

Guia de implantação de BYOD sem fio para FlexConnect

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Topologia](#)

[Registro de dispositivos e provisionamento de solicitantes](#)

[Portal de registro de ativos](#)

[Portal de autorregistro](#)

[Autenticação e provisionamento](#)

[Provisionamento para iOS \(iPhone/iPad/iPod\)](#)

[Provisionamento para Android](#)

[Autorregistro de SSID Wireless BYOD duplo](#)

[Registro automático de BYOD sem fio de SSID único](#)

[Configuração de recurso](#)

[Configuração de WLAN](#)

[Configuração do AP FlexConnect](#)

[Configuração do ISE](#)

[Experiência do usuário - Provisionamento do iOS](#)

[SSID duplo](#)

[SSID único](#)

[Experiência do usuário - Provisionamento do Android](#)

[SSID duplo](#)

[Portal Meus dispositivos](#)

[Referência - Certificados](#)

[Informações Relacionadas](#)

Introduction

Os dispositivos móveis estão se tornando mais poderosos computacionalmente e populares entre os consumidores. Milhões desses dispositivos são vendidos para consumidores com Wi-Fi de alta velocidade para que os usuários possam se comunicar e colaborar. Os clientes estão acostumados com o aumento de produtividade que esses dispositivos móveis trazem para suas vidas e buscam trazer sua experiência pessoal para o espaço de trabalho. Isso cria as necessidades de funcionalidade de uma solução de consumerização de TI (BYOD) no local de trabalho.

Este documento fornece a implantação da filial para a solução BYOD. Um funcionário se conecta a um identificador de conjunto de serviços (SSID) corporativo com seu novo iPad e é redirecionado para um portal de autorregistro. O Cisco Identity Services Engine (ISE) autentica o usuário no Active Directory (AD) corporativo e faz o download de um certificado com um endereço MAC do iPad incorporado e nome de usuário para o iPad, juntamente com um perfil suplicante que impõe o uso do Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) como um método para conectividade dot1x. Com base na política de autorização no ISE, o usuário pode se conectar com o uso do dot1x e obter acesso aos recursos apropriados.

As funcionalidades do ISE nas versões do software Cisco Wireless LAN Controller anteriores à 7.2.110.0 não suportavam clientes de switching locais que se associam através de pontos de acesso (APs) FlexConnect. A versão 7.2.110.0 oferece suporte a essas funcionalidades do ISE para APs FlexConnect para switching local e clientes autenticados centralmente. Além disso, a versão 7.2.110.0 integrada ao ISE 1.1.1 fornece (mas não se limita a) esses recursos da solução BYOD para redes sem fio:

- Criação de perfis e postura de dispositivos
- Registro de dispositivos e provisionamento de solicitantes
- Integração de dispositivos pessoais (provisionar dispositivos iOS ou Android)

Observação: embora sejam compatíveis, outros dispositivos, como laptops e estações de trabalho sem fio PC ou Mac, não estão incluídos neste guia.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Switches Cisco Catalyst
- Controladores Cisco Wireless LAN (WLAN)
- Software Cisco WLAN Controller (WLC) versão 7.2.110.0 e posterior
- APs 802.11n no modo FlexConnect
- Software Cisco ISE versão 1.1.1 e posterior
- Windows 2008 AD com CA (Autoridade de Certificação)
- Servidor DHCP
- Servidor DNS (Domain Name System)
- Network Time Protocol (NTP)
- Laptop sem fio, smartphone e tablet do cliente (Apple iOS, Android, Windows e Mac)

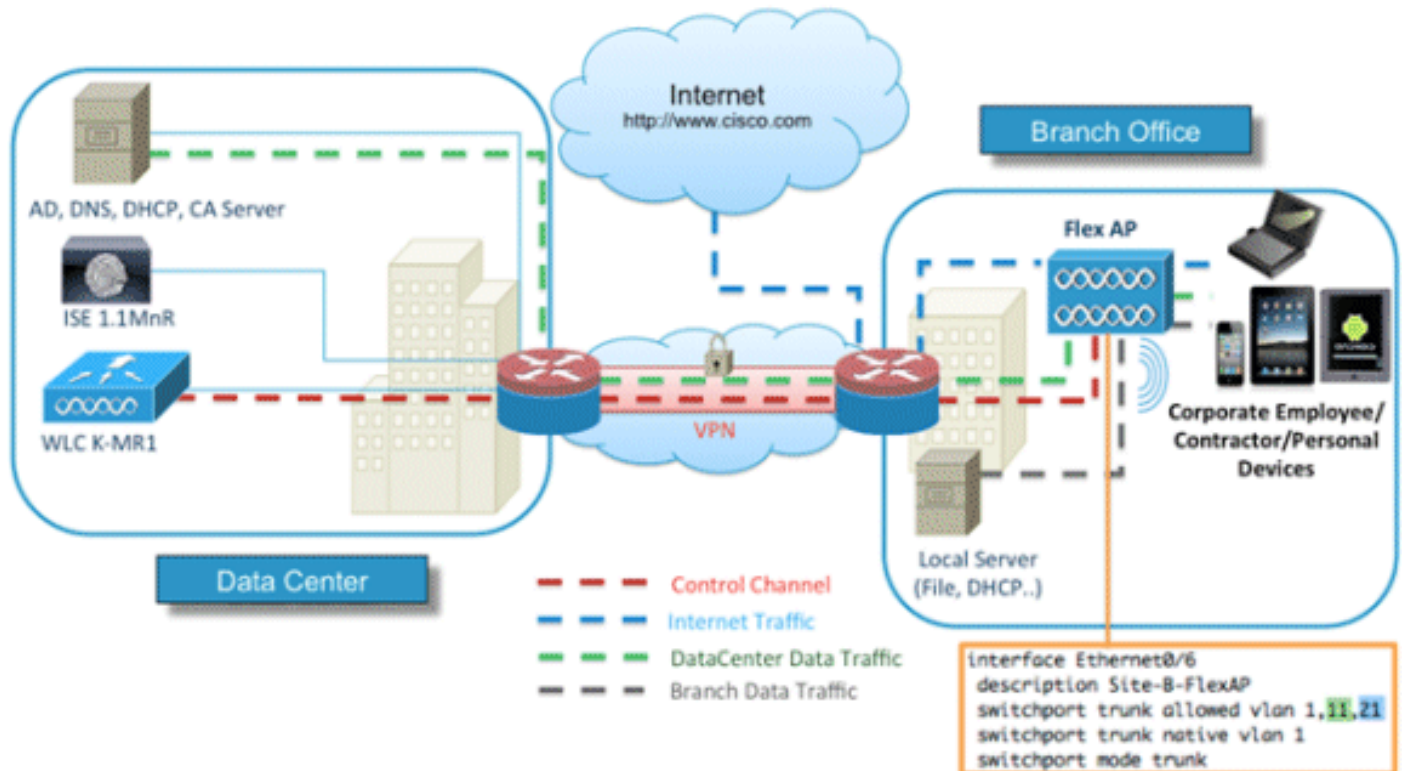
Observação: consulte [Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 7.2.110.0](#) para obter informações importantes sobre esta versão de software. Faça login no site Cisco.com para obter as notas de versão mais recentes

antes de carregar e testar o software.

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

Topologia

Uma configuração de rede mínima, como mostrado neste diagrama, é necessária para implementar e testar corretamente estes recursos:



Para esta simulação, você precisa de uma rede com um AP FlexConnect, um site local/remoto com DHCP local, DNS, WLC e ISE. O AP FlexConnect é conectado a um tronco para testar a comutação local com várias VLANs.

Registro de dispositivos e provisionamento de solicitantes

Um dispositivo deve ser registrado para que seu solicitante nativo possa provisionar a autenticação dot1x. Com base na política de autenticação correta, o usuário é redirecionado para a página de convidado e autenticado pelas credenciais do funcionário. O usuário vê a página de registro do dispositivo, que solicita as informações do dispositivo. O processo de provisionamento do dispositivo é iniciado. Se o sistema operacional (SO) não tiver suporte para provisionamento, o usuário será redirecionado para o Asset Registration Portal para marcar esse dispositivo para acesso MAC Authentication Bypass (MAB). Se o SO for suportado, o processo de registro é iniciado e configura o solicitante nativo do dispositivo para autenticação dot1x.

Portal de registro de ativos

O Portal de registro de ativos é o elemento da plataforma ISE que permite que os funcionários iniciem a integração de endpoints por meio de um processo de autenticação e registro.

Os administradores podem excluir ativos da página de identidades de endpoints. Cada funcionário pode editar, deletar e colocar na lista negra os ativos que registrou. Os pontos finais da lista negra são atribuídos a um grupo de identidade da lista negra e uma política de autorização é criada para impedir o acesso à rede por pontos finais da lista negra.

Portal de autorregistro

No fluxo de Autenticação da Web Central (CWA), os funcionários são redirecionados para um portal que permite que eles insiram suas credenciais, autentiquem e insiram as especificações do ativo específico que desejam registrar. Esse portal é chamado de Portal de autoprovisionamento e é semelhante ao Portal de registro de dispositivos. Ele permite que os funcionários insiram o endereço MAC, bem como uma descrição significativa do endpoint.

Autenticação e provisionamento

Depois que os funcionários selecionam o portal de autorregistro, eles são solicitados a fornecer um conjunto de credenciais válidas de funcionário para prosseguir para a fase de provisionamento. Após a autenticação bem-sucedida, o ponto final pode ser provisionado no banco de dados de pontos finais e um certificado é gerado para o ponto final. Um link na página permite que o funcionário faça o download do Assistente do Piloto Requerente (SPW).

Observação: consulte o artigo [FlexConnect Feature Matrix](#) da Cisco para visualizar a matriz de recursos mais recente do FlexConnect para BYOD.

Provisionamento para iOS (iPhone/iPad/iPod)

Para a configuração EAP-TLS, o ISE segue o processo de inscrição do Apple Over-the-Air (OTA):

- Após a autenticação bem-sucedida, o mecanismo de avaliação avalia as políticas de provisionamento do cliente, o que resulta em um perfil do solicitante.
- Se o perfil do solicitante for para a configuração EAP-TLS, o processo OTA determinará se o ISE está usando autoassinado ou assinado por uma CA desconhecida. Se uma das condições for verdadeira, o usuário será solicitado a baixar o certificado do ISE ou da CA antes do início do processo de registro.
- Para outros métodos EAP, o ISE envia o perfil final após a autenticação bem-sucedida.

Provisionamento para Android

Devido a considerações de segurança, o agente Android deve ser baixado do site do Android Marketplace e não pode ser provisionado do ISE. A Cisco faz o upload de uma versão candidata a lançamento do assistente no Android Marketplace por meio da conta do editor do Cisco Android Marketplace.

Este é o processo de provisionamento do Android:

1. A Cisco usa o Software Development Kit (SDK) para criar o pacote Android com a extensão .apk.
2. A Cisco carrega um pacote no mercado Android.
3. O usuário configura a política no provisionamento do cliente com os parâmetros apropriados.
4. Após o registro do dispositivo, o usuário final é redirecionado para o serviço de provisionamento do cliente quando a autenticação dot1x falha.
5. A página do portal de provisionamento fornece um botão que redireciona o usuário para o portal do marketplace Android, onde ele pode baixar o SPW.
6. O Cisco SPW é iniciado e executa o provisionamento do solicitante: O SPW descobre o ISE e faz download do perfil do ISE. O SPW cria um par de certificado/chave para EAP-TLS. O SPW faz uma chamada de solicitação de proxy SCEP (Simple Certificate Enrollment Protocol) para o ISE e obtém o certificado. O SPW aplica os perfis wireless. O SPW acionará uma nova autenticação se os perfis forem aplicados com êxito. O SPW é encerrado.

Autorregistro de SSID Wireless BYOD duplo

Este é o processo para o autorregistro duplo de SSID sem fio BYOD:

1. O usuário se associa ao SSID convidado.
2. O usuário abre um navegador e é redirecionado para o ISE CWA Guest Portal.
3. O usuário insere um nome de usuário e uma senha de funcionário no Portal do convidado.
4. O ISE autentica o usuário e, com base no fato de que ele é um funcionário e não um convidado, redireciona o usuário para a página de convidado do Registro de dispositivo do funcionário.
5. O endereço MAC é preenchido previamente na página de convidado Device Registration da DeviceID. O usuário insere uma descrição e aceita a Política de Uso Aceitável (AUP), se necessário.
6. O usuário seleciona **Aceitar** e começa a baixar e instalar o SPW.
7. O suplicante para o dispositivo desse usuário é fornecido junto com todos os certificados.
8. CoA ocorre, e o dispositivo se reassocia ao SSID corporativo (CORP) e se autentica com EAP-TLS (ou outro método de autorização em uso para aquele suplicante).

Registro automático de BYOD sem fio de SSID único

Neste cenário, há um único SSID para acesso corporativo (CORP) que oferece suporte a PEAP (Protected Extensible Authentication Protocol) e EAP-TLS. Não há SSID de convidado.

Este é o processo para o autorregistro SSID sem fio BYOD:

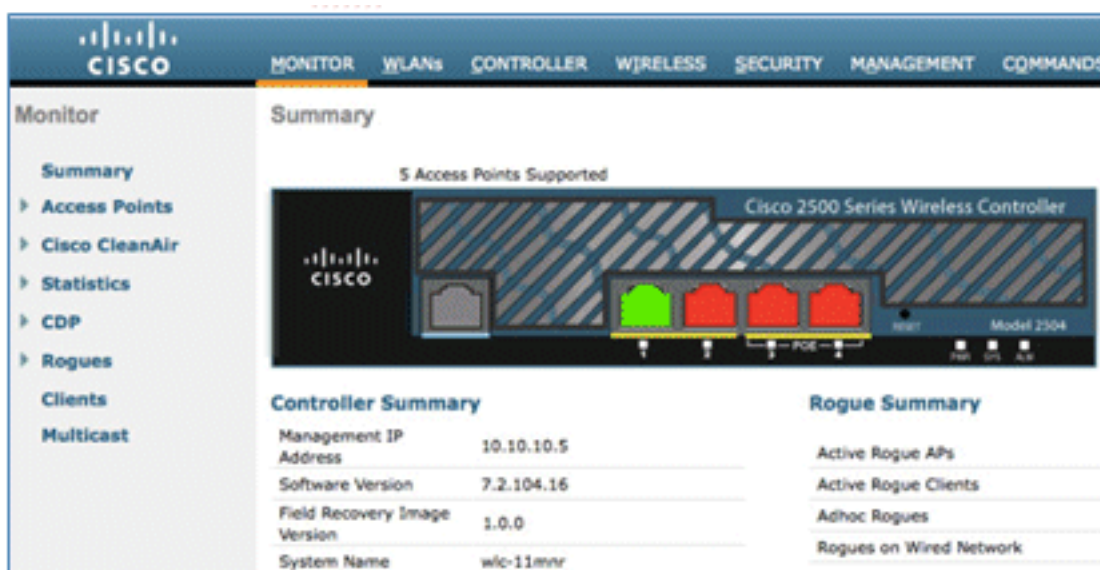
1. O usuário se associa à CORP.
2. O usuário insere um nome de usuário e uma senha de funcionário no solicitante para a autenticação PEAP.
3. O ISE autentica o usuário e, com base no método PEAP, fornece uma política de autorização de aceitação com redirecionamento para a página de convidado do Registro de dispositivos de funcionários.

4. O usuário abre um navegador e é redirecionado para a página de convidado do Registro de Dispositivo de Funcionário.
5. O endereço MAC é preenchido previamente na página de convidado Device Registration da DeviceID. O usuário insere uma descrição e aceita a AUP.
6. O usuário seleciona **Aceitar** e começa a baixar e instalar o SPW.
7. O suplicante para o dispositivo desse usuário é fornecido junto com todos os certificados.
8. CoA ocorre, e o dispositivo se reassocia ao SSID CORP e se autentica com EAP-TLS.

Configuração de recurso

Conclua estas etapas para iniciar a configuração:

1. Para este guia, certifique-se de que a versão da WLC seja 7.2.110.0 ou posterior.



2. Navegue para **Security > RADIUS > Authentication** e adicione o servidor RADIUS ao WLC.



3. Adicione o ISE 1.1.1 ao WLC:

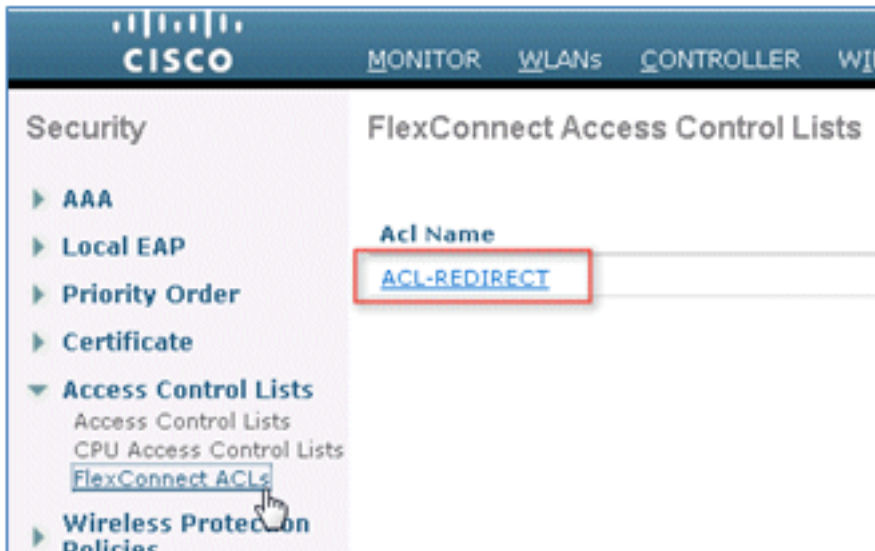
Insira um segredo compartilhado. Defina Suporte para RFC 3576 como **Habilitado**.

MONITOR		WLANs		CONTROLLER		WIRELESS		SECURITY		MANAGEMENT		COMMANDS		HELP		FEEDBACK	
RADIUS Authentication Servers > Edit																	
Server Index	1																
Server Address	10.10.10.60																
Shared Secret Format	ASCII																
Shared Secret	***																
Confirm Shared Secret	***																
Key Wrap	<input type="checkbox"/> (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	<input checked="" type="checkbox"/> Enable																
Management	<input checked="" type="checkbox"/> Enable																
IPSec	<input type="checkbox"/> Enable																

4. Adicione o mesmo servidor ISE como um servidor de contabilização RADIUS.

MONITOR		WLANs		CONTROLLER		WIRELESS		SECURITY		MANAGEMENT		COMMANDS		HELP		FEEDBACK	
RADIUS Accounting Servers > Edit																	
Server Index	1																
Server Address	10.10.10.60																
Shared Secret Format	ASCII																
Shared Secret	***																
Confirm Shared Secret	***																
Port Number	1813																
Server Status	Enabled																
Server Timeout	2 seconds																
Network User	<input checked="" type="checkbox"/> Enable																
IPSec	<input type="checkbox"/> Enable																

5. Crie uma ACL de pré-autenticação de WLC para usar na política do ISE posteriormente. Navegue até WLC > **Security** > Access Control Lists > FlexConnect ACLs e crie uma nova ACL FlexConnect chamada ACL-REDIRECT (neste exemplo).



6. Nas regras da ACL, permita todo o tráfego de/para o ISE e permita o tráfego do cliente durante o provisionamento do requerente.

Para a primeira regra (sequência 1):

Defina Source como **Any**. Defina o IP (endereço ISE)/máscara de rede **255.255.255.255**. Defina a ação como **Permit**.

Access Control Lists > Rules > Edit

Sequence:

Source:

Destination: IP Address: Netmask:

Protocol:

DSCP:

Direction:

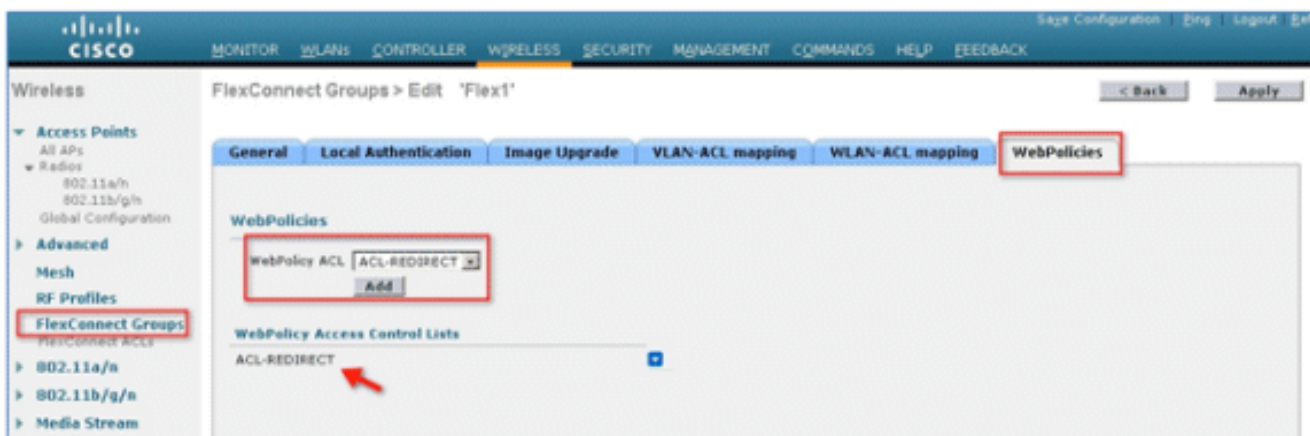
Action:

Para a segunda regra (sequência 2), defina o IP de origem (endereço ISE)/máscara 255.255.255.255 como **Any** e Action para **Permit**.

General								
Access List Name		ACL-REDIRECT						
Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	
1	Permit	0.0.0.0 0.0.0.0	/ 10.10.10.60 255.255.255.255	/ Any	Any	Any	Any	<input checked="" type="checkbox"/>
2	Permit	10.10.10.60 255.255.255.255	/ 0.0.0.0 0.0.0.0	/ Any	Any	Any	Any	<input checked="" type="checkbox"/>

7. Crie um novo Grupo FlexConnect chamado Flex1 (neste exemplo):

Navegue até a guia **FlexConnect Group > WebPolicies**. No campo WebPolicy ACL, clique em **Add** e selecione **ACL-REDIRECT** ou a ACL FlexConnect criada anteriormente. Confirme se ele preenche o campo **WebPolicy Access Control Lists**.



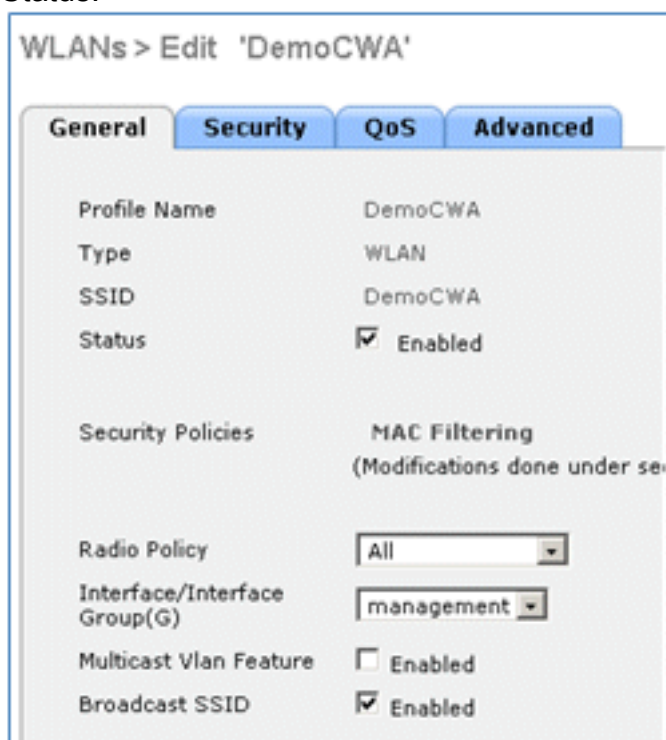
8. Clique em **Aplicar** e **Salvar** configuração.

Configuração de WLAN

Conclua estes passos para configurar a WLAN:

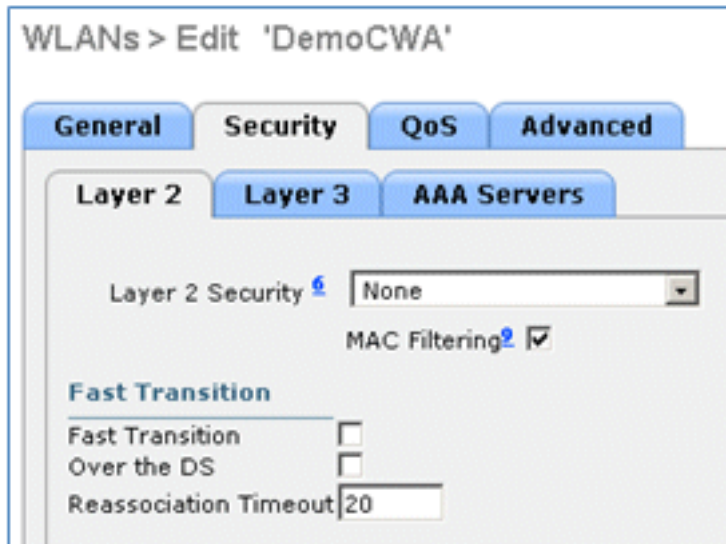
1. Crie um SSID de WLAN aberta para o exemplo de SSID duplo:

Insira um nome de WLAN: **DemoCWA** (neste exemplo). Selecione a opção **Enabled** para Status.



