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 Ative Diretory (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 <u>Release Notes for Cisco Wireless LAN Controllers and Lightweight</u> <u>Access Points for Release 7.2.110.0</u> 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 <u>FlexConnect Feature Matrix</u> 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.

	MONITOR	<u>W</u> LANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP EEEOBA	cĸ
Security	RADIUS	Authentic	ation Serve	rs					
AAA General RADIUS Authentication Accounting Fallback TACACS+ LDAP Local Met Linese	Call Stat Use AES MAC De Network User	ion ID Type ¹ Key Wrap Imiter Managemen	System M (Designed Hyphen Server t Index	AC Address 1 for FIPS custome	rs and require	es a key wrap comp	oliant RADIUS se	rver) Admin Status	
MAC Filtering Disabled Clients	۲	۲	1	10.10.10.60	1812	D	sabled	Enabled	

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	FEEDBAC
RADIUS Authent	ication Server	s > Edit					
Server Index		1					
Server Address		10.10.10.60					
Shared Secret Form	at	ASCII :					
Shared Secret							
Confirm Shared Sec	ret						
Key Wrap	0	(Designed fo	r FIPS custom	ers and requires a l	key wrap complia	nt RADIU	S server)
Port Number		1812					
Server Status		Enabled :					
Support for RFC 357	76	Enabled :					
Server Timeout		2 second	ds				
Network User		Enable					
Management		Enable					
IPSec		Enable					

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

IANA	SECURITY	WIRELESS	ROLLER	22	WLANS	MONITOR
		Edit	ervers >	ting	Account	RADIUS
			4		22	201-10125
			1		dex	Server In
		0.10.60	10.10		dress	Server Ad
		tI +	ASC	at	ecret Forma	Shared S
					ecret	Shared S
				ret	shared Seco	Confirm S
			1813		ber	Port Num
		bled :	Enal		atus	Server St
		seconds	2		meout	Server Ti
		able	Er Er		User	Network
		Enable				IPSec
		seconds nable Enable	••• 1813 Enal 2 S Er	ret	ihared Secr ber atus meout User	Confirm S Port Num Server St Server Til Network IPSec

 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).

cisco		<u>W</u> LANs		WIF
Security	FlexConr	nect Acc	ess Control Li	sts
 AAA Local EAP Priority Order Certificate 	Acl Name	ECT		
Access Control Lists Access Control Lists CPU Access Control Lists FlexConnect ACLs Wireless Protection Policies				

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	1		
Source	Any :		
		IP Address	Netmask
Destination	IP Address ‡	10.10.10.60	255.255.255.255
Protocol	Any :		
DSCP	Any ÷		
Direction	Any ÷		
Action	Permit ‡		

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

Gene	ral										
Access	s List Name	ACL-RED	IR	ECT							
Seq	Action	Source IP/Mask	:	Destination IP/Mask		Protocol	Source Port	Dest Port	DSC	P	
1	Permit	0.0.0.0 0.0.0.0	/	10.10.10.60 255.255.255.255	/	Any	Any	Any	Any		•
2	Permit	10.10.10.60 255.255.255.255	1	0.0.0.0	1	Any	Any	Any	Any		

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**.

ululu cisco	MONITOR WLANS CONTROLLER WORELESS SECURITY MANAGEMENT COMMANDS HELP EEEDD	Sage Configuration Eing Logout Bef ACK
Wireless	FlexConnect Groups > Edit 'Flex1'	< Back Apply
Access Points All APs Redios 802.11a/n 802.11b/g/n Global Configuration Advanced Mesh RF Profiles FlexConnect Groups Meximize Accs 802.11a/n 802.11b/g/n Media Stream	General Local Authentication Image Upgrade VLAN-ACL mapping WLAN-ACL mapping WebPolicies	WebPolicies

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.

WLANs > E	dit 'Demo	CWA'	
General	Security	QoS	Advanced
Profile Na	me	DemoC	WA
Туре		WLAN	
SSID		DemoC	WA
Status		F Enab	led
Security F	Policies	MAC F (Modifica	iltering tions done under se
Radio Poli	icy	All	
Interface/ Group(G)	/Interface	manage	ement 💌
Multicast	Vlan Feature	Enabl	led
Broadcast	t SSID	F Enabl	led

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)

Layer 2	Layer 3	AAA S	ervers
			y- 103
act Tuan	sition		

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

Servidores de Autenticação e Conta: HabilitadoServidor 1: <endereço IP do ISE>

Layer 2 Layer 3	AAA Servers
Select AAA servers below	to override use of default servers on this WLAN
Radius Servers	
Radius Server Overwrite	e interface Enabled
Radius Server Overwrit	e interface Enabled Authentication Servers Accounting Servers Enabled Servers
Radius Server Overwrit	e interface Enabled Authentication Servers Accounting Servers Enabled IP:10.10.10.60, Port:1812 IP:10.10.10.60, Port:1813
Radius Server Overwrit Server 1 Server 2	e interface Enabled Authentication Servers Accounting Servers Enabled IP:10.10.10.60, Port:1812 None None None

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.

