



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

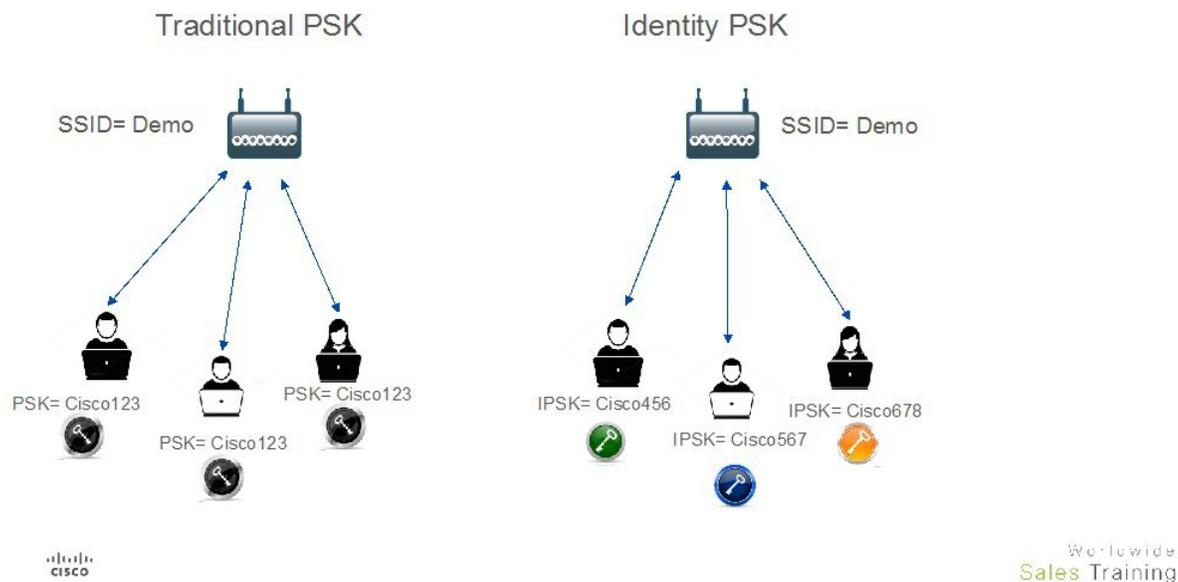
CLI コマンドを使用した IPSK の設定 23

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サブ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。

Traditional Vs Identity PSK



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。

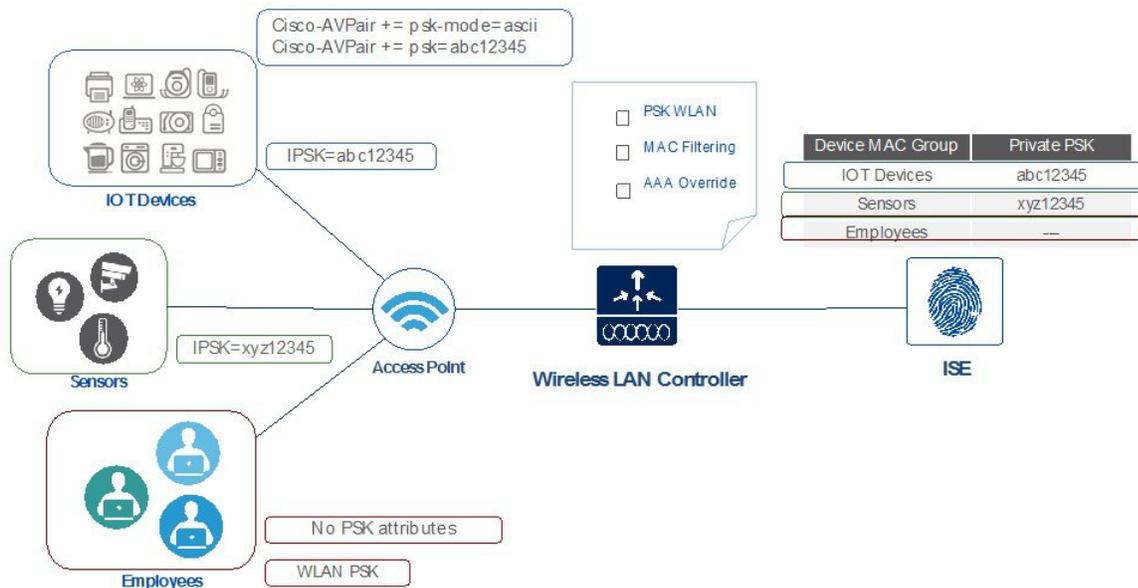
クライアントがアクセスポイントからブロードキャストされている SSID にアソシエーション要求を送信すると、ワイヤレス LAN コントローラはクライアントの特定の MAC アドレスを含む RADIUS 要求パケットを形成し、RADIUS サーバに中継します。

