

ACS 5.2およびWLCを使用したPEAPおよびEAP-FAST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](#)

[設定](#)

[ネットワーク図](#)

[前提](#)

[設定手順](#)

[RADIUS サーバの設定](#)

[ネットワーク リソースの設定](#)

[ユーザの設定](#)

[ポリシー要素の定義](#)

[アクセス ポリシーの適用](#)

[WLC の設定](#)

[WLC での認証サーバの詳細設定](#)

[ダイナミック インターフェイス \(VLAN \) の設定](#)

[WLAN \(SSID \) の設定](#)

[無線クライアント ユーティリティの設定](#)

[PEAP-MSCHAPv2 \(user1 \)](#)

[EAP-FAST \(user2 \)](#)

[確認](#)

[user1 \(PEAP-MSCHAPv2 \) の検証](#)

[user2 \(EAP-FAST \) の検証](#)

[トラブルシューティング](#)

[トラブルシューティングのためのコマンド](#)

[関連情報](#)

はじめに

このドキュメントでは、Access Control Server (ACS) 5.2 などの外部 RADIUS サーバを使用して拡張認証プロトコル (EAP) 認証のためのワイヤレス LAN コントローラ (WLC) を設定する方法について説明します。

前提条件

要件

この設定を行う前に、以下の要件を満たしていることを確認してください。

- WLC および Lightweight アクセス ポイント (LAP) に関する基本的な知識があること
- AAA サーバに関する実務的な知識があること
- 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があること

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 7.0.220.0 が稼働している Cisco 5508 WLC
- Cisco 3502 シリーズ LAP
- Intel 6300-N ドライバ バージョン 14.3 対応の Microsoft Windows 7 ネイティブ サプリカント
- バージョン 5.2 が稼働している Cisco Secure ACS
- Cisco 3560 シリーズ スイッチ

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。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細については、『[シスコテクニカルティップスの表記法](#)』を参照してください。

