cisco.



8.5 Identity PSK 機能導入ガイド

製品や機能の概要 2
IPSK ソリューション 3
8.5 リリースでの IPSK の設定手順 3
コントローラ設定の手順 6
IPSK と組み合わせた WLC ローカル ポリシー 10
WLC のプロファイリングとポリシー エンジンの概要 11
範囲と目的 12
プロファイリングおよびポリシーの設定 13
WLAN でのポリシーのマッピング 17
エンドユーザデバイスの設定 20
まとめ 22
CLI コマンドを使用した IPSK の設定 23

改訂: 2018年11月28日

製品や機能の概要

「IoT: Internet of Things(モノのインターネット)」の到来により、インターネットに接続されるデバイスの数は非常 に増加しています。これらのすべてのデバイスが802.1xサプリカントをサポートしているわけではなく、インターネッ トに接続するための代替メカニズムが必要です。セキュリティメカニズムの1つである WPA-PSK が代替手段として 考えられます。現在の設定では、事前共有キーは同じ WLAN に接続するすべてのクライアントで同じです。教育機関 などの一部の設置環境では、これによりキーが不正ユーザに共有され、セキュリティ違反をもたらします。したがっ て、前述の内容やその他の要件により、大規模な環境ではクライアントごとに一意の事前共有キーを準備しておく必要 が生じます。

- Identity PSK は、同じ SSID の個人またはユーザ グループのために作成された一意の事前共有キーです。
- クライアントに複雑な設定は必要ありません。PSK と同じシンプルさで、IoT、BYOD、ゲストに対して最適に展開できます。
- •802.1x 未対応のほとんどのデバイスでサポートされるため、より強力な IoT セキュリティを実現します。
- ・他に影響を与えずに1つのデバイスまたは個人に対するアクセスを簡単に取り消せます。
- ・何千ものキーを簡単に管理でき、AAA サーバを介して配布することができます。



上の図に示すように、従来のPSKでは、特定のSSIDに接続するすべてのクライアントのキーは同じなので、セキュリ ティ上の問題につながります。Identity PSKでは、同じSSIDに接続するクライアントごとに別のキーを設定できます。

IPSK ソリューション

クライアントの認証時に、AAA サーバはクライアントの MAC アドレスを認証し、Cisco-AVPair リストの一部として パスフレーズ(設定されている場合)を送信します。WLC は RADIUS 応答の一部としてこれを受信し、PSK の計算の ため追加処理します。

クライアントがアクセスポイントからブロードキャストされているSSIDにアソシエーション要求を送信すると、ワイ ヤレスLAN コントローラはクライアントの特定のMACアドレスを含むRADIUS要求パケットを形成し、RADIUSサー バに中継します。

RADIUSサーバは認証を実行し、クライアントが許可されているかどうか、およびWLCへの応答としてACCESS-ACCEPT または ACCESS-REJECT のいずれかを送信するかどうかをチェックします。

Identity PSK をサポートするために、認証サーバは、認証応答を送信するだけでなく、この特定のクライアントに対して AV Pair パスフレーズを提供します。これは PSK の計算のためにさらに使用されます。

RADIUS サーバは、クライアントに特有のユーザ名、VLAN、QoS などの追加パラメータをこの応答で提供することもできます。単一ユーザが所有している複数のデバイスのためにパスフレーズを同一にしておくこともできます。



Private PSK On The same WLAN

8.5 リリースでの IPSK の設定手順

IPSK は、Cisco AV-pair をサポートする AAA サーバで設定できます。この導入ガイドでは、Cisco Identity Service Engine での設定に焦点を合わせます。ISE 2.2 構成手順

手順

ステップ1 次のように ISE でテスト対象のワイヤレスコントローラを追加し、[Radius Authentication Setting] で secret password を設定して [Submit] をクリックします。

dentity Service	ces Engine	Home ► Conte	xt Visibility	• Operations	▶ Policy	 Administration 	🗌 🕨 Wo	ork Centers	
► System ► Identit	y Management	- Network Resources	Device F	Portal Manageme	ent pxGrid S	Services + Feed	Service	Threat Centric N	NAC
✓ Network Devices	Network Device O	Groups Network De	vice Profiles	External RADIU	JS Servers	RADIUS Server Se	equences	NAC Managers	E
	0								
Network devices		Network Devi	ices						
Default Device		8 m 8			A F = 1		Maria	20.00	
Device Security Settings	S	/ Edit Add			Export +	Generate PAC	× Delete	•	
		Name	10.2 10.1	10.10.2/32			All Location	1 tions	
dede Martin Oraciana	-								
System Identity Services	nagement Network	Context Visibility Resources Device Pr	Operations	Policy Admir Active Admir	Eeed Service	Fork Centers			
Network Devices Network	work Device Groups	Network Device Profiles	External RADIUS S	Servers RADIUS S	erver Sequences	NAC Managers Ex	ternal MDM	Location Services	
	0								
Network devices	Netwo	work Devices	York Device						
Default Device			Name NAD						
Device Security Securitys		Des	cription Wireless	Controller					
		* IP Address: 10.10.10.2	2 /	32	_				
		* Device	Profile data Cisco	• @					
		Mada							
		Software \	Version 85	*					
			0.5						
		* Network Device Group							
	ſ	Device Type All Device Typ	es 📀 Se	et To Default					
		IPSEC Is IPSEC Device	ce 📀 S	et To Default					
	× .	All Locations	S	et To Default					
	×.	RADIUS Authentication	Settings						
		TACACS Authentication	Settings						
		SNMP Settings							
		Advanced TrustSec Sett	ings						
	Sub	mit Cancel							

