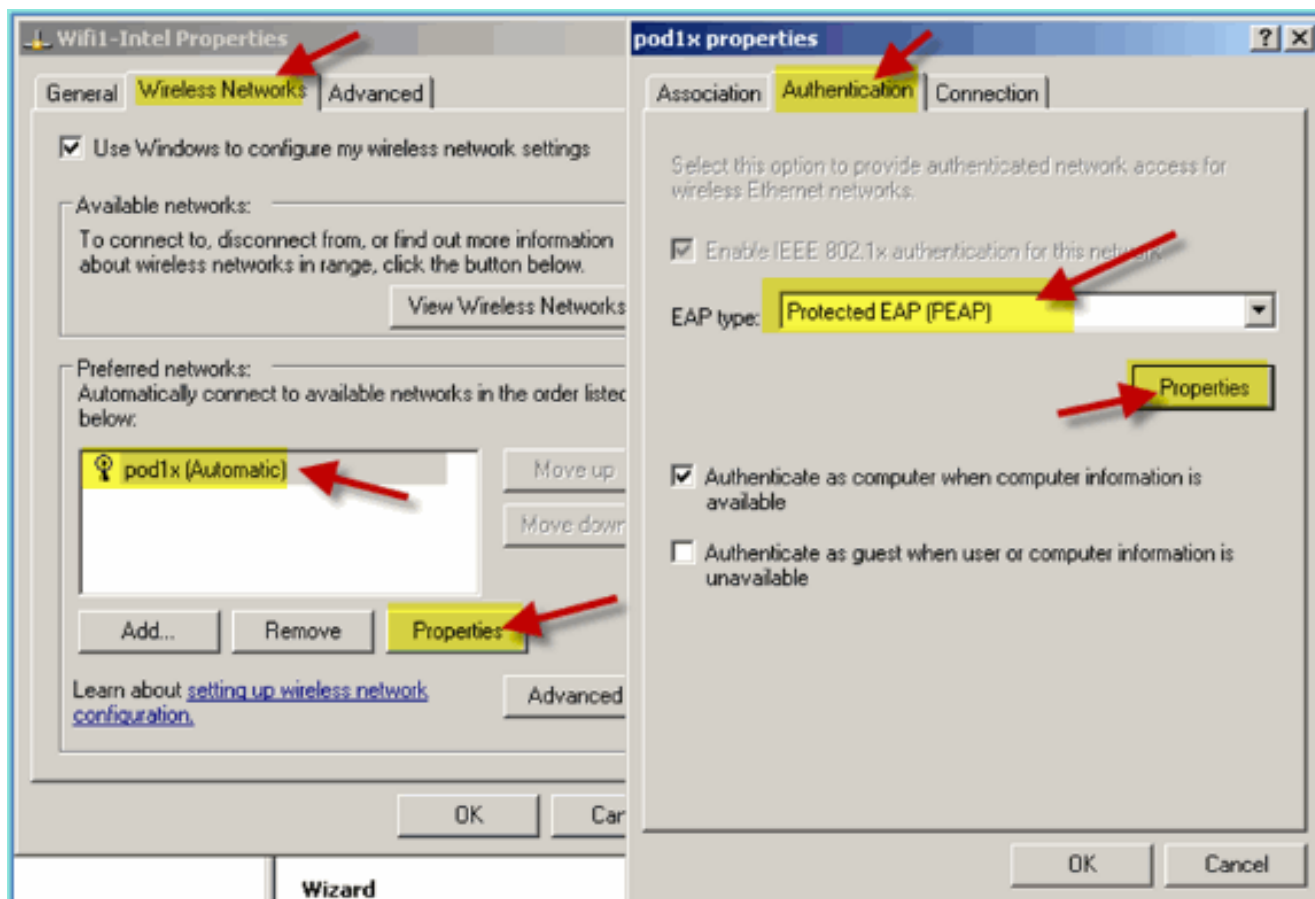
1. No laptop, vá para as configurações de WLAN. Ative o WIFI e conecte-se ao SSID do POD habilitado para 802.1X criado no exercício anterior.