Authentication prior web-auth user	ity order for	-	
Not Used LOCAL LDAP	> <	Order Used For Authentic	Up Down

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

Permitir Substituição de AAA: HabilitadoEstado do NAC: Radius NAC

Allow AAA Override	F Enabled	04629
Coverage Hole Detection	SF Enabled	DHCP Sarvar Covers
Enable Section Timeout	ge (1800 Session Timeout (secs)	DHCP Addr. Assignment C Anguin
Aironat 18	F Enabled	Nanagement Frame Protection (NFI
Diagnostic Channel	C Evabled	
Overvide Interface ACL	Pol None B (Pol None B	1979 Class Protection . Collonal
F2F Blocking Action	Considered 20	BTIN Period (in beacan intervals)
Clerit Exclusion	Citrabled	
Maximum Allowed Clients	F	802.11.wh (1 - 255) [1 802.113/p/n (1 - 255) [1
Static 3F Tunneling 🛤	L'Endlind	NAC
Wi-Fi Direct Clients Police	Doubled #	NAC State Radius NAC 💌
Recipum Allowed		Load Balancing and Band Select
Clarity Fer MP Radio	100 million	Client Load Balancing

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.

Enabled
 F manual

7. Clique em Aplicar e Salvar configuração.



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

WLANs > Edit 'Demo	1x'
General Security	QoS Advanced
Profile Name	Demoix
Туре	WLAN
SSID	Demolx
Status	Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under secu
Radio Policy	All
Interface/Interface Group(G)	management 💌
Multicast Vlan Feature	Enabled
Broadcast SSID	Enabled

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.IX: **Habilitar**

	dit 'Demo	1x'		
Seneral	Security	QoS	Advanc	ed
Layer 2	Layer 3	AAA S	ervers	
Lawar 2	Samuritu 🖣 🗍	WDA+WDA	>	
Layer 2	M	AC Filtering	2 [
Fast Trans	ition			
-	-			
Reassociatio	on Timeout 20 2 Parameter) rs		
Reassociatio WPA+WPA WPA Pol	on Timeout 20 2 Parameter	ns		
Reassociatio WPA+WPA WPA Pol WPA2 Po	on Timeout 20 2 Parameter icy blicy	rs T R		
Reassociatio WPA+WPA WPA Pol WPA2 Po WPA2 Er	on Timeout 20 2 Parameter icy blicy hcryption	rs T P AE	s En	KIP
Reassociatio WPA+WPA WPA Pol WPA2 Po WPA2 Er Authentica	on Timeout 20 2 Parameter licy blicy hcryption ition Key Ma	rs F F AE	s ⊏n t	KIP
Reassociatio WPA+WPA WPA Pol WPA2 Po WPA2 Er Authentica 802.1X	on Timeout 20 2 Parameter icy blicy hcryption ition Key Ma	rs	s ⊡π t	KIP
Reassociatio WPA+WPA WPA Pol WPA2 Po WPA2 Er Authentica 802.1X CCKM	on Timeout 20 2 Parameter icy olicy ncryption ition Key Ma F g	rs	s ⊡n t	KIP

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

Permitir Substituição de AAA: HabilitadoEstado do NAC: Radius NAC

Now AAA Override	P Enabled	84627
Coverage Hole Detection	P Enabled	DHCP Server Coveride
Inable Session Timesut	ge (1800	THE AND ADDRESS IF A
irunat IB	P Enabled	the second second second second
iagnostic Channel	Cenabled	ranagement France Fredection (NFF)
warride biterface ACL	Put Note 2 Put Note 2	1899 Classi Protection # Colored #
OF Blacking Action	Disabled B	BUILTY Period (in Annual Internals)
Sent Exclusion	Wanahad Int	
	Timeout Value (secs)	862.33.m/h (3 - 299) 3
Santa #	9	882.118/ph (1 - 298) 1
and a literation of	Ended	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>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK
WLANs								Entries 1 - 5 of 5
Current F	ilter: Nor	ne [Change	Filter] [Clear	Filter]	1	Create New	• 6	0
	ID Type	Profile Na	me	v	VLAN SSID		Admin Status	Security Policies
E 1	10,45	85×			EEH .		Disable	[#PA2[Auth(902.14)]
C 2	WLAS				1		Enabled	[WPA/][Auth(PSE)]
2	WLAN	Demo1x		C	emo1x		Enabled	[WPA2][Auth(802.1X)]
	WLAN	DemoCWA		C)emoCWA		Enabled	MAC Filtering
Γ1	90,45	fig.			le :		Disable	d 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>W</u> LANs		WIRELESS
All APs			
Current Fil	ter		None
Number o	f APs		2
AP Name		AP	Model
Site-B-Flex		AI	R-LAP1262N-A-K

2. Clique na guia FlexConnect.



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

VLAN Support	2	
Native VLAN ID	1	VLAN Mappings
FlexConnect Group Name	Not Con	figured 😡

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

	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY
All APs	> Site-B-	FlexAP > VLA	N Mapping	S
AP Nam	e	Site-B-FlexAP		
Base Ra	dio MAC	e8:04:62:0a:68:80	D	
WLAN Id	SSID			VLAN ID
3	Demo1x			21
4	DemoCW/	A		21
				1
	-			and the second se

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>.

