ISEからActive Directoryへのグループマップに基 づくWLCを使用したダイナミックVLAN割り当 ての設定

内容

は じ め に 前 提 条件: 要件 使用するコンポーネント 表記法 RADIUS サーバによるダイナミック VLAN 割り当て 設定 ネットワーク図 コンフィギュレーション: ISE と AD の統合および ISE でのユーザー認証と認証ポリシーの設定 SID「office hg」のdot1x認証およびAAAオーバーライドをサポートするWLC設定 確認

はじめに

このドキュメントでは、ダイナミック VLAN 割り当ての概念について説明します。

前提条件

このドキュメントでは、ワイヤレスLAN(WLAN)クライアントを特定のVLANにダイナミックに割 り当てるようにワイヤレスLANコントローラ(WLC)とIdentity Services Engine(ISE)サーバを設定 する方法について説明します。

要件

次の項目に関する知識があることが推奨されます。

- ワイヤレスLANコントローラ(WLC)とLightweightアクセスポイント(LAP)に関する基礎知識
- ISEなどの認証、認可、アカウンティング(AAA)サーバの機能に関する知識
- ワイヤレス ネットワークとワイヤレスのセキュリティ問題に関する全般的な知識
- ・ダイナミックVLAN割り当てに関する実践的で構成可能な知識
- Microsoft Windows ADサービス、ドメインコントローラ、およびDNSの概念に関する基本 的な知識

アクセスポイントプロトコルのコントロールとプロビジョニング(CAPWAP)に関する基礎知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ・ファームウェア リリース 8.8.111.0 が稼働する Cisco 5520 シリーズ WLC
- ・ Cisco 4800 シリーズ AP
- ネイティブWindowsサプリカントおよびAnyconnect NAM
- Cisco Secure ISE バージョン 2.3.0.298
- ・ ドメイン コントローラとして設定された Microsoft Windows 2016 Server
- Cisco 2950 シリーズ スイッチバージョン 15.2(4)E1

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

表記法

表記法の詳細については、『<u>シスコ テクニカル ティップスの表記法</u>』を参照してください。

RADIUS サーバによるダイナミック VLAN 割り当て

一般的な WLAN システムでは、Service Set Identifier(SSID)(コントローラの用語では WLAN)に関連付けられたすべてのクライアントに適用されるスタティックなポリシーが各 WLAN に存在します。この方式は強力ですが、異なる QoS ポリシーやセキュリティ ポリシーを 継承するために各クライアントを異なる SSID に関連付ける必要があるので、さまざまな制約が あります。

シスコのWLANソリューションは、IDネットワーキングのサポートによってこの制限に対処しま す。これにより、ネットワークは単一のSSIDをアドバタイズできますが、ユーザクレデンシャ ルに基づいて、特定のユーザが異なるQoS、VLAN属性、セキュリティポリシーを継承できるよ うになります。

ダイナミック VLAN 割り当ては、ユーザが入力したクレデンシャルに基づいてワイヤレス ユーザ を特定の VLAN に割り当てる機能です。ユーザを特定のVLANに割り当てるタスクは、Cisco ISEなどのRADIUS認証サーバによって処理されます。たとえば、これを利用すると、キャンパス ネットワーク内を移動するワイヤレス ホストを同じ VLAN に割り当てることができます。

Cisco ISEサーバは、内部データベースを含む複数のデータベースの1つに対してワイヤレスユー

ザを認証します。例:

- 内部 DB
- Active Directory
- ・ 汎用の Lightweight Directory Access Protocol (LDAP)
- Open Database Connectivity (ODBC) に準拠したリレーショナル データベース
- ・ Rivest, Shamir, and Adelman (RSA) SecurID トークン サーバ
- RADIUS に準拠したトークン サーバ

<u>Cisco ISE 認証プロトコルとサポートされている外部 ID ソース</u>には、ISE 内部および外部データ ベースでサポートされるさまざまな認証プロトコルが記載されています。

このドキュメントでは、Windows Active Directory(AD)外部データベースを使用するワイヤレスユ ーザの認証について説明します。

認証に成功すると、ISEはWindowsデータベースからそのユーザのグループ情報を取得し、ユー ザをそれぞれの認可プロファイルに関連付けます。

クライアントがコントローラに登録されているLAPとの関連付けを試みると、LAPからWLCに対して、それぞれのEAP方式を使用してユーザのクレデンシャルが渡されます。