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

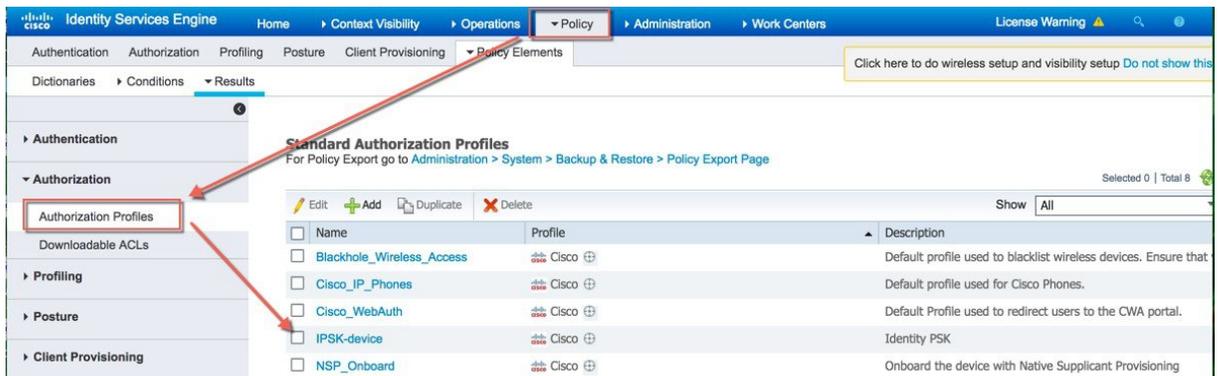
IPSK は、Cisco AV-pair をサポートする AAA サーバで設定できます。この導入ガイドでは、Cisco Identity Service Engine での設定に焦点を合わせます。ISE 2.2 構成手順

