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

Contents

Integração de ISE para AD e configuração de ot1x e substituição de AAA para SSID offiguracão da VLC para suportar autenticação dot1x e substituição de AAA para SSID V=rificar T=vubleshooting

Introdução

Este documento descreve o conceito de atribuição de VLAN dinâmica.

Pré-requisitos

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

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

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

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

Componentes Utilizados

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

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

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

Conventions

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Configurar

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

Diagrama de Rede



Configurações

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

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

VLAN1477: 192.168.77.0/24. Gateway: 192.168.77.1 VLAN1478: 192.168.78.0/24. Gateway: 192.168.78.1

• Este documento usa 802.1x comPEAP-mschapv2como o mecanismo de segurança.



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

Estas suposições são feitas antes de você executar esta configuração:

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

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

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

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

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



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

ternal Identity Sources		Connection		
	<u>نې</u>	* Join Point Name	AD urdenen een	
Certificate Authentication Profile		Join Foint Name	AD.wiaaan.com	U.
Cive Directory		 Active Directory Domain 	wlaaan.com	()
EDAP LDAP			L	
CDBC				
RADIUS Token		Cubmit Cancel		
RSA SecurID		Submic Cancel		
SAML Id Providers				
Social Login				

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

Connection Whiteliste	d Domains PassiveID	Groups Attributes	Advanced Settings	
Join Point Name AD. Active Directory Domain wla	vlaaan.com aan.com	0		
양글 Join 양글 Leave 🧕 Test User 🍯	Diagnostic Tool Status	Domain Controller	Site	
rmanchur-ise.wlaaan.com	STANDALONE A Not Joint	ed	Sile	
	Join Domain Please specify the credentials required • AD User Name () • Password	d to Join ISE node(s) to the Active Dire Administrator	ctory Domain.	

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

external Identity Sources	Connection Whitelist	ed Domains Passi	veID Groups	Attributes Advanced	Settings	
Certificate Authentication Profile Certificate Authentication Certificate Authentication Certificate Authentication Certificate Certi	Join Point Name AD Active Directory Domain with	.wlaaan.com aaan.com		ı ı		
RADIUS Token	♀ Join ♀ Leave 및 Test User	🔁 Diagnostic Tool 🛛 🛞 Refr	esh Table			
RSA SecurID	ISE Node	 ISE Node Role 	Status	Domain Controller	Site	
SAML Id Providers	rmanchur-ise.wlaaan.com	STANDALONE	Operational	WIN-CFA29CSRIL9.wlaaan.com	Default-First-Site-Name	

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

executar os testes necessários para a conectividade do AD.

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

> Active directory >

> Groups

, clique emAdde escolhaSelect Groups from Active Directory.

► System Veldentity Management The Network Re	sources	
Identities Groups External Identity Sources	Identity Source Sequences	
External Identity Sources	Connection Whitelisted Domains PassiveID Groups Attributes	Advanced Settings
@ • E • 😥 •	/ Edit - Add - X Delete Group Update SID Values	
Certificate Authentication Profile Active Directory	Nam Select Groups From Directory SID	No data suslishin
Call AD.wlaaan.com		No data avallable
CDBC		
RADIUS Token		
RSA SecurID		
Social Login		

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

Escolha os respectivos grupos na lista de grupos do AD e pressioneok.