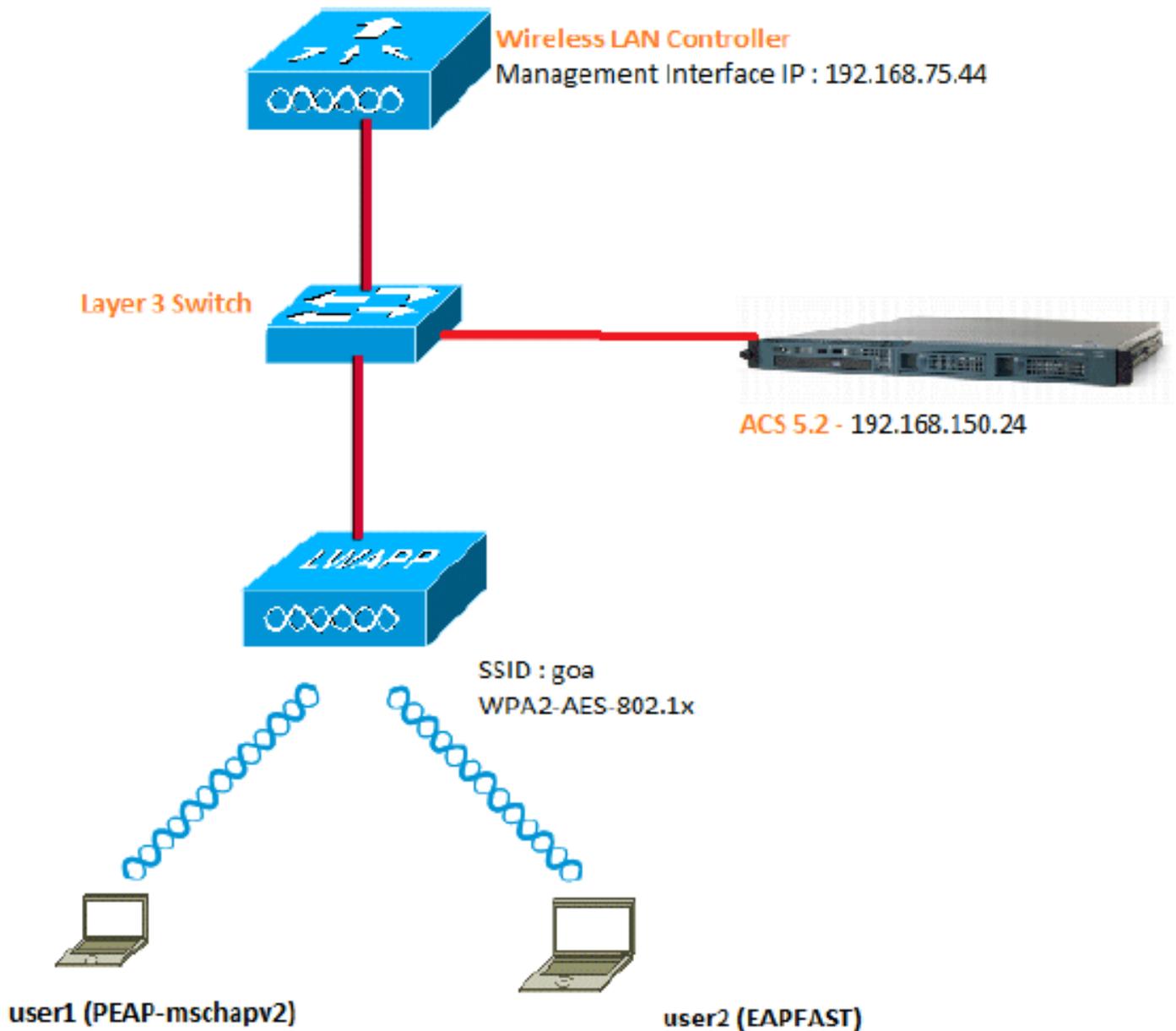
設定

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ています。

注：このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool (登録ユーザ専用) を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことをご了承ください。

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



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。

- ACS (RADIUS) サーバの IP アドレスは 192.168.150.24 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 192.168.75.44 です。
- DHCP サーバのアドレスは 192.168.150.25 です。
- VLAN 253 がこの設定を通して使用されます。両方のユーザが同じ SSID "goa" に接続します。ただし、user1 は PEAP-MSCHAPv2 を使用して認証するように、user2 は EAP-FAST を使用して認証するように設定されます。
- ユーザは VLAN 253 で割り当てられます。
 - VLAN 253:192.168.153.x/24。ゲートウェイ : 192.168.153.1
 - VLAN 75:192.168.75.x/24ゲートウェイ : 192.168.75.1

前提

- スイッチには、レイヤ 3 VLAN がすべて設定されています。
- DHCP サーバには DHCP スコープが割り当てられています。
- ネットワーク内すべてのデバイス間ではレイヤ 3 接続が確立しています。
- LAP はすでに WLC に登録されています。
- 各 VLAN は /24 マスクを使用しています。
- ACS 5.2 には自己署名証明書がインストールされています。

設定手順

この設定は、大きく次の 3 つに分類されます。

1. [RADIUS サーバの設定](#)
2. [WLC の設定](#)
3. [無線クライアント ユーティリティの設定](#)

RADIUS サーバの設定

RADIUS サーバの設定は次の 4 つのステップで構成されます。

1. [ネットワーク リソースの設定](#)
2. [ユーザの設定](#)
3. [ポリシー要素の定義](#)
4. [アクセス ポリシーの適用](#)

ACS 5.x は、ポリシーベースのアクセス コントロール システムです。つまり、ACS 5.x では、4.x バージョンで使用されていたグループベースのモデルの代わりに、ルールベース ポリシー モデルが使用されています。