	Identity Services Engine Uservane admin Passed Based Basenber uservane Robien koging in ³
afflates in the U.S and certain other countries.	cisco

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).

Advan	ced Settings	Groups	Attributes	
	• De	omain Name corp	.rf-demo.com	
ne or more nodes may be	selected for Join	or Leave operation	ns. If a node is joined then a leav	e operation is
connection				
아nection. 약을 Join 약을 Leave 약을 Te	est Connection 🔹			
9월 Join 9월 Leave 9월 Te 그 ISE Node	est Connection	ISE Node Role	Status	

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

oonneedon.	
👷 Join 🛛 👷 Leave	👷 Test Connection 👻
ISE Node	Basic Test
✓ ise11-mnr	Detailed Test
* User Name: paul * Password:	X Cancel

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).

CISCO Identity Services Engine	
🛕 Home Operations 🔻 Policy 🔻 Admin	istration 🔻
🔆 System 🦉 Identity Management	Network Resources 🛛 🛃 Web Portal Manage
Identities Groups External Identity Sources	Identity Source Sequences Settings
External Identity Sources	Certificate Authentication Profile
∲•	
Certificate Authentication Profile	Con Trace Co
2 Active Directory	Name 🐨
LDAP ()	
RADIUS Token ()	
RSA SecurID	

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**.

* Name	CertAuth	
Description		
Principal Username X509 Attribute	Common Name	¥
Perform Binary Certificate Comp	arison with Certificate retrieved	from LDAP or Active Directory
DAR/AD Instance Name		

9. Confirme se a nova CAP foi adicionada.

CISCO Identity Services Engine	
💧 Home Operations 🔻 Policy 🔻 Admini	stration 🔻
🔆 System 🦉 Identity Management 📰 I	Network Resources 🛛 🛃 Web Portal Management
Identities Groups External Identity Sources	Identity Source Sequences Settings
External Identity Sources	Certificate Authentication Profile
♦•	/ Edit win Add Dis Dunlicate Y Delete
Certificate Authentication Profile	
Active Directory	L Name
🚞 LDAP 🛞	L Certiesen
RADIUS Token ()	
RSA SecurID 🛞	

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

CISCO Identity Services Engine	
🛕 Home Operations 🔻 Policy 🔻 Admi	inistration 🔻
🔆 System 👰 Identity Management	Network Resources 🛛 🛃 Web Portal Management
Identities Groups External Identity Sources	Identity Source Sequences Settings
Identity Source Sequence	
/ Edit -Add Duplicate X Delete	
Name S	Description
Guest_Portal_Sequence	A built-in Identity Sequence for the Guest Portal
MyDevices_Portal_Sequence	A built-in Identity Sequence for the My Devices Po
Sponsor_Portal_Sequence	A built-in Identity Sequence for the Sponsor Portal

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

cisco Id	entity Services Engine
💧 Home 🚽	Operations Policy Administration
🔆 System	Veb Portal Mana
Identities (Broups External Identity Sources Identity Source Sequences Settings
Identity Source Sequ Identity Source Identity Source	vences List > New Identity Source Sequence rce Sequence urce Sequence
* Name	TestSequence
Description	
 Certificate 	Based Authentication

12. Role para baixo até Certificate Based Authentication:

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

 Certificate Based Authentication 	
Select Certificate Authentication Profile	CertAuth 💌
 Authentication Search List 	

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.

 Authentication Search List 		
A set of identity sources that wil	I be accessed in sequence until first authentication	succeeds
Available	Selected	_
	Internal Users	×
	*	V X

14. Clique em Submit para salvar.

 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
Submit

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

CISCO Identity Services Engine		
🛕 Home Operations 🔹 Policy 🔹 Administ	ration 🔹	
🔆 System 🛛 👰 Identity Management 🖉 Ne	twork Resources 🛃 Web Portal Management	
Identities Groups External Identity Sources	Identity Source Sequences Settings	
Identity Source Sequence		
Edit Add L Duplicate Celete		
Name	Description	Identity Stores
Guest_Portal_Sequence	A built-in Identity Sequence for the Guest Portal	Internal Users
MyDevices_Portal_Sequence	A built-in Identity Sequence for the My Devices Portal	Internal Users
Sponsor_Portal_Sequence	A built-in Identity Sequence for the Sponsor Portal	Internal Users
TestSequence		CertAuth, Internal Users, Internal Endpoints

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.