Sele This	e ct Direct dialog is u	cory Groups sed to select groups from the Directo	ry.						×
	Domain	wlaaan.com]				
1	Name Filter	*	SID Filter	*	Type Filter	GLOBAL		*	
		Retrieve Groups 13 Groups Retrie	ved.						
	Name		*	Group SID			Group Type		
	wlaaan.co	m/Users/Cloneable Domain Controll	ers	S-1-5-21-2222429329-410808516	4-322034527	1-522	GLOBAL		
	wlaaan.co	m/Users/DnsUpdateProxy		S-1-5-21-2222429329-410808516	4-322034527	1-1102	GLOBAL		
	wlaaan.co	m/Users/Domain Admins		S-1-5-21-2222429329-410808516	4-322034527	1-512	GLOBAL		
	wlaaan.co	om/Users/Domain Computers		S-1-5-21-2222429329-410808516	4-322034527	1-515	GLOBAL		
	wlaaan.co	om/Users/Domain Controllers		S-1-5-21-2222429329-410808516	4-322034527	1-516	GLOBAL		
	wlaaan.co	m/Users/Domain Guests		S-1-5-21-2222429329-410808516	4-322034527	1-514	GLOBAL		
	wlaaan.co	m/Users/Domain Users		S-1-5-21-2222429329-410808516	4-322034527	1-513	GLOBAL		
	wlaaan.co	m/Users/Group Policy Creator Owne	ers	S-1-5-21-2222429329-410808516	4-322034527	1-520	GLOBAL		
	wlaaan.co	om/Users/HR		S-1-5-21-2222429329-410808516	4-322034527	1-1105	GLOBAL		
	wlaaan.co	om/Users/Key Admins		S-1-5-21-2222429329-410808516	4-322034527	1-526	GLOBAL		
	wlaaan.co	om/Users/Marketing		S-1-5-21-2222429329-410808516	4-322034527	1-1104	GLOBAL		
	wlaaan.co	om/Users/Protected Users		S-1-5-21-2222429329-410808516	4-322034527	1-525	GLOBAL		
	wlaaan.co	m/Users/Read-only Domain Control	ers	S-1-5-21-2222429329-410808516	4-322034527	1-521	GLOBAL		



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

	Со	nnection		Whitelisted	Domains	PassiveID	Groups	Attributes	Advanced Settings	
1	Edit	📥 Add 👻	X De	lete Group	Update SID Values					
	Nam	ne li maa r	2000		-,		SID			
	wlaa	an.com/Use	ers/HR			-	S-1-5-21-22224	29329-4108085164-3220	345271-1105	
	wlaa	aan.com/Use	ers/Mar	keting			S-1-5-21-22224	29329-4108085164-3220	345271-1104	
Sa	/e	Reset								

9. Adicione a WLC à lista de dispositivos de rede do ISE - navegue atéAdministration > Network Resources > Network Devices e pressioneAdd.

Conclua a configuração, fornecendo o endereço IP de gerenciamento da WLC e o segredo compartilhado RADIUS entre a WLC e o ISE.

Identity Services E	ngine Home + Context Visibility + Operations + Policy - Administration + Work Centers
System Identity Management	gement = Network Resources > Device Portal Management pxGrid Services > Feed Service > Threat Centric NAC
Network Devices Network	k Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM + Location Services
	0
Network Devices	Network Devices List > New Network Device
Default Device	• Name <u>Mr (5520</u>
Device Security Settings	
	IP Address * *IP: 10.48.71.20 / 32
	IPv6 is supported only for TACACS, At least one IPv4 must be defined when RADIUS is selected
	* Device Profile 🛛 🏎 Cisco 🖡 🕀
	MotelName
	* Network Device Group
	Location LAB O Set To Default
	IPSEC Is IPSEC Device O Set To Default
	ncreu V mereuen
	BADIII & Authonication Cettione
	- retuino russenacion ocumpa
	RADIUS UDP Settings
	Protocol RADIUS
	Shared Secret Show
	CoA Port 1700 Set To Default
	RADIUS DTLS Settings ()

- 10. Agora, depois de ter ingressado no ISE para o AD e adicionado a WLC à lista de dispositivos, você pode iniciar a configuração de políticas de autenticação e autorização para usuários.
 - Crie um perfil de autorização para atribuir usuários de Marketing à VLAN1477 e do grupo de RH à VLAN1478.