ACS 5.x のルールベース ポリシー モデルを使用すると、以前のグループベースの手法よりも強力な柔軟なアクセス コントロールを実現できます。

以前のグループベース モデルでは、グループを使用してポリシーを定義していました。これは、グループに次の 3 つのタイプの情報が結合されていたためです。

- 識別情報：この情報は、AD グループまたは LDAP グループでのメンバーシップ、または ACS 内部ユーザの静的割り当てに基づいています。

- その他の制限または条件：時間制限、デバイス制限など。
- 許可：VLAN または Cisco IOS® の特権レベル。

ACS 5.x ポリシー モデルは、次の形式のルールに基づいています。

- If condition then result

たとえば、グループベース モデルに関して記述されている次の情報を使用します。

- If identity-condition, restriction-condition then authorization-profile

これにより、ユーザがネットワークにアクセスするための条件だけでなく、特定の条件を満たす場合に必要な承認レベルに基づいて、柔軟に制限できるようになります。

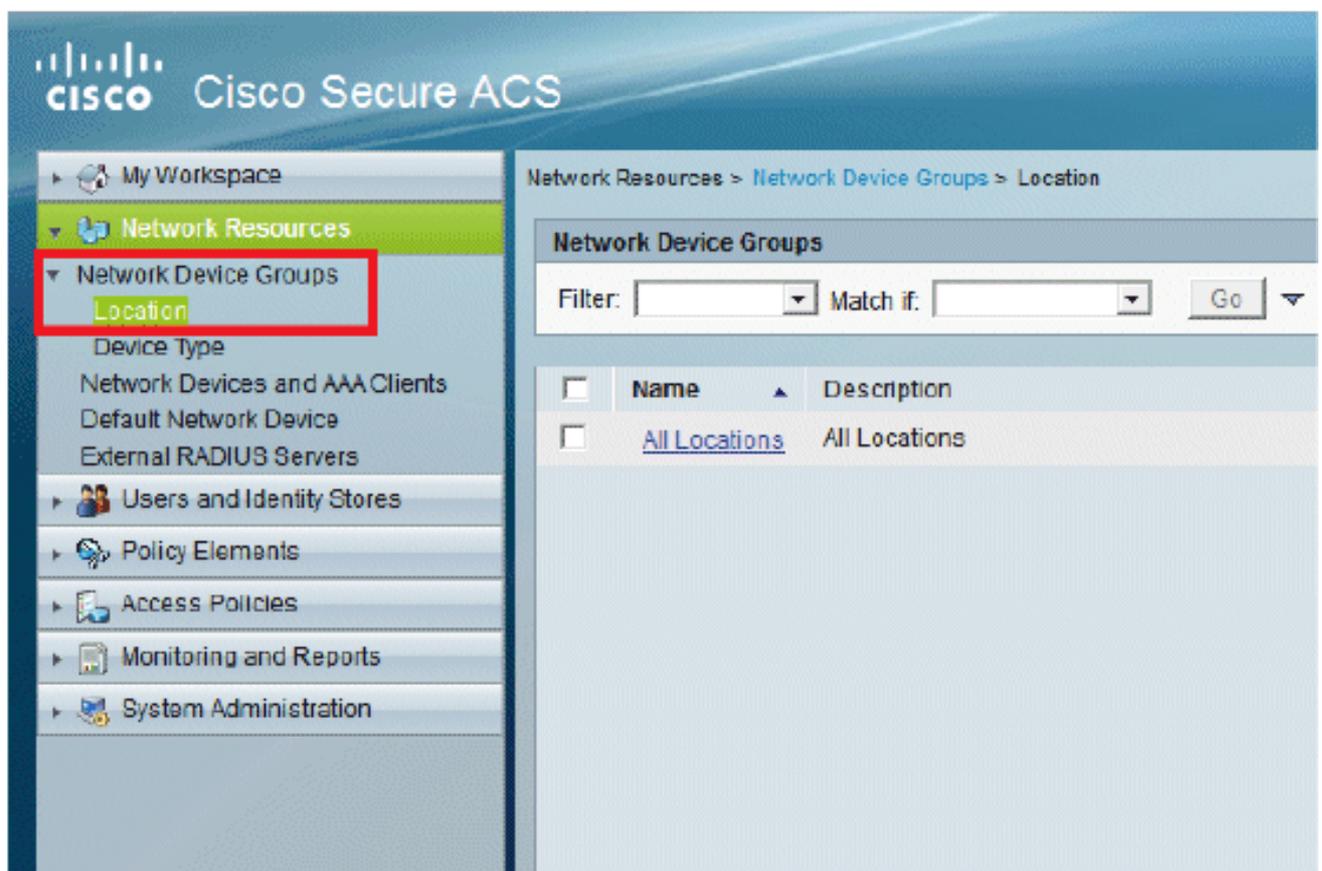
ネットワーク リソースの設定

ここでは、RADIUS サーバ上の WLC 用に AAA クライアントを設定します。

この手順では、WLC から RADIUS サーバにユーザ クレデンシャルを渡せるように、RADIUS サーバで AAA クライアントとして WLC を追加する方法について説明します。