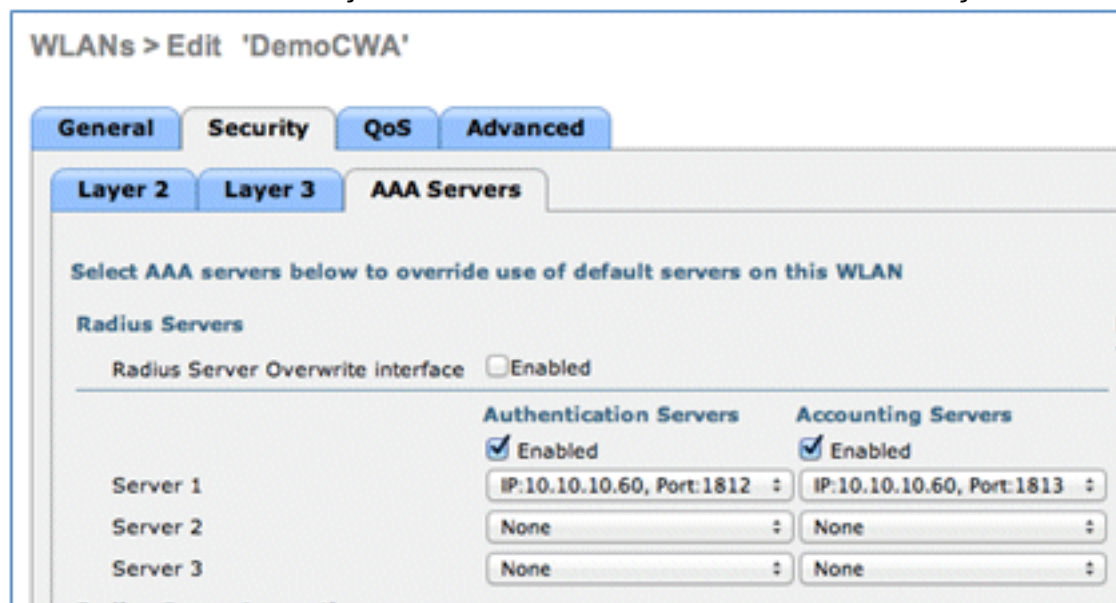
2. Navegue até a guia **Security > Layer 2** e defina estes atributos:

Segurança da camada 2: **nenhuma**MAC Filtering (Filtragem de endereços MAC): **Enabled (Habilitado)** (caixa marcada)Transição Rápida: **Desabilitada** (caixa não marcada)

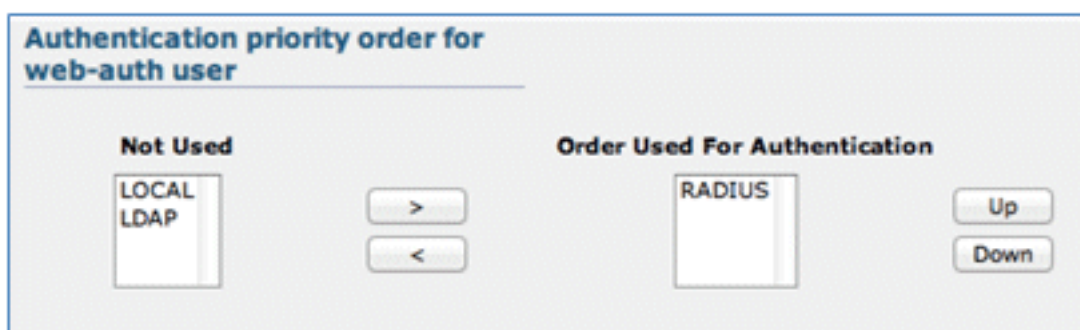


3. Vá até a guia **AAA Servers** e defina estes atributos:

Servidores de Autenticação e Conta: **Habilitado**Servidor 1: <endereço IP do ISE>

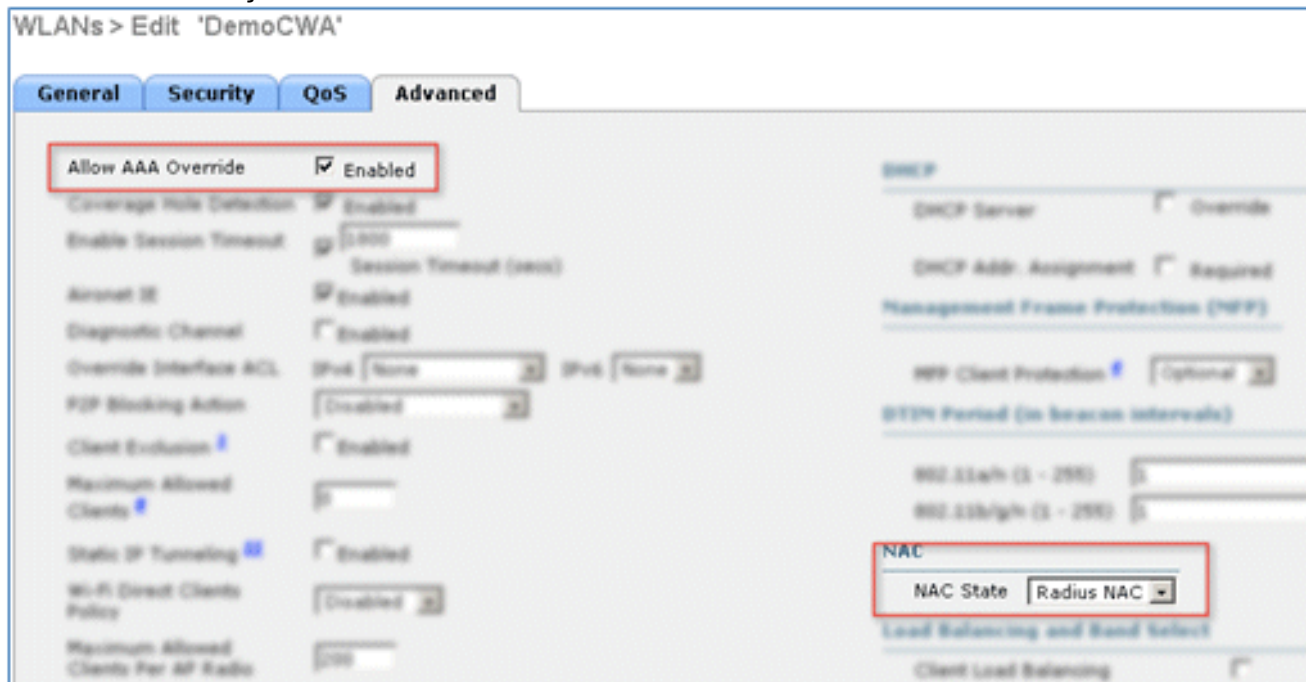


4. Role para baixo a partir da guia **AAA Servers**. Em Authentication priority order for web-auth user, certifique-se de que **RADIUS** seja usado para autenticação e que os outros não sejam usados.



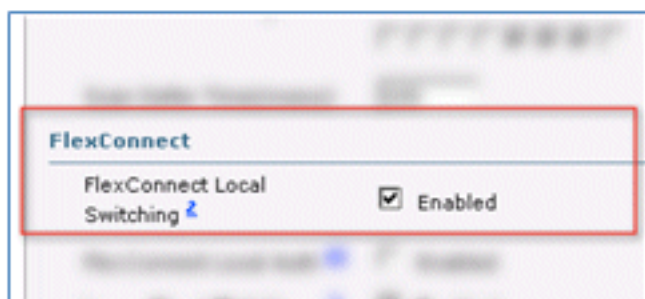
5. Vá até a guia **Avançado** e defina estes atributos:

Permitir Substituição de AAA: **Habilitado** Estado do NAC: **Radius NAC**

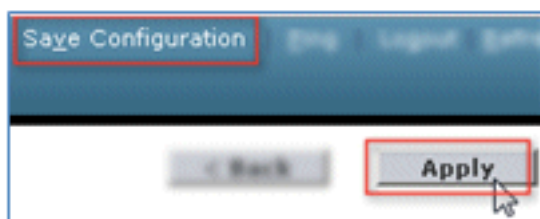


Observação: o Network Admission Control (NAC) RADIUS não é suportado quando o AP FlexConnect está no modo desconectado. Assim, se o AP FlexConnect estiver no modo autônomo e perder a conexão com a WLC, todos os clientes serão desconectados e o SSID não será mais anunciado.

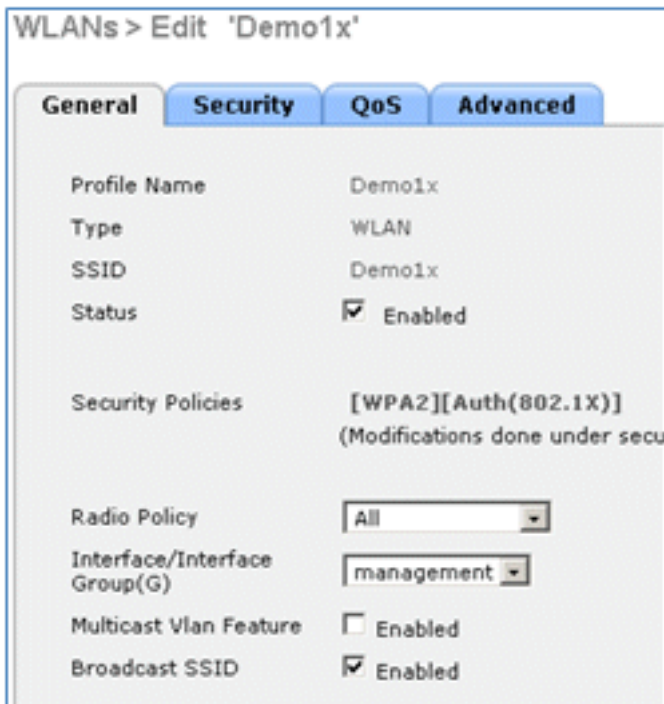
6. Role para baixo na guia Avançado e defina o FlexConnect Local Switching como **Enabled**.



7. Clique em **Aplicar** e **Salvar configuração**.

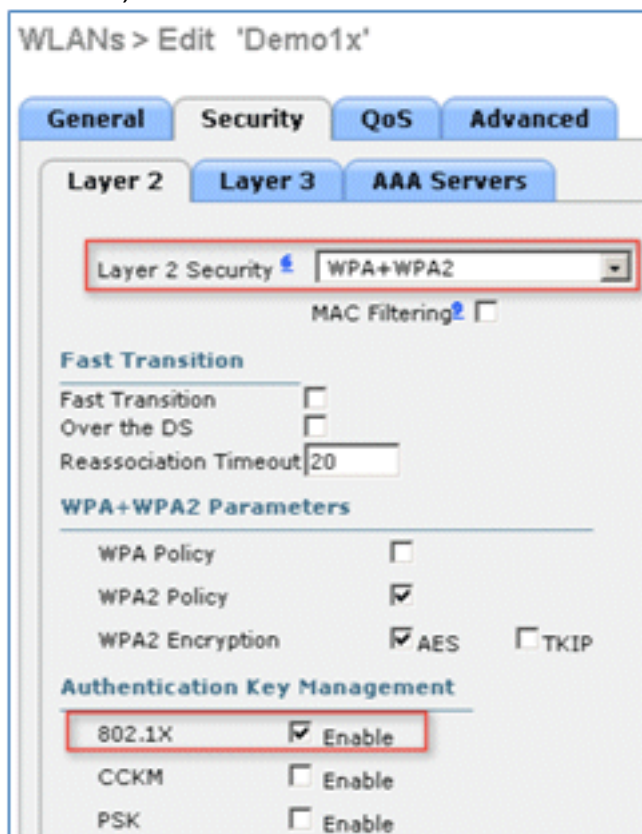


8. Crie um SSID de WLAN 802.1X chamado **Demo1x** (neste exemplo) para cenários de SSID simples e duplos.



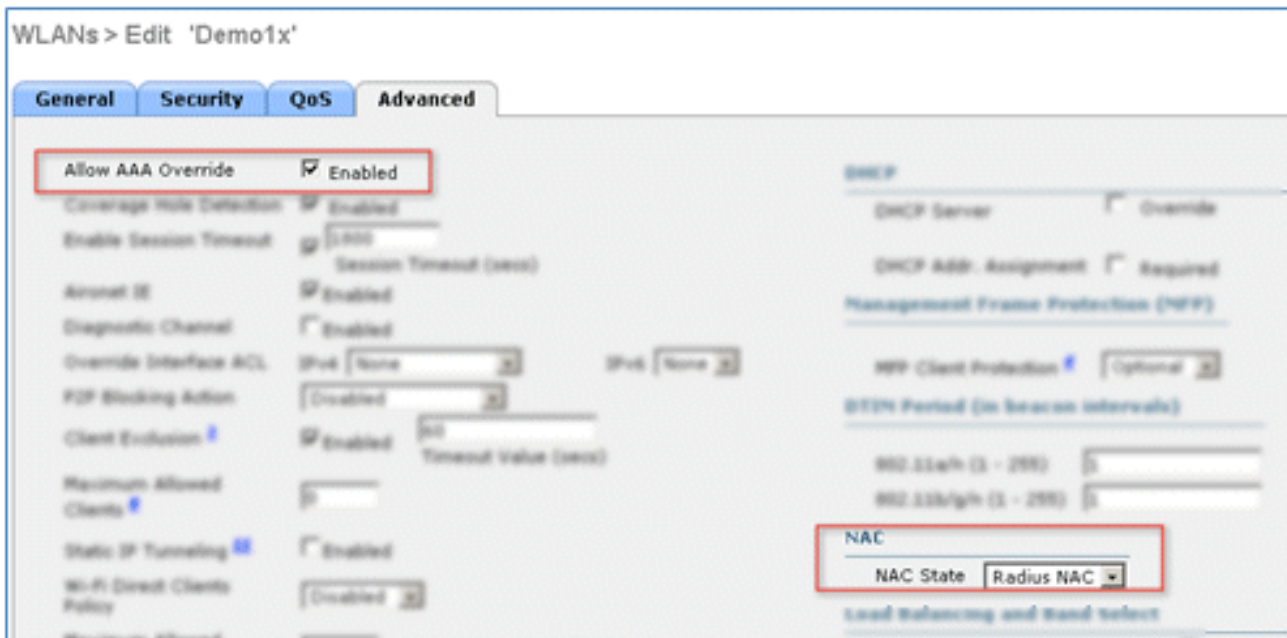
9. Navegue até a guia **Security > Layer 2** e defina estes atributos:

Segurança da camada 2: **WPA+WPA2** Transição Rápida: **Desabilitada** (caixa não marcada) Gerenciamento de chave de autenticação: 802.1X: **Habilitar**

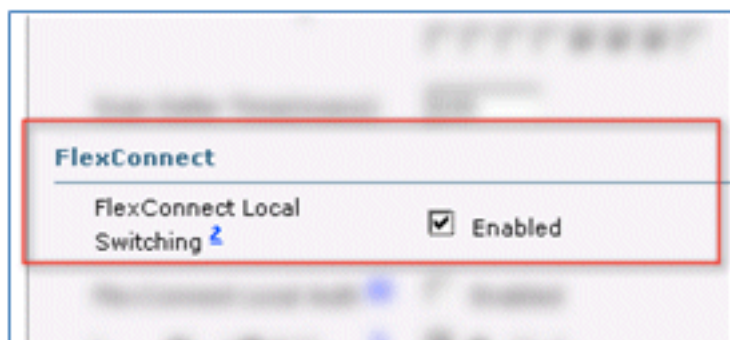


10. Vá até a guia **Avançado** e defina estes atributos:

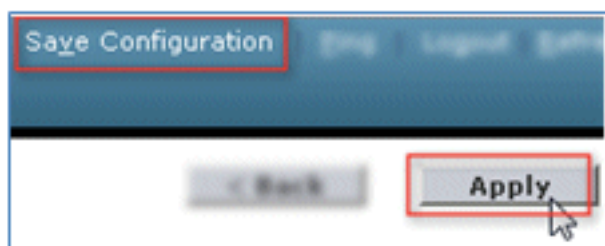
Permitir Substituição de AAA: **Habilitado** Estado do NAC: **Radius NAC**



11. Role para baixo na guia **Advanced** e defina o FlexConnect Local Switching como **Enabled**.



12. Clique em **Aplicar** e **Salvar configuração**.



13. Confirme se as duas novas WLANs foram criadas.

MONITOR <u>WLANs</u> CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK						
WLANs						Entries 1 - 5 of 1
Current Filter:		None	[Change Filter]	[Clear Filter]	<input type="button" value="Create New"/>	<input type="button" value="Go"/>
<input type="checkbox"/>	WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
<input type="checkbox"/>	1	WLAN	802x	802x	Disabled	[WPA2][Auth(802.1X)]
<input type="checkbox"/>	2	WLAN	8	8	Enabled	[WPA2][Auth(PSK)]
<input type="checkbox"/>	3	WLAN	Demo1x	Demo1x	Enabled	[WPA2][Auth(802.1X)]
<input type="checkbox"/>	4	WLAN	DemoCWA	DemoCWA	Enabled	MAC Filtering
<input type="checkbox"/>	5	WLAN	Flex	Flex	Disabled	Web-Auth

Configuração do AP FlexConnect

Conclua estas etapas para configurar o AP FlexConnect:

1. Navegue até **WLC > Wireless** e clique no AP FlexConnect de destino.

MONITOR <u>WLANs</u> CONTROLLER <u>WIRELESS</u>	
All APs	
Current Filter	None
Number of APs	2
AP Name	AP Model
Site-B-FlexAP	AIR-LAP1262N-A-K

2. Clique na guia **FlexConnect**.

MONITOR <u>WLANs</u> CONTROLLER <u>WIRELESS</u> SECURITY MANAGEMENT COMMANDS HELP FEEDBACK						
All APs > Details for Site-B-FlexAP						
General	Credentials	Interfaces	High Availability	Inventory	FlexConnect	Advanced

3. Habilite o suporte à VLAN (caixa marcada), defina o ID da VLAN nativa e clique em **Mapeamentos de VLAN**.

VLAN Support

Native VLAN ID **VLAN Mappings**

FlexConnect Group Name Not Configured

4. Defina o VLAN ID como 21 (neste exemplo) para o SSID para switching local.

MONITOR WLANs CONTROLLER WIRELESS SECURITY M

All APs > Site-B-FlexAP > VLAN Mappings

AP Name Site-B-FlexAP

Base Radio MAC e8:04:62:0a:68:80

WLAN Id	SSID	VLAN ID
3	Demo1x	<input type="text" value="21"/>
4	DemoCWA	<input type="text" value="21"/>

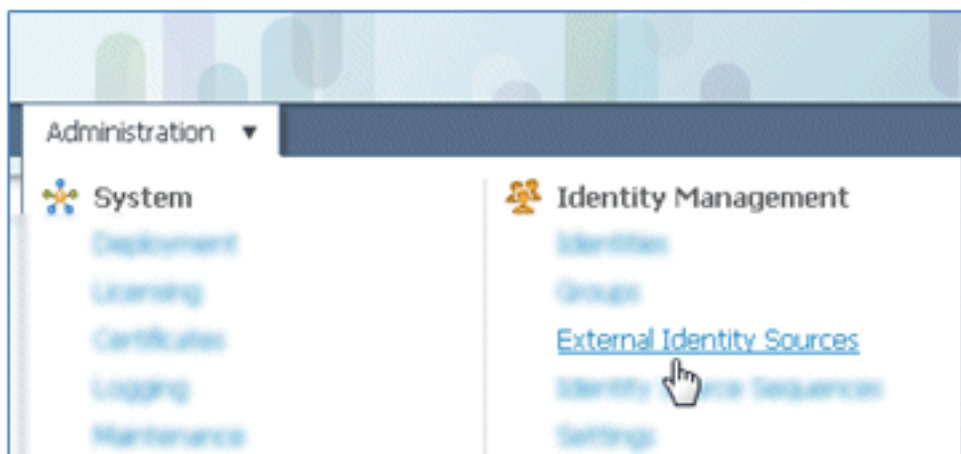
5. Clique em Aplicar e Salvar configuração.

Configuração do ISE

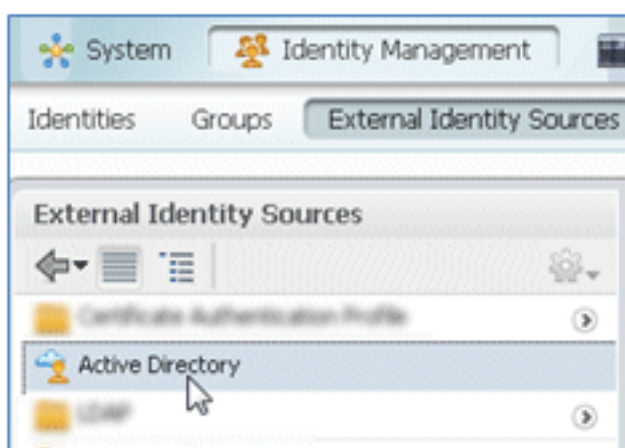
Conclua estas etapas para configurar o ISE:

1. Faça login no servidor ISE: <https://ise>.

2. Navegue até **Administração > Gerenciamento de identidades > Fontes de identidade externas**.

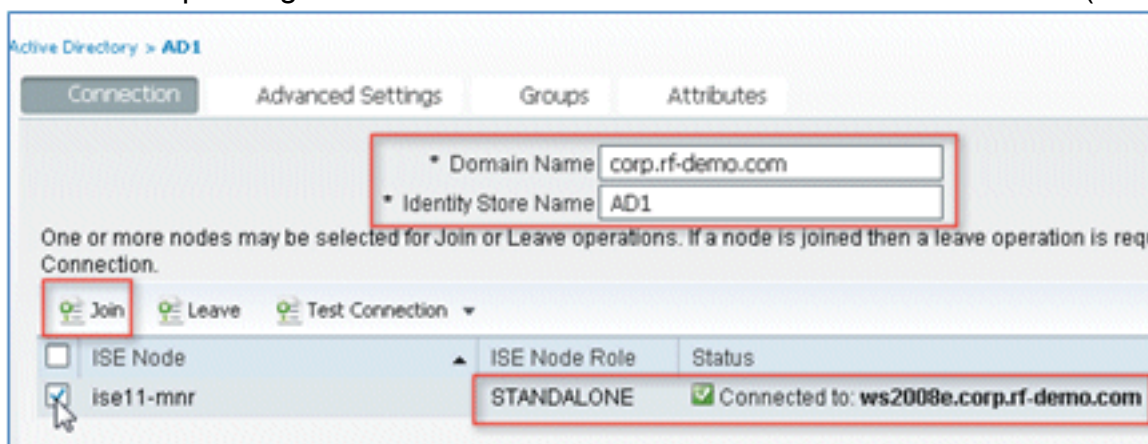


3. Clique em **Ative Diretory**.

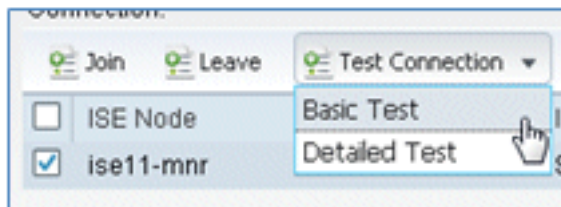


4. Na guia Conexão:

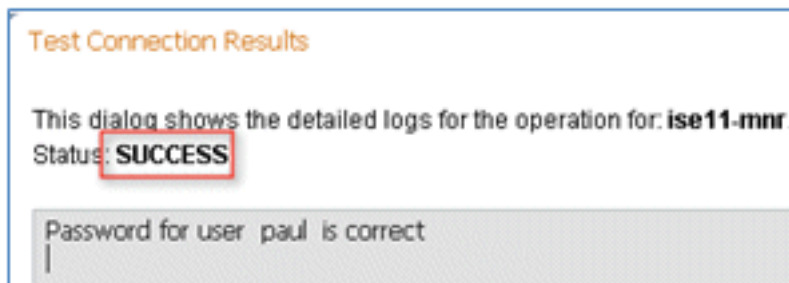
Adicione o Nome de domínio de **corp.rf-demo.com** (neste exemplo) e altere o padrão do Nome de armazenamento de identidade para **AD1**. Clique em **Save Configuration**. Clique em **Ingressar** e forneça o nome de usuário e a senha da conta de Administrador do AD necessários para ingressar. O Status deve ser verde. Habilitar **Conectado a:** (caixa marcada).



5. Execute um teste de conexão básico com o AD com um usuário de domínio atual.

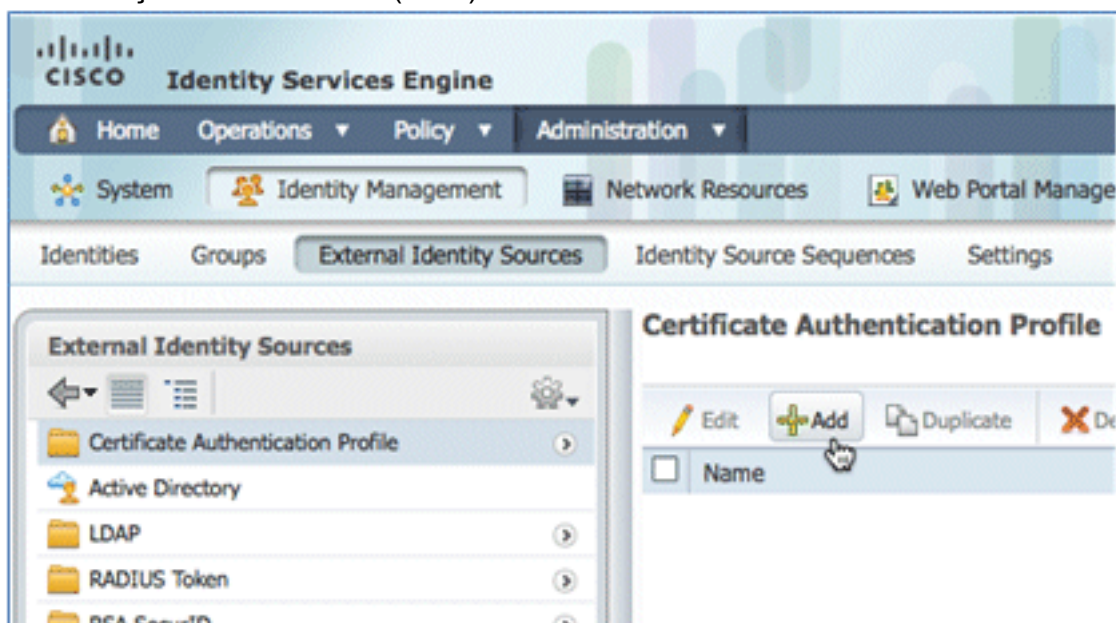


6. Se a conexão com o AD for bem-sucedida, uma caixa de diálogo confirmará que a senha está correta.



7. Navegue até **Administração > Gerenciamento de identidades > Fontes de identidade externas**:

Clique em **Certificate Authentication Profile**. Clique em **Add** para obter um novo perfil de autenticação de certificado (CAP).



8. Insira um nome de **CertAuth** (neste exemplo) para o CAP; para o Atributo Username X509 Principal, selecione **Common Name**; em seguida, clique em **Submit**.