手順

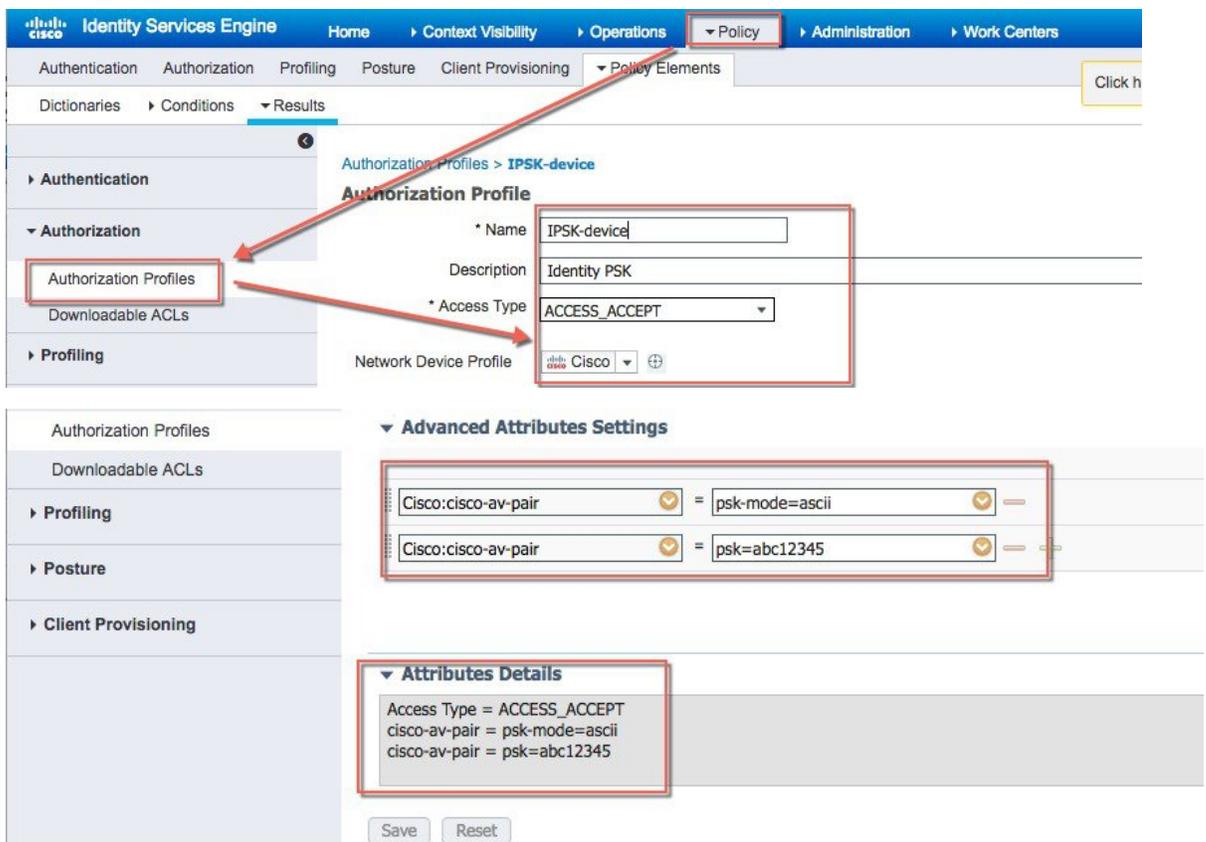
ステップ1 次のように ISE でテスト対象のワイヤレスコントローラを追加し、[Radius Authentication Setting] で secret password を設定して [Submit] をクリックします。

The image consists of two screenshots from the Cisco Identity Services Engine (ISE) Administration console. The top screenshot shows the 'Network Devices' page with a table listing devices. A red box highlights the 'Add' button and a row for a device named 'NAD_10.10.10.2' with IP/Mask '10.10.10.2/32'. The bottom screenshot shows the 'New Network Device' configuration page. Fields include: Name (NAD), Description (Wireless Controller), IP Address (10.10.10.2 / 32), Device Profile (Cisco), Model Name (3504), Software Version (8.5), and Network Device Group settings. At the bottom, there are checkboxes for 'RADIUS Authentication Settings', 'TACACS Authentication Settings', 'SNMP Settings', and 'Advanced TrustSec Settings'. A red arrow points to the 'RADIUS Authentication Settings' checkbox.

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。



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。



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。

Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order. For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

First Matched Rule Applies:

▶ Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	IdentityPSK	if (Wireless_MAB AND Radius:Calling-Station-ID EQUALS A0:3B:E3:95:73:4E)	then IPSK-device
✓	IdentityPSK_copy	if (Wireless_MAB AND Radius:Calling-Station-ID EQUALS f4:5c:89:8f:10:43)	then IPSK-device
✓	Wireless Black List Default	if Blacklist AND Wireless_Access	then Blackhole_Wireless_Access
✓	Profiled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	IdentityPSK	if Any and Wireless_MAB AND Radius:Callin...	then IPSK-device
✓	IdentityPSK_copy	if Wireless_MAB AND Radiu f4:5c:89:8f:10:43	
✓	Wireless Black List Default	if Blacklist AND Wireless_Ad	
✓	Profiled Cisco IP Phones	if Cisco-IP-Phone	
✓	Profiled Non Cisco IP Phones	if Non_Cisco_Profiled_Phones	then Non_Cisco_IP_Phones