次のステップを実行します。

1. ACS GUI から [Network Resources] > [Network Device Groups] > [Location] に移動し、[Create] (最下部) をクリックします。



2. 必要なフィールドを追加して [Submit] をクリックします。

Network Resources > Network Device Groups > Location > Create

Device Group - General

Name: LAB

Description: LAB Devices

Parent: All Locations

= Required fields

次の確認画面が表示されます。

CISCO Cisco Secure ACS

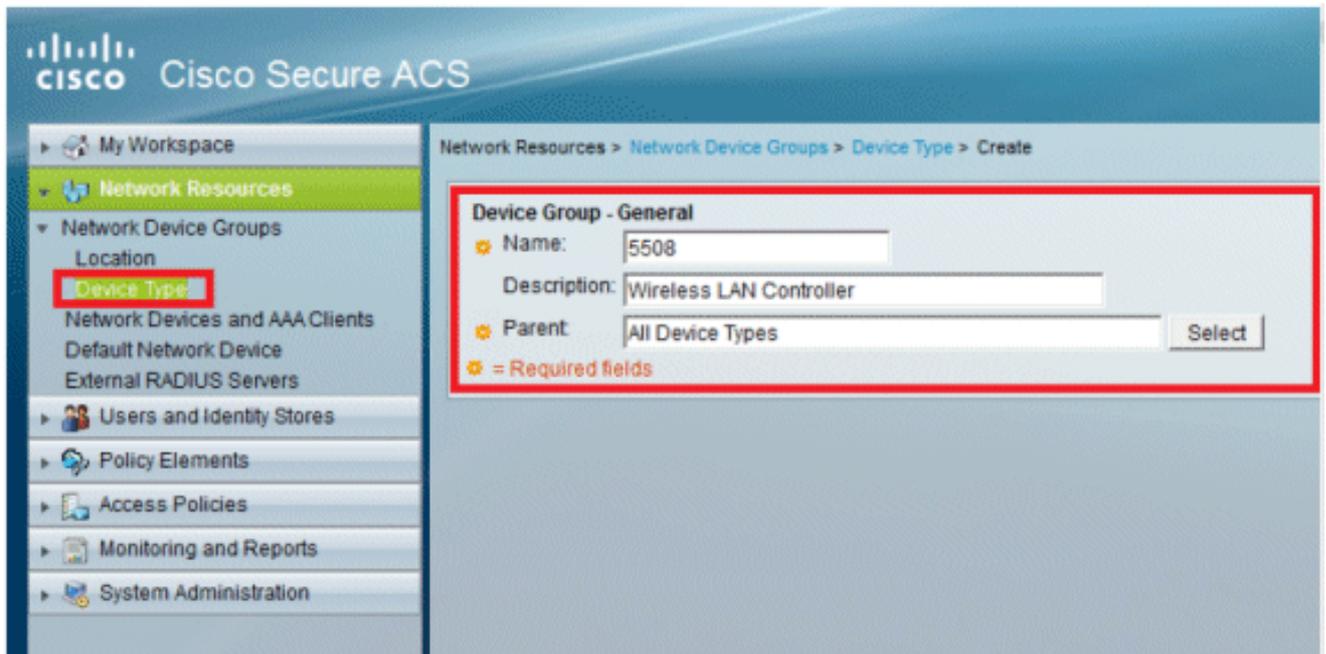
Network Resources > Network Device Groups > Location