ステップ2 以下の例に示すように、[Policy] > [Results] > [Authorization] > [Authorization Profiles] > [IPSK-Device] で Authorization Profile を作成し、確認します。

dentity Services Engine Ho	me	s Policy Administration Work Centers	License Warning 🔺 🔍 🔞
Authentication Authorization Profiling	Posture Client Provisioning Postcy	Elements	Click here to do wireless setup and visibility setup Do not show this
Dictionaries Conditions Results			
Authentication	Standard Authorization Profiles	rstern > Backup & Restore > Policy Export Page	
- Authorization		na de la production de la construcción de la construcción de la construcción de la construcción de Estas se	Selected 0 Total 8
Authorization Profiles	🥖 Edit 🕂 Add 🖓 Duplicate 🗙 De	lete	Show All
Downloadable ACLs	Name	Profile	Description
Downloadable ACLS	Blackhole_Wireless_Access	🗰 Cisco 🕀	Default profile used to blacklist wireless devices. Ensure that
Profiling	Cisco_IP_Phones	就 Cisco 🕀	Default profile used for Cisco Phones.
▶ Posture	Cisco_WebAuth	誌 Cisco 🕀	Default Profile used to redirect users to the CWA portal.
	IPSK-device	🗰 Cisco 🕀	Identity PSK
Client Provisioning	NSP_Onboard	🚓 Cisco 🕀	Onboard the device with Native Supplicant Provisioning

ステップ3 以下の例に示すように、[Access Type] が [Access_Accept]、cisco-av-pair が psk-mode と psk password で設定 した Authorization Profile を作成します。

dentity Services Engine	Home	 Operations 		Administration	Work Centers	
Authentication Authorization Profili	ng Posture Client Provisionin	g Policy Elem	ents			Click h
Dictionaries ► Conditions	s					
Authentication	Authorization Profiles > IPSK-de	evice				
- Authorization	* Name IP	SK-device				
Authorization Profiles	Description Id	lentity PSK				
Downloadable ACLs	* Access Type AC	CCESS_ACCEPT	*			
▶ Profiling	Network Device Profile	🖁 Cisco 🔻 🕀				
Authorization Profiles	- Advanced Attribu	tes Settings				
Downloadable ACLs						
▶ Profiling	Cisco:cisco-av-pair	0	= psk-mod	le=ascii	O -	
Posture	Cisco:cisco-av-pair	0	= psk=abo	:12345		
Client Provisioning						
	▼ Attributes Details					
	Access Type = ACCESS cisco-av-pair = psk-mod cisco-av-pair = psk=aba	_ACCEPT de=ascii c12345				
	Save Reset	J				

- ステップ4 次の例に示すように、[Policy] > [Authorization] で IPSK で使用されるすべてのデバイスまたはユーザ MAC アドレスのルールを設定します。必要であれば、複数の MAC アドレス エントリを使用できます。
 - (注) ルールは、ステップ3で作成したプロファイルにリンクされます。
 - (注) デバイスのMacアドレスが正しく設定されていることを確認してください。今回の例では、Apple 製 MacBook の Mac アドレスを設定しています。

uth efine	e the Auth	on Policy	iles based on ide	entity group	s and/or other conditions. Drag and drop rules to change the order		Click here to do wireless	5 51
irst	Matched F	Rule Applies			chorr ago			
E St	Exception	ns (0)	°					
	Status	Rule Name		Conditio	ns (identity groups and other conditions)	1	Permissions	
		IdentityPSK		(Wireles A0:3B:E	s_MAB AND Radius:Calling-Station-ID EQUALS 3:95:73:4E)	then	IPSK-device	
		IdentityPSK_copy		(Wireles f4:5c:89	s_MAB AND Radius:Calling-Station-ID EQUALS 8f:10:43)	then	IPSK-device	
	~	Wireless Black List Default	1	Blackli	t AND Wireless_Access	then	Blackhole_Wireless_Acce	ess
		Profiled Cisco IP Phones	i	Cisco-I	P-Phone	then	Cisco_IP_Phones	
	Status F	Rule Name	Conditions (id	lentity groups	and other conditions) Permissions			
		IdentityPSK	if Any	<a>and	Wireless_MAB AND Radius:Callin Chem IPSK-device	1		
ø	I	dentityPSK_copy	f4:5c:89:8f:10	B AND Radiu :43)	Condition Name Description Wireless_MAB ONormalised Radius:RadiusFlowType EQUALS Wire	lessMAB	AND -	
	V	Vireless Black List Default	If Blacklist AN	Wireless_A	Radius:Calling-Sta 📀 Equals 👻	A0:3B:E	:3:95:73:4E 📀	
	F F	Profiled Cisco IP Phones	Cisco-IP-Pho	ne	MAC address v			