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。

The screenshot shows the Cisco WLAN configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', and 'MANAGEMENT'. The left sidebar shows 'WLANs' with sub-items 'WLANs' and 'Advanced'. The main content area is titled 'WLANs > Edit 'Identity PSK''. The 'Security' tab is selected, showing the following configuration:

Profile Name	Identity PSK
Type	WLAN
SSID	Pod1-IPSK
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	MAC Filtering[WPA2][Auth(PSK)] (Modifications done under security tab will appear)
Radio Policy	All
Interface/Interface Group(G)	management
Multicast Vlan Feature	<input type="checkbox"/> Enabled
Broadcast SSID	<input checked="" type="checkbox"/> Enabled
NAS-ID	none

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。

The screenshot shows the Cisco WLC configuration interface for a WLAN named 'Identity PSK'. The 'Security' tab is selected, and the 'Layer 2' sub-tab is active. The 'Layer 2 Security' dropdown is set to 'WPA+WPA2', and 'MAC Filtering' is checked. Under 'Fast Transition', 'Fast Transition Over the DS' is checked and 'Reassociation Timeout' is set to 20 seconds. Under 'Protected Management Frame', 'PMF' is set to 'Disabled'. The 'WPA+WPA2 Parameters' section shows 'WPA2 Policy' checked, 'WPA2 Encryption' set to 'AES', and 'OSEN Policy' unchecked.

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。

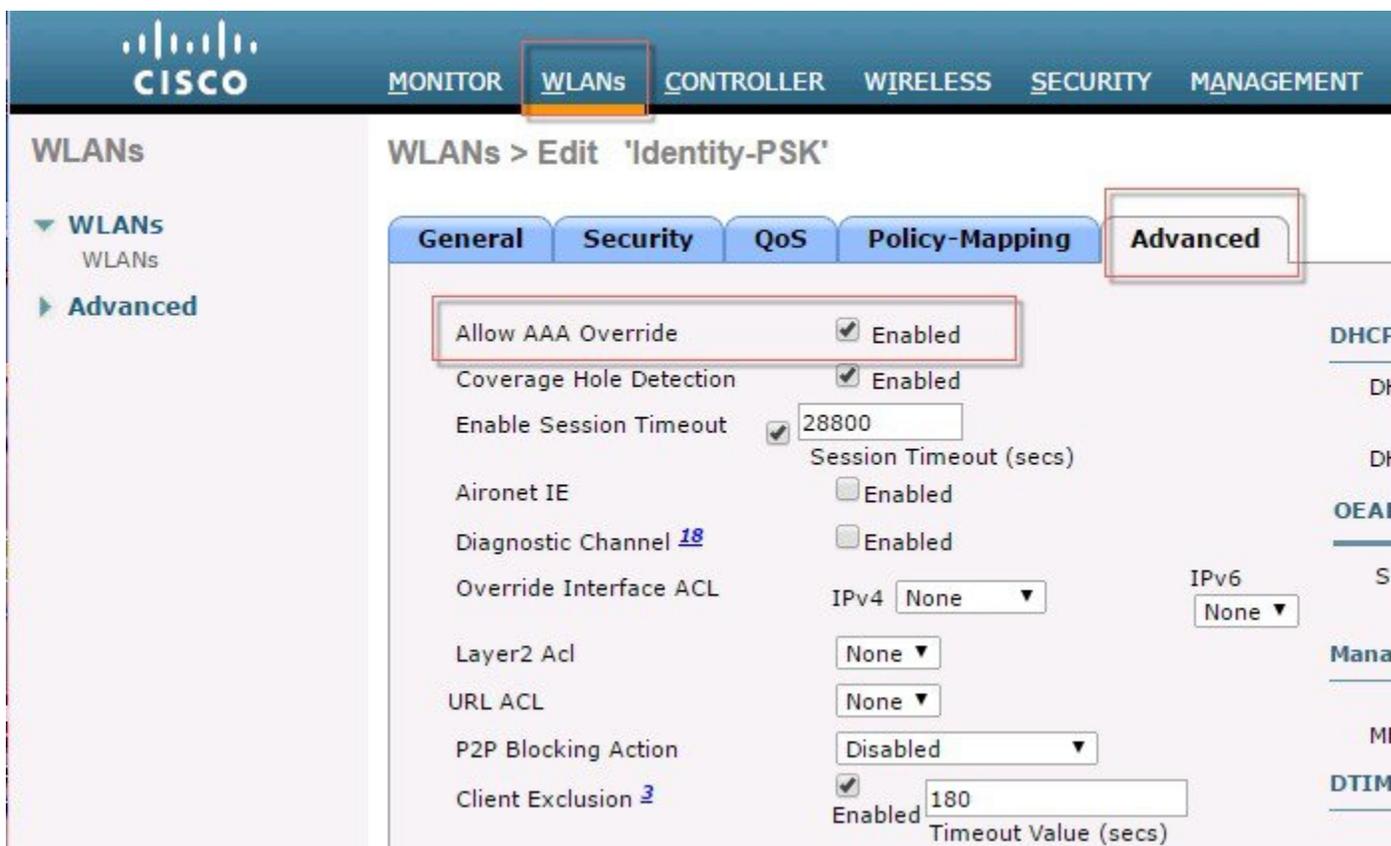
The screenshot shows the 'Authentication Key Management' section in the configuration interface. The 'PSK' option is checked and highlighted with a red box. The 'PSK Format' dropdown is set to 'ASCII'. A red arrow points to the PSK key field, which contains a masked value represented by six dots.