2. Acessar as propriedades da rede para a interface WIFI.

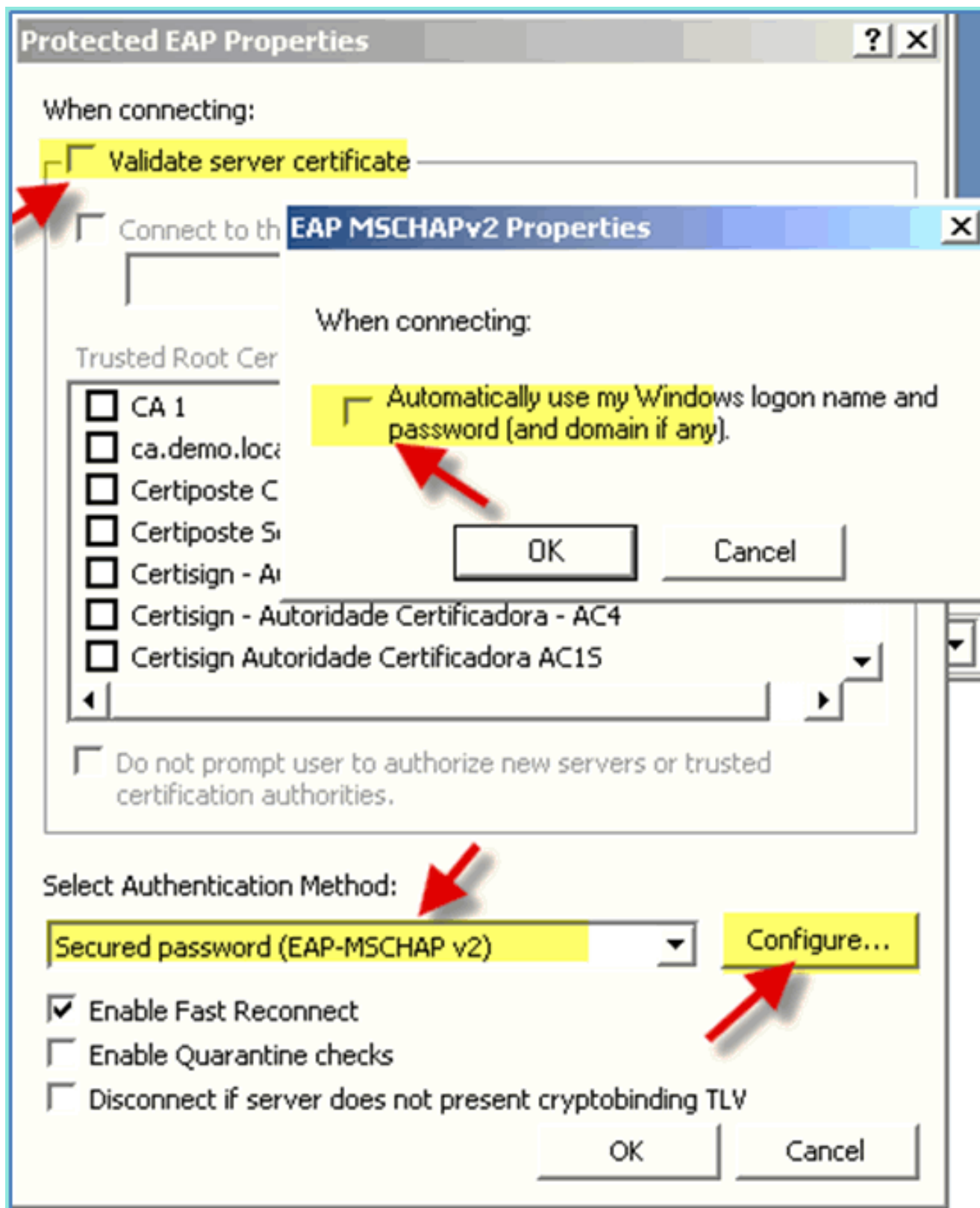


3. Navegue até a guia **Wireless Networks**. Selecione as propriedades da rede SSID do pod > guia Autenticação > Tipo de EAP = EAP Protegido (PEAP).