Navegue atéPolicy > Policy Elements > Results > Authorization > Authorization profiles e clique no botãoAddpara criar um novo perfil.

dentity Services Engine Ho	ome ► Context Visibility ► Operations ► Po	icy Administration Work Centers	
Policy Sets Profiling Posture Client F	Provisioning Policy Elements		
Dictionaries + Conditions - Results			
0			
Authentication	Standard Authorization Profiles		
- Authorization	For Policy Export go to Administration > System > Back	up & Restore > Policy Export Page	
Authorization Drafiles	/ Edit 🕂 Add 🕒 Duplicate 🗙 Delete		
Authorization Profiles	Name	Profile	Description
Downloadable ACLs	Blackhole_Wireless_Access	🚓 Cisco 🕀	Default profile used to blacklist wireless dev
Profiling	Cisco_IP_Phones	🗱 Cisco 🕀	Default profile used for Cisco Phones.
▶ Posture	Cisco_Temporal_Onboard	🗰 Cisco 🕀	Onboard the device with Cisco temporal ag
	Cisco_WebAuth	inte Cisco 🕀	Default Profile used to redirect users to the
Client Provisioning	NSP_Onboard	🔐 Cisco 🕀	Onboard the device with Native Supplicant
	Non_Cisco_IP_Phones	📸 Cisco 🕀	Default Profile used for Non Cisco Phones.
	DenyAccess		Default Profile with access type as Access-
	PermitAccess		Default Profile with access type as Access-

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

Decinaries • Condition • Authentization • Authentization Profiles • Authentization Profiles • Name • Authentization Profiles • Secretary • Posture • Access Type		
Authorization Profiles - New Authorization Profile • Authorization Profiles • Authorization Profiles • Authorization Profiles • Profiling • Profiling • Profiling • Client Provisioning • Common Tasks • Authorization Profiles • Authorization Profiles • Authorization Profiles • Name • Common Tasks • Authorization Profile • VLN • Tag ID 1 • Edit Tag ID Name 1:071	Dictionaries Conditions Results	
Authonization Authorization Profile • Authorization Profiles • Name Downloadable ACLs • Access Type • Profiling • Access Type • Posture • Access Type • Posture Service Template • Client Provisioning • Common Tasks • DACL Name • ACL (Filter-ID) • Servicy Torup • VLN • VLN Tag ID 1 Edit Tag Edit Tag • Advanced Attributes Settings • Advanced Attributes Settings	0	Authorization Profiles > New Authorization Profile
• Authorization • Nome Marketing Downloadable ACLs • Access Type Access Type • Profiling • Access Type Access Type • Posture • Service Template • • Client Provisioning • Common Tasks • • ACL (Filter-ID) • • • Service Attributes Settings • VLN • Advanced Attributes Settings • Advanced Attributes Settings	Authentication	Authorization Profile
Authorization Profiles Downloadabie ACLs Profiling Posture Client Provisioning Common Tasks DACL Name ACL (Fitter-ID) Security Group VLN Tag ID 1 Edit Tag, ID/Name [1477]	- Authorization	• Name Marketing
Downloadable ACLs * Access Type ACCESS ACCEPT * Profiling Network Device Profile Clisco * * * Posture Service Tempiate * * Client Provisioning Track Movement * * Common Tasks DACL Name • ACL (Filter-ID) • Security Group * VLAN Tag ID 1 Edit Tag ID Name [1477]	Authorization Profiles	Description Marketing
Profiling Posture • Client Provisioning • Client Provisioning • Common Tasks • OACL (Filter-ID) • Security Group • VLN • VLN • Tag ID 1 Edit Tage ID/Name 1477]	Downloadable ACLs	* Access Type ACCESS ACCEPT *
Posture • Client Provisioning Service Template :: • Client Provisioning Tack Movement :: • Passive identity Tracking :: Passive identity Tracking :: • Common Tasks DACL Name :: DACL (Filter-ID) :: Security Group :: VLN :: VLN :: Advanced Attributes Settings	Profiling	Network Device Profile 🛛 🗯 Cisco 🔻 🕀
Client Provisioning Track Movement @ Passive Identity Tracking @ Common Tasks DACL Name @ ACL (Filter-ID) @ Security Group @ VLAN Tag ID 1 Edit Tag ID Name [1477]	→ Posture	Service Template
Passive Identity Tracking	Client Provisioning	Track Movement
✓ Common Tasks DACL Name ACL (Fiter-ID) Security Group VLAN Tag ID 1 Edit Tag ID/Name 1477 ✓ Advanced Attributes Settings Select an item		Passive Identity Tracking 🔲 🕧
Common Tasks DACL Name ACL (Filter-ID) Security Group VLAN Tag ID 1 Edit Tag IDIName 14777 Advanced Attributes Settings Select an item C = C + +		
✓ Common Tasks DACL Name ACL (Filter-ID) Security Group ✓ VLAN Tag ID 1 Edit Tag ID/Name 1477] ✓ Advanced Attributes Settings Select an item ♥ = ● ● ● ●		
 DACL Name ACL (Filter-ID) Security Group ✓ VLAN Tag ID 1 Edit Tag ID/Name 1477] 		• Common Tasks
 ACL (Filter-ID) Security Group ✓ VLAN Tag ID 1 Edit Tag ID/Name 1477] ✓ Advanced Attributes Settings Select an item =		DACL Name
 ACL (Filter-ID) Security Group ✓ VLAN Tag ID 1 Edit Tag ID/Name 1477] ✓ Advanced Attributes Settings Select an item =		
 Security Group ✓ VLAN Tag ID 1 Edit Tag ID/Name 1477 ✓ Advanced Attributes Settings Select an item		ACL (Filter-ID)
✓ VLAN Tag ID 1 Edit.Tag ID/Name 1477] ✓ Advanced Attributes Settings Select an item		Security Group
✓ VLAN Tag ID 1 Edit.Tag ID/Name 1477 ✓ Advanced Attributes Settings Select an item		
✓ Advanced Attributes Settings Select an item Image: Select an item		VLAN Tag ID 1 Edit Tag ID/Name 1477
✓ Advanced Attributes Settings Select an item Image: Select an item		
✓ Advanced Attributes Settings Select an item Image: Select an item		
Select an item Image: Control of the select an item		Advanced Attributes Settings
		Select an item 🕑 = 💿 — 🕂
✓ Attributes Details		▼ Attributes Details
Access Type = ACCESS_ACCEPT		Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:1477 Tunnel-Type = 1:13		Tunnel-Private-Group-ID = 1:1477 Tunnel-Type = 1:13
Tunnel-Medium-Type = 1:6		Tunnel-Medium-Type = 1:6
Submit Cancel		Submit Cancel