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。

The screenshot shows the Cisco ISE GUI for configuring a WLAN. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', and 'MANAGEMENT'. The left sidebar shows 'WLANs' with sub-items 'WLANs' and 'Advanced'. The main content area is titled 'WLANs > Edit 'Identity-PSK''. Below this are tabs for 'General', 'Security', 'QoS', 'Policy-Mapping', and 'Advanced'. Under the 'Security' tab, there are sub-tabs for 'Layer 2', 'Layer 3', and 'AAA Servers'. The 'AAA Servers' sub-tab is active, showing a section titled 'Select AAA servers below to override use of default servers on this WLAN'. Below this is a 'RADIUS Servers' section with two checkboxes: 'RADIUS Server Overwrite interface' and 'Apply Cisco ISE Default Settings', both currently unchecked. At the bottom, there are two columns: 'Authentication Servers' and 'Accounting Servers'. Each column has a checkbox for 'Enabled' (checked) and a table with two rows: 'Server 1' and 'Server 2'. The 'Server 1' row is highlighted with a red box and shows 'IP:10.91.104.106, Port:1812' for Authentication and 'IP:10.91.104.106, Port:1813' for Accounting. The 'Server 2' row shows 'None' for both.

	Authentication Servers	Accounting Servers
Server 1	IP:10.91.104.106, Port:1812	IP:10.91.104.106, Port:1813
Server 2	None	None

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



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るプロファイル名、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。

The screenshot displays the Cisco WLC Security Policy configuration interface. The main configuration area is titled 'Policy > Edit' and shows the following details:

- Policy Name:** IPSK-test
- Policy Id:** 1
- Match Criteria:**
 - Match Role String:** (Empty text input field, highlighted with a red box)
 - Match EAP Type:** none (dropdown menu)
- Device List:**
 - Device Type:** (Empty dropdown menu)
 - Add:** (Button)
- Action:**
 - IPv4 ACL: none (dropdown menu)
 - URL ACL: none (dropdown menu)
 - VLAN ID: 0 (text input field)
 - Qos Policy: none (dropdown menu)
 - Average Data Rate(kbps): 0 (text input field)
 - Average Real time Data Rate(kbps): 0 (text input field)
 - Burst Data Rate(kbps): 0 (text input field)
 - Burst Real time Data Rate(kbps): 0 (text input field)
 - Session Timeout (seconds): 1800 (text input field)
 - Sleeping Client Timeout (min): 720 (text input field)
 - Flexconnect ACL: none (dropdown menu)
 - AVC Profile: none (dropdown menu)
 - mDNS Profile: none (dropdown menu)
 - OpenDNS Profile: none (dropdown menu)
- Active Hours:**
 - Day:** Mon (dropdown menu)
 - Start Time:** (Hours) (Mins) (input fields)
 - End Time:** (Hours) (Mins) (input fields)
 - Add:** (Button)

At the bottom of the page, there is a table structure with columns for 'Day', 'Start Time', and '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一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。

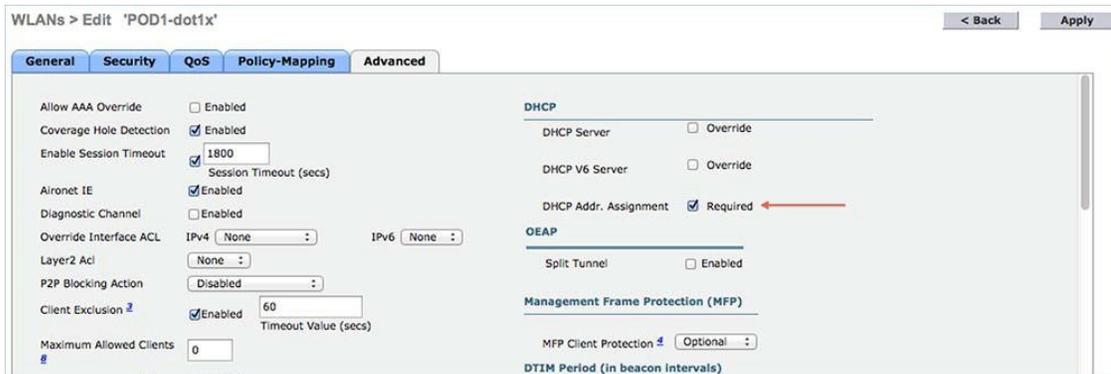
- VLAN
- ACL
- セッション タイムアウト
- QoS
- スリープ状態のクライアント
- FlexConnect ACL
- AVC プロファイル
- mDNS プロファイル
- オープン DNS プロファイル
- セキュリティ グループ タグ

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。

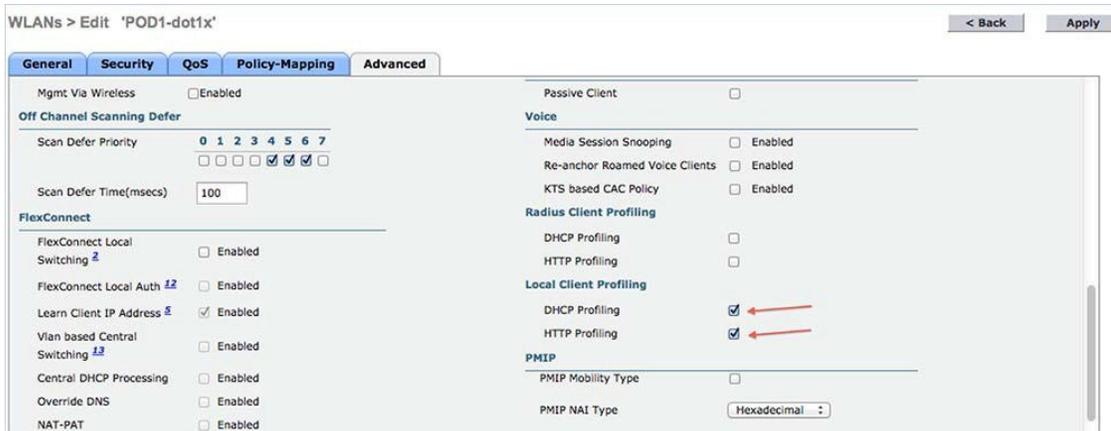
プロファイリングおよびポリシーの設定

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]。



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。



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。



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。



ポリシー名を設定した後、[Role]、[EAP Type]、[DeviceType] 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。