ステップ5 上記のすべての手順が実行され、すべての設定が適用され保存されたことを確認します。

コントローラ設定の手順

手順

ステップ1 次の例の Pod1-IPSK に示すように、コントローラの WLAN を作成します。

iliilii cisco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> ONTROLL	.er w <u>i</u> reless <u>s</u> ecu	IRITY MANAGEMENT
WLANs	WLANs > Edit 'Identity PS	SK'	
▼ WLANs WLANs	General Security Qo	Policy-Mapping	Advanced
▶ Advanced	Profile Name Type SSID Status Security Policies	Identity PSK WLAN Pod1-IPSK C Enabled	Auth(PSK)]
	Radio Policy Interface/Interface Group(G) Multicast Vlan Feature Broadcast SSID NAS-ID	Mac Fintering[WFA2][(Modifications done under All ▼ management ▼ Enabled Enabled none	security tab will appea

ステップ2 WLAN でセキュリティとして WPA2/PSK に設定し、MAC フィルタリングを有効にします。以下の例では、PSK キーとして PSK = 12345678 を使用しています。

uluilu cisco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> ONTROLLER W <u>I</u> RELESS <u>S</u> ECURITY M <u>A</u> NAGEMENT
WLANs	WLANs > Edit 'Identity PSK'
WLANs	General Security QoS Policy-Mapping Advanced
Advanced	Layer 2 Layer 3 AAA Servers
	Layer 2 Security WPA+WPA2 MAC Filtering Fast Transition Fast Transition Adaptive Over the DS Reassociation Timeout 20 Seconds Protected Management Frame PMF Disabled WPA+WPA2 Parameters
	WPA Policy
	WPA2 Policy WPA2 Encryption OSEN Policy OSEN Policy

ステップ3 WLAN でセキュリティとして WPA2/PSK に設定し、PSK を設定します。以下の例では、PSK キーとして PSK = 12345678 を使用しています。

Advanced	Authentication Key Management 19
	802.1X Enable
	PSK 🕑 Enable
	FT 802.1X Enable FT PSK Enable PSK Format ASCII V

ステップ4 WLC で認証サーバを ISE IP アドレスを使用して設定し、上記の手順で作成した WLAN Pod1-IPSK に適用 します。この例では、ISE の IP アドレスは 10.91.104.106 です。

iliilii cisco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> ONTROLLER W <u>I</u> RELESS <u>S</u> ECURITY M <u>A</u> NAGE	EMEN
WLANs	WLANs > Edit 'Identity-PSK'	
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 V RADIUS Servers RADIUS Server Overwrite interface Enabled Apply Cisco ISE Default Settings Enabled	WLAN
	Authentication Servers Accounting Servers	
	🖤 Enabled 🖤 Enabled	
	Server 1 IP:10.91.104.106, Port:1812 V IP:10.91.104.106, Port:18	13 🔻
	Server 2 None V None	

ステップ5 最後に、[WLAN advanced settings] で AAA Override を有効にします。

CISCO	MONITOR WLANS CONTROL	ller W <u>i</u> reless <u>s</u> ecu	irity m <u>a</u> nageme
WLANs	WLANs > Edit 'Identity-F	PSK'	
WLANs	General Security Q	oS Policy-Mapping	Advanced
▶ Advanced	Allow AAA Override	🕑 Enabled	
	Coverage Hole Detection Enable Session Timeout	Enabled 28800 Section Timesuit (case)	
	Aironet IE	Enabled	
	Diagnostic Channel <u>18</u> Override Interface ACL	□Enabled IPv4 None ▼	IPv6
	Layer2 Acl	None T	[None -
	URL ACL P2P Blocking Action	None T	1
	Client Exclusion 3	Enabled 180	

IPSK と組み合わせた WLC ローカル ポリシー

AVC と同じように、mDNS またはオープン DNS プロファイルは、特定のデバイスタイプのクライアントのためにロー カルポリシーにマップできます。IPSK は、コントローラのローカルポリシーと組み合わせたり、特定の WLAN にマッ ピングしたりすることもできます。AV-pair=PSK-mode および PSK-password を ISE などの AAA サーバで設定する場 合、管理者は、別の AV-pair=roleを追加することで、たとえば、教師または学生のグループに対して、その特定のロー ルに対するローカルポリシーを設定することもできます。各ローカルポリシーは異なったプロファイル名、ACL、ロー ル、デバイスタイプ、および、同じ WLAN でプロファイルにより許可されていないサービスを利用/拒否することがで きることから、ポリシーを制限/許可する AAA オーバーライドに基づいて、アクティブ時間までも使用して設定できま す。