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

 Depois que os perfis de autorização forem configurados, você poderá definir políticas de autenticação para usuários sem fio. Isso pode ser feito configurandoCustomou modificando o conjuntoDefaultde políticas. Neste exemplo, o conjunto de políticas padrão é modificado. Navegue atéPolicy > Policy Sets > Default. Por padrão, para o tipo dedot1xautenticação, o ISE usaráAll_User_ID_Stores, embora funcione mesmo com as configurações padrão atuais, já que AD faz parte da lista de origem de identidade de All_User_ID_Stores, este exemplo usa uma regra mais específicawLC_labpara esse controlador de LAB respectivo e usa AD como a única origem para autenticação.

icy Sets Profiling Posture Client P	ovisioning + Pol	cy Elements		Click here to do wireless setup and visibility setup Do not show	this again.
icy Sets → Default				Reset	Sav
Status Policy Set Name	Descrip	ion	Conditions	Allowed Protocols / Server Sequer	ce Hr
arch					
Default	Default p	olicy set		Default Network Access * *	+ •
Authentication Policy (4)					
+ Status Rule Name	Condi	ions		Use Hits	Action
Search					
Ø MAB	OR	Wired_MAB		Internal Endpoints * *	0
		Wireless_M		> Options	-
		Wireless_60	x	AD wisses com	
V 🕢 WLC_Mb	AND	E DEVICE De	Type EQUALS AE Device Types#WLC-lab	Designed 0	۰
		E DEVICE LO	on EQUALS AI Locations#LAB	 Optimis 	
Q 2001	0.0	Wired_802		Al_User_ID_Stores * *	•
U Denx	ÜR	Wireless_80	x	> Options	•
				Al_User_ID_Stores × *	-
 Default 				> Options	Ŷ
Authorization Policy - Local Exception	5				
Authorization Policy - Global Exception	ns				
Authoritation Daliay (12)					