(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 [Add]
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]

352901

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。

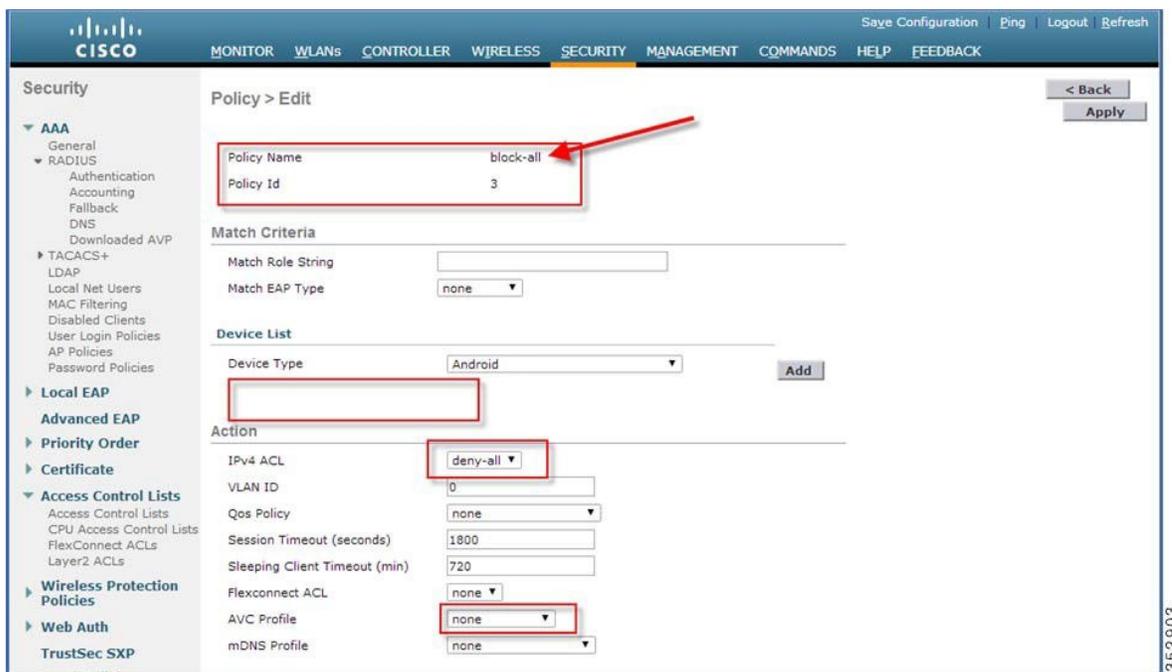
ローカルポリシーに他のACLが適用されていない場合、Apple-iPad以外の他のデバイスは、すべてのポリシーの最終フィルタ機能が [Allow all] なので、アプリケーションにアクセスできます。