WLCは(EAPをカプセル化して)RADIUSプロトコルを使用してこれらのクレデンシャルを ISEに送信し、ISEはKERBEROSプロトコルを使用して検証のためにユーザのクレデンシャルを ADに渡します。

AD では、そのユーザークレデンシャルを検証し、認証に成功した場合は ISE に通知します。

認証に成功すると、ISE サーバーから WLC に特定の Internet Engineering Task Force(IETF)属 性が渡されます。これらのRADIUS属性により、ワイヤレスクライアントに割り当てる必要があ るVLAN IDが決まります。ユーザはこの事前設定済みの VLAN ID に常に割り当てられるので、ク ライアントの SSID(WLC の用語では WLAN)は無視されます。

VLAN ID の割り当てに使用される RADIUS ユーザ属性は次のとおりです。

- ・ IETF 64(トンネルタイプ)―これをVLANに設定します
- IETF 65(トンネルミディアムタイプ)—これを802に設定
- ・ IETF 81(トンネルプライベートグループID) これをVLAN IDに設定します

VLAN ID は 12 ビットで、1 ~ 4094 の値(両端の値を含む)を取ります。RFC 2868 で定義され ているように、IEEE 802.1X で使用される Tunnel-Private-Group-ID は文字列型であるため、 VLAN ID の整数値は文字列としてエンコードされます。これらのトンネル属性が送信される際に は、Tag フィールドの値を設定する必要があります。

RFC 2868のセクション3.1で述べられているように、Tagフィールドは1オクテットの長さを持ち

、同じトンネルを参照する同じパケット内の属性をグループ化する手段を提供することを目的としています。このフィールドで有効な値は、0x01 ~ 0x1F(両端を含む)です。Tag フィールドを使用しない場合は、このフィールドをゼロ(0x00)に設定する必要があります。すべての RADIUS 属性の詳細は、RFC 2868 を参照してください。

設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供します。

ネットワーク図



コンフィギュレーション

この図で使用されているコンポーネントの設定の詳細は、次のとおりです。

- ISE(RADIUS)サーバのIPアドレスは10.48.39.128です。
- WLC の管理インターフェイスおよび AP マネージャ インターフェイスのアドレスは 10.48.71.20 です。
- DHCPサーバはLANネットワークにあり、クライアントプールごとに設定されます。図には 示されていません。
- VLAN1477 と VLAN1478 は、この設定全体で使用されます。マーケティング部門のユーザ はVLAN1477に配置されるように設定され、人事部門のユーザはRADIUSサーバによって VLAN1478に配置されるように設定されます 両方のユーザが同じSSID(office_hq)に接続す る場合.

VLAN1477:192.168.77.0/24。ゲートウェイ:192.168.77.1 VLAN1478:192.168.78.0/24ゲートウェイ:192.168.78.1

• このドキュメントでは、セキュリティメカニズムとしてPEAP-mschapv2 802.1xを使用します。



注:シスコでは、WLANを保護するために、EAP-FAST認証やEAP-TLS認証などの高度な

認証方式を使用することを推奨しています。

これらの前提は、この設定を実行する前に実施済みです。

- LAPはすでにWLCに登録されています
- DHCPサーバにDHCPスコープが割り当てられている
- ネットワーク内のすべてのデバイス間にレイヤ3接続が存在する
- このドキュメントでは、ワイヤレス側で必要な設定について説明し、有線ネットワークが確 立されていることを前提としています
- それぞれのユーザとグループはADで設定されます

ISE と AD のグループマッピングに基づいて、WLC でダイナミック VLAN 割り当てを行うには、 次の手順を実行する必要があります。

- 1. ISE と AD の統合および ISE でのユーザー認証と認証ポリシーの設定.
- 2. SSID「office_hq」のdot1x認証およびAAAオーバーライドをサポートするためのWLC設定。
- 3. エンドクライアントのサプリカントの設定.
- ISE と AD の統合および ISE でのユーザー認証と認証ポリシーの設定
 - 1. adminアカウントを使用してISE Web UIインターフェイスにログインします。
 - 2. Administration > Identity management > External Identity Sources > Active directoryに移動します。