System Aldentity Management	🖬 Network Resources 🛛 🛃 Web
Identities Groups External Identity Source	Identity Source Sequences
dentity Source Sequence	U.
/Edit 🕂 Add 🖓 Duplicate 🗙 Delete	
/Edit +Add Duplicate XDelete	Description
/ Edit +Add Duplicate XDelete	Description A Built-in Identity Sequence
	Description A Built-in Identity Sequence A Built-in Identity Sequence
Edit Add Duplicate Celete Name Guest_Portal_Sequence MyDevices_Portal_Sequence Sponsor_Portal_Sequence	Description A Built-in Identity Sequence A Built-in Identity Sequence A built-in Identity 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 sequência 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.

Name Name	Description	Identity Stores
Guest_Portal_Sequence	 A Built-in Identity Sequence For The Guest Portal	Internal Users, AD1
States and a state while and a		States and a state of the state

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.

cisco Identity Services Engine				
💧 Home Operations 🔹 Policy 🔹 Adminis	stration 🔹	🛃 Web Portal	Management	
Network Devices Network Device Groups Exte	mal RADIUS Servers	RADIUS Serve	r Sequences	s
Network Devices	/ Edit de Add	P Duplicate	@ Import	
Network Devices	Name	 IP/Mask 	Locatio	m

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

Network Devices List > New Net	work Device	
Network Devices		
* Name Description	WLC	
* IP Address:	10.10.10.5	32
Model Name Software Version		
 Network Devic 	e Group	
Location	All Locations	Set To Default
Device Type	All Device Types 📀	Set To Default

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.

Protocol RADIUS	
Plotocol Reploy	
* Shared Secret	
Enable KeyWrap	
* Key Encryption Key	
Message Authenticator Code Key	
Key Input Format	

- 25. Clique em Submit.
- 26. Navegue até ISE > Policy > Policy Elements > Results.

CISCO Identity Service	es Engine
🛕 Home Operations 🔻	Policy Administration
System A Identity I Network Devices Network Devices	 Authentication Authorization Profiling Posture Client Provisioning Security Group Access
Network Devices	Egress Policy Network Device Authorization
Default Device	Policy Elements Dictionaries Conditions Results

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

CISCO Identity Services Engine	
🛕 Home Operations 🔻 Policy 🔻 Admin	istration 🔻
🛃 Authentication 🛛 💽 Authorization 🔀 P	Profiling 🔗 Posture 😡 Client Provisioning
Dictionaries Conditions Results	
Results	Standard Authorization Profiles
	/ Edit Add Duplicate X Delete
Authentication	Name V
Authorization	Biscolst_Access
Authorization Profiles	
Gathist_Access	DenvAccess

28. Dê a este perfil estes valores:

Nome: CWA

Authorization Profiles > Authorization	New Authorization Profile Profile
* Name	CWA
Description	
* Access Type	ACCESS_ACCEPT +

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							
ULAN VLAN							
Voice Domain Permissio	n						
Web Authentication	Centralized	•	ACL	ACL-REDIRECT	Redirect	Default	٣

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



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



31. Dê a este perfil estes valores:

Nome: Provisionar

Authorization Profiles > Authorization	New Authorization Profile Profile
* Name	Provision
Description	
* Access Type	ACCESS_ACCEPT *

Habilitar autenticação da Web (caixa marcada):

Valor de Autenticação da Web: Provisionamento do Requerente



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



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 Profil	e
* Name	WirelessSP
Description	

36. Insira estes valores:

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

Operating System	ALL 💠		
Connection Type	Wired		
	Vireless		
		*SSID	Demoix
		Security	WPA2 Enterprise +
* Allowed Protocol	PEAP		v
Optional Settings	TLS PEAP	ę	3
Submit Cancel			

- 37. Clique em Submit.
- 38. Click Save.

* Allowed Protocol	TLS	•
* Key Size	1024	
Save Reset		

39. Confirme se o novo perfil foi adicionado.

/ Edit 🕂 Add 👻 🕒 Duplicat	te XDelete
Name	Туре
Recorder Courses	
Wireless	NativeSPProfile

40. Navegue até Policy > Client Provisioning.



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

Nome da regra: iOSGrupos de Identidade: Qualquer

	Rule Name	Ic	lentity Gr	oups	Operating Syste	ims	Other Co	nditions
- 2	IOS	If	Any	and	Choose a	- ar	nd Condit	ion(s)
					Choose an	Operatin	ng System	8+

Sistemas Operacionais: Mac iOS All

Operating System Grou	ips
	Q
∲•	ŵ.
Android	
Mac OSX	
Mac iOS All	
🚞 Windows All 🖼	۲

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

ther Conditions	Results
	then Result 🕀 🧙

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



WizardProfile	
	(م
◆- ■ '≣	-∰ -
Clear Selection	
Wireless	

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

			Rule Name	I	(dentity Gro	oups	(Operating Systems		Other Conditions		Results	
1	2	٠	105	If [Any	\$	and [Mac IOS All 🛛 🔶	and	Condition(s)	\$ then [WrelessSP	\diamond

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. Àdireita da regra, selecione a seta a ser expandida.