Certificate Authentication Profiles List > New Certificate Authentication Profile

Certificate Authentication Profile

* Name

Description

Principal Username X509 Attribute

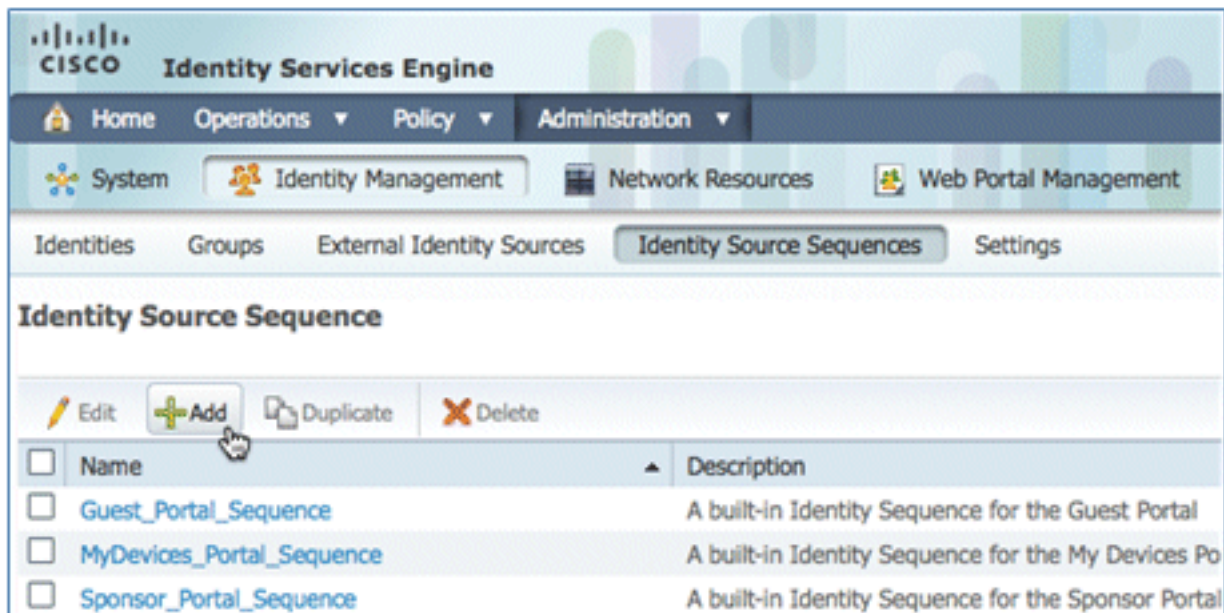
Perform Binary Certificate Comparison with Certificate retrieved from LDAP or Active Directory

LDAP/AD Instance Name

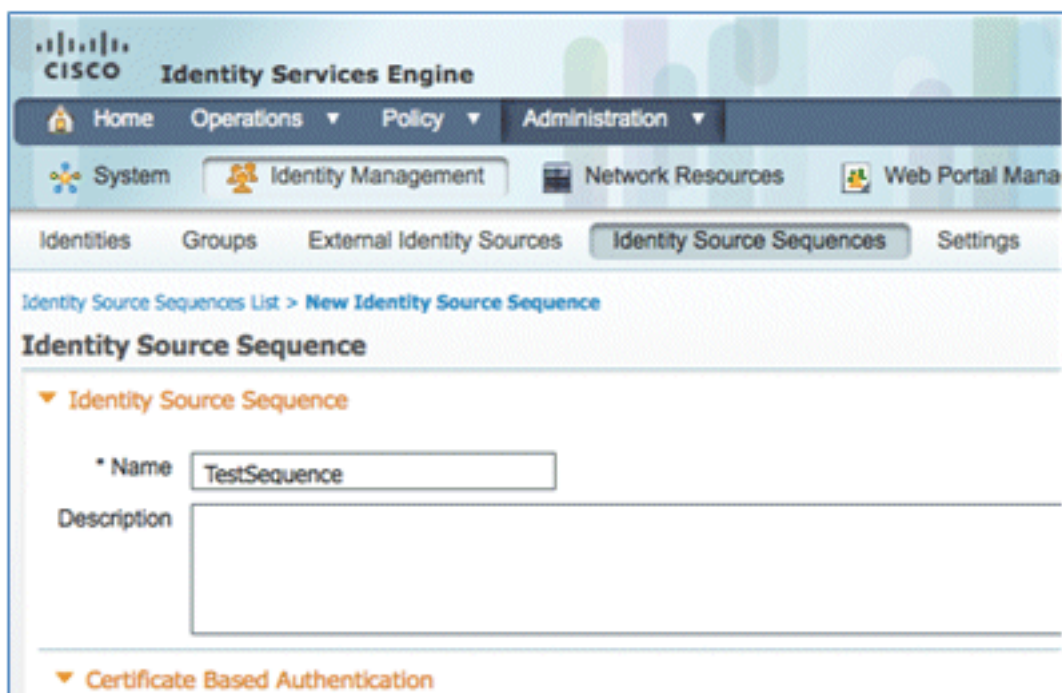
9. Confirme se a nova CAP foi adicionada.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation menu includes Home, Operations, Policy, and Administration. Under Administration, there are tabs for System, Identity Management, Network Resources, and Web Portal Management. The 'External Identity Sources' tab is active, showing a list of sources: Certificate Authentication Profile, Active Directory, LDAP, RADIUS Token, and RSA SecurID. The 'Certificate Authentication Profile' source is selected, and the main content area displays the configuration page for this source. The page has buttons for Edit, Add, Duplicate, and Delete. Below these buttons is a table with two columns: Name and CertAuth. The 'CertAuth' entry is highlighted, and a red arrow points to it.

10. Navegue até **Administração > Gerenciamento de identidades > Sequências de origem de identidade** e clique em **Adicionar** .

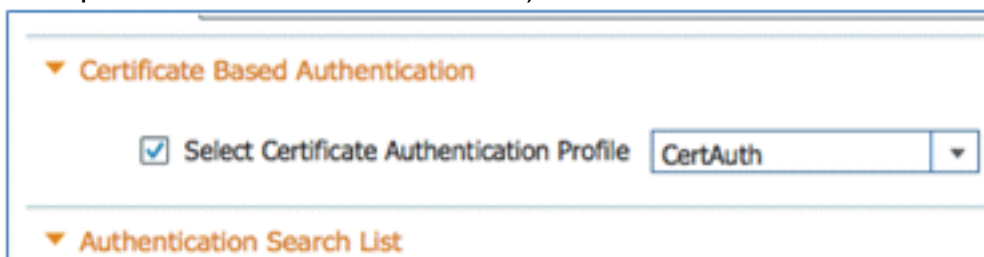


11. Dê à sequência um nome de **TestSequence** (neste exemplo).



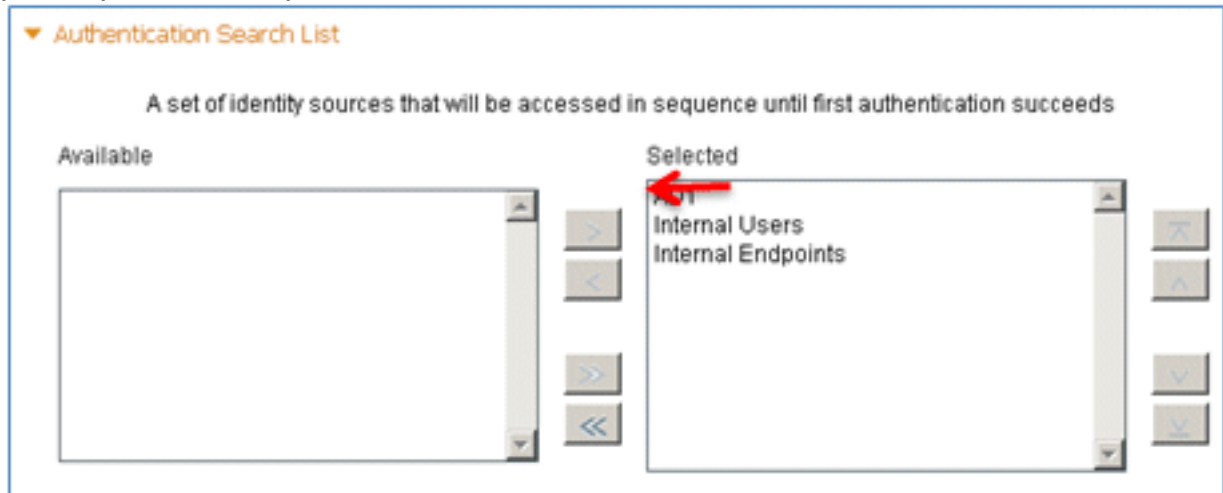
12. Role para baixo até **Certificate Based Authentication**:

Enable **Select Certificate Authentication Profile** (caixa marcada). Selecione **CertAuth** (ou outro perfil CAP criado anteriormente).

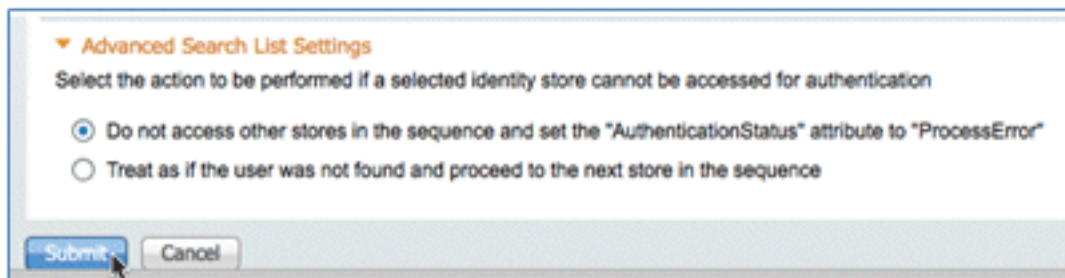


13. Role para baixo até **Authentication Search List**:

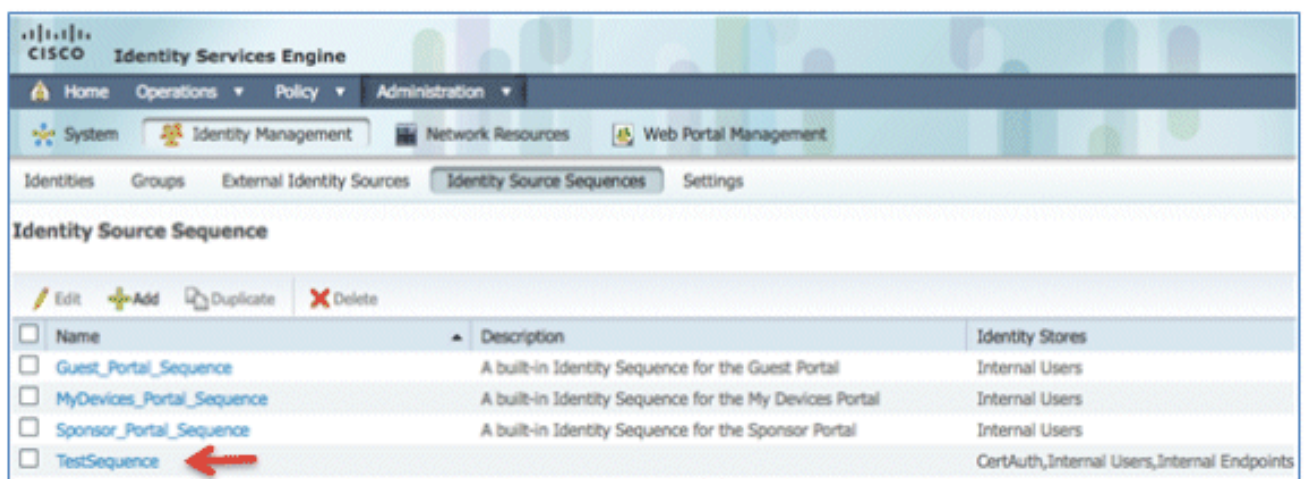
Mova o AD1 de Disponível para Selecionado. Clique no botão para cima para mover AD1 para a prioridade superior.



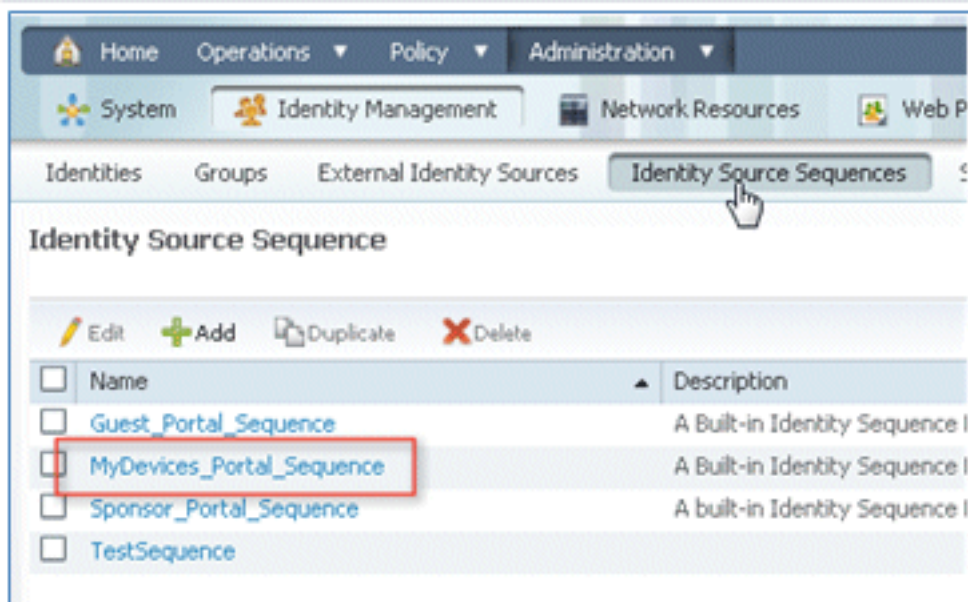
14. Clique em **Submit** para salvar.



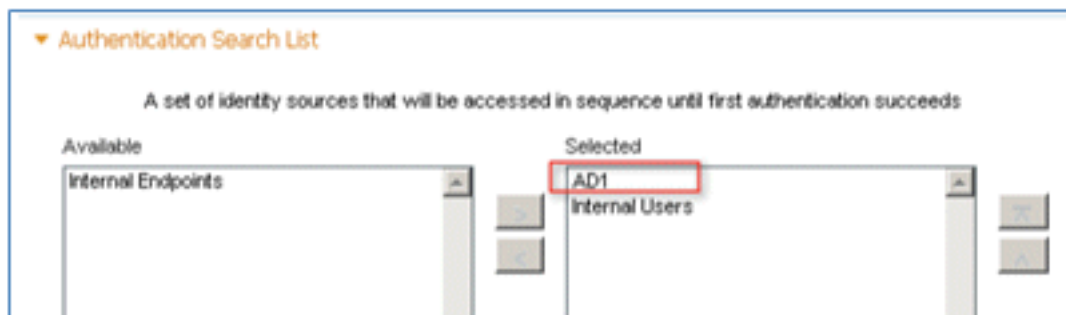
15. Confirme se a nova Sequência de origem de identidade foi adicionada.



16. Use o AD para autenticar o portal Meus dispositivos. Navegue até ISE > **Administração** > Gerenciamento de identidades > Sequência de origem de identidade e edite MyDevices_Portal_Sequence.



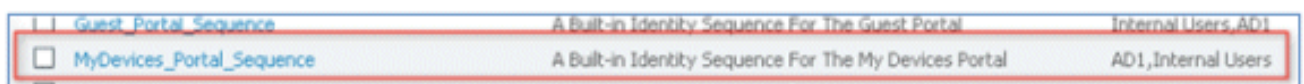
17. Adicione **AD1** à lista Selecionado e clique no botão para cima para mover AD1 para a prioridade superior.



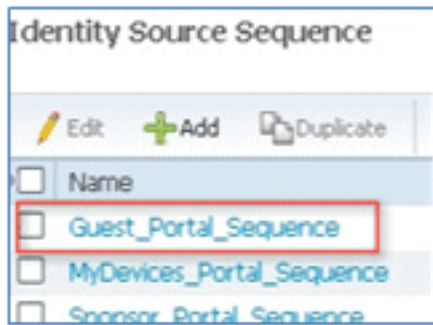
18. Click **Save**.



19. Confirme se a seqüência do Repositório de Identidades para MyDevices_Portal_Sequence contém **AD1**.



20. Repita as etapas 16-19 para adicionar AD1 para Guest_Portal_Sequence e clique em **Save**.



21. Confirme se Guest_Portal_Sequence contém **AD1**.

<input type="checkbox"/>	Name	Description	Identity Stores
<input type="checkbox"/>	Guest_Portal_Sequence	A Built-in Identity Sequence For The Guest Portal	Internal Users,AD1

22. Para adicionar a WLC ao dispositivo de acesso à rede (WLC), navegue para **Administração > Recursos de rede > Dispositivos de rede** e clique em **Adicionar**.



23. Adicione o nome da WLC, o endereço IP, a máscara de sub-rede, etc.

Network Devices List > New Network Device

Network Devices

* Name

Description

* IP Address: /

Model Name

Software Version

* Network Device Group

Location

Device Type

24. Role para baixo até Authentication Settings (Configurações de autenticação) e digite Shared Secret (Segredo compartilhado). Isso deve corresponder ao segredo compartilhado do RADIUS da WLC.

Authentication Settings

Enable Authentication Settings

Protocol **RADIUS**

* Shared Secret

Enable KeyWrap ⓘ

* Key Encryption Key

* Message Authenticator Code Key

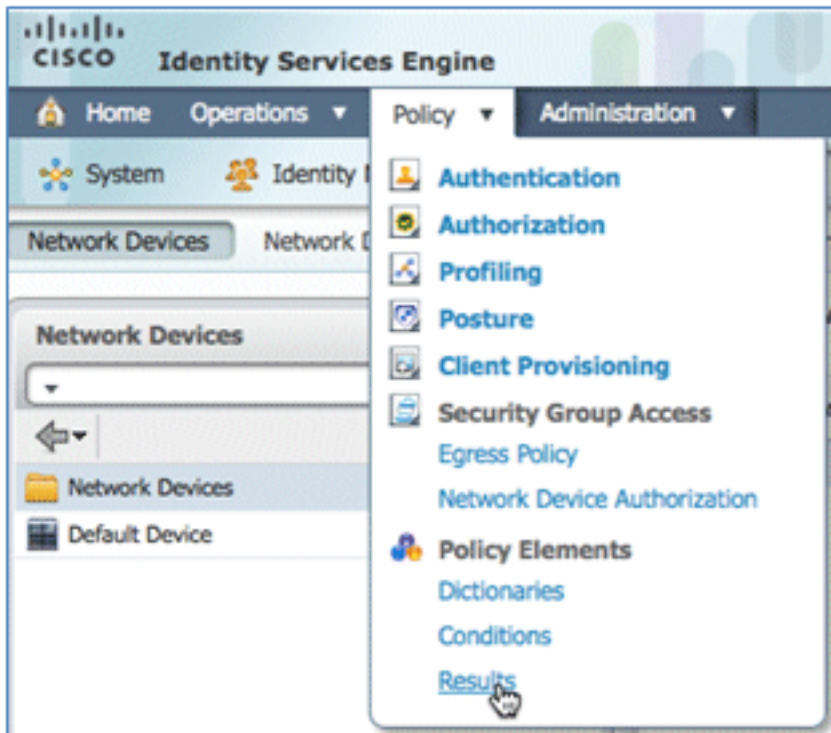
Key Input Format ASCII HEXADECIMAL

▶ SNMP Settings

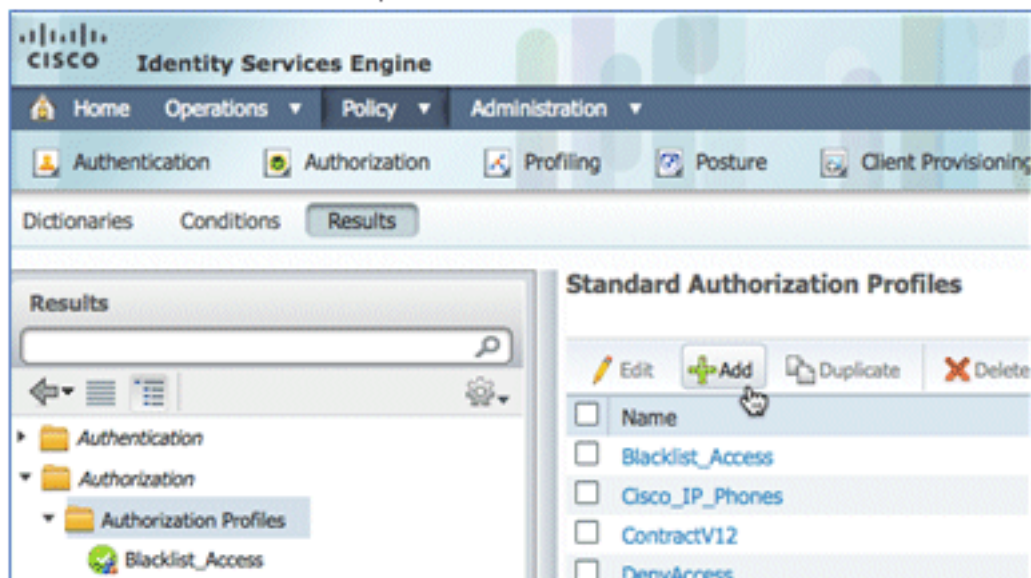
▶ SGA Attributes

25. Clique em Submit.

26. Navegue até ISE > Policy > Policy Elements > Results.



27. Expanda **Results** e **Authorization**, clique em **Authorization Profiles** e clique em **Add** para obter um novo perfil.



28. Dê a este perfil estes valores:

Nome: **CWA**

Authorization Profiles > New Authorization Profile

Authorization Profile

* Name

Description

* Access Type

Habilitar autenticação da Web (caixa marcada):

Autenticação da Web: **centralizada**ACL: **ACL-REDIRECT** (Isso deve corresponder ao nome da ACL de pré-autenticação da WLC.)Redirecionar: **Padrão**

▼ Common Tasks

DACL Name

VLAN

Voice Domain Permission

Web Authentication ACL Redirect

29. Clique em **Enviar** e confirme se o perfil de autorização do CWA foi adicionado.

Standard Authorization Profiles

Edit Add Duplicate Delete

<input type="checkbox"/>	Name
<input type="checkbox"/>	Blacklist_Access
<input type="checkbox"/>	CWA
<input type="checkbox"/>	Cisco_IP_Phones

30. Clique em **Add** para criar um novo perfil de autorização.

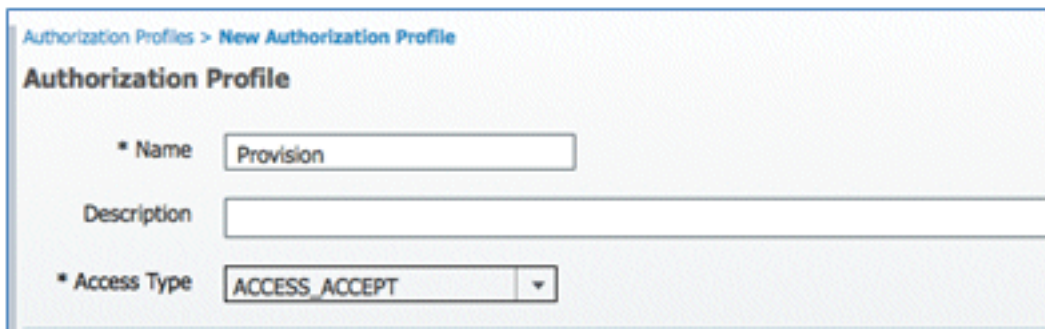
Standard Authorization Profiles

Edit Add Duplicate Delete

<input type="checkbox"/>	Name
<input type="checkbox"/>	Blacklist_Access
<input type="checkbox"/>	CWA
<input type="checkbox"/>	Cisco_IP_Phones

31. Dê a este perfil estes valores:

Nome: **Provisionar**



Authorization Profiles > New Authorization Profile

Authorization Profile

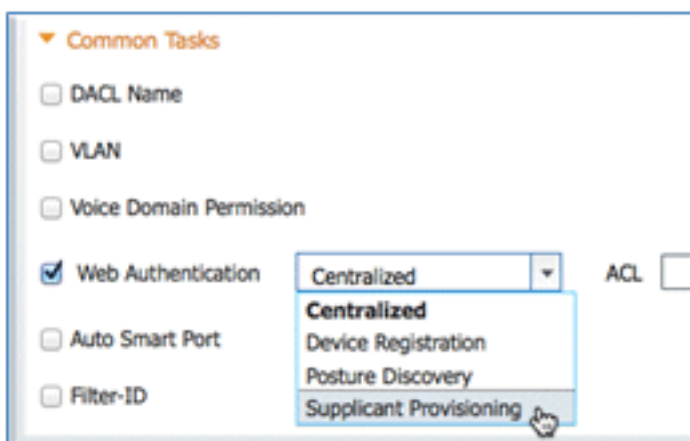
* Name

Description

* Access Type

Habilitar autenticação da Web (caixa marcada):

Valor de Autenticação da Web: **Provisionamento do Requerente**



▼ Common Tasks

DACL Name

VLAN

Voice Domain Permission

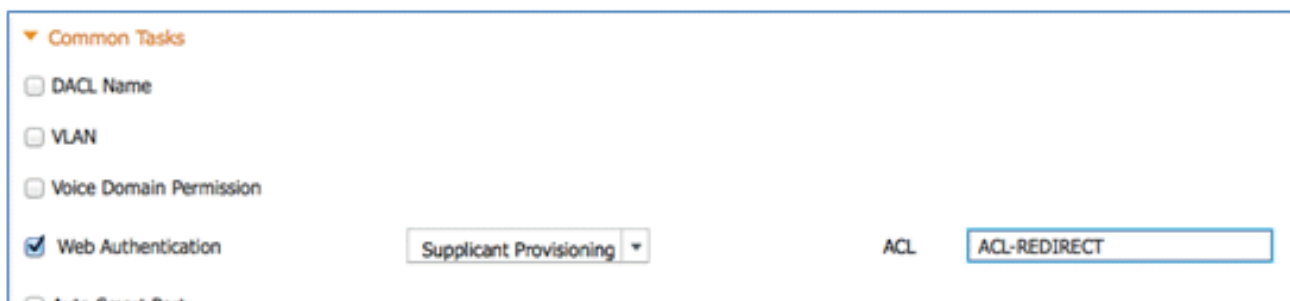
Web Authentication ACL

Auto Smart Port

Filter-ID

Centralized
Device Registration
Posture Discovery
Supplicant Provisioning

ACL: **ACL-REDIRECT** (Isso deve corresponder ao nome da ACL de pré-autenticação da WLC.)