 Addをクリックし、Active Directory Join Point Name設定でドメイン名とIDストア名を入力 します。この例では、ISEがドメインに登録されwlaaan.com、ジョインポイントが AD.wlaaan.comとして指定されます。ローカルで有効なISE名です。

External Identity Sources		Connection		
@ • E •	÷	t Join Point Name	AD uters are	1 .
 Certificate Authentication Profile 		Join Point Name	AD.wiaaan.com] ()
Contractive Directory		 Active Directory Domain 	wlaaan.com] (i)
EDAP				-
CDBC				
RADIUS Token		Cubmit Consol		
RSA SecurID		Submic		
SAML Id Providers				
Cocial Login				

4. Submitのボタンを押すと、ポップアップウィンドウが開き、ISEをすぐにADに参加させるか どうかを尋ねられます。Yesを押し、Active Directoryユーザクレデンシャルと管理者権限を 入力して、ドメインに新しいホストを追加します。

Connection Whitelister	l Domains Passiv	eID Groups	Attributes	Advanced Settings	
• Join Point Name AD.v • Active Directory Domain wlas	laaan.com		(i) (i)		
👷 Join 🔮 Leave 🙎 Test User 🧧	Diagnostic Tool 🛛 🛞 Refre	sh Table			
ISE Node	▲ ISE Node Role	Status	Domain Controller	Site	
rmanchur-ise.wlaaan.com	STANDALONE	A Not Joined			
	Join Domain Please specify the crede • AD U Specify Organizat Store Cr	ntials required to Join ISE ser Name (i) Administrato * Password ****** ional Unit (i) redentials (i)	node(s) to the Active Dire	ctory Domain.	Ì

5. この時点を過ぎると、ISEがADに正常に登録されます。

nal Identity Sources	Connection Whitelisted Domains	PassiveID Groups Attributes Advance	ed Settings
E E E Cerificate Authentication Profile Active Directory LDAP DAP	Join Point Name AD.wlaaan.com Active Directory Domain wlaaan.com	0	
RADIUS Token	👷 Join 😟 Leave 👤 Test User 💼 Diagnostic Tool	😵 Refresh Table	
RSA SecurID	ISE Node ISE Node	le Role Status Domain Controller	Site
SAML Id Providers	rmanchur-ise.wlaaan.com STAND/	ALONE Operational WIN-CFA29CSRIL9.wlaaan.com	Default-First-Site-Name

登録プロセスに問題がある場合は、Diagnostic Tool を使用して、AD接続に必要なテストを実行できます。

6. それぞれの認可プロファイルを割り当てるために使用されるアクティブなディレクトリのグ ループを取得する必要があります。Administration > Identity management > External Identity Sources > Active directory >

> Groups に移動し、をクリックしてAddを選択Select Groups from Active Directoryします。

► System Identity Management 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	
Active Directory AD.wlaaan.com	Add Group	No data available
RSA SecuriD		
SAML IG Providers		

7. 新しいポップアップウィンドウが開き、特定のグループを取得するためのフィルタを指定す るか、ADからすべてのグループを取得することができます。 ADグループリストからそれぞれのグループを選択し、oxを押します。

Select Directory Groups × This dialog is used to select groups from the Directory. Domain wlaaan.com Name Filter * SID Filter * Type Filter GLOBAL Ŧ Retrieve Groups... 13 Groups Retrieved. Group SID Group Type Name wlaaan.com/Users/Cloneable Domain Controllers S-1-5-21-2222429329-4108085164-3220345271-522 GLOBAL wlaaan.com/Users/DnsUpdateProxy S-1-5-21-2222429329-4108085164-3220345271-1102 GLOBAL wlaaan.com/Users/Domain Admins S-1-5-21-2222429329-4108085164-3220345271-512 GLOBAL wlaaan.com/Users/Domain Computers S-1-5-21-2222429329-4108085164-3220345271-515 GLOBAL wlaaan.com/Users/Domain Controllers S-1-5-21-2222429329-4108085164-3220345271-516 GLOBAL wlaaan.com/Users/Domain Guests S-1-5-21-2222429329-4108085164-3220345271-514 GLOBAL wlaaan.com/Users/Domain Users S-1-5-21-2222429329-4108085164-3220345271-513 GLOBAL wlaaan.com/Users/Group Policy Creator Owners S-1-5-21-2222429329-4108085164-3220345271-520 GLOBAL ✓ wlaaan.com/Users/HR S-1-5-21-2222429329-4108085164-3220345271-1105 GLOBAL wlaaan.com/Users/Key Admins S-1-5-21-2222429329-4108085164-3220345271-526 GLOBAL wlaaan.com/Users/Marketing S-1-5-21-2222429329-4108085164-3220345271-1104 GLOBAL wlaaan.com/Users/Protected Users S-1-5-21-2222429329-4108085164-3220345271-525 GLOBAL wlaaan.com/Users/Read-only Domain Controllers S-1-5-21-2222429329-4108085164-3220345271-521 GLOBAL