同一の WLAN で IPSK とローカル ポリシーを組み合わせると、多くのさまざまな展開シナリオで制限なく使用できます。

たとえば、学内管理者は、学生が IPSK でログインし、グループ Students に属する学生のみ、特定のアプリケーション に特定の帯域幅と特定のデバイスで、特定の時間アクセスできるローカル ポリシーを適用するように設定できます。 IPSK とローカル ポリシーを組み合わせることで、実質的に無制限の多様な機能を使用できます。

CISCO	MONITOR WL	ANS <u>C</u> ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS
ecurity	Policy > Edit					
AAA General	Policy Name				IPSK-test	
 RADIUS Authentication Accounting Fallback 	Policy Id				1	
DNS Developeded W/D	Match Criteria					
TACACS+ LDAP Local Net Users MAC Filtering	Match Role Strin Match EAP Type	19	none T]		
Disabled Clients Uses Legin Policies	Device List					
AP Policies Password Policies	Device Type				Add	
Advanced EAP Priority Order	Action					
Certificate	IPv4 ACL		none	T		
Access Control Lists	URL ACL		none	T		
Wireless Protection	VLAN ID		0			
Policies	Qos Policy		none	•		
Web Auth	Average Data Ra	ate(kbps)	0			
TrustSec	Average Real tim	ne Data Rate(kbps)	0			
	Burst Data Rate	(kbps)	0			
Advanced	Burst Real time	Data Rate(kbps)	0			
	Session Timeou	t (seconds)	1800			
	Sleeping Client 1	Timeout (min)	720			
	Flexconnect AC		none V			
	AVC Profile	50.	none	•	T	
	mDNS Profile		none	T		
	OpenDNS Profile	•	none 🔻	<u> </u>		
	Active Hours					
	Day		Mon	-		
	Start Time		Hours	s Mins		
	End Time		Hours	s Mins		
			Add			
	Day	Start Ti	me	E	End Time	

WLC のプロファイリングとポリシー エンジンの概要

Cisco では、ISE を介してデバイスの識別、オンボーディング、ポスチャ、およびポリシーを実行する、豊富な機能を 提供しています。WLC では新たに、ネットワーク上のエンドデバイスを識別するために DHCP、HTTP などのプロト コルに基づくデバイスのプロファイリングを行います。ユーザは、デバイス ベースのポリシーを設定し、ネットワー ク上のユーザごと、またはデバイスポリシーごとに適用できます。WLC では、ユーザごと、またはデバイスエンドポ イントごとに基づく統計情報とデバイスごとの適切なポリシーも表示できます。 BYOD (Bring Your Own Device) では、この機能がネットワーク上のさまざまなデバイスの理解に影響します。この機能を使うことで、WLC 自身で小規模に BYOD を実装できます。

範囲と目的

このセクションでは、AireOS8.5 コードを動かしている Cisco WLC でプロファイリングとポリシーを設定して実行します。

プロファイリングとポリシーの適用は、2つの異なるコンポーネントとして設定します。WLC での設定は、前のセク ションで設定したように、IPSK セキュリティを使用してネットワークに参加するクライアントに特有な定義済みパラ メータに基づきます。対象のポリシー属性は次のとおりです。

- 1. Role: ユーザが属するユーザタイプまたはユーザグループを定義
- 2. PSK-mode : ASCII

PSK-password:特定のPSK パスワードとデバイスのMACアドレスとの一致

たとえば、学生、従業員など

3. Device: デバイスのタイプを定義

たとえば、Windows マシン、スマートフォン、iPad や iPhone などの Apple デバイス

4. Time of day:設定で、エンドポイントがネットワーク上で許可される時間を定義

上記のパラメータはポリシーー致属性として設定できます。WLCでは、上記のパラメータに(エンドポイントごとに) 一致する通信を検出すると、ポリシーを適用します。ポリシーの適用は次のようなセッション属性に基づいています。

- VLAN
- ACL
- •セッションタイムアウト
- QoS
- •スリープ状態のクライアント
- FlexConnect ACL
- AVC プロファイル
- mDNS プロファイル
- ・オープン DNS プロファイル
- ・セキュリティグループタグ

ユーザは、これらのポリシーを設定し、指定したポリシーをエンドポイントに適用できます。ワイヤレス クライアン トは、MAC アドレス、MAC OUI、DHCP、HTTP ユーザ エージェント(HTTP プロファイリングを成功させるために は、Internetへのアクセスが必要)に基づいて、プロファイリングされます。WLC はこれらの属性と定義済みの分類プ ロファイルを使用して、デバイスを識別します。

プロファイリングおよびポリシーの設定

手順

ステップ1 WLAN でデバイス プロファイリングを設定するには、ネイティブ プロファイリングおよびポリシーを設定する対象となる特定の WLAN に移動して、[Advanced] をクリックします。[Allow AAA Override] が有効になっている場合は、無効にします。[DHCP]の [DHCP Addr. Assignment]。