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

Policy Sets Pr	Policy Sea Prolling Peakure Citert Provisioning + Policy Demena						Click here to do wireless setup and visibility setup Do not show this a		
Policy Sets -	Default						•	losot	Save
Status	Policy Set Name	Description	Conditions			Allowed Prote	ocols / Server Se	equence	Hits
Search								_	
0	Default	Default policy set				Default Netwo	ork Access	** +	0
> Authenticati	on Policy (4)								
> Authorizatio	n Policy - Local Exceptions								
> Authorizatio	n Policy - Global Exceptions								
✓ Authorizatio	n Policy (14)								
+ Statu	s Rule Name	Conditions			Results Profiles	Security Groups		Hits	Actions
Search	Wireless_Marketing	AND E A	Vreiess, Access D x4aaan.com ExternalGroups EQUALS x4aaan.com/Users/Marketing		Marketing	+ Select from list	- +	•	•
I, 0	Wireless_HR	AND H AS	Vreless_Access D wlaaan.com ExternalGroups EQUALS wlaaan.com/Users/HR		INR	Select from list	• •	0	۰

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

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

cisco	MONITOR WLANS CONTROLLER	R WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Security	RADIUS Authentication Serve	ers > New
 AAA General RADIUS Authentication Accounting Auth Cached Users Fallback DNS Downloaded AVP TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies Advanced EAP Priority Order Certificate Access Control Lists Wireless Protection Policies Web Auth TrustSec Local Policies Umbrella Advanced 	Server Index (Priority) Server IP Address(Ipv4/Ipv6) Shared Secret Format Shared Secret Confirm Shared Secret Apply Cisco ISE Default settings Apply Cisco ACA Default settings Key Wrap Port Number Server Status Support for CoA Server Timeout Network User Management Management Retransmit Timeout Tunnel Proxy PAC Provisioning IPSec Cisco ACA	2 ¢ 10.48.39.128 ASCII ¢ (Designed for FIPS customers and requires a key wrap compliant RADIUS server) 1812 Enabled ¢ Enabled ¢ 5 seconds 2 Enable 5 seconds Enable 1 Enable 1 Enable

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

WLANS WLANS WLANS Current Filter: None [Change Filter] Clear Filter] Advanced WLAN ID Type Profile Name WLAN SSID Admin Status Security Policies 1 WLAN test Enabled (WPA2](Auth(980.1X)) 1 2 WLAN AndroidAP AndroidAP Enabled (WPA2](Auth(PSK)) 1 253 WLAN BTER-BTwifi-public BTwifi-public Enabled (WPA2](Auth(PSK)) 1	WLANS WLA	LANs					
WLANS WLANS Current Filter: None [Change Filter] Clear Filter) Create New<* Go > Advanced WLAN ID Type Profile Name WLAN SSID Admin Status Security Policies 1 WLAN test test Enabled (WPA2)[Auth(802.1X)) Image: Comparison of the status 2 WLAN AndroidAP AndroidAP Enabled (WPA2)[Auth(PSK)] Image: Comparison of the status 253 WLAN BTER-BTwifi-public BTwifi-public Enabled (WPA2)[Auth(PSK)] Image: Comparison of the status	VILANS Curre						
Advanced WLAN ID Type Profile Name WLAN SSID Admin Status Security Policies 1 WLAN test test Enabled (WPA2)[Auth(802.1X)] 2 2 WLAN AndroidAP AndroidAP Enabled (WPA2)[Auth(P5K)] 2 253 WLAN BTER-BTwifi-public BTwifi-public Enabled (WPA2)[Auth(P5K)] 2	W LAINS	rrent Filter: No	ne [Change Fil	ter] [Clear Filter]		Create New	ŧ Go
1 WLAN test Enabled (WPA2][Auth(802.1X)] Image: Comparison of the	► Advanced	WLAN ID Type	Profile Name	WLAN SSID	Admin	Status Security Policies	
2 WLAN AndroidAP AndroidAP Enabled [WPA2][Auth(PSK)] Image: Comparison of the state of t	01	1 WLAN	test	test	Enabled	[WPA2][Auth(802.1X)]	
253 WLAN BTER-BTwifi-public BTwifi-public Enabled [WPA2][Auth(PSK)]	0 2	2 WLAN	AndroidAP	AndroidAP	Enabled	[WPA2][Auth(PSK)]	
	0 2	253 WLAN	BTER-BTwifi-public	BTwifi-public	Enabled	[WPA2][Auth(PSK)]	