OK Cancel

		Connect	ion		Whiteliste	d Domains	PassiveID		Groups	Attr	ibutes	Advanced Settings	
1	Ed		Add -	XD	elete Group	Update SID V	alues						
_	N		100 -	~ ~	ciece oroup	opulation of the			SID				
		vame						•		400000 44	00005464.00	00045074 4405	
	N	viaaan.co	om/Use	ers/HH	(S-1-5-21-2222	429329-41	08085164-32	20345271-1105	
	W	vlaaan.co	om/Use	ers/Ma	arketing				S-1-5-21-2222	2429329-41	08085164-32	20345271-1104	
Sa	ve	Rese	et										

9. ISEネットワークデバイスリストへのWLCの追加:Administration > Network Resources > Network Devicesに移動し、Addを押します。 WLC と ISE 間の WLC 管理 IP アドレスと RADIUS 共有秘密を指定して、設定を完了しま す。

Identity Services Engine	Home > Context Visibility > Operations > Policy = Administration > Work Centers
System Identity Management	Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC
Network Devices Network Device	Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM + Location Services
6	9
Network Devices	Network Devices List > New Network Device
Default Device	Network Devices
Device Security Settings	Decentation
	IP Address * * IP: 10.48.71.20 / 32
	O IPv6 is supported only for TACACS, At least one IPv4 must be defined when RADIUS is selected
	· Device Prome and Cisco •
	Model Name 🔪
	Software Version +
	* Network Device Group
	Location LAB Set To Default
	IPSEC Is IPSEC Device Set To Default
	Device Type WLC-lab Set To Default
	RADIUS Authentication Settings
	KADIUS UDP Settings
	* Shared Secret
	Cod Port 1700
	CONFOR 1/00 Set to beaut
	I romios nirs samula (1)

- 10. ISEをADに参加させ、デバイスリストにWLCを追加した後、ユーザの認証ポリシーと認可 ポリシーの設定を開始できます。
 - MarketingからVLAN1477に、またHRグループからVLAN1478にユーザを割り当てるには、認可プロファイルを作成します。

新しいプロファイルを作成するには、Policy > Policy Elements > Results > Authorization > Authorization profilesに移動し、Addボタンをクリックします。

dentity Services Engine	Home ► Context Visibility ► 0	Operations - Policy	 Administration 	Work Centers	
Policy Sets Profiling Posture Cli	ent Provisioning Policy Elements				
Dictionaries + Conditions - Results	5				
0					
Authentication	Standard Authorization Pr	ofiles			
- Authorization	For Policy Export go to Administrat	ion > System > Backup & F	Restore > Policy Export	Page	
	/ Edit 🕂 Add 🕞 Duplicate	X Delete			
Authorization Profiles	Name		Profile		Description
Downloadable ACLs	Blackhole_Wireless_Access		誌 Cisco 🕀		Default profile used to blacklist wireless dev
Profiling	Cisco_IP_Phones		👬 Cisco 🕀		Default profile used for Cisco Phones.
▶ Posture	Cisco_Temporal_Onboard		誌 Cisco 🕀		Onboard the device with Cisco temporal ag
	Cisco_WebAuth		📸 Cisco 🕀		Default Profile used to redirect users to the
Client Provisioning	NSP_Onboard		👬 Cisco 🕀		Onboard the device with Native Supplicant
	Non_Cisco_IP_Phones		誌 Cisco 🕀		Default Profile used for Non Cisco Phones.
	DenyAccess				Default Profile with access type as Access-
	PermitAccess				Default Profile with access type as Access-