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。



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。

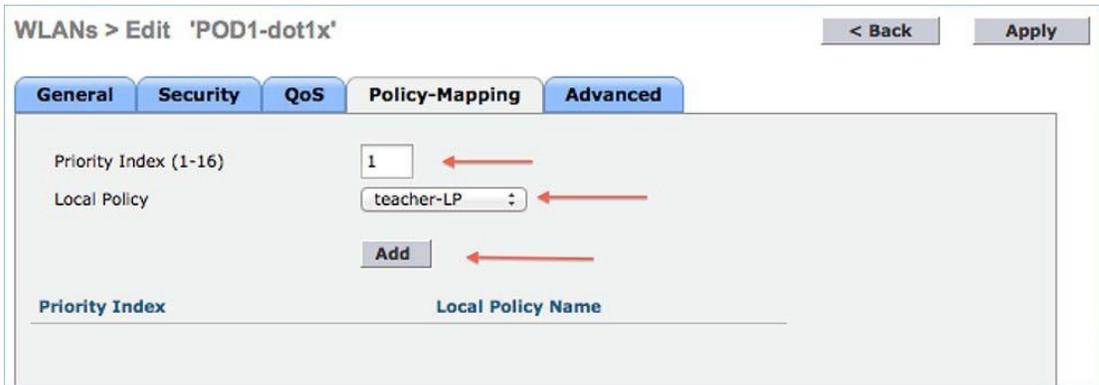


WLAN でのポリシーのマッピング

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。



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



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。

General	Security	QoS	Policy-Mapping	Advanced
Allow AAA Override	<input checked="" type="checkbox"/>	Enabled		
Coverage Hole Detection	<input checked="" type="checkbox"/>	Enabled		
Enable Session Timeout	<input checked="" type="checkbox"/>	1800	Session Timeout (secs)	
Aironet IE	<input checked="" type="checkbox"/>	Enabled		
Diagnostic Channel	<input type="checkbox"/>	Enabled		
Override Interface ACL	IPV4	None	IPV6	None
Layer2 Acl		None		
URL ACL		None		
P2P Blocking Action		Disabled		
Client Exclusion	<input checked="" type="checkbox"/>	Enabled	60	Timeout Value (secs)
Maximum Allowed Clients		0		
Static IP Tunneling	<input type="checkbox"/>	Enabled		
Wi-Fi Direct Clients Policy		Disabled		
Maximum Allowed Clients Per AP Radio		200		
DHCP				
DHCP Server	<input type="checkbox"/>	Override		
DHCP Addr. Assignment	<input checked="" type="checkbox"/>	Required		
OEAP				
Split Tunnel	<input type="checkbox"/>	Enabled		
Management Frame Protection (MFP)				
MFP Client Protection		Optional		
DTIM Period (in beacon intervals)				
802.11a/n (1 - 255)		1		
802.11b/g/n (1 - 255)		1		
NAC				
NAC State		None		
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。

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionarys Conditions Results

Authorization Profile

* Name:

Description:

* Access Type:

Network Device Profile:

Service Template:

Track Movement:

Passive Identity Tracking:

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	+ ←

Attributes Details

```

Access Type = ACCESS_ACCEPT
cisco-av-pair = psk-mode=ascii
cisco-av-pair = psk=abc12345
cisco-av-pair = role=teacher

```

Save 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。

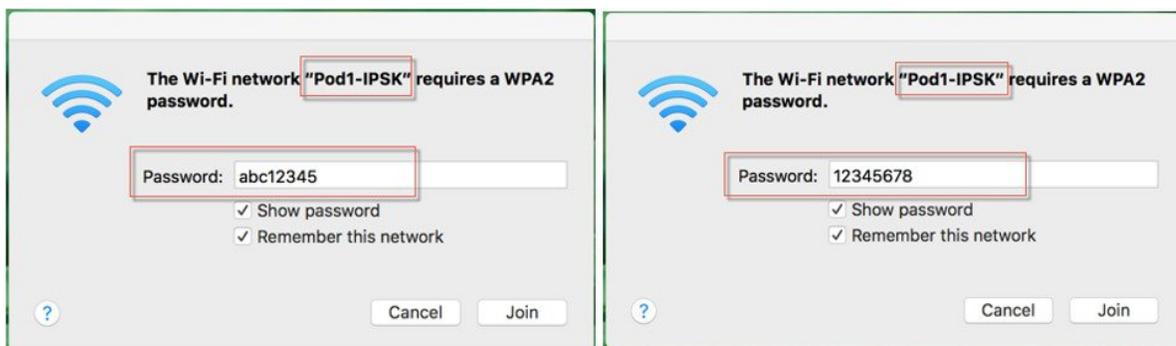
---接続に**成功**しました

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



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

General **AVC Statistics**

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

362909

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。



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/>