									selfe comparation. End, reduce Benefit
cisco	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK	C Alone
WLANs	WLANs > New								< Back Apply
WLANs WLANs Advanced	Type Profile Name SSID ID	offici offici 3	AN B e_hq e_hb B			}			

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

WLANs > Edit 'office_hq'

General See	curity QoS	Policy-Map	ping Adva	nced			
Layer 2	ayer 3 AAA Se	ervers					
Layer 2 Secur	rity ⁶ WPA+WPA2 MAC Filtering	÷ +)				
Fast Transition							
Fast Transition Over the DS Reassociation Tin	Ada aneout 20 Seconds	ptive 🕈					
Protected Mana	gement Frame						
PMF	Disa	abled \$					
WPA+WPA2 Pa	rameters						
WPA Policy							
WPA2 Policy	V						
WPA2 Encrypt	tion 🗸 🗹 AES	5 TKIP	CCMP256	GCMP128	GCMP256		
OSEN Policy							
Authentication	Key Management	<u>19</u>					
802.1X	🕑 Enable						

WLANs	WLANs > Edit 'office_hq'	
WLANs WLANs	General Security QoS Policy-Mapping Advanced	
Advanced	Layer 2 Layer 3 AAA Servers	
	Select AAA servers below to override use of default servers on this WLAN RADIUS Servers RADIUS Server Overwrite interface Enabled Apply Cisco ISE Default Settings Enabled Authentication Servers EAP Parameters Enabled Prilo.48.39.128, Port:1812 ‡ Server 1 IP:10.48.39.128, Port:1812 ‡ Server 2 None Server 3 None Server 4 None Server 5 None Server 6 None Authorization ACA Server Accounting ACA Server Enabled Enabled	

neral Security QoS Pe	Dlicy-Mapping Advanced		
Allow AAA Override	Enabled	DHCP	
Coverage Hole Detection	Enabled	DHCP Server Override	
Enable Session Timeout 2 1800 Aironet IE	Timeout (secs)	DHCP Addr. Assignment CRequired Management Frame Protection (MFP)	
Diagnostic Channel AS Override Interface ACL	IPv4 None IPv6 None IPv6	MFP Client Protection 4 Optional \$	
Layer2 Acl	None 🛊	DTIM Period (in beacon intervals)	
IRL ACL P2P Blocking Action Client Exclusion ²	None ¢ Disabled ¢ 2 Enabled 180 Timeout Value (secs)	802.11a/n (1 - 255) 1 802.11b/g/n (1 - 255) 1	
Maximum Allowed Clients ⁸	0	NAC State None	
Static IP Tunneling 11	Enabled	Load Balancing and Band Select	
Wi-Fi Direct Clients Policy	Disabled \$	Client Load Balancing	_
Maximum Allowed Clients Per AP Radio	200	Client Band Select	
Clear HotSpot Configuration	Enabled	Passive Client	

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

iliilii cisco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u>		WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Controller								
General	General Information	ı						
Icons	Interface Name	vlan147	77					
Inventory	MAC Address	00:a3:8	3e:e3:5a:1a					
Interfaces Interface Groups	Configuration				_			
Multicast	Guest Lan							
Network Routes	Quarantine							
Fabric Configuration	Quarantine Vlan Id	0						
Redundancy	NAS-ID	none						
Mobility Management	Physical Information	n						
Ports	Port Number	t	L					
▶ NTP	Backup Port	C)					
▶ CDP	Active Port	1	L					
▶ PMIPv6	Enable Dynamic AP Man	nagement						
Tunneling	Interface Address							
▶ IPv6								
▶ mDNS	VLAN Identifier	1	1477					
Advanced	IP Address	1	192.168.77.5					
Lawful Interception	Netmask	2	255.255.255.0	_				
	Gateway		192.168.77.1					
	Profix Longth							
	IPv6 Gateway							
	Link Local IPv6 Address	L.	 e80::2a3:8eff:f	ee3:5a1a/64				
	DHCP Information			,				
	Primary DHCP Service		192 168 77 1					
	Secondary DHCP Server	,	192.100.//.1					
	DHCP Provy Mode		Global 🛔					