Network Device Groups

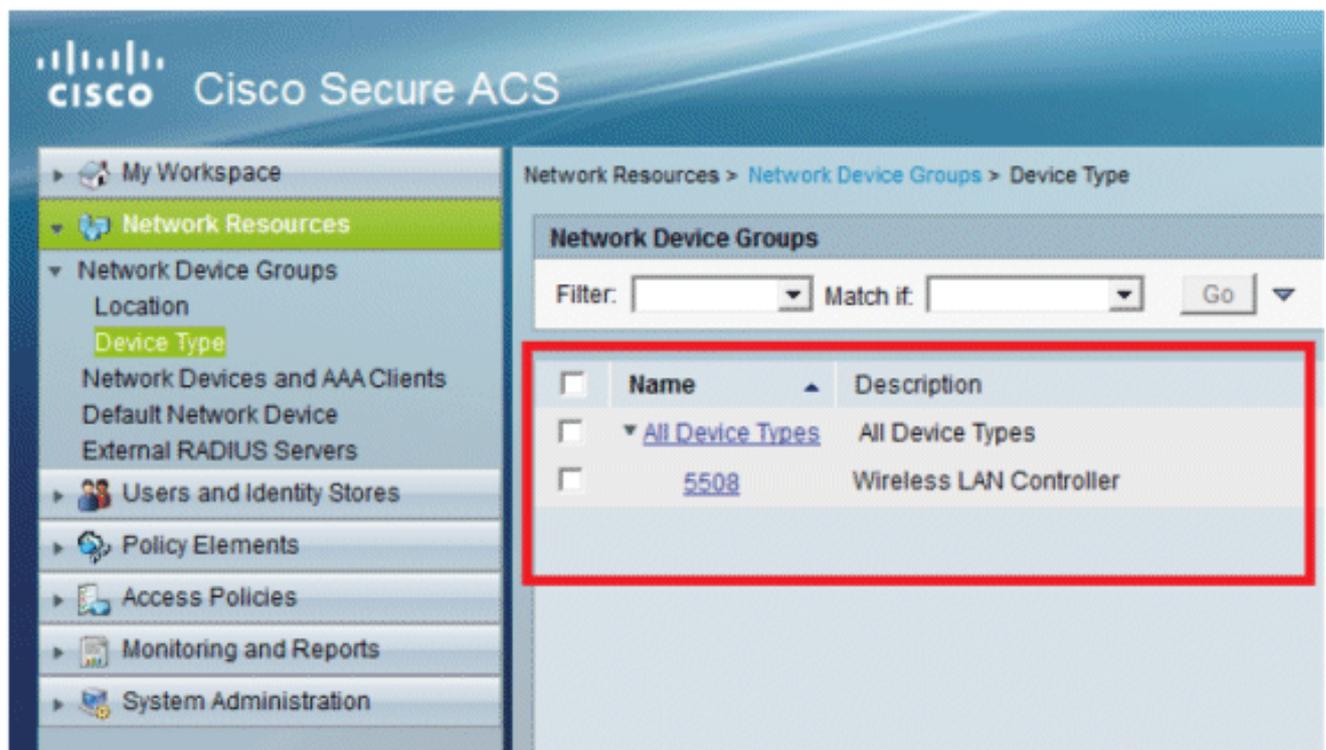
Filter: Match if:

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	▼ All Locations	All Locations
<input type="checkbox"/>	LAB	LAB Devices

3. [Device Type] > [Create] をクリックします。



4. [Submit] をクリックします。次の確認画面が表示されます。



5. [Network Resources] > [Network Devices and AAA Clients] に移動します。

6. [Create] をクリックして、次のように詳細を入力します。

Network Resources > Network Devices and AAA Clients > Create

Name:

Description:

Network Device Groups

Location:

Device Type:

IP Address

Single IP Address IP Range(s)

IP:

Authentication Options

TACACS+

RADIUS

Shared Secret:

CoA port:

Enable KeyWrap

Key Encryption Key:

Message Authenticator Code Key:

Key Input Format: ASCII HEXADECIMAL

* - Required fields

7. [Submit] をクリックします。次の確認画面が表示されます。

Network Resources > Network Devices and AAA Clients

Network Devices

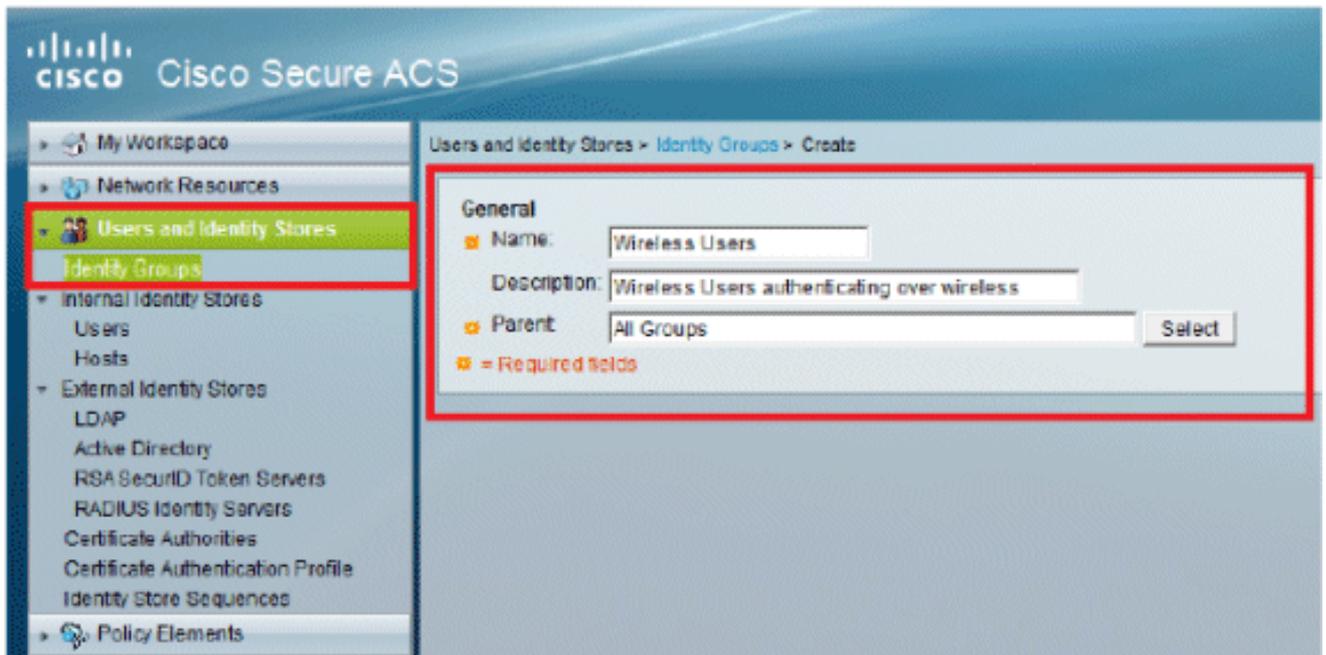
Filter: Match it:

<input type="checkbox"/>	Name	IP / Mask	NDG:Location	NDG:Device Type	Description
<input type="checkbox"/>	WLC-5508	192.168.75.44/32	All Locations:LAB	All Device Types:5508	Wireless LAN Controller