Allow AAA Override Enabled DHCP Coverage Hole Detection Ø Enabled DHCP Server Override Enable Session Timeout Ø Enabled DHCP V6 Server Override Aironet IE Ø Enabled DHCP Addr. Assignment Ø Required Diagnostic Channel Enabled DHCP Addr. Assignment Ø Required Override Interface ACL IPv4 None IPv6 None : OEAP Layer2 Acl None Split Tunnel Enabled P2P Blocking Action Disabled Management Frame Protection (MFP)	Seneral S	Security	QoS I	Policy-Mapping	Advanced			
Coverage Hole Detection	Allow AAA Ov	verride	Enable	d		DHCP		
Enable Session Timeout Session Timeout (secs) DHCP V6 Server Override Aironet IE ØEnabled Diagnostic Channel Enabled Override Interface ACL IPV4 None : IPv6 None : OEAP Layer2 Acl None : Split Tunnel Enabled P2P Blocking Action Disabled : G0 Management Frame Protection (MFP)	Coverage Hol	le Detection	S Enable	d		DHCP Server	Override	
Aironet IE Ø Enabled Diagnostic Channel Enabled Override Interface ACL IPv4 None : 1Pv6 None : OEAP Layer2 Acl None : 0Sabled :: Split Tunnel Disabled :: Enabled	Enable Sessio	on Timeout	Sessio	on Timeout (secs)		DHCP V6 Server	Override	
Diagnostic Channel Enabled DHC P AGAT. Assignment & Required Layer 2 Ad None : IPv6 None : OEAP 228 Bicking Action Disabled : Split Tunnel Enabled P29 Bicking Action Disabled : Management Frame Protection (MFP)	Aironet IE		Enabled	t			d and the	
Override Interface ACL IPv4 None : IPv6 None : OEAP Layer2 Acl None : Split Tunnel Enabled P2P Blocking Action Disabled : Implement Frame Protection (MFP)	Diagnostic Ch	hannel	Enabled	t		DHCP Addr. Assignment	Rednied	
Layer2 Acl None : Split Tunnel Enabled P2P Blocking Action Disabled : Client Enabled Management Frame Protection (MFP)	Override Inte	erface ACL	IPv4 Nor	ne :	1Pv6 None :	OEAP		
P2P Blocking Action Disabled : Management Frame Protection (MFP)	Layer2 Acl		None :	:)		Split Tunnel	Enabled	
Client Bydyrian 3 60 Management Frame Protection (MFP)	P2P Blocking	Action	Disabled	:				
CICIL CAUVERING CONSIST	Client Exclusi	ion 2	Eashlad	60		Management Frame Prote	ction (MFP)	
	Maximum Alle	lowed Clients	0			MFP Client Protection 4	Optional :	
Maximum Allowed Clients 0 MFP Client Protection d Optional :	2					DTIM Period (in beacon in	tervals)	

ステップ2 [DHCP Required] オプションを有効にした後、スクロール ダウンし、[Local Client Profiling] で、[DHCP Profiling] と [HTTP Profiling] が有効でない場合は有効にして、[Apply] をクリックします。

/LANs > Edit 'POD1-d	ot1x'				< Back	Apply
General Security	QoS Policy-Mapping	Advanced				
Mgmt Via Wireless	Enabled		Passive Client	0		
Off Channel Scanning Defer			Voice			
Scan Defer Priority	0 1 2 3 4 5 6 7		Media Session Snooping	Enabled	-	
			Re-anchor Roamed Voice Clients	Enabled		
Scan Defer Time(msecs)	100		KTS based CAC Policy	Enabled		
FlexConnect	· · · · · · · · · · · · · · · · · · ·		Radius Client Profiling			
FlexConnect Local			DHCP Profiling	0		
Switching 2	Enabled		HTTP Profiling	0		
FlexConnect Local Auth 12	Enabled		Local Client Profiling			
Learn Client IP Address 🧕	Senabled		DHCP Profiling	☑ ←		
Vian based Central	Enabled		HTTP Profiling			
Switching 13	Enabled		PMIP			
Central DHCP Processing	Enabled		PMIP Mobility Type	0	- 54	
Override DNS	Enabled		PMIP NAI Type	Hexadecimal :		
NAT-PAT	Enabled					0

WLC GUI から WLAN でポリシーを作成

ステップ3 プロファイルを設定したら、ローカルポリシーの作成とWLANでの適用に進みます。WLCメニューバーで、[Security] > [Local Policies] に移動すると、ポリシー リストの作成画面が表示されます。

uluilu cisco	Monitor Wlans <u>C</u> ontroller Wireless	<u>security management commands help f</u> eedback
Security	General	
AAA General RADIUS Authentication Accounting Falback DNS TACACS+ Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies	Maximum Local Database entries (on next reboot). Number of entries, already used	2048 (Current Maximum is 2048) 3
Local EAP		
Priority Order		
Certificate Control Lists Wireless Protection Policies Web Auth TrustSec SXP Local Policies	-	
Advanced		

ステップ4 [Local Policy List] で、[New] をクリックして、ポリシー名を作成します。この例では、teacher-LP をポリ シー名として使用していますが、任意の名前を使用して独自のポリシーを定義することもできます。