4. Clique em Propriedades EAP.

5. Defina o seguinte: Validar certificado do servidor: Desabilitado
Método de autenticação: senha segura (EAP-MSCHAP v2)



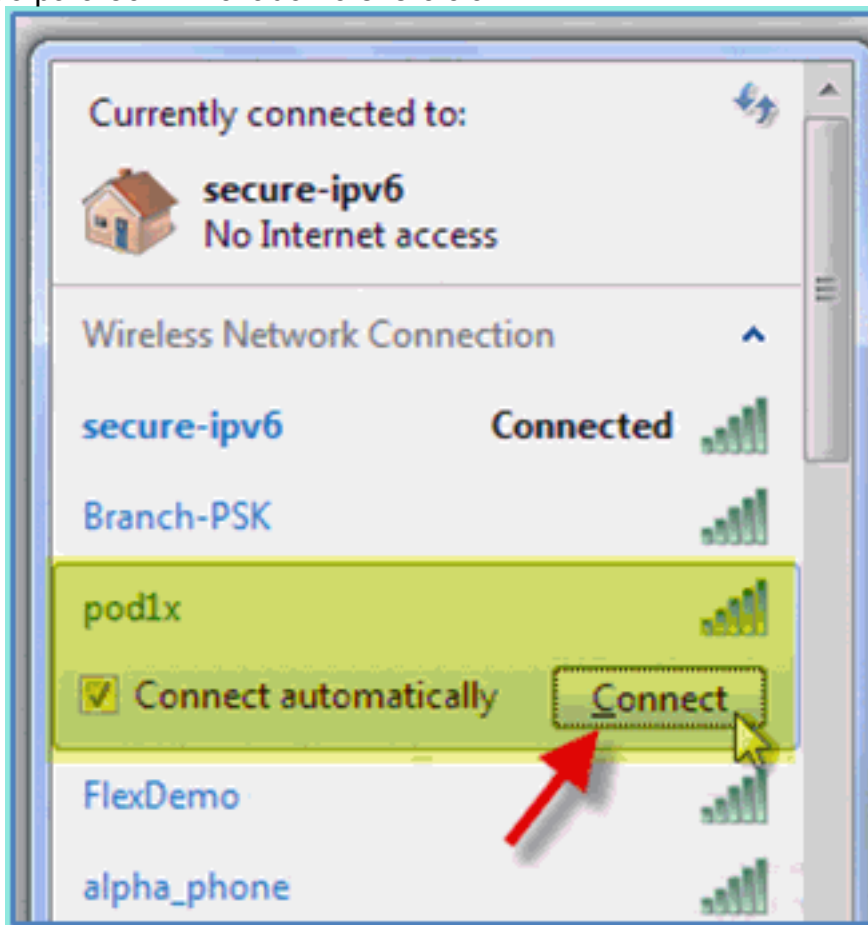
6. Clique em **OK** em todas as janelas para concluir essa tarefa de configuração.
7. O cliente Windows XP solicita o nome de usuário e a senha. Neste exemplo, é aduser/XXXX.
8. Confirme a conectividade de rede, o endereçamento IP (v4).

[Referência: Wireless Authentication for Microsoft Windows 7 \(Autenticação sem fio para Microsoft Windows 7\)](#)

Associe-se à WLC através de um SSID autenticado como um usuário INTERNO (ou usuário AD