• 各グループのVLAN情報を使用して認可プロファイルの設定を完了します。この例で はMarketingグループの設定を示します。

Dictionaries + Conditions - Results	
Q	
► Authentication	Authorization Profiles > New Authorization Profile
✓ Authorization	* Name Marketing
Authorization Profiles	Description Marketing
Downloadable ACLs	* Access Type ACCESS_ACCEPT *
▶ Profiling	Network Device Profile 🛛 🌐 🕀
Posture	Service Template
Client Provisioning	Track Movement
	Passive Identity Tracking 🔄 🕧
	▼ Common Tasks
	DACI Name
	Broc Reine
	ACL (Filter-ID)
	Security Group
	Advanced Attributes Settings
	Select an item 💟 = 🚺 🔿 — 🕂
	Manager and an and a second seco
	▼ Attributes Details
	Access Type = ACCESS_ACCEPT Tunnel-Fixed-Group-ID = 1:1477 Tunnel-Type = 1:13 Tunnel-Medium-Type = 1:6
	Submit Cancel

他のグループについても同様の設定を行い、それぞれのVLANタグ属性を設定する必要があります。

 認可プロファイルを設定した後、ワイヤレスユーザの認証ポリシーを定義できます。 この操作は、ポリシーセットを設定CustomDefault するか、変更することで実行できます。この例では、デフォルトポリシーセットを変更します。Policy > Policy Sets > Defaultに移動します。dot1x認証タイプのデフォルトではAll_User_ID_Storesが使用されますが、ADはAll_User_ID_StoresWLC_labのアイデンティティソースリストの一部であるため、現在のデフォルト設定でも機能します。この例では、それぞれのLABコントローラに対してより具体的なルールを使用し、認証の唯一のソースとしてADを使用します。

	era l'en	and course outside	waioning Pro	cy Liementa		Click here to do wireless setup and visibility setup Do	not show th	is again.
olicy	Sets →	Default					Reset	Sav
	Status	Policy Set Name	Descrip	6on	Conditions	Allowed Protocols / Server	r Sequenc	e H
Search								
	0	Default	Default p	tolicy set		Default Network Access	** *	
❤ Aut	enticatio	on Policy (4)						
۲	Statut	s Rule Name	Condi	tions		Use	Hits	Action
Searc	h							
	0	1440	OP	Wired_MAB		Internal Endpoints * *		
_			OR	Wireless_MA		> Options		-
				Wireless_802		10-ton or 1		
1	ø	WLC_lab	AND	E DEVICE Devi	pe EQUALS AI Device Types#WLC-lab	A Massion A	0	۰
				E DEVICE Loop	EQUALS Al Locations#LA8	Options		
	0	Derty	OB	Wired_802.10		Al_User_D_Stores × *		•
			OR	Wireless_802		> Options	Ŭ	~
	0	Defent				All_User_ID_Stores × *		~
		Denor				> Options	, v	Ť
> Aut	orization	Policy - Local Exceptions						
> Aut	orization	Policy - Global Exception	15					
	orization	Policy (12)						

 次に、グループメンバーシップに基づいてそれぞれの認可プロファイルを割り当てる ユーザの認可ポリシーを作成する必要があります。Authorization policyのセクションに移動 し、この要件を満たすためにポリシーを作成します。

Policy Se	ets Pro	Sling Posture Olient Provisioning	g 🕨 Poli	cy Demo	nts	Click here to do wireless setup and visibility	setup Do no	t show this	again.
Policy S	Sets +	Default					C	Reset	Save
	Status	Policy Set Name	Descript	tion	Conditions	Allowed Protocols	/ Server S	equence	Hits
Search									
	0	Default	Default p	olicy set		Default Network A	.0055	** +	0
> Auth	enticatio	n Policy (4)							
> Auth	orization	Policy - Local Exceptions							
> Auth	orization	Policy - Global Exceptions							
♥ Auth	orization	Policy (14)							
۲	Status	Rule Name	Condit	tions		Results Profiles Security Groups		Hits	Actions
Search	h								
1	0	Wreless_Marketing	AND	E F	Wreless_Access AD wlasan.com ExternalGroups EQUALS wlasan.com/Users/Marketing	(*Manadag) + Select tran lat	-	0	۰
.,	ø	Wreiess_HR	AND	С - н	Wineless_Access AD wisaan.com/Users/HR	C Selection lat		۰	۰