If	Wireless_MAB	¢	allow protocols	Allowed Protocol : Default Netw	and	L2

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**

use	TestSequence 🗢
	Identity Source TestSequence
	Options
	If authentication failed Reject
History	If user not found Continue
	If process failed Drop 🔹

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

~	٠	Dot1X	: If	Wired_802.	1X ⊕ 🕋	allow protocol
~		Default Rule (If no match)	: al	low protocols	Allowed Prot	ocol : Default Ne

Con	npound Condition
	(م
4	/ 🗐 📜 👘 🏭 -
	Wired_MAB
	Wireless_MAB
	Wired_802.1X
	Wireless_802.1X Jhn
	Switch_Local_Web_Authentication
	WLC_Web_Authentication
:If :all	Wired_802.1X Conditions Below t Condition Name

Condição: Wireless_802.1X

Origem da Identidade: TestSequence

Identity Source TestSequence	se for authe
Options	Identitu Cource Liet
If authentication failed Reject	
If user not found Reject 🔹	(م)
If process failed Drop 🔹	♦• ■ '=
Note: For authentications using PEAP, LEAP, EAP-FAST or RADIUS	Internal Endpoints
it is not possible to continue processing when authentication fails	Internal Users
If continue option is selected in these cases, requests will be reject	Guest_Portal_Sequence
	Sponsor_Portal_Sequence
	MyDevices_Portal_Sequence
	TestSequence
Internal Users 🗢	CertAuth
	DenyAccess

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.

Except	time (III)		
	the second secon		
Standa	ard		
SI	tatus Rule Name	Conditions (identity groups and other conditions)	Permissions
	Black List Default	if Blacklist	then Blackist_Access
E	Profiled Cisco IP Phones	f Cisco-IP-Phone	then Cisco_IP_Phone

59. Àdireita 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.

	Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
I.		Black List Default	if Blacklist	then Blackist_Access
		Profiled Osco IP Phones	Cisco-IP-Phone	then Osco_IP_Phones
11	- 🖬	Standard Rule 1	f Any O and Condition(s) O	then AuthZ Profil
		Default	If no matches, then PermitAccess	

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**.

Cisco-IP-Phone		then Cisco_IP_Phone
f Any 💠 an	d Select Condition	Select Existing Condition from Library (2) or Create

62. Selecione Compound Conditions > Wireless_MAB.

Q
ŵ.,
b_Authentica
5
F
h

63. No Perfil de AuthZ, clique no sinal de mais (+) e selecione Padrão.
| | Profiles | |
|----------------|-----------------------|-------|
| | | P |
| lcy Elements | ₫- | -
 |
| | 🧰 Inline Posture Node | ۲ |
| | Ecurity Group | ۲ |
| | Standard 🕞 | ۲ |
| rmissions | | |
| cklist_Access | | |
| co_IP_Phones | | |
| AuthZ Profil 🗢 | | |
| Select an item |) = + | |
| | | |

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. Àdireita da mesma regra, clique na seta para baixo ao lado de Editar e selecione Inserir

nova regra abaixo.

Edit I 👻
Insert New Rule Above
Insert New Rule Below
Duplicate Above 🖞

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.

🖉 🗹 OpenCWA	# Wireless_MAB	then CWA
💉 🔽 🔹 Standard Rule 1	Any 💠 and Condition(s)	💠 then AuthZ Profil 💠

69. Altere a condição para Wireless_802.1X.

Condition(s)	- then AuthZ Profil	
Add All Conditions Belo	w to Library	
Condition Name	Expression	
Wireless_802.1X	Radius:Service-Type EQUALS Framed AND Radius:NAS-Port	* -

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.

1 (00) ·····			Dictionaries	
				Q
			♦• 🔳 🗉	\$¥+
os and other conditions)				-
		then		
		then		
		then		
Condition(s)	0			
tAccess	_		· · ·	
Condition Name	Expression			
Wireless_802.1X 📀	Radius:Service-	Type E	Network Access	
٥	Select Attrit	oute 🤇		

72. Selecione AuthenticationMethod e insira estes valores:



AuthenticationMethod: igual a

Network Access:Au📀	-
	Equals Not Equals

Selecione MSCHAPV2.



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

and	Condition(s)	🗢 then 🛛 AuthZ Profil 💠		
-				
	Condition Name	Expression	AND	
	Wireless_802.1X 📀	Radius:Service-Type EQUALS Framed AND Radius:NAS-Port		ŵ.
	♦	Network Access:Au Equals * MSCHAPV2 *	0	⊜ .

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

then	AuthZ Profil	Dor	
	Select an item 📀	- +	

Standard	ž. -
	٩ د
∲- ■ '≣	ŵ.
and the second second	
Se Provision	
$\mathbf{\hat{v}}$	

74. Clique em Concluído.



75. Àdireita 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.