▼ Common Tasks

DACL Name

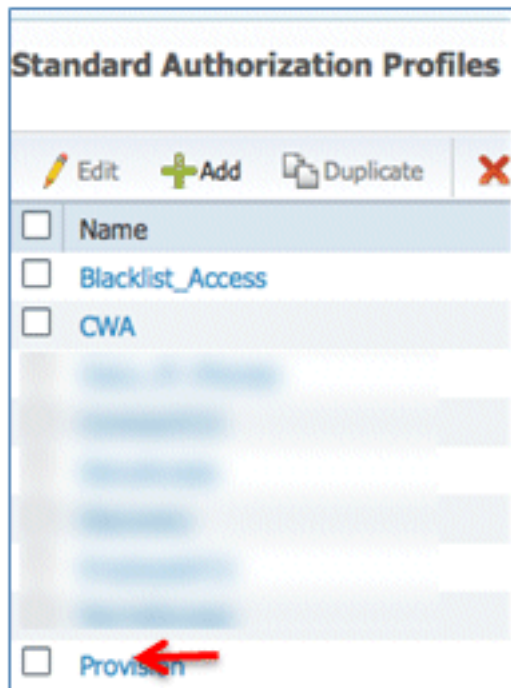
VLAN

Voice Domain Permission

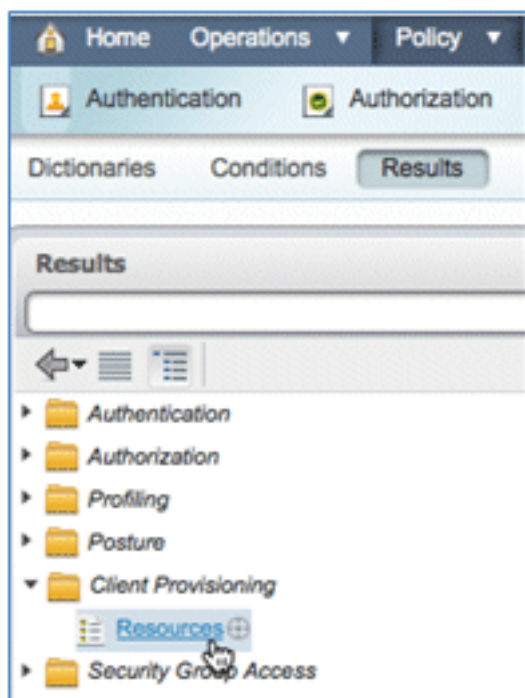
Web Authentication ACL

Auto Smart Port

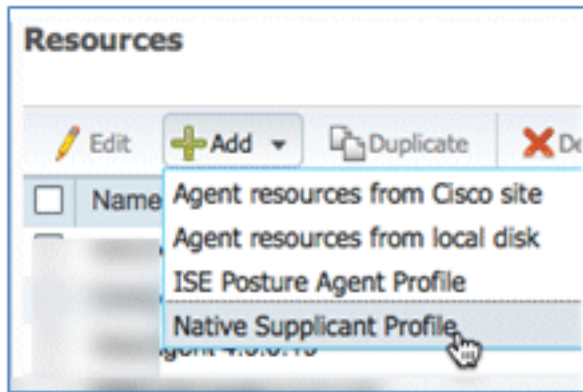
32. Clique em **Enviar** e confirme se o perfil de autorização Provisionar foi adicionado.



33. Role para baixo em Resultados, expanda **Provisionamento de cliente** e clique em **Recursos**.



34. Selecione **Perfil do Requerente Nativo**.



35. Dê ao perfil o nome **WirelessSP** (neste exemplo).

Native Supplicant Profile

* Name

Description

36. Insira estes valores:

Tipo de conexão: **sem fio**SSID: **Demo1x** (este valor é da configuração WLAN do WLC 802.1x)Protocolo permitido: **TL**S
Tamanho da chave: **1024**

* Operating System

* Connection Type Wired
 Wireless

*SSID

Security

* Allowed Protocol

► Optional Settings
TLS
PEAP

37. Clique em Submit.

38. Click **Save**.

* Allowed Protocol

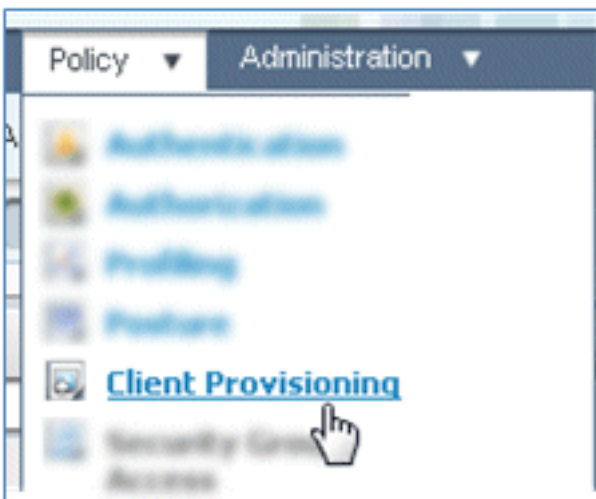
* Key Size

39. Confirme se o novo perfil foi adicionado.

Resources

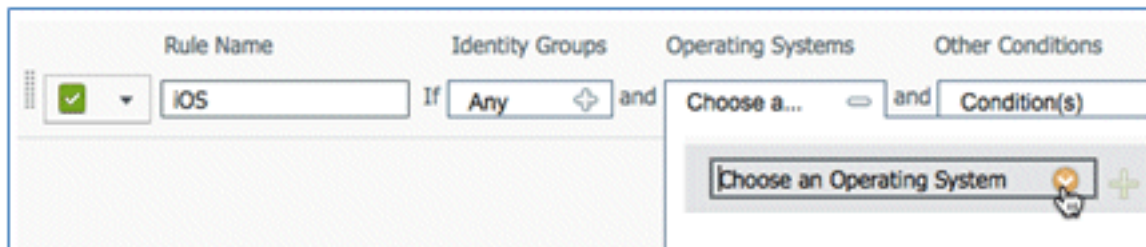
<input type="checkbox"/>	Name	Type
<input type="checkbox"/>	WirelessS	NativeSPProfile

40. Navegue até **Policy > Client Provisioning**.

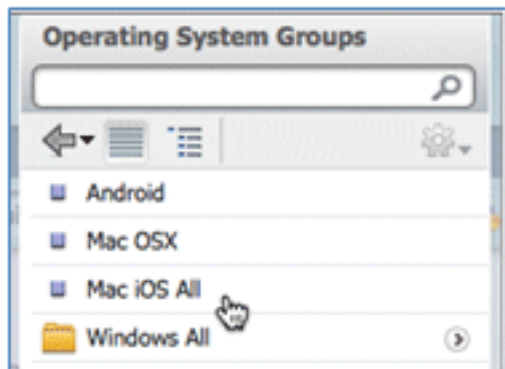


41. Insira estes valores para a regra de provisionamento de dispositivos iOS:

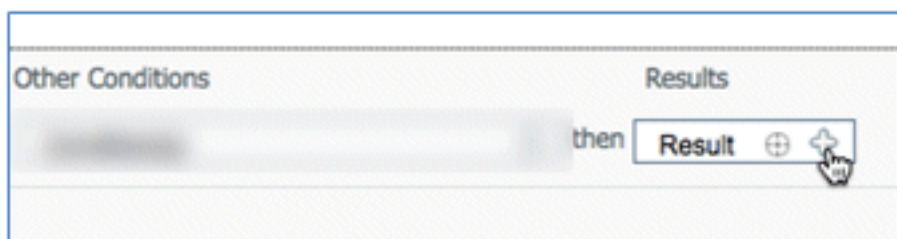
Nome da regra: **iOS** Grupos de Identidade: **Qualquer**



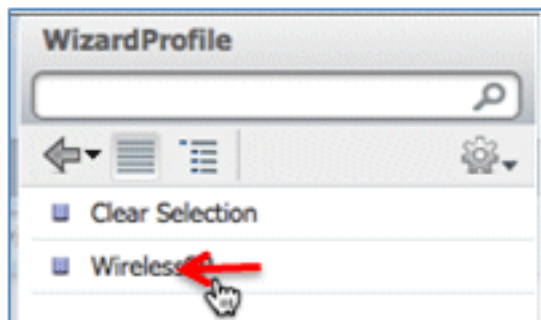
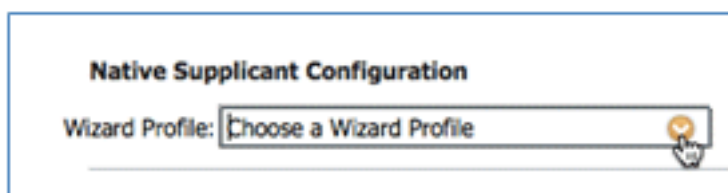
Sistemas Operacionais: **Mac iOS All**



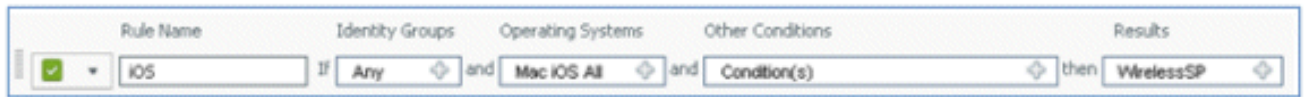
Resultados: **WirelessSP** (este é o perfil de requerente nativo criado anteriormente)



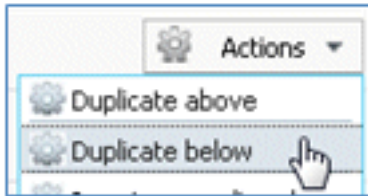
Navegue até **Results > Wizard Profile** (lista suspensa) > **WirelessSP**.



42. Confirme se o perfil de provisionamento do iOS foi adicionado.



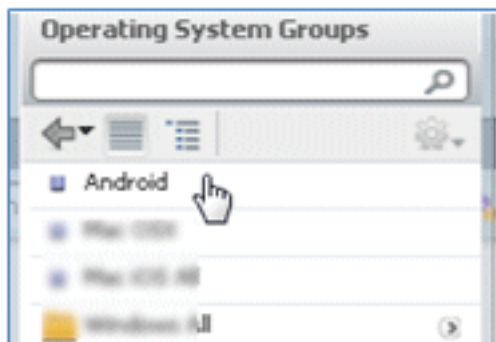
43. No lado direito da primeira regra, localize a lista suspensa Ações e selecione **Duplicar abaixo** (ou acima).



44. Altere o Nome da nova regra para **Android**.



45. Altere os Sistemas Operacionais para **Android**.

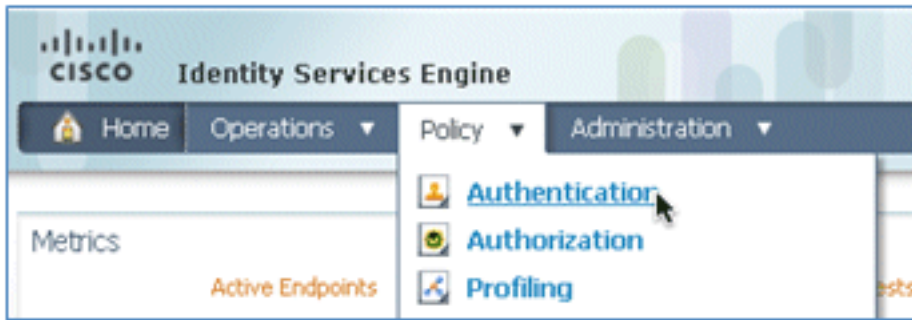


46. Deixe outros valores inalterados.

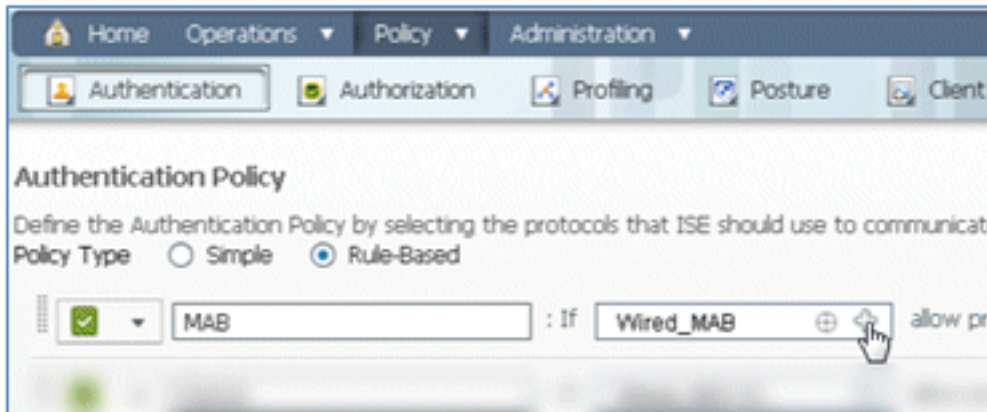
47. Clique em **Save (Salvar)** (tela inferior esquerda).



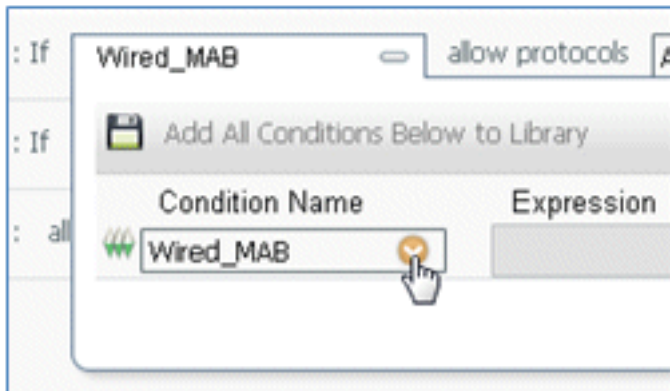
48. Navegue até **ISE > Política > Autenticação**.



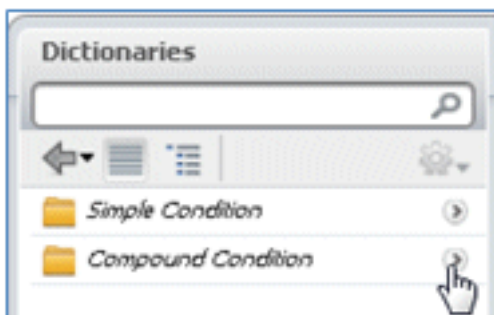
49. Modifique a condição para incluir Wireless_MAB e expanda **Wired_MAB**.



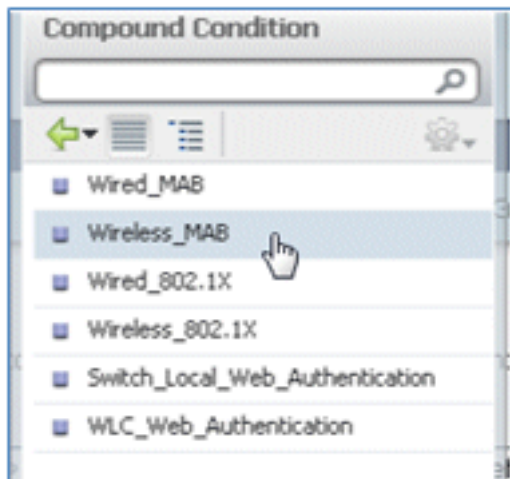
50. Clique na lista suspensa **Nome da condição**.



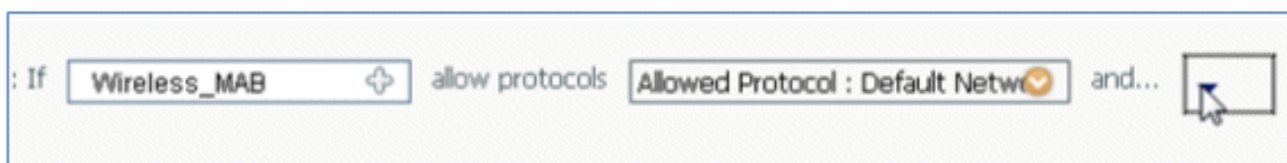
51. Selecione **Dicionários > Condição composta**.



52. Selecione **Wireless_MAB**.

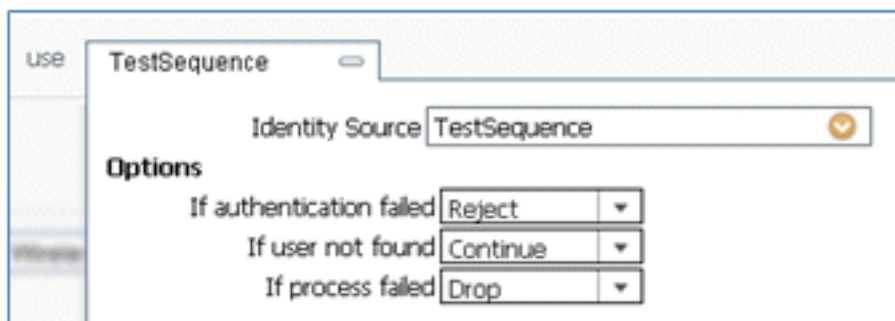


53. À direita da regra, selecione a seta a ser expandida.

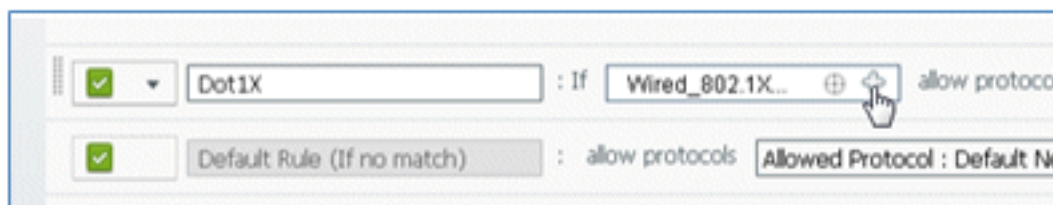


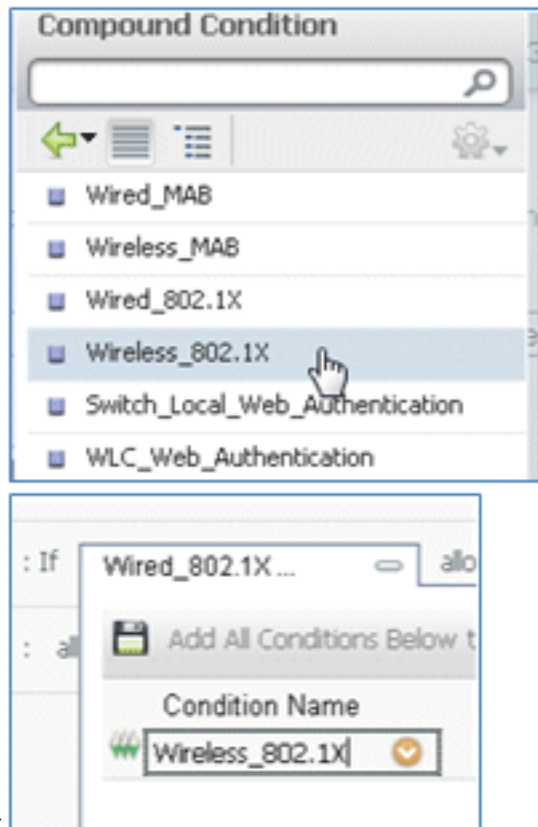
54. Selecione estes valores na lista suspensa:

Origem da Identidade: **TestSequence** (esse é o valor criado anteriormente) Se a autenticação falhou: **Rejeitar** Se o usuário não for encontrado: **Continuar** Se o processo falhar: **Descartar**



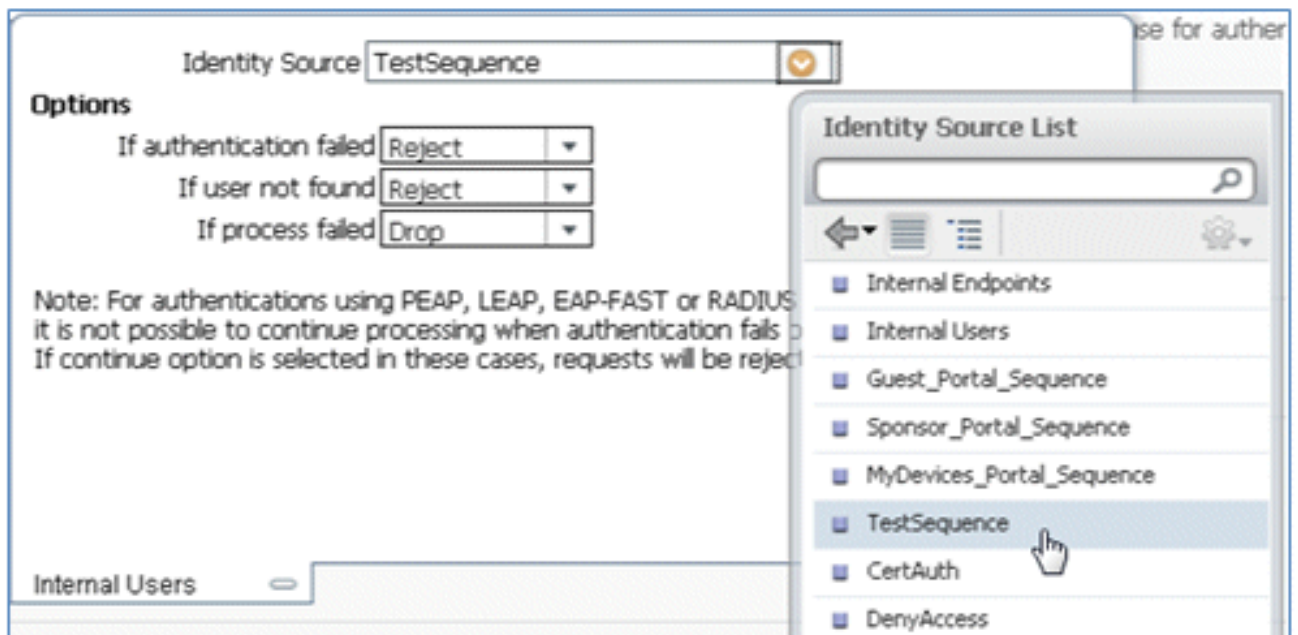
55. Vá para a regra **Dot1X** e altere estes valores:





Condição: **Wireless_802.1X**

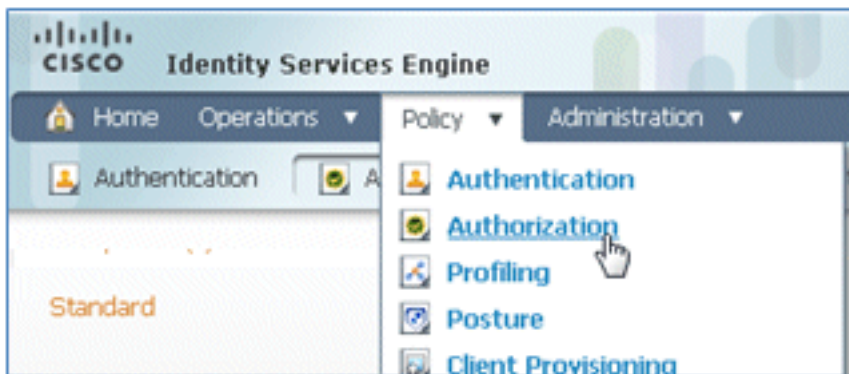
Origem da Identidade: **TestSequence**



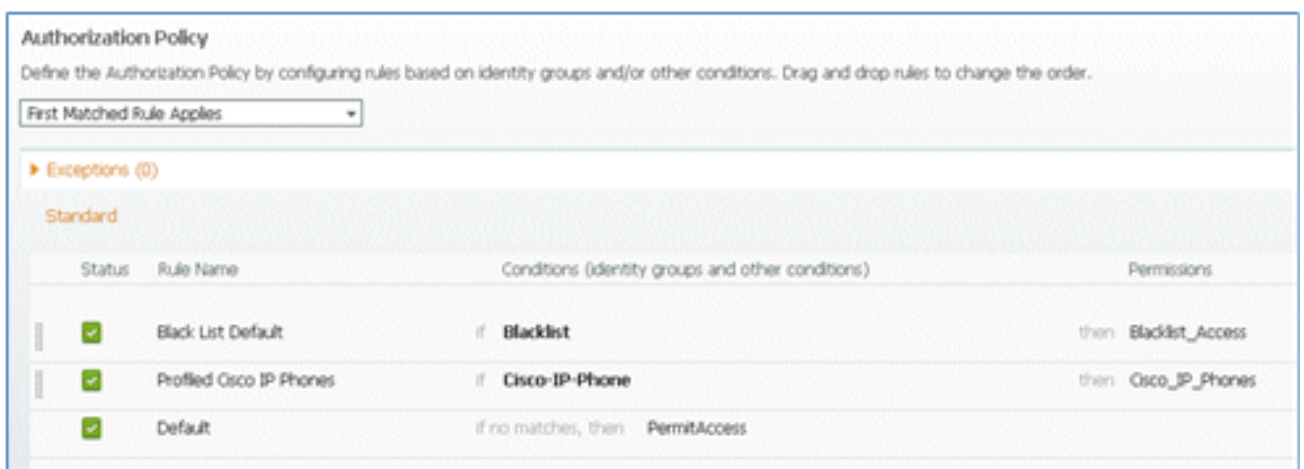
56. Click **Save**.



57. Navegue até ISE > Política > Autorização.



58. As regras padrão (como Padrão da lista negra, Com perfil e Padrão) já estão configuradas a partir da instalação; as duas primeiras podem ser ignoradas; a regra padrão será editada posteriormente.



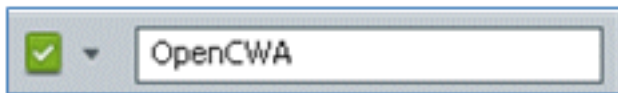
59. À direita da segunda regra (Profiled Cisco IP Phones), clique na seta para baixo ao lado de Edit (Editar) e selecione **Insert New Rule Below (Inserir nova regra abaixo)**.



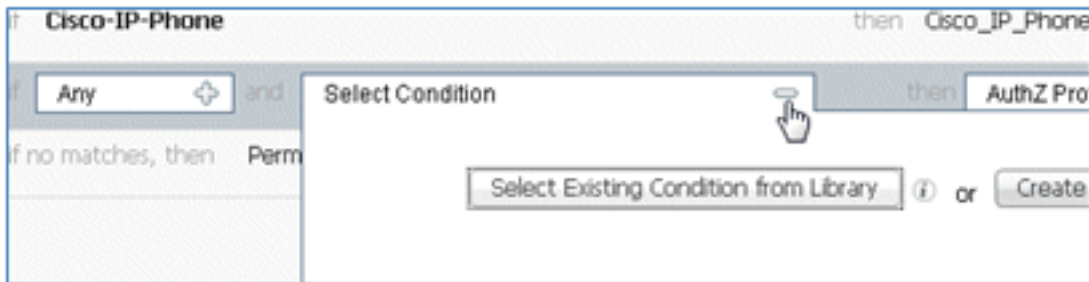
Um novo número de regra padrão é adicionado.