SSID「office_hq」のdot1x認証およびAAAオーバーライドをサポートするWLC設定

1. WLC上のRADIUS認証サーバとしてISEを設定します。Web UIインターフェイスのSecurity > AAA > RADIUS > Authentication セクションに移動し、ISE IPアドレスと共有秘密情報を指定します。

cisco	MONITOR WLANS CONTROLLER	WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Security	RADIUS Authentication Serve	ers > New
Security AAA General RADIUS Authentication Accounting Auth Cached Users Fallback DNS Downloaded AVP TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Dassuered Belision	RADIUS Authentication Server 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	<pre>2 \$ 2 \$ 10.48.39.128 ASCII \$</pre>
Local EAP	Support for CoA	Enabled \$
Advanced EAP	Server Timeout	5 seconds
Priority Order	Network User	C Enable
Certificate	Management	
Access Control Lists	Tunnel Provy	Enable
Wireless Protection Policies	PAC Provisioning	Enable
Web Auth	IPSec	Enable
TrustSec	Cisco ACA	Enable
Local Policies		
Umbrella		
Advanced		

2. WLCのWLANsセクションでSSIDoffice_hqを設定します。この例では、SSIDにWPA2/AES+dot1xお よびAAAの上書きを設定しています。適切なVLANはRADIUSを介して割り当てられるため 、WLANにはinterfaceDummyが選択されます。このダミーインターフェイスをWLC上に作成 し、IPアドレスを割り当てる必要がありますが、IPアドレスが有効である必要はなく、また 配置するVLANをアップリンクスイッチ内に作成することもできないため、VLANが割り当 てられていない場合は、クライアントはどこにも移動できません。

CISCO		<u>M</u> LANs (ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK			
WLANs	WLANs											
VLANs	Current Filter	a None		[Change Filte	er] [Clear Filter	1				Create New	¢	Go
Advanced	WLAN ID	Туре	Profile Na	me		WLAN SSID		Ad	min Status	Security Policies		
		WLAN	test			test		Ena	abled	[WPA2][Auth(802.1X)]		
	0 2	WLAN	AndroidAP			AndroidAP		Ena	abled	[WPA2][Auth(PSK)]		

							Saye Configuration Bing Logout Befresh
cisco	MONITOR WLANS	CONTROLLER	WIRELESS SEC	CURITY MANAGEMENT	COMMANDS HELP	FEEDBACK	A Home
WLANs	WLANs > New						< Back Apply
WLANs WUANs Advanced	Type Profile Name SSID ID	wLAN office office 3 ¢	ha ha				

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:1813 † Server 1 IP:10.48.39.128, Port:1813 † Server 2 None Server 3 None Server 4 None Server 5 None Server 6 None Authorization ACA Server Enabled Enabled Enabled	

eneral Security QoS P	olicy-Mapping Advanced	
Allow AAA Override	Enabled	DHCP
Coverage Hole Detection	Enabled	DHCP Server Override
Enable Session Timeout 2 1800 Session Aironet IE	Timeout (secs)	DHCP Addr. Assignment CRequired Management Frame Protection (MFP)
Diagnostic Channel 18	Enabled	
Override Interface ACL	IPv4 None IPv6 None IPv6	MFP Client Protection 2 Optional -
Layer2 Acl	None \$	DTIM Period (in beacon intervals)
URL ACL	None 🛊	
P2P Blocking Action	Disabled \$	802.11a/n (1 - 255) 1
Client Exclusion 2	Enabled I80 Timeout Value (secs)	802.11b/g/n (1 - 255) 1 NAC
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

3. また、ユーザVLAN用のダイナミックインターフェイスをWLC上で作成する必要もあります 。Controller > Interfaces UIメニューに移動します。 WLC は、その VLAN にダイナミックインター フェイスがある場合にのみ、AAA 経由で受信した VLAN の割り当てを受け入れます。

	<u>M</u> ONITOR <u>W</u> LANs	CONTROLLER	WIRELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Controller								
General	General Informatio	on						
Icons	Interface Name	vlan14	77					
Inventory	MAC Address	00:a3:	8e: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	on						
Ports	Port Number		1					
▶ NTP	Backup Port		0					
► CDP	Active Port		1					
▶ PMIPv6	Enable Dynamic AP Ma	anagement						
Tunneling	Interface Address							
▶ IPv6		_						
▶ mDNS	VLAN Identifier		14//					
Advanced	IP Address		255 255 255 0					
Lawful Interception	Gateway		192.168.77.1					
	IPv6 Address							
	Prefix Length		128					
	IPv6 Gateway		::					
	Link Local IPv6 Addres	ss	fe80::2a3:8eff:f	fee3:5a1a/64				
	DHCP Information							
	Primary DHCP Server		192.168.77.1					
	Secondary DHCP Serv	er						
	DHCP Proxy Mode		Global 🛟					
		-	<u> </u>					