-									
💉 💟 👻 Standard Rule 1) #[Any	\diamond	and	Condition(s)	<u>♦</u>	then	AuthZ Profil	0

77. Em Condições, selecione Condições Compostas.

	Dictionaries	
		Q
	∳- ■ '≣	\@+
ant Dravisioning	Simple Conditions	۲
	Compound Conditions	A.
	Time and Date Conditions	80
Condition(s)		
Condition(s) Add All Conditions E Condition Name		

78. Selecione Wireless_802.1X.



79. Adicione um atributo AND.

Wireless_802.1X	⇔ then ♦	
Add All Conditions Belo	w to Library	
Condition Name	Expression	
Wireless_802.1X 📀	Radius:Service-Type EQUALS Framed AND Radius:NAS-Port	5

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



81. Localize e selecione Radius.

			Dictionaries		
	V.a.		◆• ■ '≡		
Client Provisioning 🔄 Secur	ity Group Acces	s 🤱	🚞 des		
			Caco-MEDM		
		these	Caso- infection		
		then	🚞 aesace		
		then	EndPoints		
	all a state		Cuert Cuert		
etwork Access:AuthenticationMe	thod	then	🔛 Allerithy Group		
Wireless 802.1X Network Acce	ss:A 🗢	1	🔛 Internal.teer		
·	,		Alcosoft 🔛		
Condition Name	Expression		and the local section of the l	AND	*
			🧰 Radius		
Wireless_802.1X 📀	Radius:Service	e-Type E/	Section 1	20-	
٥	Select Attr	ibute 💟		O	

82. Selecione Calling-Station-ID-[31].



83. Selecione Iguais.

Radius:Service-Type EQUALS F	ramed AND Radius:NAS-	Port
Radius:Calling-Statio	auals dim	O
N	ot Equals	

84. Vá para CERTIFICATE e clique na seta para a direita.

Standard
⇔- ≣ '≣
Carthadan, Access
CHA
😋 Caco JP JPares
Cambractiviti2
Carry-Recess
Ca Discovery
Canal Complexiter (C. 1)
PermitAccess
🔐 Provinsion 🕤

85. Selecione Nome Alternativo do Assunto.



86. Para o perfil AuthZ, selecione Standard.

	Profiles			
		R		
	◆- ■ '=	\$÷-		
v Elements	🔛 Jahn Posture Node			
	🛄 finants irrap			
	Standard	R		
_IP_Phones		0		
sion	-			
AuthZ Profil 🗢				
Select an item	4			

87. Selecione **Permit Access**.



88. Clique em Concluído.



Este é um exemplo da regra:

1	OpenCHA /	Vindex_P10	The second	CHR
1	Riha i	Minister, 802.1X VIII. Nativali Access Authenticator/Hethod 8/2/4L5 HSDH4Pv2 3		Provision
1	AllowRule	Wireless_802: 1X Radus:Caling-Station-ID EQUALS CERTIFICATE:Subject Alternative Name	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.

Standard	
∻- ≣ '≣	
Cush	
Caso, JP , Phare	
Carlo Constructions (III)	

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.

OpenCWA	If	Wireless_MAB	then	CWA
PEAPrule	ť	(Wireless_802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2)	then	Provision
AllowRule	đ	(Wireless_802.1X AND Radius:Calling-Station-ID EQUALS CERTIFICATE:Subject Alternative Name)	then	PermitAccess
Default	ifi	io 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.)

P Certificat	e Authority	
* Name	mySCEP	
Description		
* URL	https://10.10.10.10/certsrv/mscep/	Test Connectivit

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.

SCEP CA Profiles			
/ Edit -Add XDelete		Show Al	- 🖗 🔶
Name	Description	URL	CA Cert Name
MySCEP		https://10.10.10.10/certsrv/mscep	RFDemo-MSCE

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.

Settings Wi-Fi Netwo	orks
Wi-Fi	
Choose a Network	
bibo	ú 🕈 🧕
✓ Demo1x	و ج 🔒
DemoCWA	÷ 🧿
Netherstorm	470

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.

A Home Operations	• Pol	ky •	Administration •						00 T
Authentications	e Endpo	oint Prote	iction Service	Alams 🧵 Repor	ts Trouble	shoot			
Live Authentications									
🙀 Add or Remove Columns 🕶	😵 Ref	resh					Refresh Every 3 secon	nds • Stow	Latest 20 records * within L
Time	Status	Detais	Identity	Endpoint ID	Network Device	Authorization Profiles	Identity Group	Posture Status	Event
Mar 25,12 12:27:57.052 AM			paul	EB.06-80.97.09-41	WLC	PermitAccess	FagisteredDevices	NotApplicable	Authentication succeeded
Mar 25,12 12:27:21.714 AM			68:06:88:97:09:41	68:05:88:97:09:41	WLC	CNA	RegisteredDevices	Pending	Authentication succeeded
Mar 25,12 12:27:20.438 AM	1				WLC				Dynamic Authorization succeeded
Mar 25,12 12:26:56.187 AM	1	à	paul	E8:06:88:97:09:41	WLC	CMA	Any,Profiled:Apple-Pad	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.