Verificar

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

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

Testar conexão com o Windows 10 e suplicante nativo:

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

← Settings	
命 Wi-Fi	
Manage known networks	12. 12.
Add a new network	Add a new network
+	Network name
Search this list \wp	office_hq
Sort by: Preference $ \smallsetminus $ Filter by: All $ \smallsetminus $	Security type
	WPA2-Enterprise AES \checkmark
	EAP method
	Protected EAP (PEAP)
11/ Constant and the second	Authentication method
	Secured password (EAP-MSCHAP v2) V
(maintain)	Connect automatically
The second second	Connect even if this network is not broadcasting
	Save Cancel

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

c	Refresh Reset Repeat Counts	Export To *														,	Filter •	۰۰
	Time	Status	Details	Repeat	Identity		Endpoint ID	Endpoint P	Authenticat	Authorization Policy	Authorizati	IP Address	Network Device	Device Port	Identity Group	Posture St	Server	
×					Bob	×	Endpoint ID	Endpoint Profil	Authentication	Authorization Policy	Authorization I	IP Address \$	Network Device	Device Port	Identity Group	Posture Statue	Server	
	Feb 15, 2019 02:16:43:300 PM	0	à	3	Bob		F4.80:50:62:14:68	Unknown	Default >> W	Default >> Wireless_HR	HR						manchur-	50
	Feb 15, 2019 02:09:56:389 PM		à		Bob		F4/8C/50/62/14/68	Unknown	Default >> W	Default >> Wireless_HR	HR		WLC5520		Unknown		manchur-	50

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

ıılıılı. cısco	MONITOR WLANS CONT	ROLLER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK		_				Saye C	onfiguration	Eing	ogout Bef A H	fresh ome
Monitor	Clients														Entr	ies 1 - 1 of	61
Summary Access Points Cisco CleanAir	Current Filter None	1	[Change_Filter] [Clear Filter)													
Statistics CDP	Client MAC Addr IP Ad (4:8c:50:62:14:6b 192.10	dress(Tov4/Tov6) 58.78.36		AP N AP40	lame 277.6D9E.6162			WLAN Profile office_hq	WLAN SSID office_hq	User Name Bob	Protocol 802.11ac(5 GHz)	Status Associated	Auth Yes	Port Sio	t Id Tur No	nel Fas No	stlane
 Rogues Clients 																	
Sleeping Clients Multicast Applications																	

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

:

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

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

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

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

		🕥 Cisco AnyConne	ect Secure Mobility Client — 🗆 🗙
		Web Authentication	N: e a browser to gain access. Connect
		Con	twork: nnected (10.103.150.57) internet
Cisco AnyConnect			× curity:
	Enter information for the connection	1.	e ney.
Media:	Wi-Fi		
Descriptive Name: SSID:	Hidden Netw office_hq office_hq	ork	Scan: can not required on current Wi-Fi.
Security:	WPA2 Enterpris	se AES	
802. 1X Configurat	on V PEAP	~	g Security: tot currently protected by Umbrella.
	OK	Cancel	Initisting,

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

	S Cisco AnyConnect Secure Mobility Client − □ ×	
Cisco AnyConnect office_hq X Please enter your username and password for the network: office_hq Username: Alice	VPN: Verify your network connection.	
Password: ******* Show Password OK Cancel	Network: Authenticating office_hq	
	Web Security: No License Key,	
	System Scan: Limited or no connectivity.	