確認

接続をテストするには、Windows 10ネイティブサプリカントとAnyconnect NAMを使用します。

EAP-PEAP認証を使用しており、ISEが自己署名証明書(SSC)を使用しているため、証明書の警告 に同意するか、証明書の検証を無効にする必要があります。企業環境では、ISEで署名済みの信 頼できる証明書を使用し、エンドユーザデバイスに適切なルート証明書が信頼できるCAリストに インストールされていることを確認する必要があります。

Windows 10およびネイティブサプリカントとの接続をテストします。

1. Network & Internet settings > Wi-Fi > Manage known networksを開き、Add new networkボタンを押して新しいネットワークプロファイルを作成します。必要な情報を入力します。

← Settings	
ش Wi-Fi	
Manage known networks	
Add a new network	Add a new network
+	Network name
Search this list	office_hq
Sort by: Preference \checkmark Filter by: All $$	Security type
	WPA2-Enterprise AES ~
	EAP method
11 contraction of the second sec	Authentication method
	Secured password (EAP-MSCHAP v2)
	Connect automatically
1772 Carlos C	Connect even if this network is not broadcasting
	Save Cancel

2. ISEの認証ログを確認し、ユーザに対して適切なプロファイルが選択されていることを確認 します。

c	Refresh Reset Repeat Counts	Export To •															Filter •	. - 0
	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 Profi	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		F4.8C.50.62.14.68	Unknown	Default >> W	Default >> Wireless_HR	HR						manchur-is	ю
	Feb 15, 2019 02:09:56.389 PM		à		800		F4/8C/50/62/14/68	Unknown	Default >> W	Default >> Wireless_HR	HR		WLC5520		Unknown		rmanchur-is	10

3. WLCでクライアントエントリをチェックし、エントリが正しいVLANに割り当てられ、 RUN状態にあることを確認します。

 cisco	MONITOR WLAN	s <u>C</u> ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK							Saye C	ionfigurat	ion <u>P</u> ing	g Logout	Befresh
Monitor	Clients																	Entries 1	- 1 of 1
Summary Access Points Cisco CleanAir	Current Filter	lone	t.	[Change_Filter]	(Clear.Filter)														
Statistics CDP	Client MAC Addr <u>f4:8c:50:62:14:6b</u>	IP Address/In 192.168.78.36	ov4/Iov6)		AP N AP40	Name 077.6D9E.6162			WLAN Profile office_hq	WLAN SSID office_hq	User Name Bob	Pro 802	tocol 11ac(5 GHz)	Status Associated	Auth Yes	Port S	lot Id	Tunnel No	Fastlane No
Rogues Clients																			
Sleeping Clients Multicast																			
Applications																			

4. WLC CLIから、 show client dertails

:

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

Client Webauth Username N/A Hostname: Device Type: Intel-Device AP 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

Windows 10およびAnyconnect NAMとの接続をテストします。

1. 使用可能なSSIDのリストからSSIDを選択し、それぞれのEAP認証タイプ(この例では PEAP)と内部認証フォームを選択します。

	Sisco AnyC	Connect Secure Mobility Client — 🗌 🗙
	Web Authent	VPN: Use a browser to gain access.
	Ľ	Network: Connected (10.103.150.57) internet
Cisco AnyConnect		× curity: e Key.
Enter informat	ion for the connection.	
Media:	Wi-Fi	
	Hidden Network	
Descriptive Name:	office_hq	Scap
SSID:	office_hq	can not required on current Wi-Fi.
Security:	WPA2 Enterprise AES	
802. 1X Configuration		
password	Y PEAP Y	g Security:
		not currently protected by Umbrella.
	OK Ca	ncel

2. ユーザー認証の対象となるユーザー名とパスワードを入力します。

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

3. ISEはSSCをクライアントに送信するため、証明書を信頼することを手動で選択する必要が あります(実稼働環境では、信頼できる証明書をISEにインストールすることを強く推奨し ます)。

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@	VPN: Verify your network connection.	
Issued To: rmanchur-ise.wlaaan.com Issued By: rmanchur-ise.wlaaan.com Expiration Date: 2020-02-13 15:03:40 UTC	Network: Authenticating	
Trust Do Not Trust	office_hq 🗎 🔐 🖂 📰	
	Web Security: No License Key.	