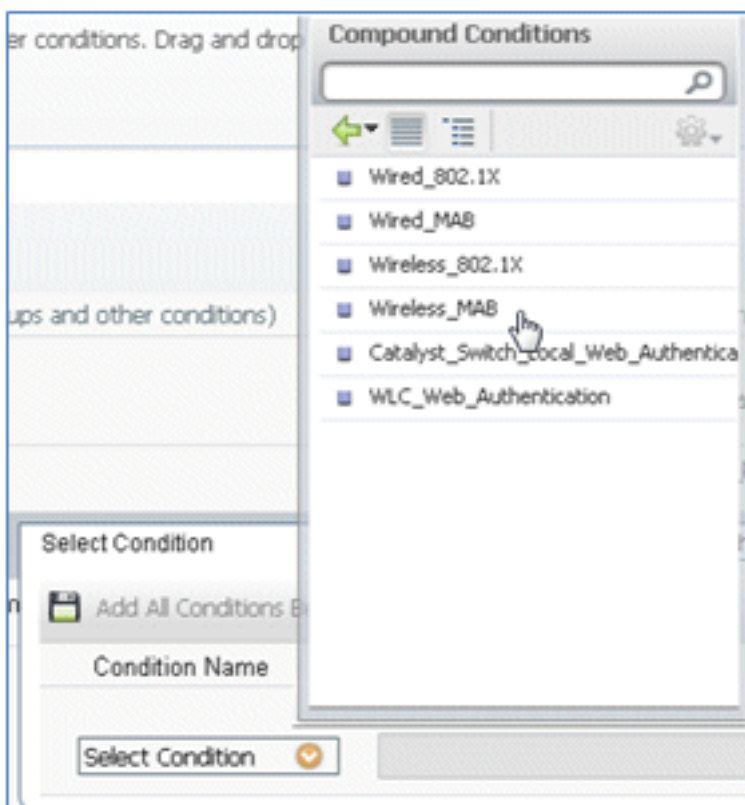
60. Altere o Nome da regra de Número da regra padrão para **OpenCWA**. Esta regra inicia o processo de registro na WLAN aberta (SSID duplo) para usuários que vêm para a rede de convidado para ter dispositivos provisionados.



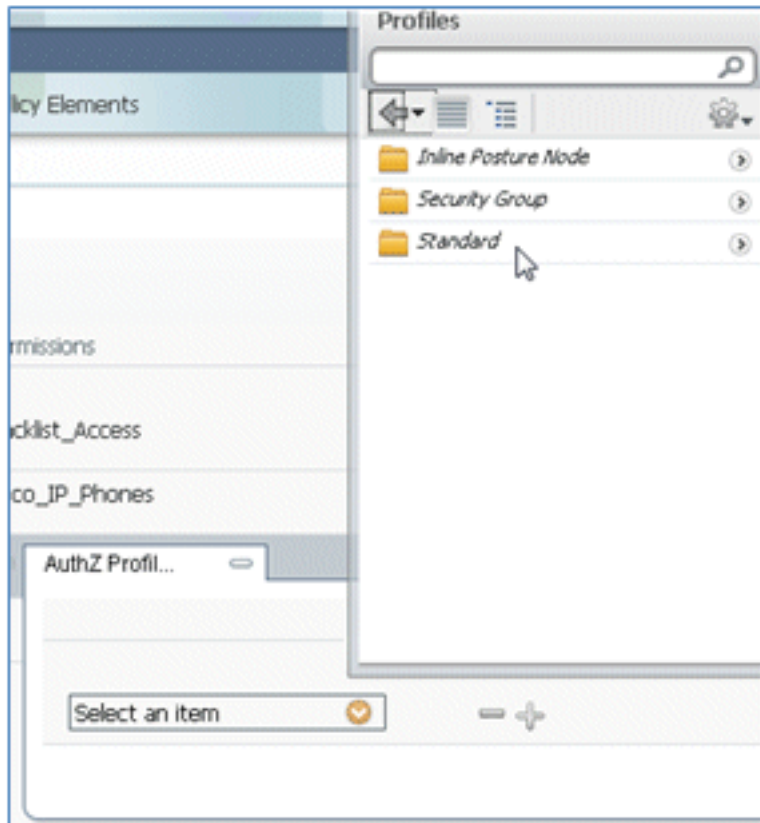
61. Clique no sinal de mais (+) para Condição(ões) e clique em **Selecionar condição existente na biblioteca**.



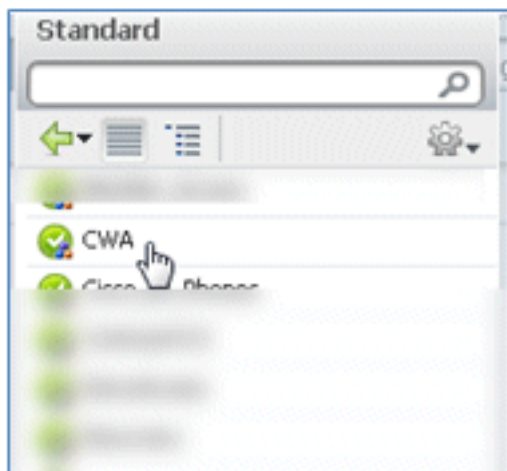
62. Selecione **Compound Conditions > Wireless_MAB**.



63. No Perfil de AuthZ, clique no sinal de mais (+) e selecione **Padrão**.



64. Selecione o **CWA** padrão (este é o perfil de autorização criado anteriormente).



65. Confirme se a regra foi adicionada com as Condições e Autorização corretas.



66. Clique em **Concluído** (à direita da regra).

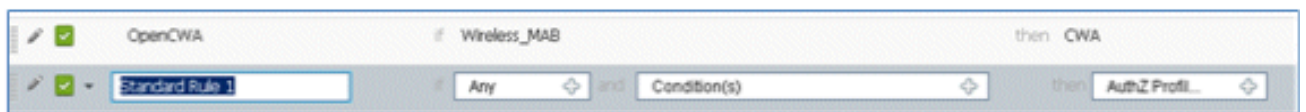


67. À direita da mesma regra, clique na seta para baixo ao lado de Editar e selecione **Inserir**

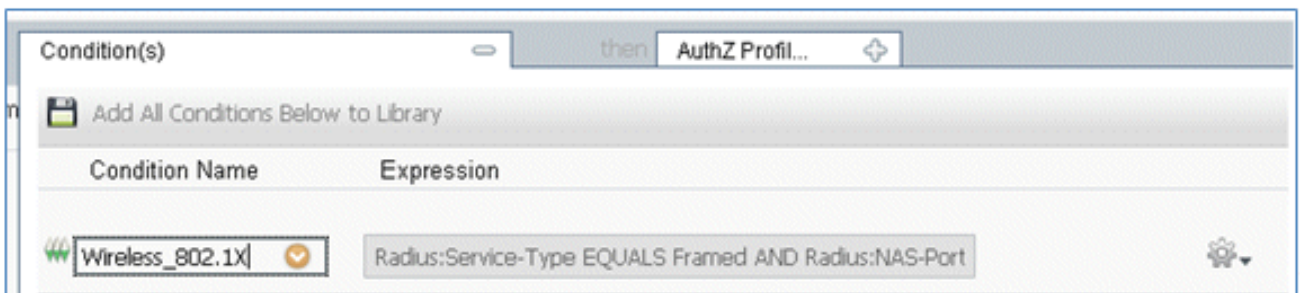
nova regra abaixo.



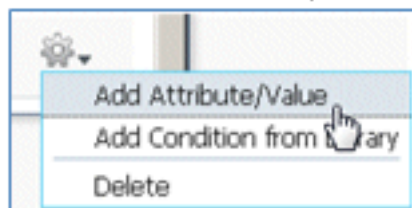
68. Altere o Rule Name de Standard Rule # para **PEAPrule** (neste exemplo). Esta regra serve para que o PEAP (também usado para um único cenário de SSID) verifique se a autenticação do 802.1X sem o Transport Layer Security (TLS) e se o provisionamento de solicitante de rede é iniciado com o perfil de autorização Provision criado anteriormente.



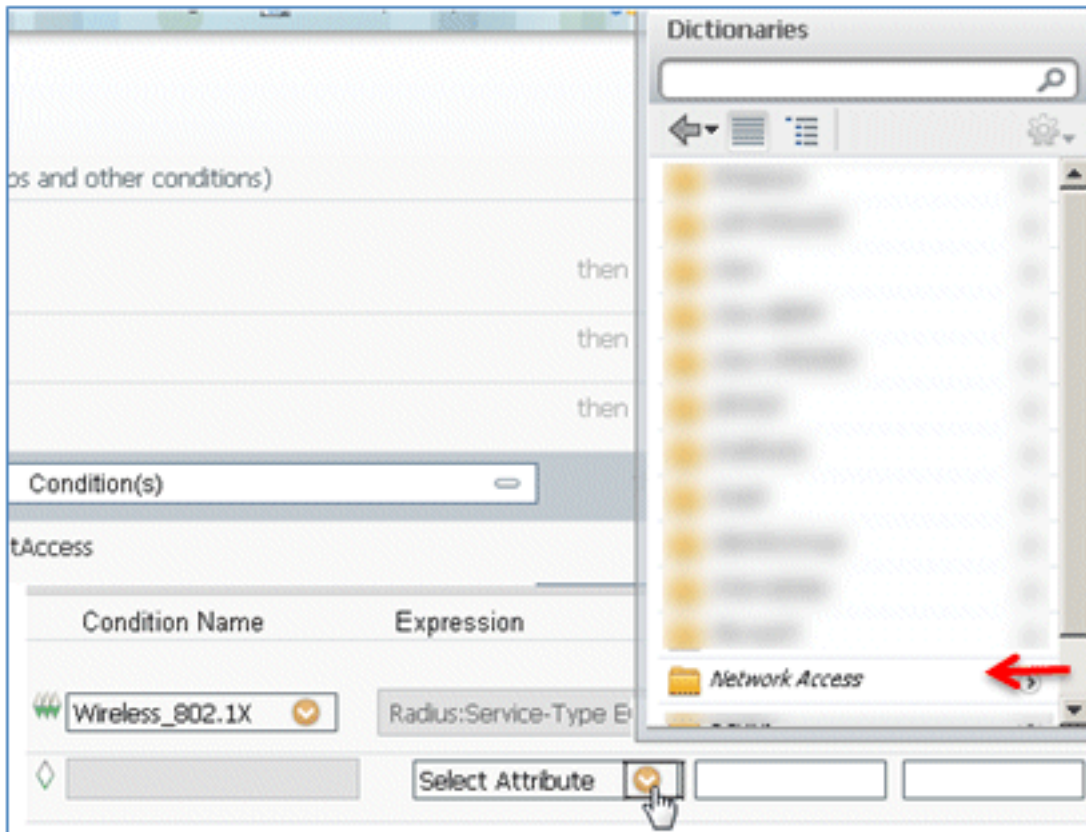
69. Altere a condição para **Wireless_802.1X**.



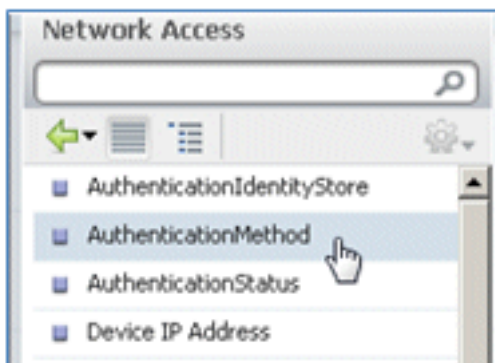
70. Clique no ícone de engrenagem no lado direito da condição e selecione **Adicionar atributo/valor**. Esta é uma condição 'and', não uma condição 'or'.



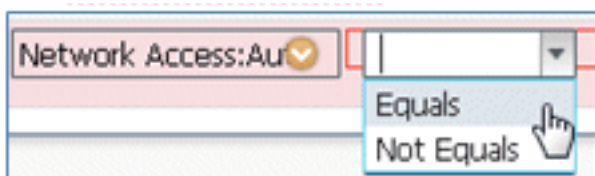
71. Localize e selecione **Network Access**.



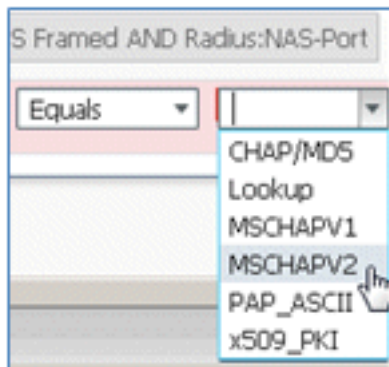
72. Seleccione **AuthenticationMethod** e insira estes valores:



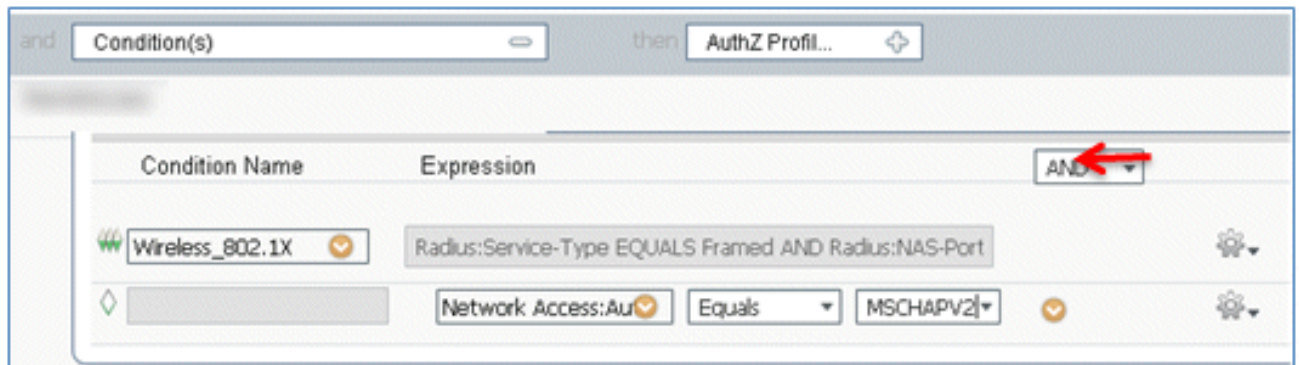
AuthenticationMethod: igual a



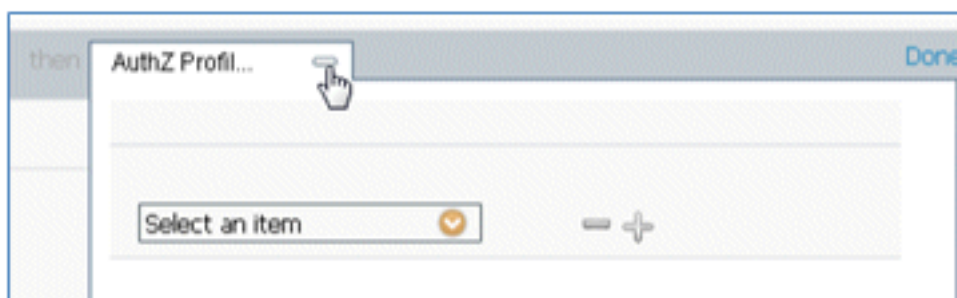
Selecione **MSCHAPV2**.

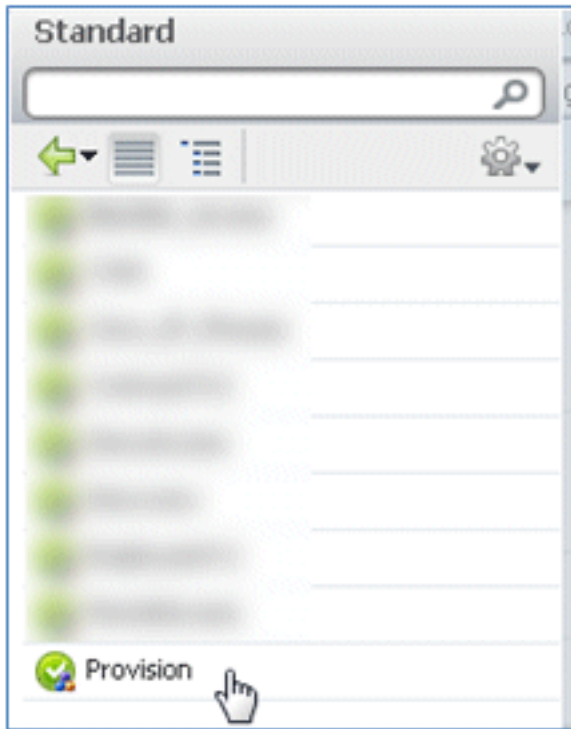


Este é um exemplo da regra; certifique-se de confirmar que a Condição é um AND.

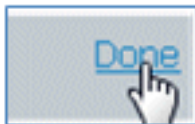


73. Em Perfil de Autorização, selecione **Padrão** > **Provisionar** (este é o Perfil de Autorização criado anteriormente).





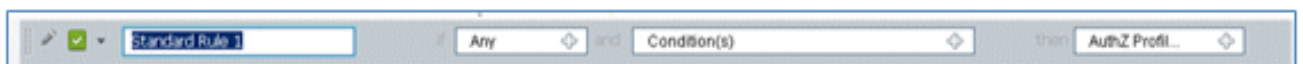
74. Clique em Concluído.



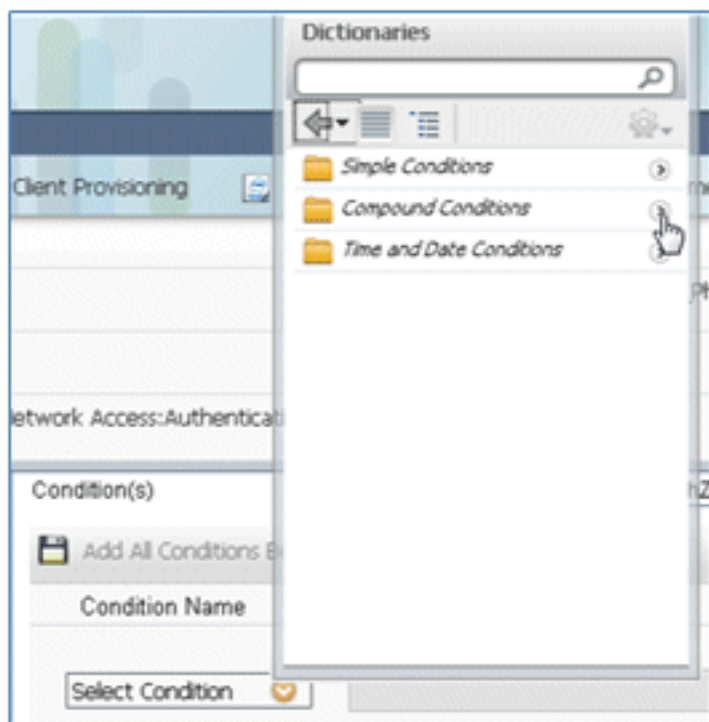
75. À direita da regra PEAP, clique na seta para baixo ao lado de Editar e selecione **Inserir nova regra abaixo**.



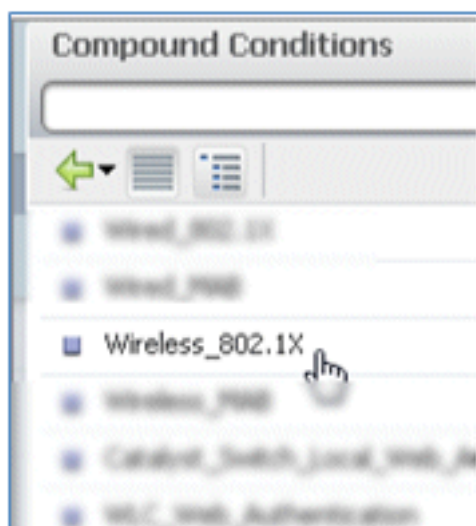
76. Altere o Nome da regra de Número da regra padrão para **AllowRule** (neste exemplo). Esta regra será usada para permitir o acesso a dispositivos registrados com certificados instalados.



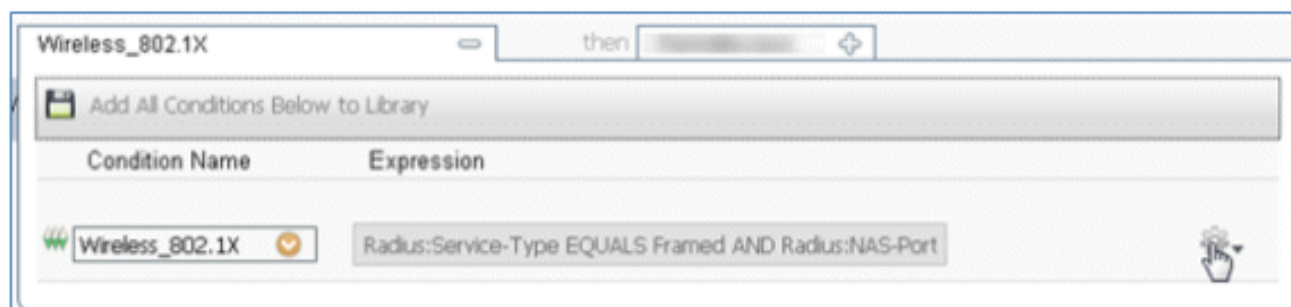
77. Em Condições, selecione **Condições Compostas**.



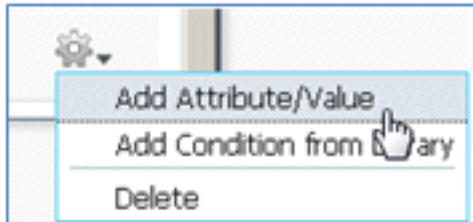
78. Selecione **Wireless_802.1X**.



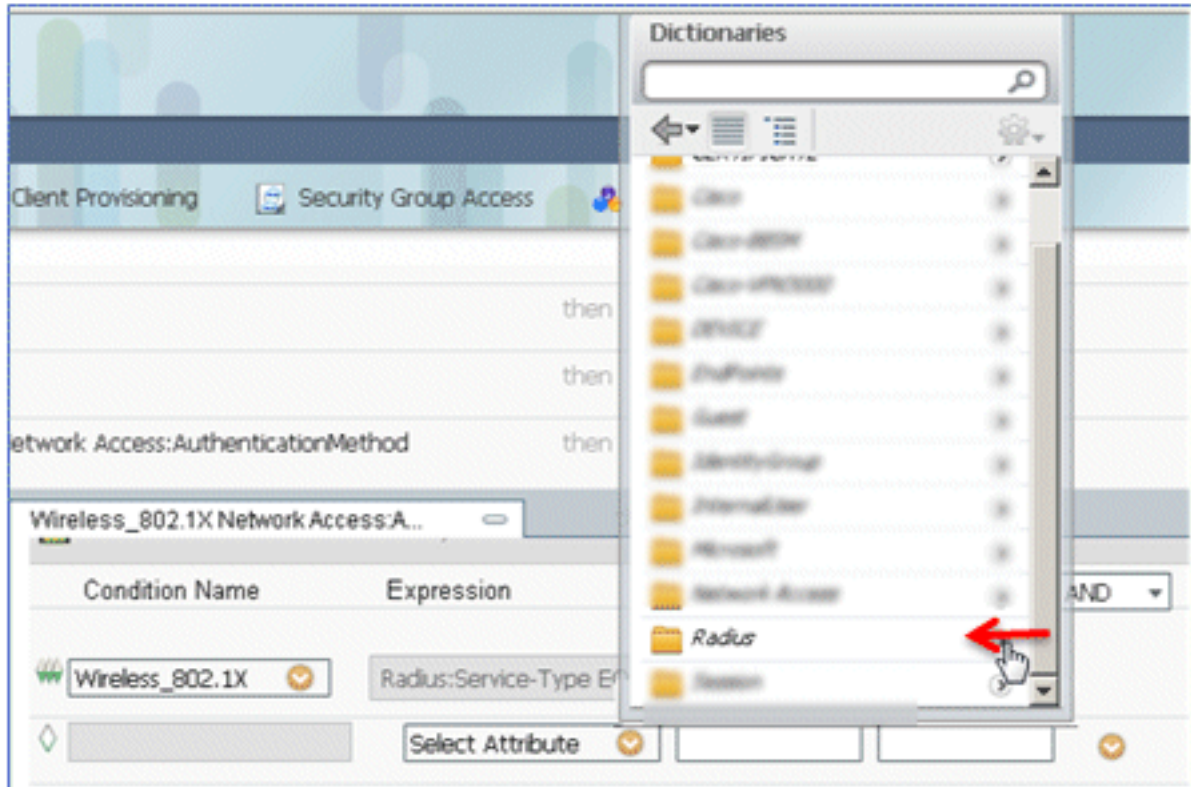
79. Adicione um atributo AND.



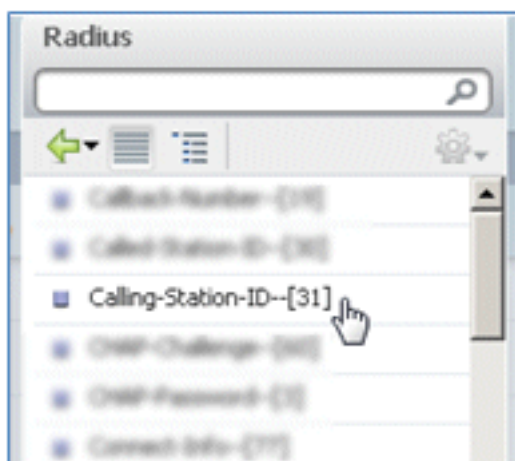
80. Clique no ícone de engrenagem no lado direito da condição e selecione **Adicionar atributo/valor**.