MONITOR			WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	FEEDBACK		
Policy > N	Vew								< Back	Apply
Policy Nar	ne	eacher-LP]		-					

ポリシー名を設定した後、[Role]、[EAP Type]、[Device Type] が一致するようなポリシーを作成できます。 また、一致条件に関連する必要なアクションを定義できます。

ここでは、[User Role] と [Device Type] を [Match Criteria] に使用していますが、必要に応じて任意のタイプ を使用できます。

- (注) [Match Role string] が AAA で定義されたロール名と同じであることを確認してください。この例では、「teacher」と定義されています。
- ステップ5 [User Role] を入力し、[Apply] をクリックします。ここではロール名「teacher」が例として使用されています。
- ステップ6 ユーザデバイスに基づいてポリシーを適用するには、[Device List] で、[Device Type] ドロップダウン リストから、ポリシーを適用するデバイス タイプを選択し、[Add] をクリックします。

ここで、[Match Criteria] に対し、デバイスタイプとして [Apple-iPad] を使用しています。Apple-iPhone やその他の Apple デバイスも同様に [Device Type] ドロップ ダウン リストから追加できます。

- (注) 任意のデバイス タイプと一致させない場合は、[Device Type] オプションを設定しないでください。
- **ステップ7** 適切なアクションを適用するには、[Action]のパラメータから選択して、ポリシーを適用します。最後のセ クションで定義されている AVC プロファイルを選択します。

uluulu cisco	MONITOR WLANS CONTROLLER	. WIRELESS SECURITY MANAGEMENT COMMANDS
Security	Policy > Edit	
AAA	Policy Name	IPSK-test
* RADIUS	Policy Id	1
Authentication Accounting	ALCON ANY	
Fallback DNS	Match Criteria	
Downloaded AVP TACACS+	Match Role String	teacher
LDAP Local Not Users	Match EAP Type	none 🔻
MAC Filtering		
 Disabled Clients User Login Policies 	Device List	
AP Policies Password Policies	Device Type	Add
Local EAP		THEN .
Advanced EAP		
Priority Order	Action	
Certificate	IPv4 ACL	none V
Access Control Lists	URL ACL	none T
Wireless Protection Policies	VLAN ID	0
Web Auth	Qos Policy	none
TrustSec	Average Data Rate(kbps)	0
Local Policies	Average Real time Data Rate(kbps)	0
OpenDNS	Burst Data Rate(kbps)	0
Advanced	Burst Real time Data Rate(kbps)	0
	Session Timeout (seconds)	1800
	Sleeping Client Timeout (min)	720
	Flexconnect ACL	none 🔻
	AVC Profile	AUTDQOS-AVC-PROFILE V
	mDNS Profile	default-mdns-profile 🔻
	OpenDNS Profile	none T
	Active Hours	
	Day	Mon
	Start Time	10 Hours 15 Mins
	End Time	22 Hours 30 Mins
		Add
	Day Start T	ime End Time

(注) ローカルポリシーの設定の詳細についてはリンク先を参照してくださいhttp://www.cisco.com/c/en/ us/td/docs/wireless/controller/8-3/config-guide/b_cg83/b_cg83_chapter_01110.html

ステップ8 ユーザは、1つ以上のローカルポリシーを作成し、「student-LP」の学生に適用できます。

(注) [Match Role string] が AAA/Radius サーバで定義されたロール名と同じであることを確認してください。

Policy > Edit					
Policy Name	student-LP				
Policy Id	6				
Match Criteria					
Match Role String	student				
Match EAP Type	none ‡				
Device List					
Device Type	Android				
Apple-iPad					
Action					
IPv4 ACL	none :				
VLAN ID	0				
Qos Policy	(none ‡)				
Session Timeout (seconds)	1800				
Sleeping Client Timeout (min)	720				
Flexconnect ACL	none 🗘				
AVC Profile	student-AVC 🛟 🛶				
mDNS Profile	(none ‡)				
Active Hours					
Day	(Mon ‡				
Start Time	Hours Mins				
End Time	Hours Mins				
	Add				

ステップ9 その他のデバイスのデフォルトのローカル ポリシーを作成します。

ローカルポリシーに他のACLが適用されていない場合、Apple-iPad以外の他のデバイスは、すべてのポリシーの最終フィルタ機能が [Allow all] なので、アプリケーションにアクセスできます。

Apple-iPad を除くすべてのデバイスのすべてのアプリケーションをブロックするために、[deny all] ACL を 作成してローカル ポリシーに適用し、その後、WLAN にそのポリシーを適用します。下記のスクリーン ショットから設定例を参照してください。

すべての IPv4 フローをブロックする ACL を作成します。

cisco	MONI	TOR 1	<u>w</u> lans		R WIRELESS	SECURITY	MANAGEMENT	COMMANDS	Save C HELP	Configuration FEEDBACK	l <u>P</u> ing Logout :	Refres
Security	Acce	ess Co	ntrol Li	ists > Edit						< Back	Add New R	tule
General	Gene	eral										
Authentication	Acces	s List Na	me	deny-all								
Accounting Fallback DNS Downloaded AVP FTACACS+	Deny	Action	Source IP/M	0 ce ask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits	
LDAP Local Net Users MAC Filtering Disabled Clients	1	Deny	0.0.0. / 0.0.0.	0 0	0.0.0.0 0.0.0.0	Any	Any	Any	Any	Any	0	