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

Cisco AnyConnect X		
The server certificate for the network 'office_hq' has failed validation. Do you want to trust it? Certificate Name: rmanchur-ise.wlaaan.com@ Issued To: rmanchur-ise.wlaaan.com Issued By: rmanchur-ise.wlaaan.com Expiration Date: 2020-02-13 15:03:40 UTC	VPN: Verify your network connection. Connect No Network Connectivity Network: Authenticating office_hq Authentication	
	Web Security: No License Key.	

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

C Refresh O Reset Repeat Count	Export To •																		T Filter -	۰۰
Time	Status	Details	Repeat	Identity		Endpoint ID		Endpoint P	Authenticat	Authorization Policy	Authoriz	ati I	P Address		Network Device	Device Port	Identity Group	Posture St	Server	Mdm
×				Alice	×	60	×	Endpoint Prof	Authentication	Authorization Policy	Authoriza	ation	IP Address		Network Device	Device Port	Identity Group	Posture Statu	Server	Mdm
Feb 15, 2019 02:51:27.163 PM	•	0	0	Alce		F4:80:50:62:14:68		Microsoft-W	Default >>	Default >> Wireless_Marketing	Marketing	1	192.168.77.32						manchur-ise	
Feb 15, 2019 02:51:24.837 PM	8	à +		Alce	٠	F4:8C:50:62:14:68	*	Morosoft-W	Default >>	Default >> Wireless_Marketing	Marketing)		*	WLC5520		Workstation �		manchur-ise 4	•

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

Clients												Entries 1 - :
Current Filter	None	[Change Filter] [Clear Filter]										
Client MAC Addr	IP Address(Ipv4/Ipv6)		AP Name	WLAN Profile	WLAN SSID	User Name	Protocol	Status	Auth	Port	Slot Id	Tunnel
f4:8c:50:62:14:6b	192.168.77.32		AP4C77.6D9E.6162	office_hq	office_hq	Alice	802.11ac(5 GHz)	Associated	Yes	1	1	No

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

:

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

Associated
RADIUS Server
Alice
Access
3
office_hq
office_hq
Not Supported
765 secs
70:69:5a:51:4e:cd
36
192.168.77.32
192.168.77.1
255.255.255.0
RUN
WPA2
802.1x
CCMP-128 (AES)
No
No
PEAP
vlan1477
1477

Troubleshooting

1. Use Otest aaa radius username

password

wlan-id

para testar a conexão RADIUS entre a WLC e o ISE e Otest aaa show radiuspara mostrar os resultados.

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

Radius Test Request	
Wlan-id	2
ApGroup Name	none
Attributes	Values
User-Name	Alice
Called-Station-Id	00-00-00-00-00:AndroidAP
Calling-Station-Id	00-11-22-33-44-55
Nas-Port	0x0000001 (1)

Nas-Ip-Address	10.48.71.20
NAS-Identifier	0x6e6f (28271)
Airespace / WLAN-Identifier	0x0000002 (2)
User-Password	cisco!123
Service-Type	0x0000008 (8)
Framed-MTU	0x00000514 (1300)
Nas-Port-Type	0x0000013 (19)
Cisco / Audit-Session-Id	1447300a000003041d5665c
Acct-Session-Id	5c66d541/00:11:22:33:44:55/743

test radius auth request successfully sent. Execute 'test aaa show radius' for response (Cisco Controller) >test aaa show radius Radius Test Request Wlan-id..... 2 ApGroup Name..... none Radius Test Response Radius Server Retry Status _____ -----1 Success 10.48.39.128 Authentication Response: Result Code: Success Attributes Values _____ _____ User-Name Alice ReauthSession:1447300a000003041d5665c State Class CACS:1447300a000003041d5665c:rmanchur-ise/339603379/59 Tunnel-Type 0x000000d (13) 0x0000006 (6) Tunnel-Medium-Type Tunnel-Group-Id 0x000005c5 (1477)

(Cisco Controller) >

2. Use o debug client

para solucionar problemas de conectividade do cliente sem fio.

3. Use Odebug aaa all enablepara solucionar problemas de autenticação e autorização na WLC.



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

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

Sobre esta tradução

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

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

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