4. ISEの認証ログを確認し、ユーザに対して適切な認可プロファイルが選択されていることを 確認します。

C Refresh O Reset Repeat Co	ints 📓 Export To •																	¥ Filter •	۰.
Time	Status	Details	Repeat	Identity		Endpoint ID		Endpoint P	Authenticat	Authorization Policy	Authorizati	IP Address		Network Device	Device Port	Identity Group	Posture St	Server	Mdm
×				Alice	×	60	×	Endpoint Prof	Authentication	Authorization Policy	Authorization	IP Address		Network Device	Device Port	Identity Group	Posture Statu	Server	Mdm
Feb 15, 2019 02:51:27.163 PM	٠	ò	0	Alice		F4.8C.50.62.14.68		Microsoft-W	Default >>	Default >> Wireless_Marketing	Marketing	192.168.77.32						manchur-ise	
Feb 15, 2019 02:51:24.837 PM	2	à +		Alce	٠	F4:8C:50:62:14:68	٠	Morosoft-W	Default >>	Default >> Wireless_Marketing	Marketing		*	WLC5520		Workstation 💠		manchur-ise 💠	

5. WLCでクライアントエントリをチェックし、エントリが正しいVLANに割り当てられ、 RUN状態にあることを確認します。

Clients											Entries 1 - :
Current Filter No	ne	[Change Filter] [Clear Filter]									
(4:8c:50:62:14:6b	192.168.77.32		AP Name AP4C77.6D9E.6162	office ho	office hg	Alice	802.11ac(5 GHz)	Associated	Yes 1	Slot Id	No

6. WLC CLIDS , show client dertails

:

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

Client State	Associated
User Authenticated by	RADIUS Server
Client User Group	Alice
Client NAC OOB State	Access
Wireless LAN Id	3
Wireless LAN Network Name (SSID)	office_hq
Wireless LAN Profile Name	office_hq
Hotspot (802.11u)	Not Supported
Connected For	765 secs
BSSID	70:69:5a:51:4e:cd
Channe1	36
IP Address	192.168.77.32
Gateway Address	192.168.77.1
Netmask	255.255.255.0
Policy Manager State	RUN
Policy Type	WPA2
Authentication Key Management	802.1x
Encryption Cipher	CCMP-128 (AES)
Protected Management Frame	No
Management Frame Protection	No
EAP Type	PEAP
Interface	vlan1477
VLAN	1477

トラブルシュート

1. WLCとISEの間のRADIUS接続をテストするにはtest aaa radius username

password

wlan-id

を使用し、結果を表示するにはtest aaa show radiusを使用します。

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

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	0x00000013 (19)
Cisco / Audit-Session-Id	1447300a0000003041d5665c
Acct-Session-Id	5c66d541/00:11:22:33:44:55/743

test radius auth request successfully sent. Execute 'test aaa show radius' for response (Cisco Controller) >test aaa show radius Radius Test Request Wlan-id..... 2 ApGroup Name..... none Radius Test Response Radius Server Retry Status _____ -----10.48.39.128 1 Success Authentication Response: Result Code: Success Attributes Values -----_____ User-Name Alice ReauthSession:1447300a000003041d5665c State Class

 Class
 CACS:1447300a000003041d5665c:rmanchur-ise/339603379/59

 Tunnel-Type
 0x000000d (13)

 Tunnel-Medium-Type
 0x0000006 (6)

 Tunnel-Group-Id
 0x000005c5 (1477)

(Cisco Controller) >

2. debug client

を使用して、ワイヤレスクライアントの接続の問題をトラブルシューティングします。

3. WLCの認証と認可の問題をトラブルシューティングするには、debug aaa all enableコマンドを使用します。



注:デバッグが行われるMACアドレスに基づいて出力を制限するには、このコマン ドとのみdebug mac addrを使用します。

4. 認証の失敗の問題とAD通信の問題を特定するには、ISEライブログとセッションログを参照してください。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。