ローカル ポリシー [Block-all] を作成し、[deny all] ACL をこれに適用し、デバイス ロールやプロファイル は選択しないでください。

lindu					Saye	Configuration Ping	Logout Refresh
CISCO	MONITOR WLANS CONTROL	LER WIRELESS SECURIT	MANAGEMENT	COMMANDS	HELP	FEEDBACK	
Security	Policy > Edit						< Back
AAA							Apply
General • RADIUS	Policy Name	block-all					
Authentication Accounting	Policy Id	3					
DNS Downloaded AVP	Match Criteria						
TACACS+ LDAP	Match Role String						
Local Net Users	Match EAP Type	none 🔻					
Disabled Clients User Login Policies	Device List						
AP Policies Password Policies	Device Type	Android	•	Add			
Local EAP	1						
Advanced EAP	Action						
Priority Order	Action				-		
Certificate	IPv4 ACL	deny-all 🔻					
Access Control Lists	VLAN ID	0					
Access Control Lists	Qos Policy	none					
FlexConnect ACLs	Session Timeout (seconds)	1800					
Layer2 ACLs	Sleeping Client Timeout (min)	720					
Wireless Protection Policies	Flexconnect ACL	none T					
Web Auth	AVC Profile	none 🔻					
TrustSec SXP	mDNS Profile	none					

WLAN でのポリシーのマッピング

手順

ステップ1 WLCメニューバーから [WLANs] に移動し、ポリシーを設定したい [WLAN ID] をクリックします。WLAN の [Edit] メニューから [Policy-Mapping] タブをクリックします。

[Priority Index] で、1 ~ 16 から任意の値を設定します。[Local Policy] ドロップダウン リストから、すでに 作成したポリシーを選択します。WLAN でポリシーを適用するには、[Add] をクリックします。ポリシー が追加されます。

	Security	QoS	Policy-Mapping	Advanced	
Priority In	ndex (1-16)		1		
Local Poli	cy		teacher-LP :	•	
			Add 🔶		

ステップ2 適切なポリシーを WLAN の [Policy-Mapping] に追加します。

	OR <u>W</u> LANS <u>C</u> ONTROLLER WIRELE	Sa <u>v</u> e Configuration <u>P</u> ing Logout <u>R</u> efresh ESS <u>S</u> ECURITY MANAGEMENT C <u>O</u> MMANDS HELP <u>F</u> EEDBACK
WLANs	WLANs > Edit 'pod3-dot1x'	< Back Apply
WLANS	General Security QoS	Policy-Mapping Advanced
Advanced	Priority Index (1-16) Local Policy	teacher-LP V
	Priority Index	Local Policy Name
	1	teacher-LP
	2	student-LP
	3	block-all

ステップ3 [Advanced] タブで、[Allow AAA Override] が IPSK のために設定されていて有効な場合は、無効にします。

eneral	Security	QoS	Policy-Mapping	Advanced			
Allow AA	A Override		🕑 Enabled //	-		DHCP	
Coverag	e Hole Detection	1	🗹 Enabled			DHCP Server	Override
Enable S	ession Timeout	✓ 180 Se	ssion Timeout (secs)			DHCP Addr. Assignment	Required
Aironet .	lE		C Enabled			OEAP	
Diagnost	tic Channel 18		Enabled		TD.C	Calit Tuppal	Concernation of the second
Override	e Interface ACL		IPv4 None ▼		None V	Split funner	
Layer2 /	Acl		None 🔻		(<u></u>)	Management Frame Prote	ection (MFP)
URL ACL			None 🔻				(
P2P Bloc	king Action		Disabled	T		MFP Client Protection 4	Optional 🔻
Client E>	clusion 3		Enabled 60			DTIM Period (in beacon i	ntervals)
Maximu	n Allowed Client	. 8	Time	eout Value (secs)	802.11a/n (1 - 255)	1
Haxinia		5-				802 11b/g/n (1 - 255)	1
Static IP	Tunneling 🖽		Enabled			002.110/g/ll (1 - 255)	1
Wi-Fi Dir	ect Clients Polic	y	Disabled	•		NAC	
Maximur Radio	n Allowed Client	s Per AP	200			NAC State None	T
al 11			—			Load Balancing and Band	Select

ステップ4 AAA ロールが正しく設定されていることを確認します。つまり、AAA サーバでのロール名はローカル ポリシーで定義されている [Role String] と一致する必要があります。以下の例は、cisco-av-pair role=teacher で 設定されている Cisco ISE サーバです。role=students に対しても同じ設定です。