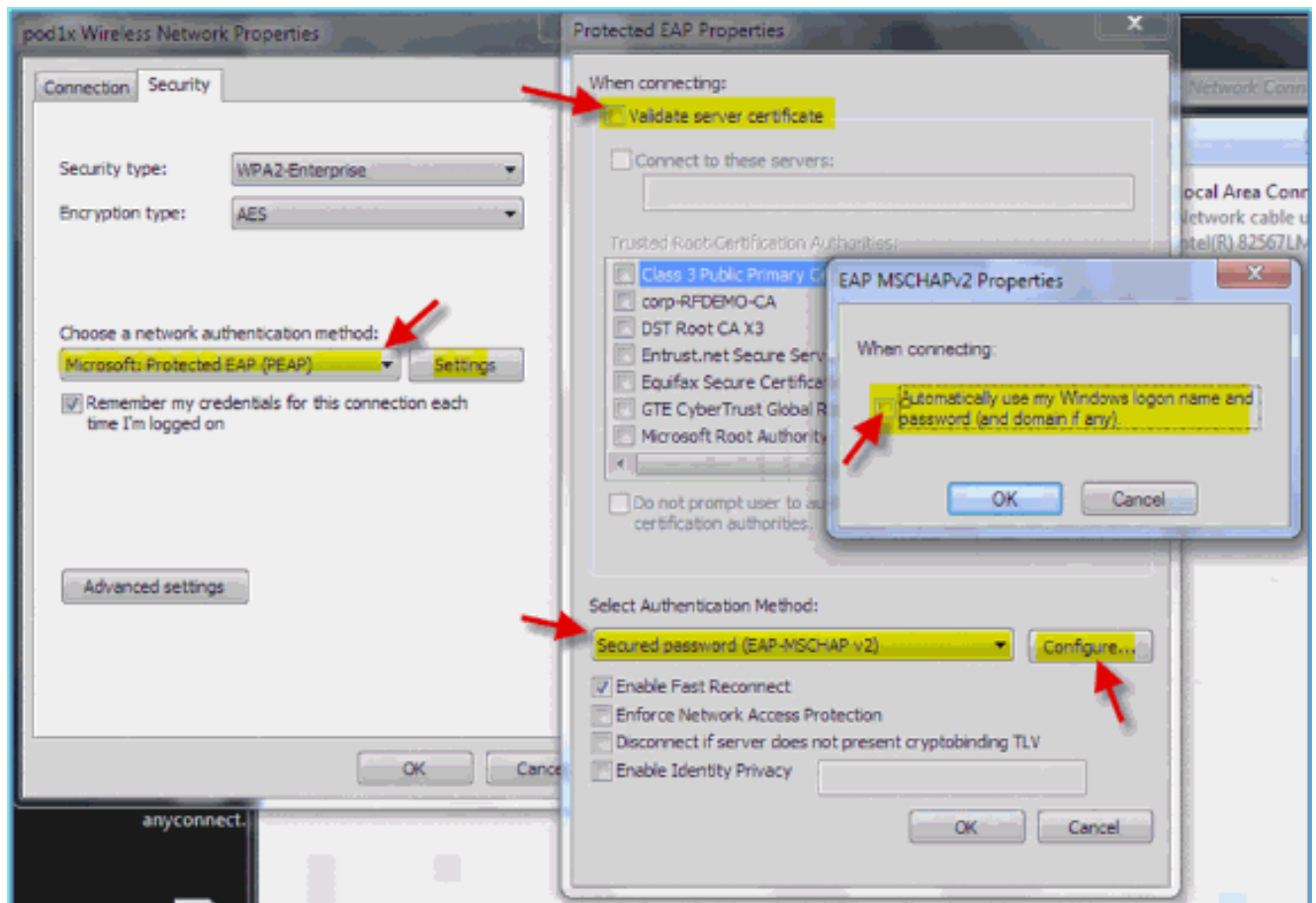
integrado) usando um laptop sem fio com Windows 7.

1. No laptop, vá para as configurações de WLAN. Ative o WIFI e conecte-se ao SSID do POD habilitado para 802.1X criado no exercício



anterior.

2. Acesse o Wireless Manager e edite o novo perfil sem fio do POD.
3. Defina o seguinte: Método de autenticação: PEAP Lembrar minhas credenciais...: Desabilitado Validar certificado do servidor (configuração avançada): Desabilitado Método de autenticação (configuração avançada): EAP-MSCHAP v2 Usar meu logon do Windows automaticamente...: Desabilitado



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.