🛕 Home Operations 🔹 Policy 💌 Admin	nistration 💌
🔆 System 🦉 Identity Management 📲	Network Resources 🛛 🛃 Web Portal Management
System Identity Management Identities Groups External Identity Source Identity Groups Identity Groups User Identity Groups Blackist Blackist Blackist Blackist Blackist Blackist Unknown	Network Resources Web Portal Management Identity Source Sequences Settings Endpoint Group * Name * Name RegisteredDevices Description Asset Registered Endpoints Identity Group Parent Group Save Reset • Endpoints Identity Group Endpoints Identity Group Endpoints
	MAC Address E8:06:88:97:09:41

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.

Endpoint Group List > Endpoint Grou	RegisteredDevices p
* Name	RegisteredDevices
Description	Asset Registered Endpoint
Parent Group	
Save Rese	
 Endpoints 	
Identity Group	o Endpoints
🕂 Add	×Remove *
MAC Addre	Remove Selected
E8:06:88:9	Remove All

2. No dispositivo iOS, navegue para **Configurações > Generais > 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.

Enter the password for "Demo1x" Cancel Enter Password Join
Username paul
Password •••••3
Mode Automatic >

6. Repita as etapas 90 e seguintes na seção Configuração do ISE até que os perfis

apropriados estejam completamente instalados.

 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.

Live Authentications									
🚔 Add or Remove Columns 💌	😵 Refi	resh					Refresh Every	3 seconds *	Show Latest 20 records
Time •	Status	Detais	Identity	Endpoint ID	Network Device	Authorization Profiles	Identity Group	Posture Status	Event
Mar 25,12 12:40:03.593 AM		ò	paul	E8.06.88.97.09.41	WLC	PermitAccess	RegisteredDevices	NotApplicable	Authentication succeeded
Mar 25,12 12:39:53.353 AM	2	ò	E8:06:88:97:09:41	E8:06:88:97:09:41	WLC	CWA	RegisteredDevices	Pending	Authentication succeeded
Mar 25,12 12:39:08.867 AM	2	à	paul	E8-06-88-97:09-41	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.

Live Authentications									
🙀 Add or Remove Columns 💌	😵 Ref	resh					Refresh Every	3 seconds *	Show Latest 20 records
Time •	Status	Detais	Identity	Endpoint ID	Network Device	Authorization Profiles	Identity Group	Posture Status	Event
Mar 25,12 12:40:03:593 AM		ò	paul	E8.06.88.97.09.41	WLC	PermitAccess	RegisteredDevices	NotApplicable	Authentication succeeded
Mar 25,12 12:39:53.353 AM	2	ò	E8:06:88:97:09:41	E8:06:88:97:09:41	WLC	CWA	RegisteredDevices	Pending	Authentication succeeded
Mar 25,12 12:39:08.867 AM		ò	paul	E8.05.88.97.09.41	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.

🕝 https://market.androi 🔾	×
CISCO Identity Services Engine 1.1 Self-Provisioning Portal	pead Log Out Abo
Device Registration This device has not been registered. To register this device, please enter the Device ID (MAC Address format recommon either A-F or a digt 0-9) and a description (optional). Please click the "Register" button to install and run the Cisco W-FI Setup Assistant application. This application tell inst certificates and configures your device to use secure will network. Clicking the "Register" button will redirect you to an where you can download the Cisco Wi-FI Setup Assistant application.	unionion where it is tall all the necessary drold market place,
Device 10 18.0C.82.40.31.A9 Description	

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.**

Certificate na	ame
Certificate name:	
paul	
Package contains One user key One user certificate	
ОК	Cancel
Can	cel

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.

	111
Certificate na	ame
Certificate name: iseca Package contains One CA certificate	
ОК	Cancel
paul is in Can	nstalled.

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://iseserver:8443/mydevices (observe o número de porta 8443) e faça login com uma conta do AD.

CISCO My Devices Portal		
	Username paul Password	

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

Add a	New De	vice	To add a device, please ent (optional); then click submi	er the Device ID (MAC Ad t to add the device.	dress) and a descriptic	n
Your De	vices	* Device ID Description	ubmit			•
State	Device ID	Descr	iption	Action		
	E8:06:88:97:0	9:41		Edit	l Logt2 🗐	

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											
Add or Remove Columns *	the Part	resh					Refresh	Every	3 seconds *	Show Latest 20 records	*
Time	Status	Detals	Identity	Endpoint ID	Network Device	Authorization Profiles	Identity Group	_	Posture Status	Event	
Mar 25,12 12:49:07.851 AM	•	ò	paul	E0:06:00:97:09:41	WLC	Blacklist_Access	Blacklet			Authentication falled	
Mar 25,12 12:40:59.057 AM	•	ò	E0.06.08.97.09.41	EB-06-88-97:09-41	WLC	Blacklist_Access	Blacklet			Authentication falled	
Mar 26 12 12-40-54 127 AM		-		10-00-00-00-00-01	WE C	Blackfut Access	Blacklet			Authentication fided	

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.