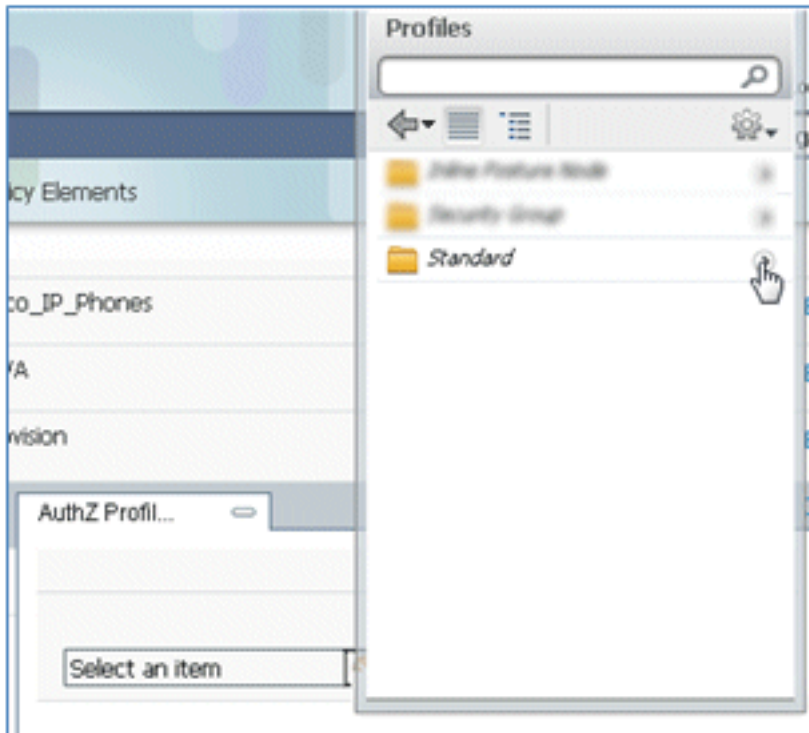
81. Localize e seleccione **Radius**.



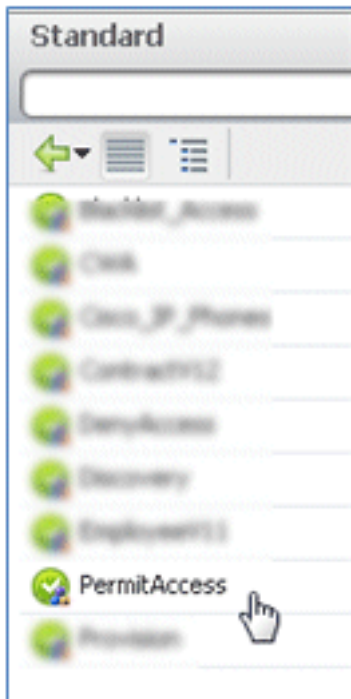
82. Seleccione **Calling-Station-ID--[31]**.



83. Seleccione **Iguais**.



87. Selecione **Permit Access**.



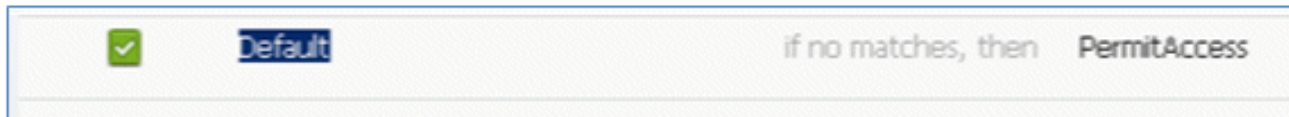
88. Clique em Concluído.



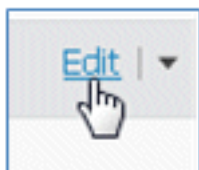
Este é um exemplo da regra:

<input checked="" type="checkbox"/>	OpenCWA	Wireless_M40	then: Deny
<input checked="" type="checkbox"/>	PerfHub	Wireless_802.1X (1): Network-Access-AuthenticationMethod EQUALS RADIUS(2)	then: Permit
<input checked="" type="checkbox"/>	AllowRule	Wireless_802.1X Radius:Calling-Station-ID EQUALS CERTIFICATE:Subject.AltitudeName	then: PermitAccess

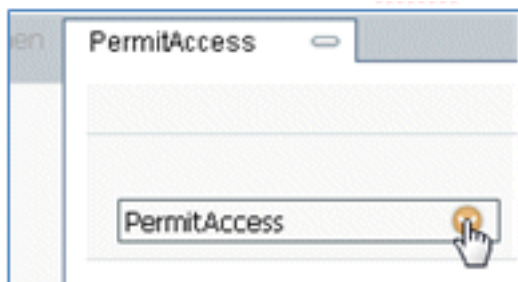
89. Localize a regra padrão para alterar PermitAccess para DenyAccess.



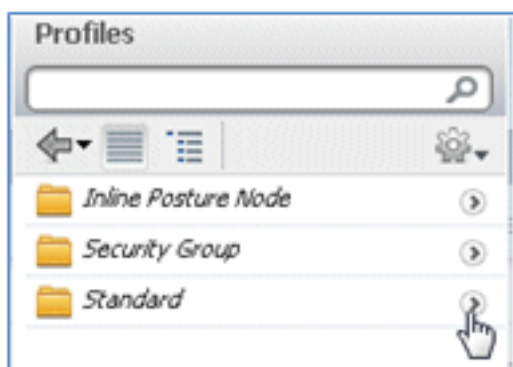
90. Clique em **Edit** para editar a regra Default.



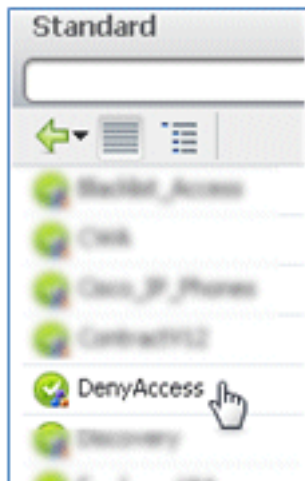
91. Vá para o perfil AuthZ existente de PermitAccess.



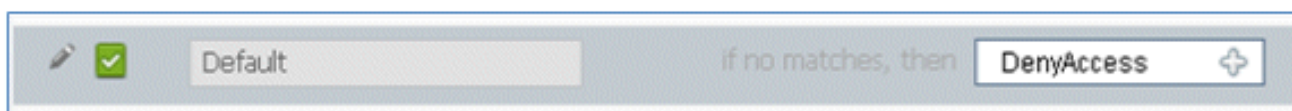
92. Selecione **Padrão**.



93. Selecione **DenyAccess**.



94. Confirme se a regra padrão tem DenyAccess se nenhuma correspondência for encontrada.



95. Clique em Concluído.



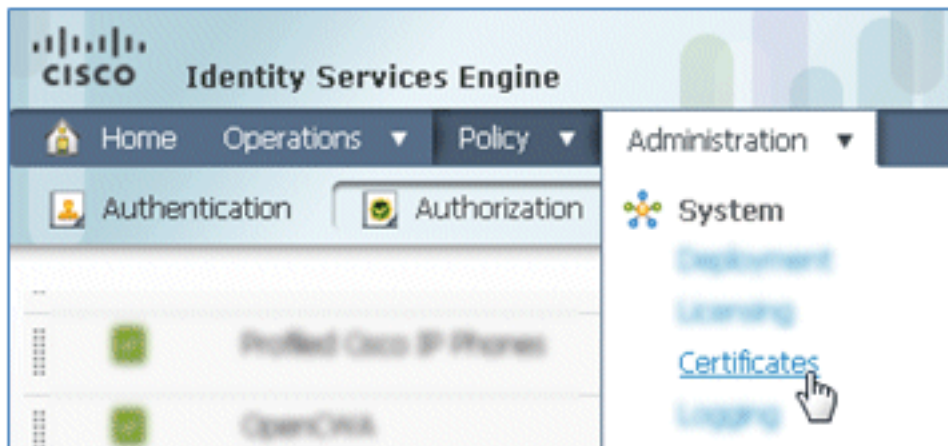
Este é um exemplo das principais regras necessárias para este teste; elas são aplicáveis a um único SSID ou a um cenário de SSID duplo.

<input checked="" type="checkbox"/>	OpenCWA	if Wireless_MAB	then CWA
<input checked="" type="checkbox"/>	PEAPrule	if (Wireless_802.1X AND Network:Access-AuthenticationMethod EQUALS MSOAPV2)	then Provision
<input checked="" type="checkbox"/>	AllowRule	if (Wireless_802.1X AND Radius:Calling-Station-ID EQUALS CERTIFICATE:Subject Alternative Name)	then PermitAccess
<input checked="" type="checkbox"/>	Default	if no matches, then	DenyAccess

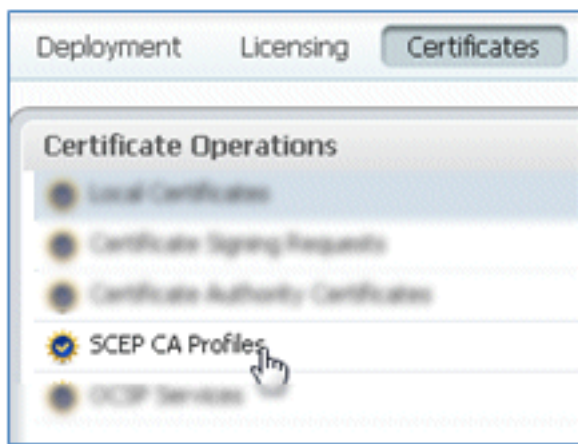
96. Click **Save**.



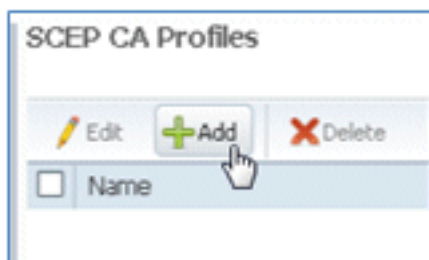
97. Navegue até ISE > **Administração** > **Sistema** > **Certificados** para configurar o servidor ISE com um perfil SCEP.



98. Em Operações de Certificado, clique em **Perfis de CA SCEP**.



99. Clique em Add.



100. Digite estes valores para este perfil:

Nome: **mySCEP** (neste exemplo) URL: **https://<ca-server>/CertSrv/mscep/** (Verifique a configuração do servidor de CA para obter o endereço correto.)

SEP Certificate Authority Certificates > New SCEP Profile

Edit Certificate

SEP Certificate Authority

* Name

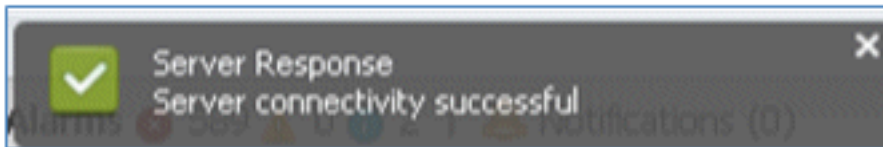
Description

* URL

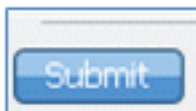
101. Clique em **Testar conectividade** para testar a conectividade da conexão SCEP.



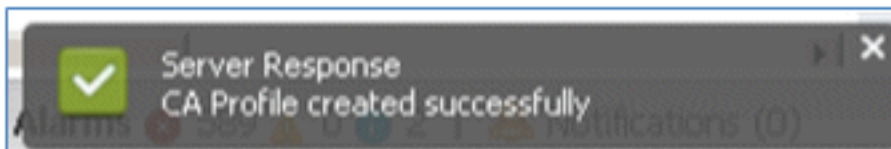
102. Essa resposta mostra que a conectividade do servidor foi bem-sucedida.



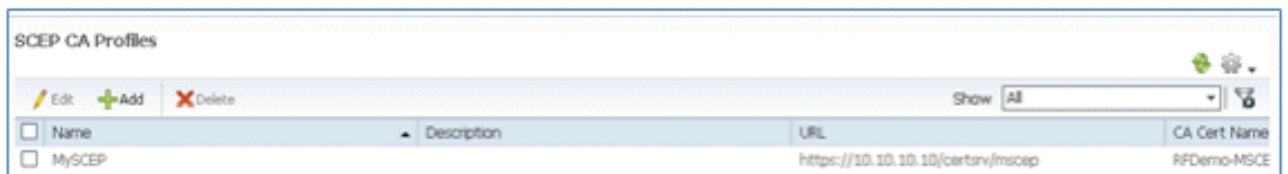
103. Clique em Submit.



104. O servidor responde que o perfil da autoridade de certificação foi criado com êxito.



105. Confirme se o perfil de CA SCEP foi adicionado.



Experiência do usuário - Provisionamento do iOS

SSID duplo

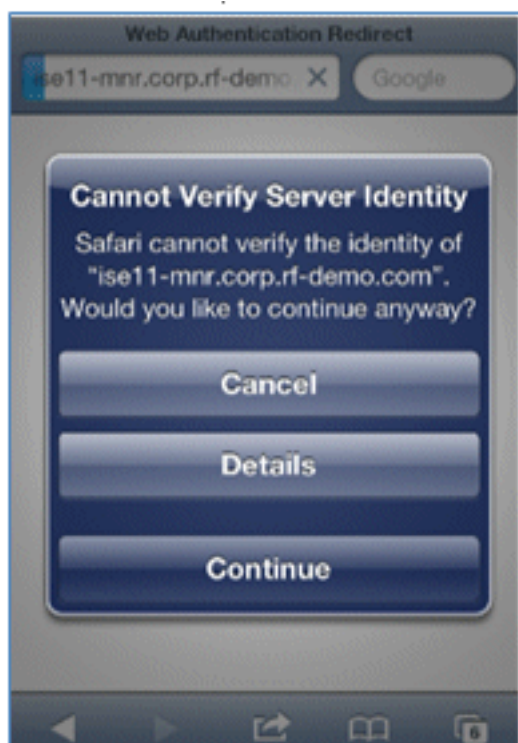
Esta seção aborda o SSID duplo e descreve como conectar-se ao convidado a ser provisionado e como conectar-se a uma WLAN 802.1x.

Conclua estas etapas para provisionar o iOS no cenário de SSID duplo:

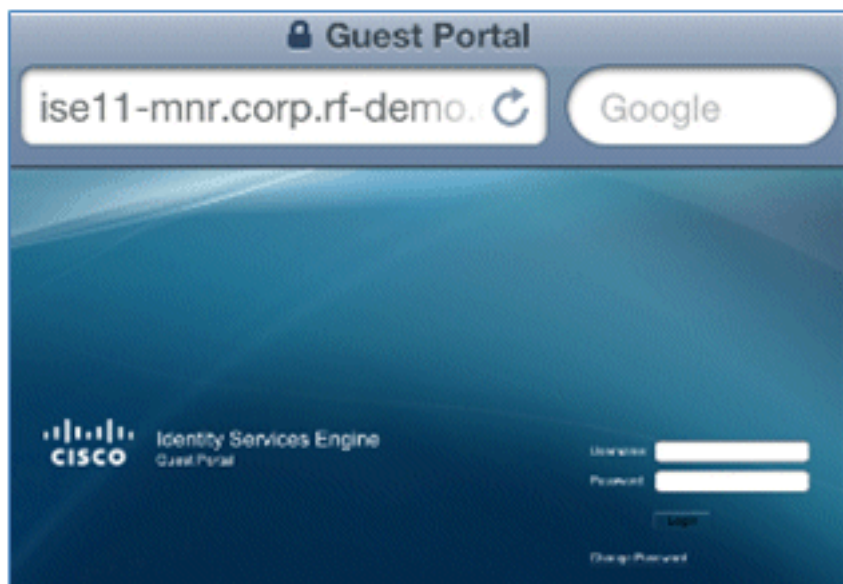
1. No dispositivo iOS, vá para **Wi-Fi Networks** e selecione **DemoCWA** (WLAN aberta configurada no WLC).



2. Abra o navegador Safari no dispositivo iOS e visite um URL acessível (por exemplo, servidor web interno/externo). O ISE o redireciona para o portal. Clique em **Continuar**.



3. Você será redirecionado ao Portal do Convidado para fazer login.



4. Faça login com uma conta de usuário e senha do AD. Instale o CA Profile quando solicitado.



5. Clique em **Instalar** certificado confiável do servidor de autoridade de certificação.



6. Clique em **Done** quando o perfil estiver completamente instalado.



7. Retorne ao navegador e clique em **Registrar**. Anote a ID do dispositivo que contém o endereço MAC do dispositivo.



8. Clique em **Install** para instalar o perfil verificado.



9. Clique em **Instalar agora**.



10. Após a conclusão do processo, o perfil do WirelessSP confirma que o perfil está instalado. Clique em **Concluído**.



11. Vá para **Wi-Fi Networks** e altere a rede para **Demo1x**. Seu dispositivo agora está conectado e usa TLS.

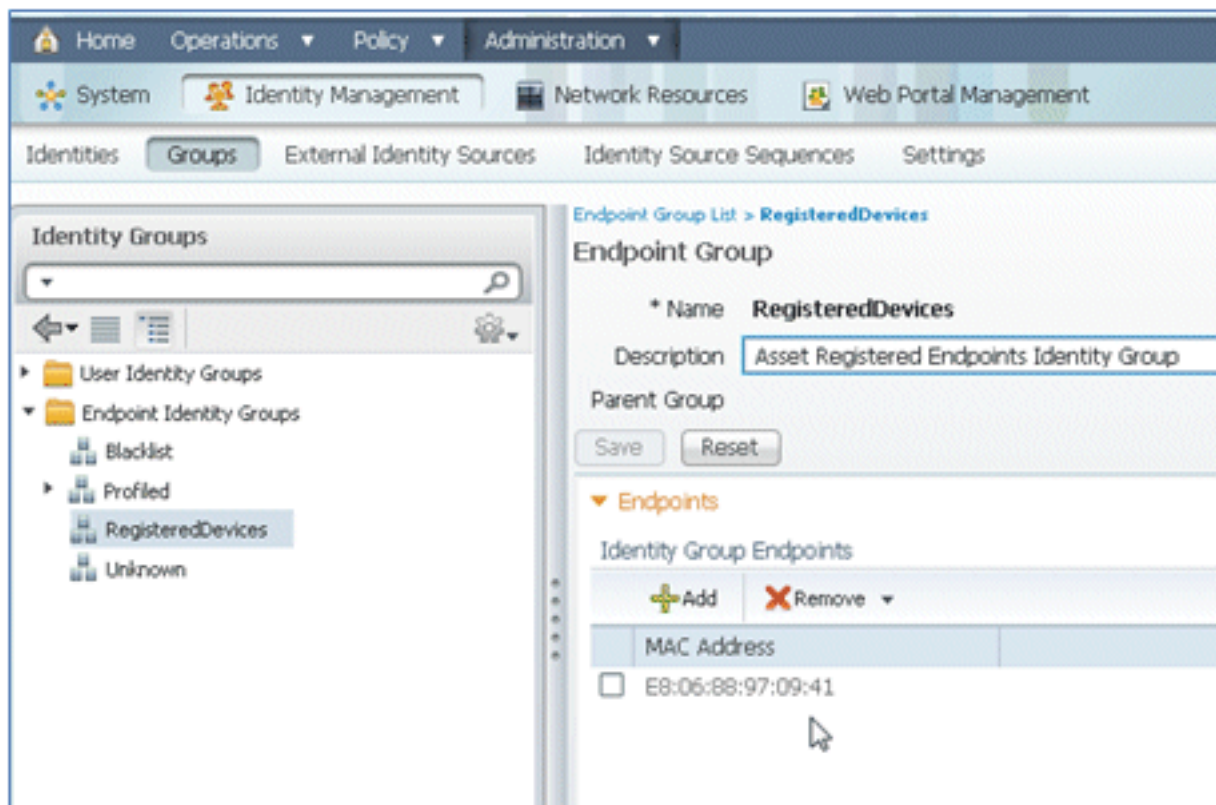


12. No ISE, navegue até **Operações > Autenticações**. Os eventos mostram o processo no qual o dispositivo está conectado à rede de convidado aberta, passa pelo processo de registro com provisionamento do solicitante e tem permissão de acesso após o registro.

Time	Status	Details	Identity	Endpoint ID	Network Device	Authorization Profile	Identity Group	Posture Status	Event
Mar 25, 12 12:27:57.052 AM	✓	🔒	paul	EB-06-98-97-09-41	WLC	PermitAccess	RegisteredDevices	NotApplicable	Authentication succeeded
Mar 25, 12 12:27:21.714 AM	✓	🔒	EB-06-98-97-09-41	EB-06-98-97-09-41	WLC	CWA	RegisteredDevices	Pending	Authentication succeeded
Mar 25, 12 12:27:20.438 AM	✓	🔒			WLC				Dynamic Authorization succeeded
Mar 25, 12 12:26:56.187 AM	✓	🔒	paul	EB-06-98-97-09-41	WLC	CWA	Any,Profiled-Apple-iPad	Pending	

13. Navegue até ISE > Administração > Gerenciamento de identidades > Grupos > Grupos de

identidade de endpoint > Dispositivos registrados. O endereço MAC foi adicionado ao banco de dados.

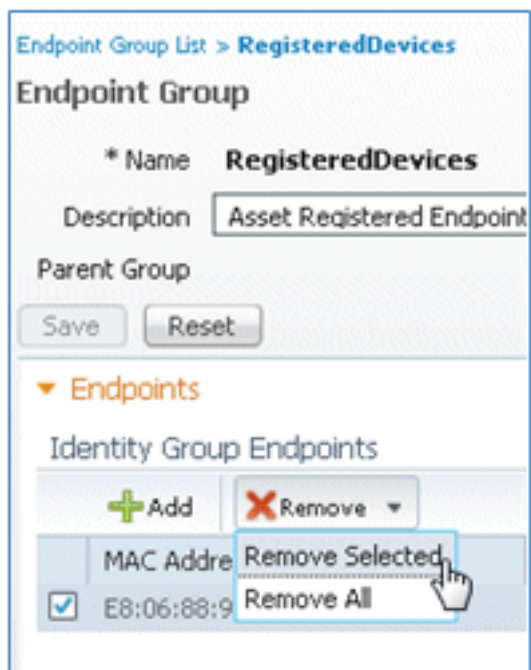


SSID único

Esta seção aborda o SSID único e descreve como se conectar diretamente a uma WLAN 802.1x, fornecer nome de usuário/senha do AD para autenticação PEAP, provisionar por meio de uma conta de convidado e reconectar com TLS.

Conclua estas etapas para provisionar o iOS no cenário de SSID único:

1. Se você estiver usando o mesmo dispositivo iOS, remova o ponto de extremidade dos Dispositivos registrados.



2. No dispositivo iOS, navegue para **Configurações > Gerais > Perfis**. Remova os perfis instalados neste exemplo.



3. Clique em **Remove** para remover os perfis anteriores.



4. Conecte-se diretamente ao 802.1x com o dispositivo existente (limpo) ou com um novo dispositivo iOS.
5. Conecte-se a **Dot1x**, insira um nome de usuário e uma senha e clique em **Ingressar**.



6. Repita as etapas 90 e seguintes na seção [Configuração do ISE](#) até que os perfis

apropriados estejam completamente instalados.

7. Navegue até **ISE > Operations > Authentications** para monitorar o processo. Este exemplo mostra o cliente que está conectado diretamente à WLAN 802.1X quando é provisionado, desconecta e reconecta à mesma WLAN com o uso de TLS.

Time	Status	Details	Identity	Endpoint ID	Network Device	Authorization Profiles	Identity Group	Posture Status	Event
Mar 25,12 12:40:03.593 AM	Success		paul	EB:06:98:97:09:41	WLC	PermitAccess	RegisteredDevices	NotApplicable	Authentication succeeded
Mar 25,12 12:39:53.353 AM	Success		EB:06:98:97:09:41	EB:06:98:97:09:41	WLC	CWA	RegisteredDevices	Pending	Authentication succeeded
Mar 25,12 12:39:08.967 AM	Success		paul	EB:06:98:97:09:41	WLC	Provision	RegisteredDevices	Pending	Authentication succeeded

8. Navegue para **WLC > Monitor > [Client MAC]**. Nos detalhes do cliente, observe que o cliente está no estado EXECUTAR, sua Comutação de dados está definida como local e a Autenticação é Central. Isso vale para clientes que se conectam ao AP FlexConnect.

Time	Status	Details	Identity	Endpoint ID	Network Device	Authorization Profiles	Identity Group	Posture Status	Event
Mar 25,12 12:40:03.593 AM	Success		paul	EB:06:98:97:09:41	WLC	PermitAccess	RegisteredDevices	NotApplicable	Authentication succeeded
Mar 25,12 12:39:53.353 AM	Success		EB:06:98:97:09:41	EB:06:98:97:09:41	WLC	CWA	RegisteredDevices	Pending	Authentication succeeded
Mar 25,12 12:39:08.967 AM	Success		paul	EB:06:98:97:09:41	WLC	Provision	RegisteredDevices	Pending	Authentication succeeded

Experiência do usuário - Provisionamento do Android

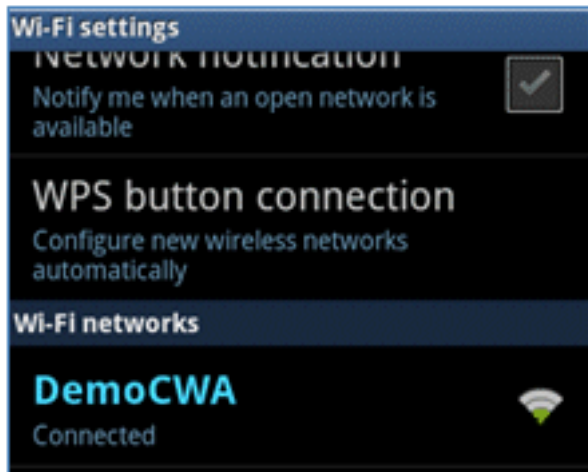
SSID duplo

Esta seção aborda o SSID duplo e descreve como conectar-se ao convidado a ser provisionado e como conectar-se a uma WLAN 802.1x.

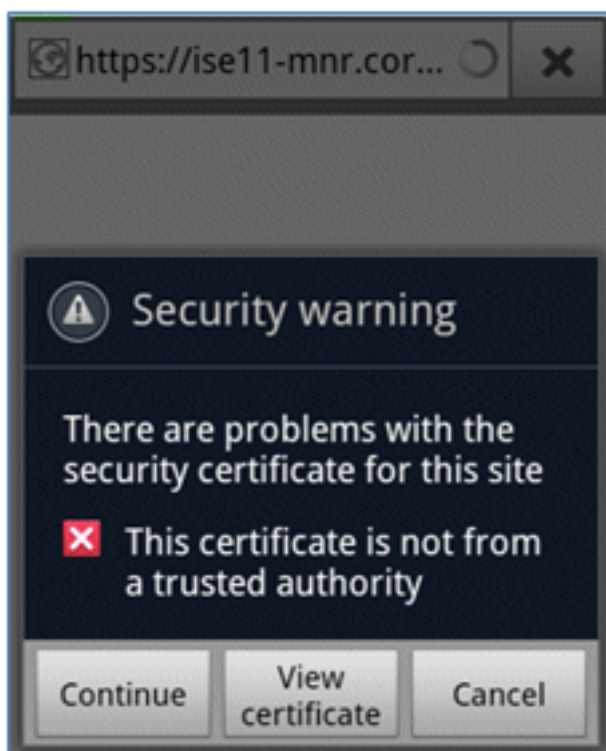
O processo de conexão para o dispositivo Android é muito semelhante ao de um dispositivo iOS (SSID único ou duplo). No entanto, uma diferença importante é que o dispositivo Android requer acesso à Internet para acessar o Google Marketplace (agora Google Play) e baixar o agente suplicante.