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
Authentication Authorization Profili	ng Posture Client Provisioning Policy Elements
Dictionaries + Conditions - Results	
0	
Authentication	
- Authorization	* Access Type Access Access
Authorization Profiles	ACCESS_ACCEPT
Downloadable ACLs	Network Device Profile
Profiling	Service Template
b Posturo	Track Movement 🗌 👔
, rosture	Passive Identity Tracking (i)
Client Provisioning	
	▼ Common Tasks
	Web Authentication (Local Web Auth)
	Airespace ACL Name
	ASA VPN
	AVC Profile Name
	✓ Advanced Attributes Settings
	Cisco:cisco-av-pair 💟 = psk-mode=ascii 💟
	Cisco:cisco-av-pair 💿 = psk=abc12345 💿 —
	Cisco:cisco-av-pair 📀 = role=teacher
	Access Type = ACCESS_ACCEPT cisco-av-pair = psk-mode=ascii cisco-av-pair = psk=abc12345 cisco-av-pair = role=teacher
	Jave Reset

エンド ユーザ デバイスの設定

手順

ステップ1 MAC アドレスが ISE で設定されているエンド ユーザ デバイスで、WLAN Pod1-IPSK に接続し、そのデバ イスの IPSK パスワード abc12345 を入力するか、または ISE で設定されたようにします。

---接続に**成功**しました

ステップ2 同じ WLAN に PSK 12345678 で接続します。

---接続に**失敗**します

ステップ3 同じ WLAN に MAC アドレスが ISE に設定されていないデバイスと PSK 12345678 で接続します。

----接続に**成功**しました

Â	The Wi-Fi password	network "Pod1-IPSK"	requires a WPA2		The Wi-Fi password	network "Pod1-IPSK" requires a	WPA2
	Password:	abc12345			Password:	12345678	
	4	 Show password Remember this network 	vork		4	 Show password Remember this network 	
		Car	ncel Join	?		Cancel	Join

ステップ4 WLC GUI から、ポリシーの適用を確認するために、[Monitor]>[Clients] に移動して [Client MAC address] を クリックします。

Clients > Detail	
Max Number of Records	10 ‡
General AVC Statist	ics
Encryption Cipher	CCMP (AES)
EAP Type	PEAP
SNMP NAC State	Access
Radius NAC State	RUN
CTS Security Group Tag	Not Applicable
AAA Override ACL Name	none
AAA Override ACL Applied Status	Unavailable
AAA Override Flex ACL	none
AAA Override Flex ACL Applied Status	Unavailable
Redirect URL	none
IPv4 ACL Name	none
FlexConnect ACL Applied Status	Unavailable
IPv4 ACL Applied Status	Unavailable
IPv6 ACL Name	none
IPv6 ACL Applied Status	Unavailable
Layer2 ACL Name	none
Layer2 ACL Applied Status	Unavailable
mDNS Profile Name	default-mdns-profile
mDNS Service Advertisement Count	0
AAA Role Type	teacher 🔶
Local Policy Applied	teacher-LP 🔶

まとめ

• Mac フィルタリングおよび AAA Override が有効化され、ISE が設定されているコントローラは、IPSK を設定した デバイスが ISE で設定された MAC アドレスを使用して WLAN に接続することを許可します。

- ISE で設定された MAC アドレスを持つデバイスは、WLAN に通常の PSK で接続できず、そのデバイスのために 設定された IPSK でのみ接続できます。
- ISE で設定された MAC アドレスを持たないデバイスは、通常の PSK のみで WLAN に接続できます。
- IPSK は、FlexConnect local switching ではサポートされません。AAA サーバで AV-Pair のサポートが必要です。
- IPSK は、FlexConnect Group ではサポートされません。
- IPSK は FSR をサポートし、高速ローミングの際に、ローミングごとの RADIUS 接続を避けるため、キーキャッシングを実行します。
- ・特定のスケジュールされた時間に IPSK の設定を有効にするには、RADIUS 応答の radius session-timeout 属性を使用できます。

CLI コマンドを使用した IPSK の設定

次の既知の CLI は、この機能のために使用されます。

config wlan mac-filtering enable <wlanId> config wlan aaa-override enable <wlanId> config wlan security wpa akm psk enable <wlanId> config wlan security wpa akm psk set-key <ascii/hex> <key> <wlanId>

既知の show コマンドは、WLAN およびクライアントの設定を表示します。

show wlan <wlanId>
show client detail <clientMac>

【注意】シスコ製品をご使用になる前に、安全上の注意(www.cisco.com/jp/go/safety_warning/)をご 確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、 日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合が ありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サ イトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、 弊社担当者にご確認ください。

©2008 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, およびCisco Systems ロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。 本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。 「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0809R) この資料の記載内容は2008 年 10月現在のものです。 この資料に記載された仕様は予告なく変更する場合があります。

cisco.

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
 http://www.cisco.com/jp
 お問い合わせ先:シスコ コンタクトセンター
 0120-092-255 (フリーコール、携帯・PHS含む)
 電話受付時間:平日 10:00~12:00、13:00~17:00
 http://www.cisco.com/jp/go/contactcenter/