Identity Groups	Endpoint Group
	* Name Blacklist Description Blacklist Identity Group Parent Group Save Reset. * Endpoints Identity Group Endpoints
	Add KRemove -
	MAC Address
	E8:06:88:97:09:41
	N N

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).

/ Edit	Add Export XDelete
	Import Local Server Certificate Generate Self-Signed Certificate
L Derau	Generate Certificate Signing Request
1	Bind CA Certificate 🖑

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

Local Certificates > Generate Certificate Signing Request Generate Certificate Signing Request			
Certificate			
* Certificate Subject	CN=ise11-mnr.corp.rf-demo.com		
* Key Length	2048 💌		
* Digest to Sign With	SHA-256 *		
Submit Cancel			

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.

Downloads	
😋 🔾 - Paul N Downlo	 Search Downloads
Organize 💌 📄 Open 💌 Share with 💌	New folder 🛛 📰 👻 🛄 🔞
★ Favorites	Name *
Nesktop	3 Save
🎉 Dropbox	ise11mnrcorprfdemocomise11.pem
' 🎉 Work	3
😹 Downloads	
Secent Places	1

9. Copiar todo o conteúdo do certificado.



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

G • (https://10.10.10.10/certsrv/	D 🖌 🖗 Cer
Windows Securit	Y	×
Connecting to 1	0.10.10.10.	
	administrator	
and the second		
	Domain: KFT7 Remember my credentials	
	ОК	Cancel

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 Certific | ate Services labsrv.corp.rf-demo.com | | | | |
|--|---|--|--|--|--|
| Submit a Certificate Request or Renewal Request | | | | | |
| To submit a sav
Saved Request | ved request to the CA, paste a base-64-encoded CN
t box. | | | | |
| Saved Request: | | | | | |
| Base-64-encoded VR01BAwwCgYIKwYBBQUHAwEwEQYJYIZIAYb4QgEB
Certificate request CCMC or 1/t6SUIOKQAyBRUp21TpHf+o27eDTVwW83bCmbD1
PKCS #10 or 0:2000 CERTIFICATE * | | | | | |
| Certificate Temp | late: | | | | |
| | Web Server 💌 | | | | |
| Additional Attrib | ites: | | | | |
| Attributes: | | | | | |
| | Submit > | | | | |

15. Clique em **Download certificate**.



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



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

🛕 Home Operations 🔻 Policy 🔻 Adminis	tration 🔻
🔆 System 🛛 👰 Identity Management 🛛 📷 M	Network Resources 🛛 🛃 Web Portal Management
Deployment Licensing Certificates Logging	g Maintenance Admin Access Settings
Certificate Operations	Local Certificates
Certificate Signing Requests Certificate Authority Certificates SCEP CA Profiles	Friend Import Local Server Certificate Generate Self-Signed Certificate Generate Certificate Signing Request
CCSP Services	Bind CA Certificate

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.

Deployment Licensing Certificates Logg	ing Maintenance Admin Access Settings
Deployment Licensing Certificates Logg Certificate Operations © Local Certificates © Certificate Signing Requests © Certificate Authority Certificates © SCEP CA Profiles © OCSP Services	Ing Maintenance Admin Access Settings Local Certificates = Bind CA Signed Certificate Bind CA Signed Certificate Bind CA Signed Certificate Certificate File C\Users\Paul Nguyen\Downloads\certnew(4).cer Browse Friendly Name
	Override Policy Replace Certificate A certificate being imported may be determined to already exist in the syst certificate. In such a case, selection of the "Replace Certificate" option will selections for the certificate. Cancel

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.

Microsoft Active Directory Certificate Services - co				
Download a CA Certificate, Certificate Ch				
To trust certificates issued from this certification				
To download a CA certificate, certificate chair				
CA certificate:				
Current [corp-RFDEMO-CA]				
Download CA certificate				
Download latest delta CRL				

21. Salve o arquivo na máquina local.

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

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.

😽 System 🛛 👰 Identity Management	Network Resources			🛃 Web Portal Managemer		
Deployment Licensing Certificates	Logging	Mainte	nance	Admin Access	Settings	
Certificate Operations		Certificate Authority Certificates				
Certificate Signing Requests	- /	Edit	-Import	t DExport	XDelete	
Certificate Authority Certificates		Friendly Name				
SCEP CA Profiles	corp-RFDEMO-CA#corp-RFDEMO-CA#00002					
🔅 OCSP Services		ise11-mnr.corp.rf-demo.com#ise11-mn				

Informações Relacionadas

- Guia de Instalação de Hardware do Cisco Identity Services Engine, Versão 1.0.4
- <u>Cisco 2000 Series Wireless LAN Controllers</u>
- <u>Cisco 4400 Series Wireless LAN Controllers</u>
- <u>Cisco Aironet 3500 Series</u>
- 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
- <u>Suporte Técnico e Documentação Cisco Systems</u>

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.