Conclua estes passos para provisionar um dispositivo Android (como o Samsung Galaxy neste exemplo) no cenário SSID duplo:

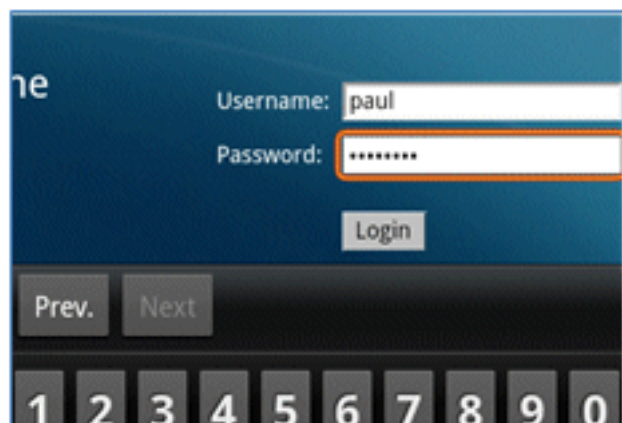
1. No dispositivo Android, use Wi-Fi para se conectar ao **DemoCWA** e abra a WLAN de convidado.



2. Aceite qualquer certificado para se conectar ao ISE.

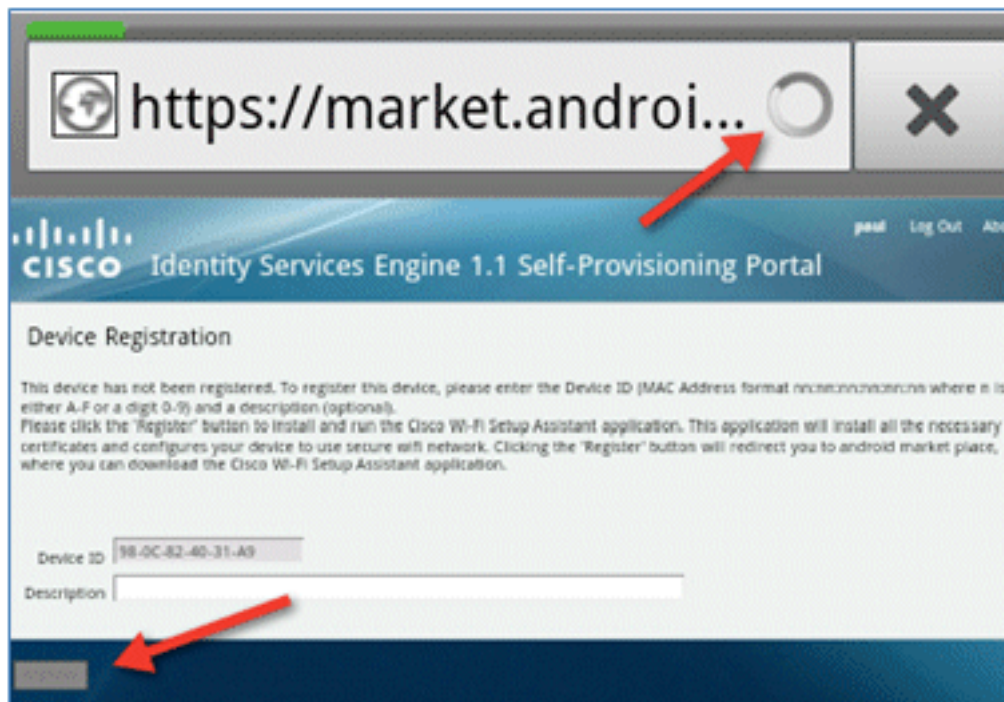


3. Insira um nome de usuário e uma senha no Portal do convidado para fazer login.

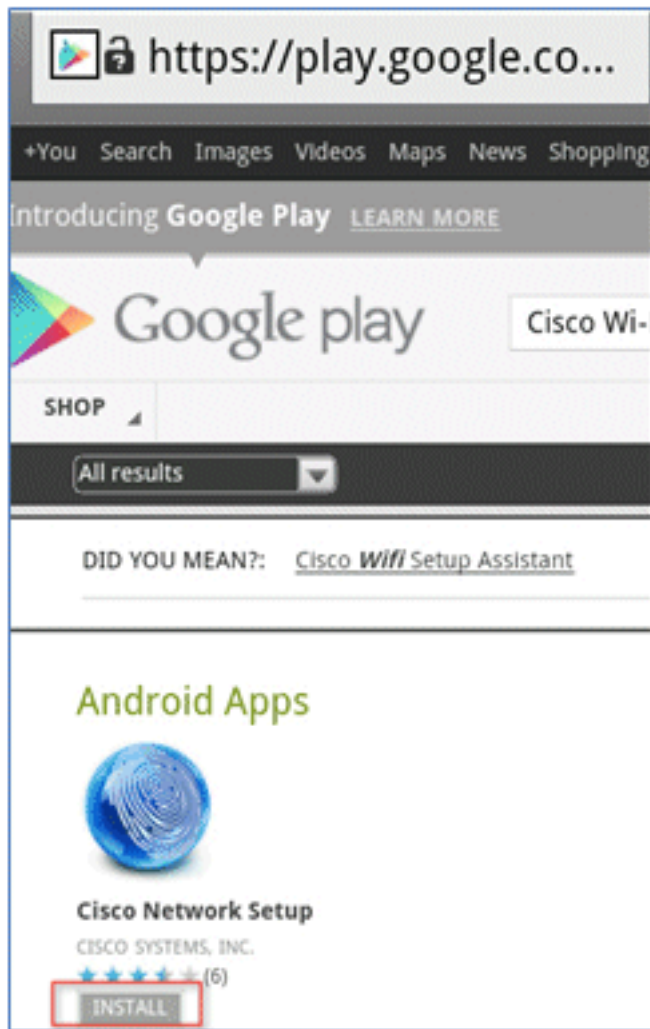


4. Clique em **Registrar**. O dispositivo tenta acessar a Internet para acessar o Google

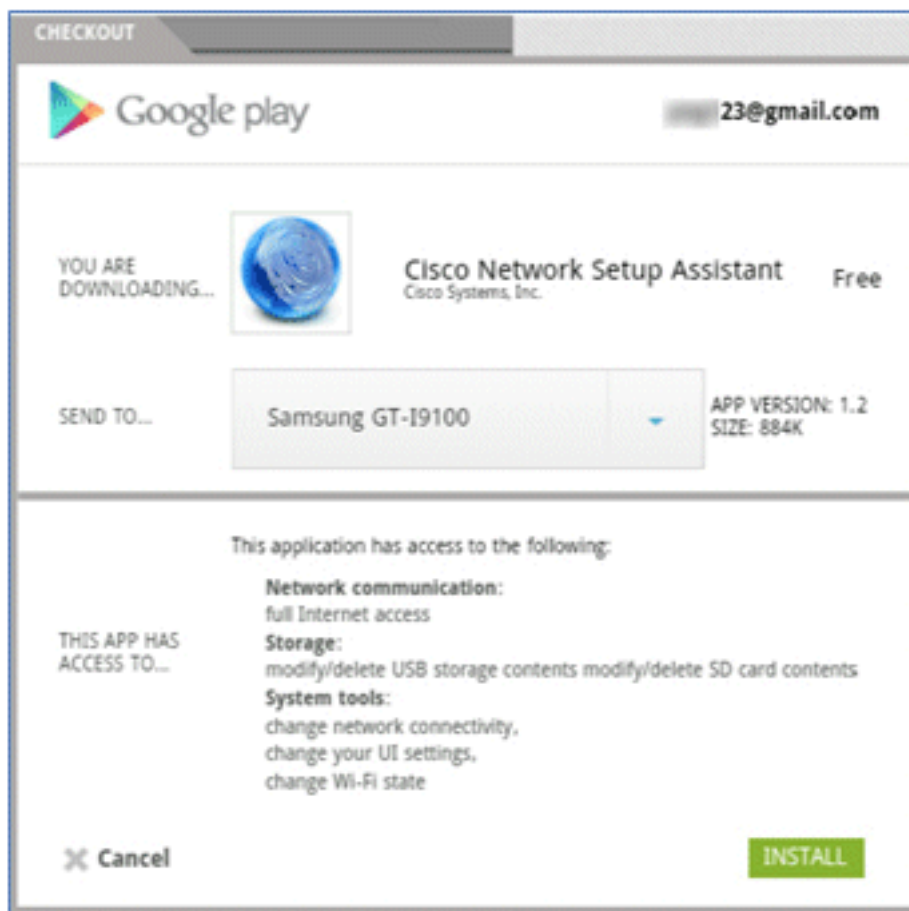
Marketplace. Adicione quaisquer regras adicionais à ACL de pré-autenticação (como ACL-REDIRECT) no controlador para permitir o acesso à Internet.



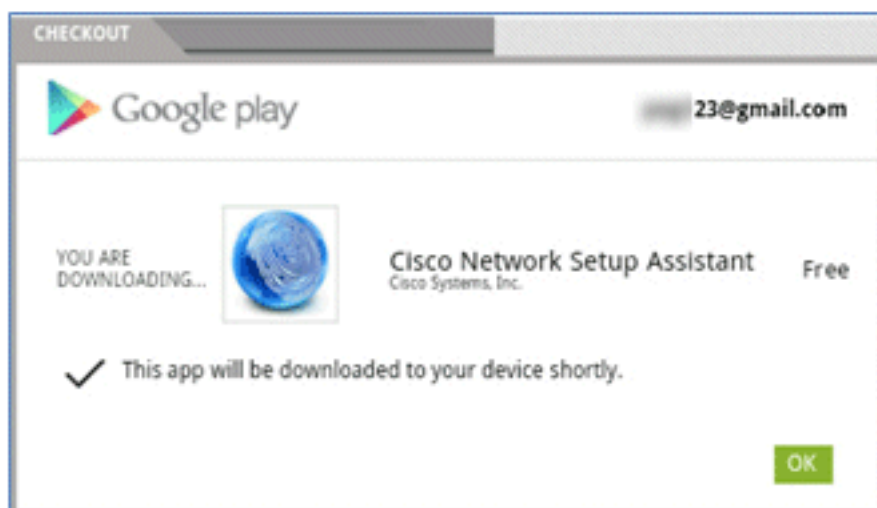
5. O Google lista a configuração de rede da Cisco como um aplicativo Android. Clique em Instalar.



6. Entre no Google e clique em **INSTALAR**.



7. Click OK.



8. No dispositivo Android, localize o aplicativo Cisco SPW instalado e abra-o.



9. Verifique se você ainda está conectado ao Portal do convidado em seu dispositivo Android.

10. Clique em **Iniciar** para iniciar o Assistente de configuração Wi-Fi.



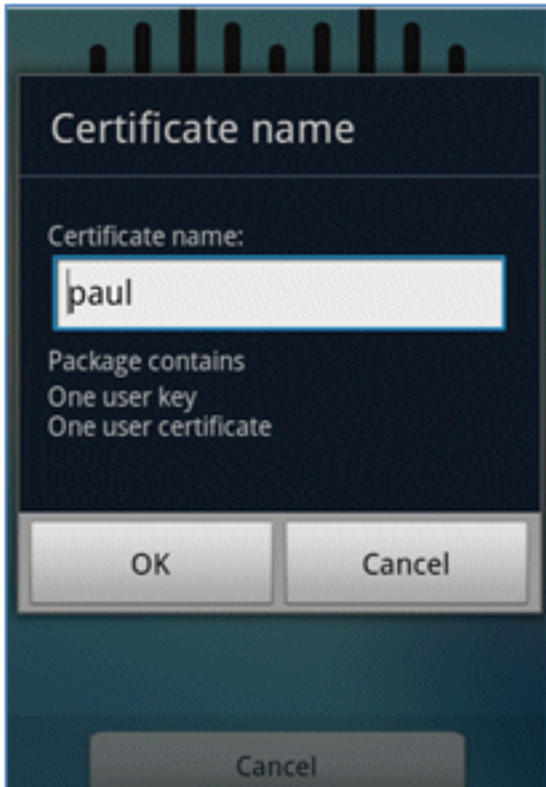
11. O Cisco SPW começa a instalar certificados.



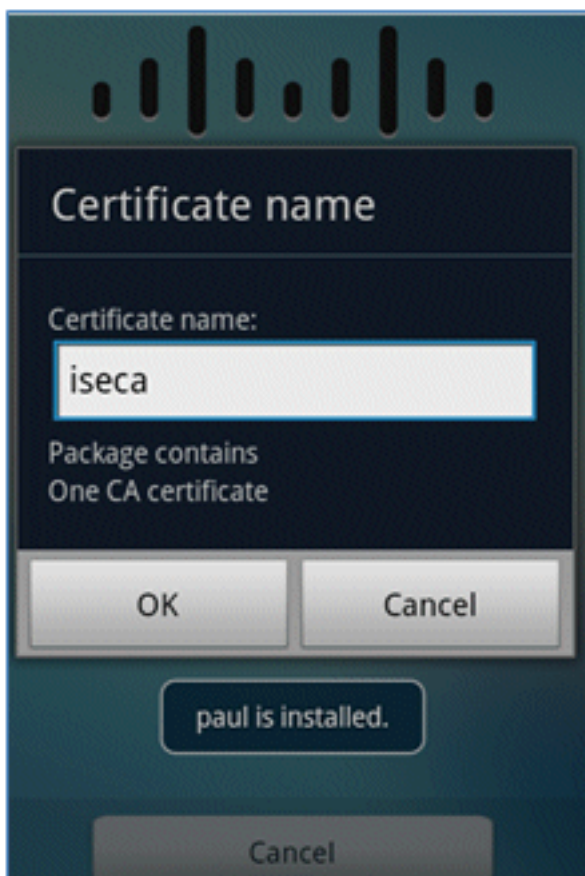
12. Quando solicitado, defina uma senha para o armazenamento de credenciais.



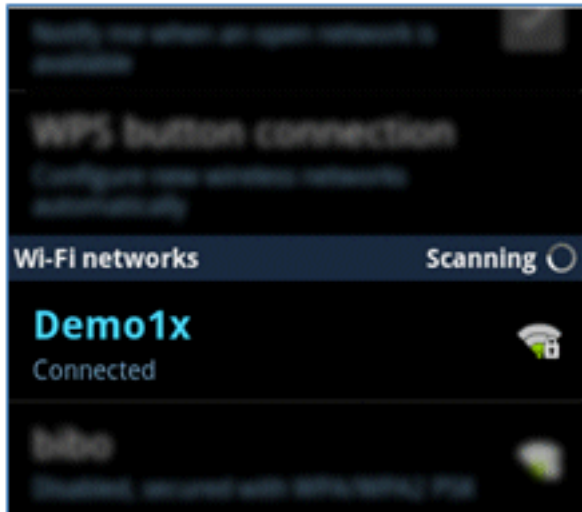
13. O Cisco SPW retorna com um nome de certificado, que contém a chave do usuário e o certificado do usuário. Clique em **OK para confirmar**.



14. O Cisco SPW continua e solicita outro nome de certificado, que contém o certificado CA. Insira o nome **iseca** (neste exemplo) e clique em **OK** para continuar.



15. O dispositivo Android agora está conectado.

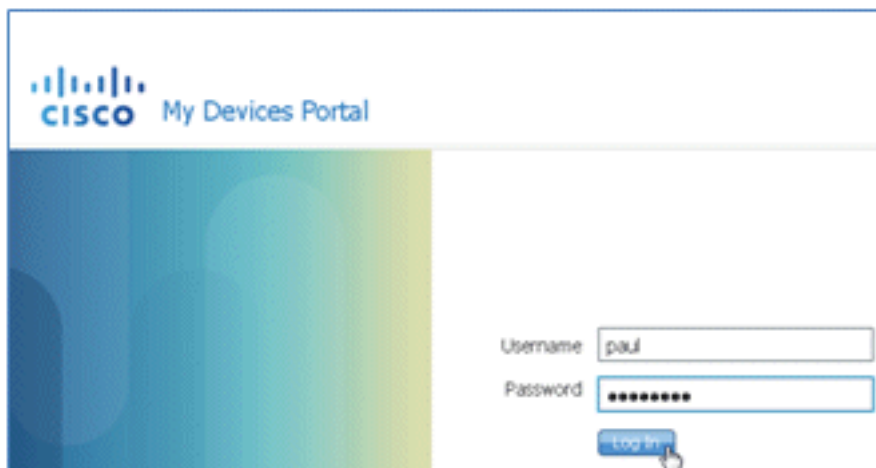


Portal Meus dispositivos

O portal Meus dispositivos permite que os usuários façam uma lista negra de dispositivos registrados anteriormente caso um dispositivo seja perdido ou roubado. Ele também permite que os usuários se reinscrevam, se necessário.

Conclua estes passos para fazer uma lista negra de um dispositivo:

1. Para fazer login no portal Meus dispositivos, abra um navegador, conecte-se a <https://ise-server:8443/mydevices> (observe o número de porta 8443) e faça login com uma conta do AD.



2. Localize o dispositivo em ID do dispositivo e clique em **Lost?** para iniciar a lista negra de um dispositivo.

Add a New Device

To add a device, please enter the Device ID (MAC Address) and a description (optional); then click submit to add the device.

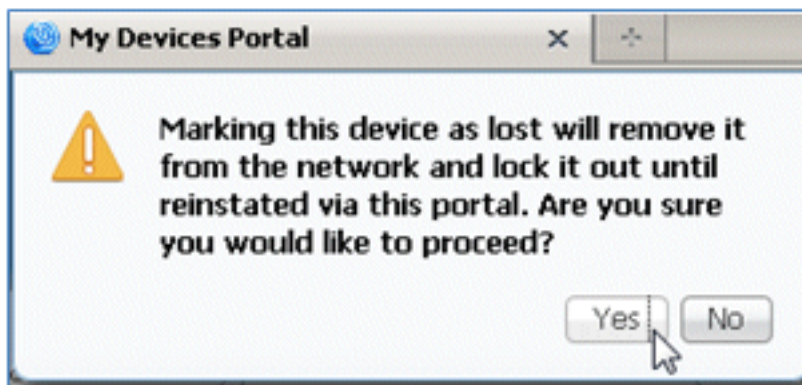
* Device ID

Description

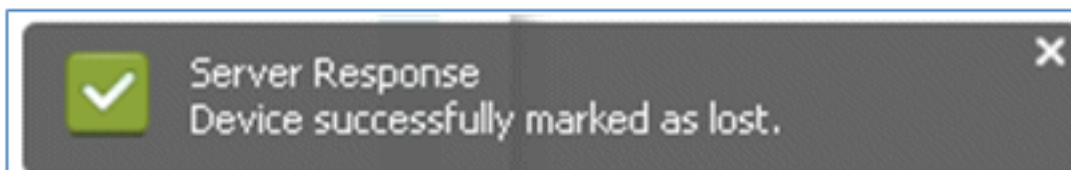
Your Devices

State	Device ID	Description	Action
	EB:06:88:97:09:41		Edit Log2

3. Quando o ISE solicitar um aviso, clique em **Yes** para continuar.



4. O ISE confirma que o dispositivo está marcado como **perdido**.



5. Qualquer tentativa de se conectar à rede com o dispositivo registrado anteriormente será bloqueada agora, mesmo que haja um certificado válido instalado. Este é um exemplo de um dispositivo na lista negra que falha na autenticação:

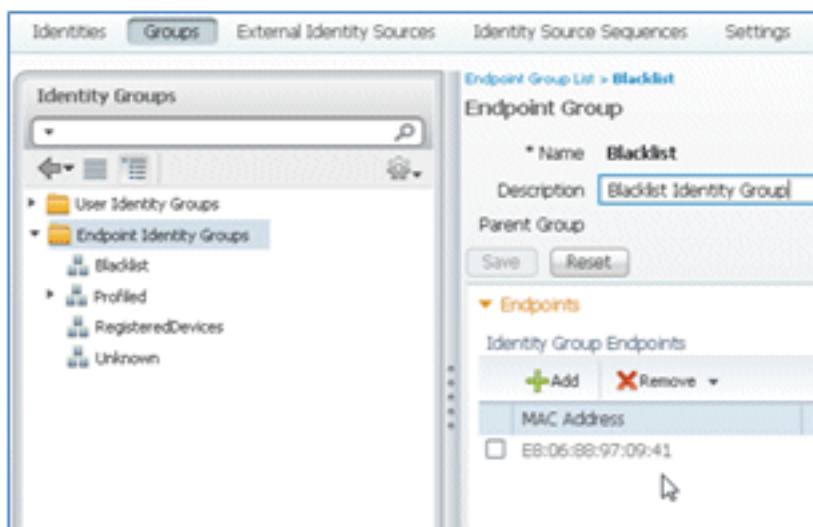
Live Authentications

Refresh: Every 3 seconds | Show: Latest 20 records

Time	Status	Details	Identity	Endpoint ID	Network Device	Authorization Profiles	Identity Group	Posture Status	Event
Mar 25, 12:49:07.851 AM	Failed	pxd		EB:06:88:97:09:41	WLC	Blacklist_Access	Blacklist		Authentication failed
Mar 25, 12:48:59.057 AM	Failed		EB:06:88:97:09:41	EB:06:88:97:09:41	WLC	Blacklist_Access	Blacklist		Authentication failed
Mar 25, 12:48:54.137 AM	Failed			EB:06:88:97:09:41	WLC	Blacklist_Access	Blacklist		Authentication failed

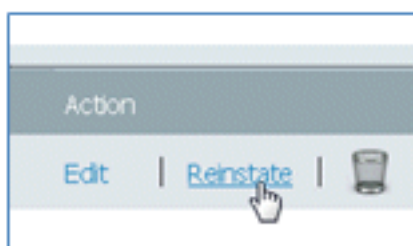
6. Um administrador pode navegar para ISE > Administração > Gerenciamento de identidades > Grupos, clicar em Grupos de identidade de endpoint > Lista negra e ver se o dispositivo

está na lista negra.

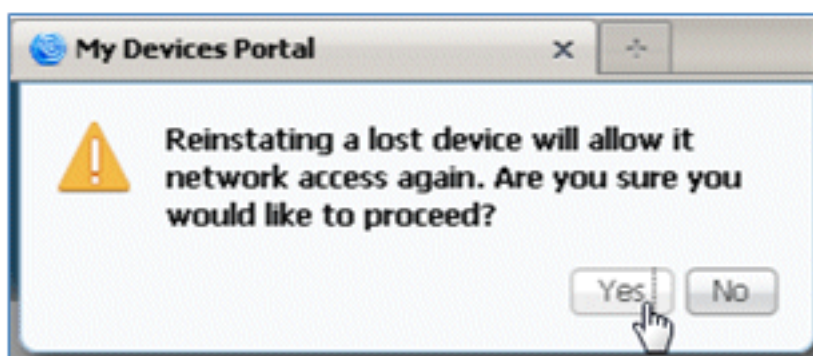


Conclua estes passos para reintegrar um dispositivo na lista negra:

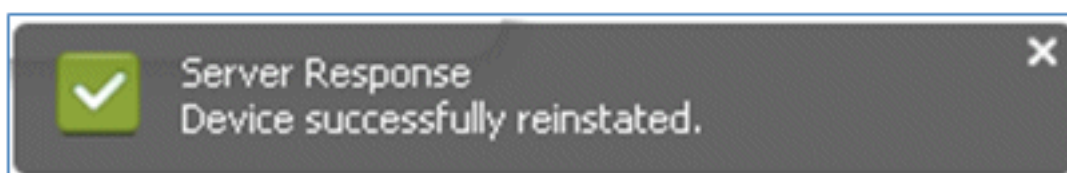
1. No portal Meus dispositivos, clique em **Reintegrar** para esse dispositivo.



2. Quando o ISE solicitar um aviso, clique em **Yes** para continuar.



3. O ISE confirma que o dispositivo foi restabelecido com êxito. Conecte o dispositivo reintegrado à rede para testar se o dispositivo agora será permitido.

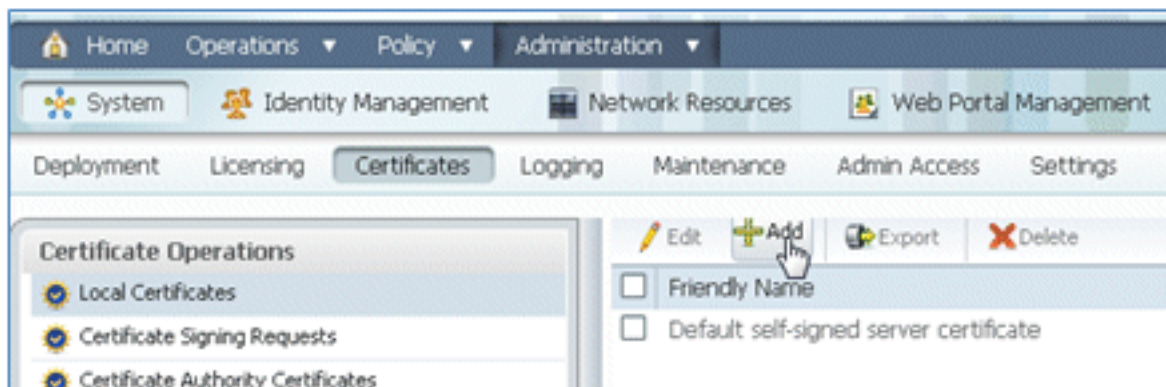


Referência - Certificados

O ISE não só requer um certificado raiz de CA válido, mas também precisa de um certificado válido assinado por CA.

Conclua estas etapas para adicionar, associar e importar o novo certificado CA confiável:

1. Navegue até ISE > Administration > System > Certificates, clique em Local Certificates e clique em Add.



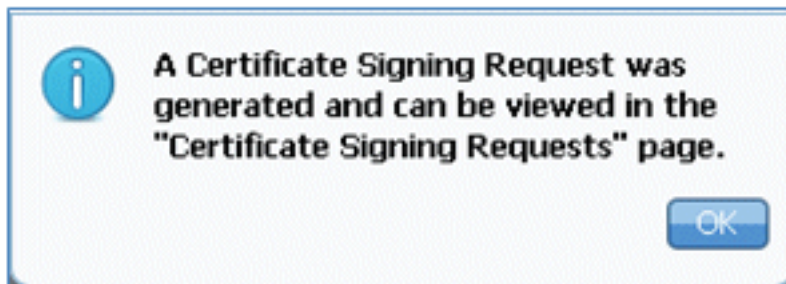
2. Selecione **Gerar CSR (Certificate Signing Request)**.



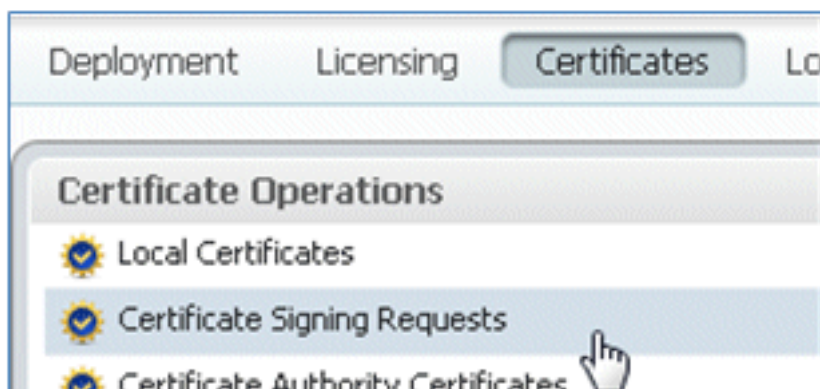
3. Insira o assunto do certificado **CN=<ISE-SERVER hostname.FQDN>**. Para os outros campos, você pode usar o padrão ou os valores exigidos pela configuração da CA. Clique em Submit.



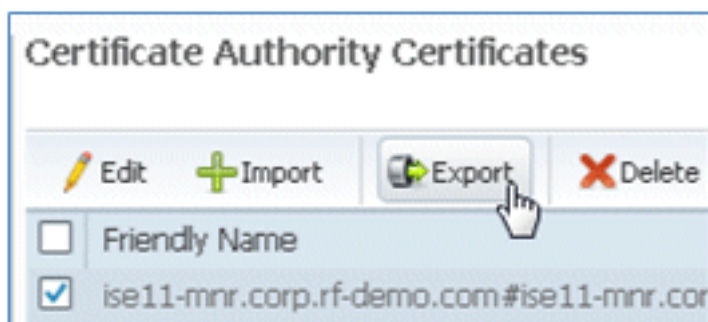
4. O ISE verifica se o CSR foi gerado.



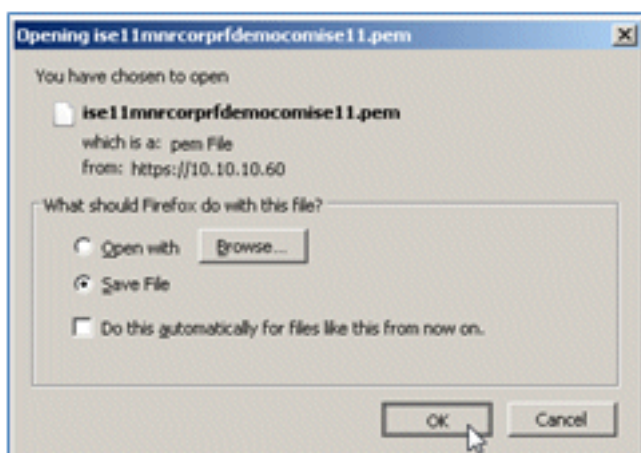
5. Para acessar o CSR, clique nas operações **Certificate Signing Requests**.



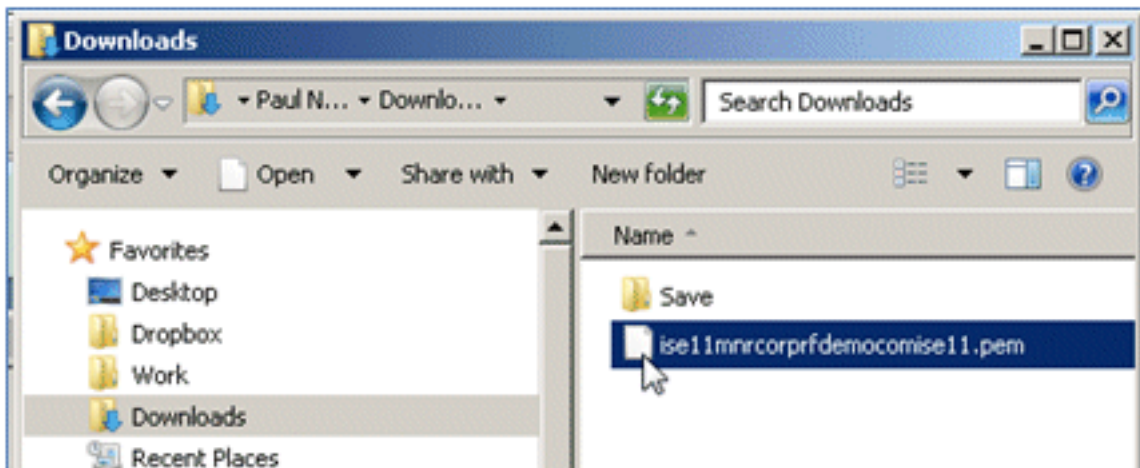
6. Selecione o CSR criado recentemente e clique em **Export**.



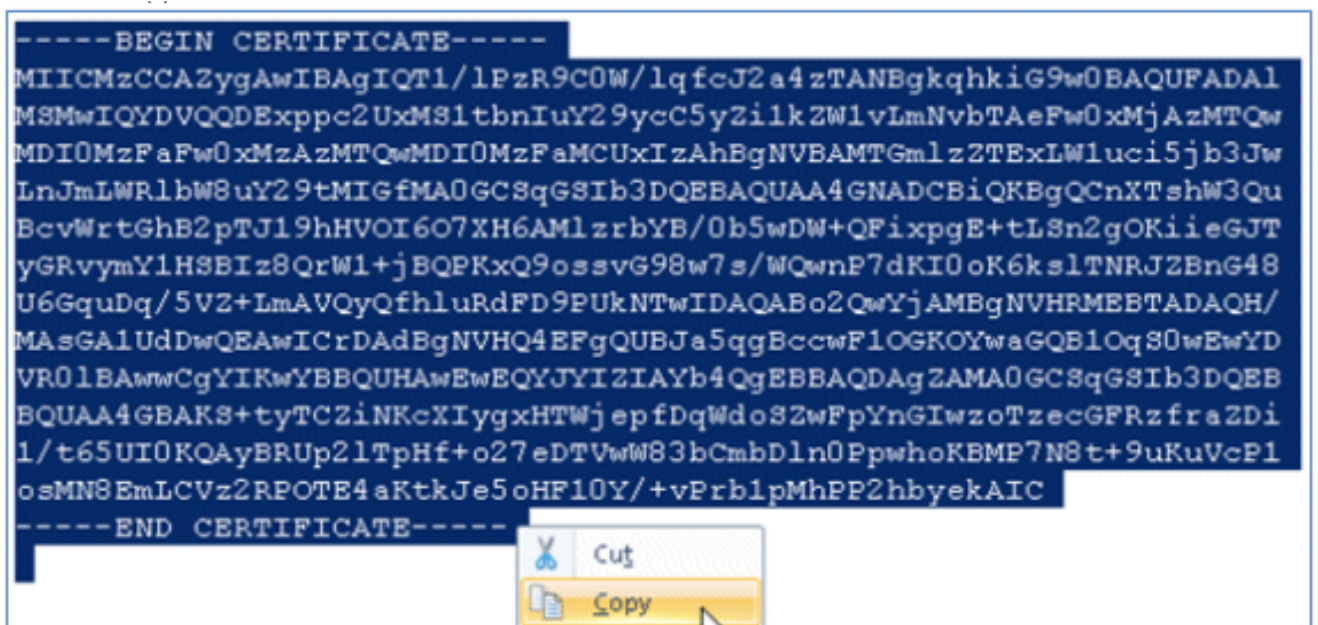
7. O ISE exporta o CSR para um arquivo .pem. Clique em **Save File** e, em seguida, clique em **OK** para salvar o arquivo na máquina local.



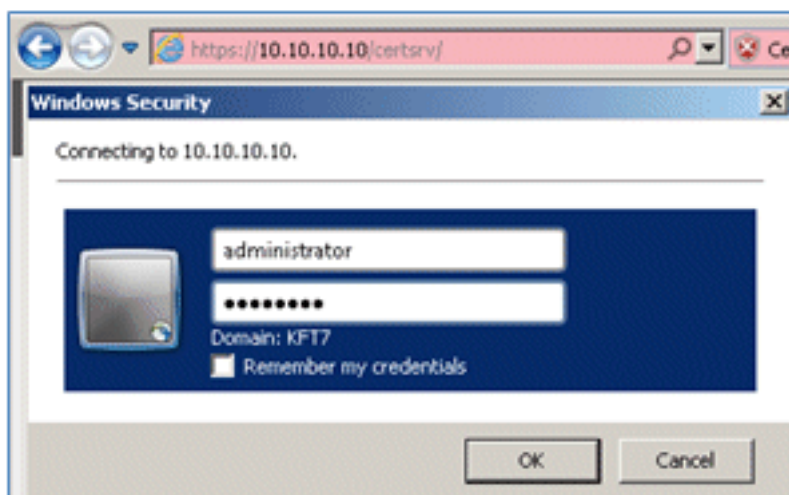
8. Localize e abra o arquivo de certificado do ISE com um editor de texto.



9. Copiar todo o conteúdo do certificado.



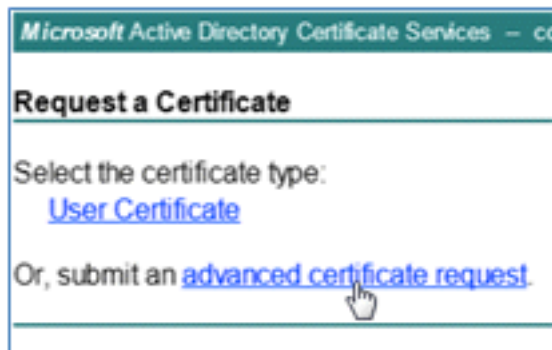
10. Conecte-se ao servidor da autoridade de certificação e faça login com uma conta de administrador. O servidor é uma autoridade de certificação Microsoft 2008 em <https://10.10.10.10/certsrv> (neste exemplo).



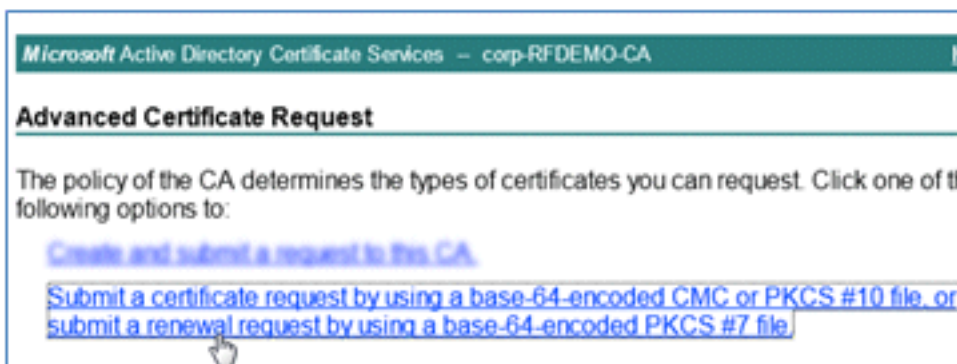
11. Clique em **Solicitar um certificado**.



12. Clique em **solicitação de certificado avançado**.



13. Clique na segunda opção para **Enviar uma solicitação de certificado usando um CMC codificado na base 64 ou ...**



14. Cole o conteúdo do arquivo de certificado do ISE (.pem) no campo Solicitação salva, verifique se o Modelo de certificado é **Servidor Web** e clique em **Enviar**.

Microsoft Certificate Services -- labsrv.corp.rf-demo.com

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CM Saved Request box.

Saved Request:

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

```
MAAGAlUdDwQEAvICrDAdBgNVHQ4EFgQUBJa5qgBc
VRO1BAwvCgYIKwYBBQUHAWewEQYJYIZIAAYb4QgEB
BQUAA4GBAKS+tyTCZ1NKcXIyqxHTWjepfDqVdoS2
1/t6SUIOKQayBRUp21TpHf+o27eDTVwW83bCmbD1
oaMNBEmLCVz2RPOTE4aKtkJe5oHF10Y/+vPrb1pM
-----END CERTIFICATE-----
```

Certificate Template:

Web Server

Additional Attributes:

Attributes:

Submit >


15. Clique em **Download certificate**.

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

Certificate Issued

The certificate you requested was issued to you.

DER encoded or Base 64 encoded

 [Download certificate](#)

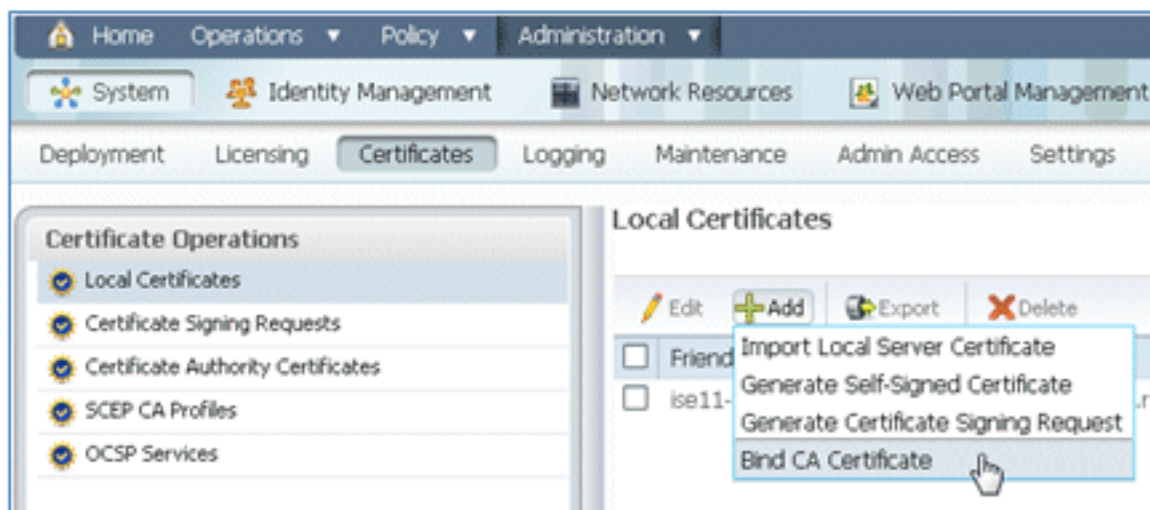
[Download certificate chain](#)

16. Salve o arquivo certnew.cer; ele será usado mais tarde para vincular-se ao ISE.

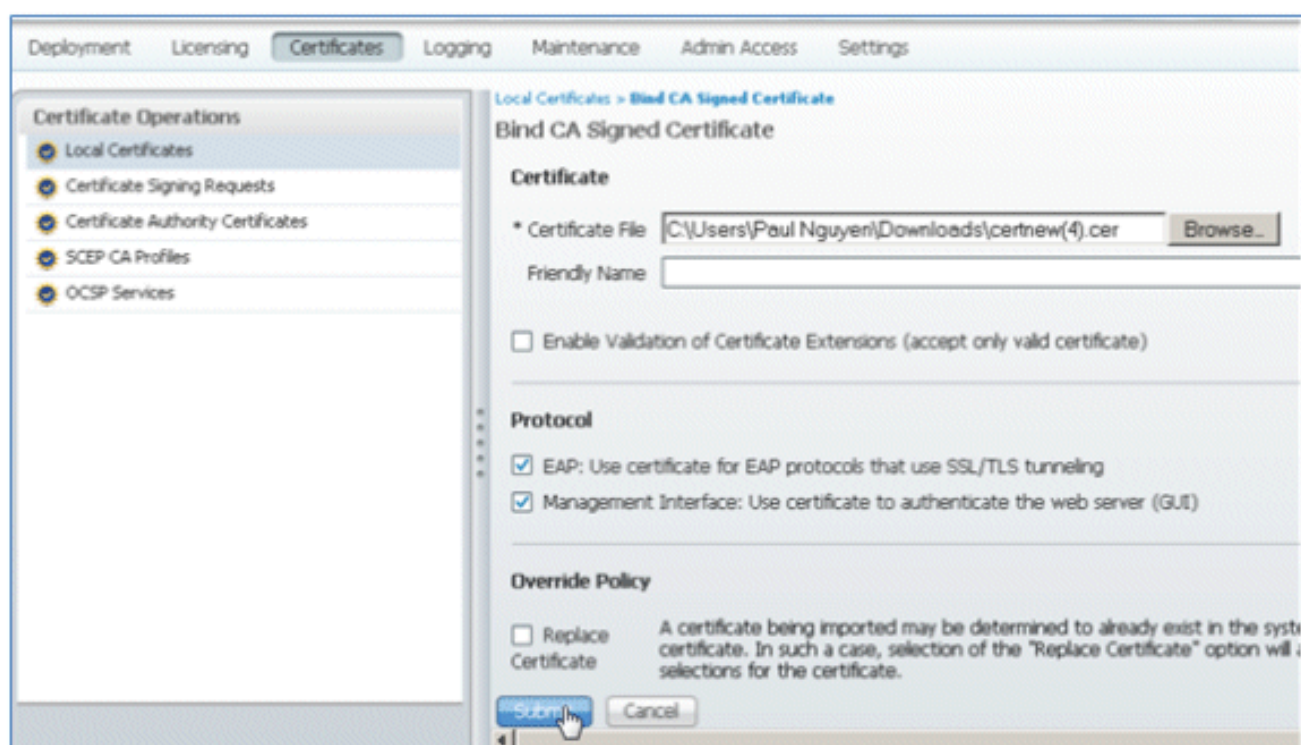
Do you want to open or save certnew.cer (921 bytes) from 10.10.10.10?

Open Save

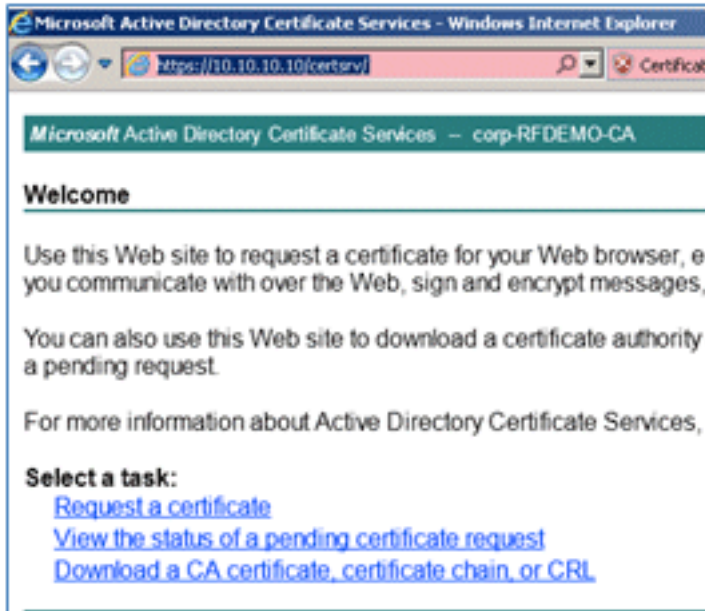
17. Em **Certificados ISE**, navegue para **Certificados locais** e clique em **Adicionar > Vincular certificado CA**.



18. Navegue até o certificado que foi salvo na máquina local na etapa anterior, ative os protocolos **EAP** e **Management Interface** (as caixas estão marcadas) e clique em **Submit**. O ISE pode levar vários minutos ou mais para reiniciar os serviços.



19. Retorne à página inicial da CA (<https://CA/certsrv/>) e clique em **Download a CA certificate, certificate chain, or CRL**.



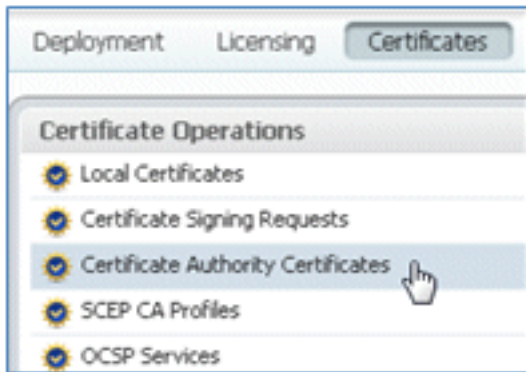
20. Clique em **Baixar certificado de CA**.



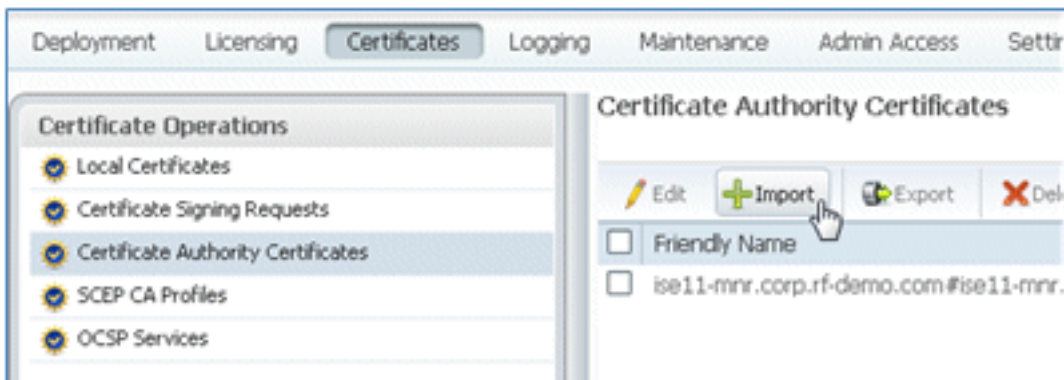
21. **Salve** o arquivo na máquina local.



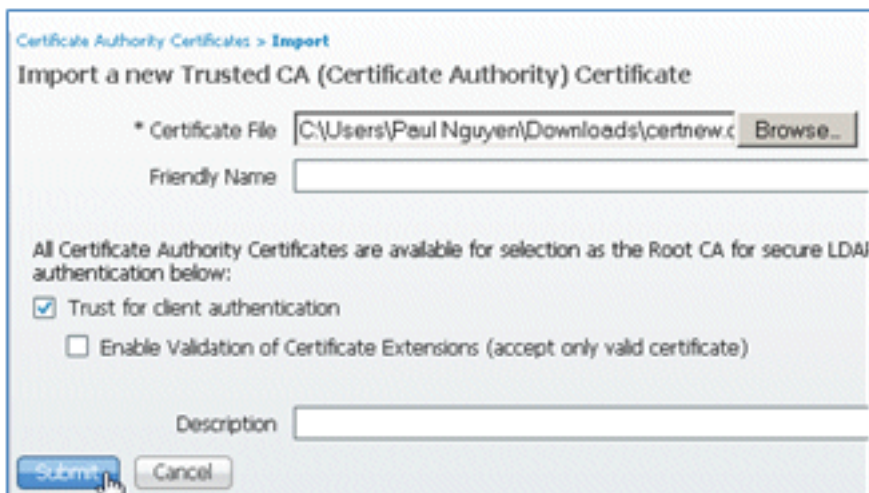
22. Com o servidor ISE on-line, vá para **Certificates** e clique em **Certificate Authority Certificates**.



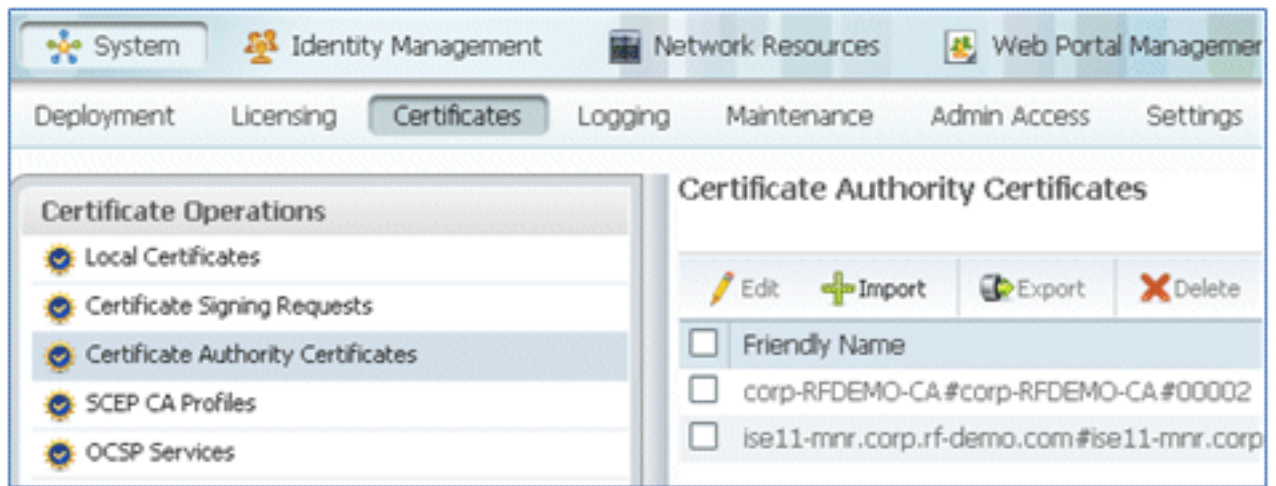
23. Clique em **Importar**.



24. Procure o certificado da autoridade de certificação, habilite **Confiar para autenticação do cliente** (caixa marcada) e clique em **Enviar**.



25. Confirme se o novo certificado CA confiável foi adicionado.



Informações Relacionadas

- [Guia de Instalação de Hardware do Cisco Identity Services Engine, Versão 1.0.4](#)
- [Cisco 2000 Series Wireless LAN Controllers](#)
- [Cisco 4400 Series Wireless LAN Controllers](#)
- [Cisco Aironet 3500 Series](#)
- [Guia de implantação do controlador sem fio de ramificações Flex 7500](#)
- [Traga seu próprio dispositivo - Autenticação de dispositivo unificada e experiência de acesso consistente](#)
- [BYOD sem fio com Identity Services Engine](#)
- [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.