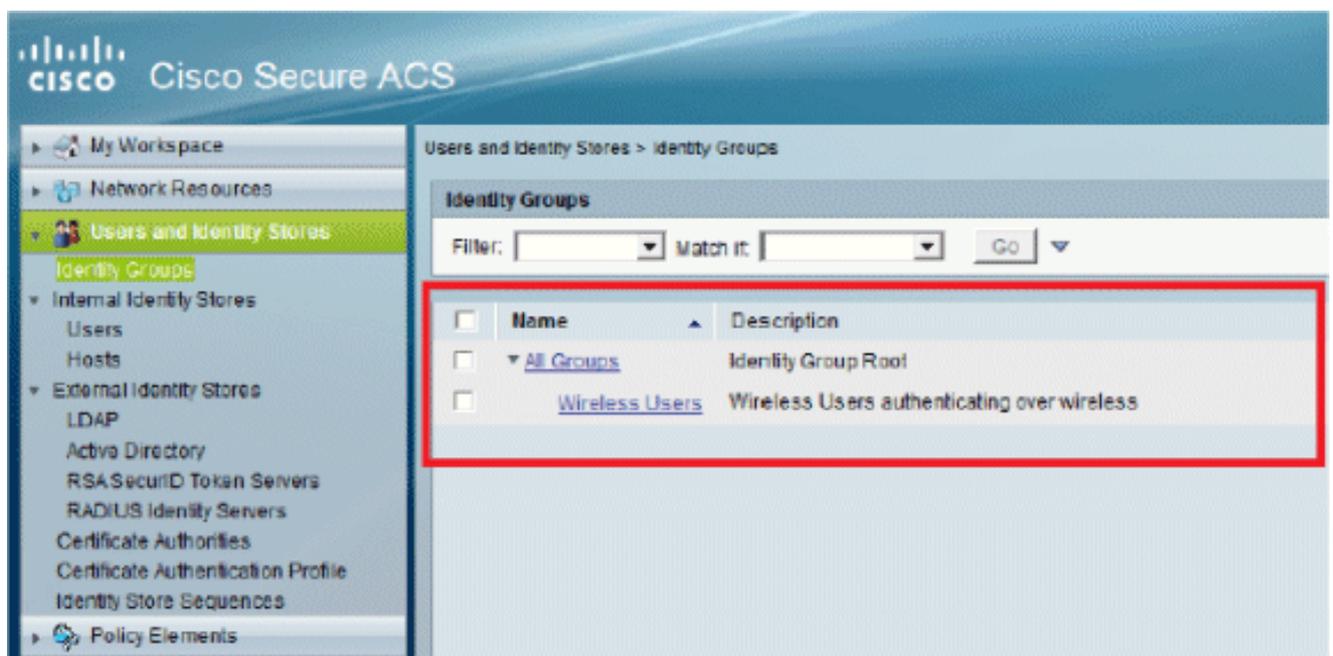
ユーザの設定

ここでは、ACS 上のローカル ユーザを作成します。両方のユーザ (user1 と user2) が "Wireless Users" というグループに割り当てられます。

1. [Users and Identity Stores] > [Identity Groups] > [Create] に移動します。

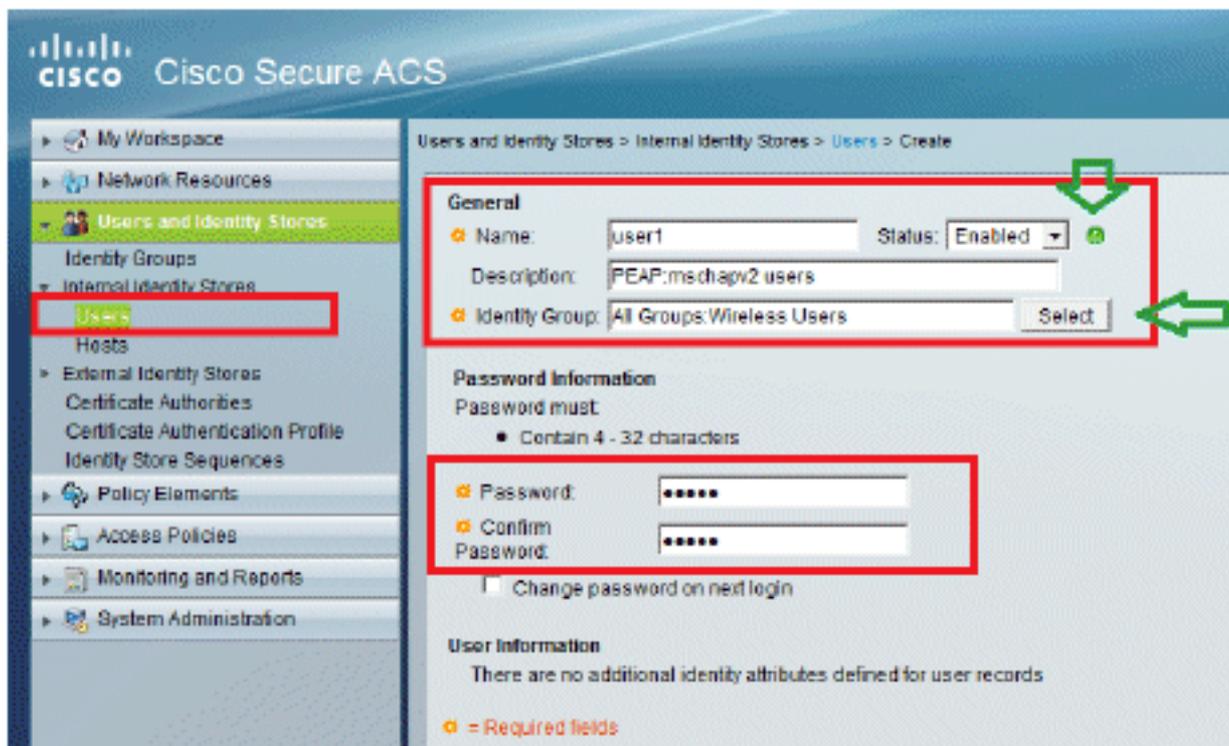


2. [Submit] をクリックすると、次のようなページが表示されます。

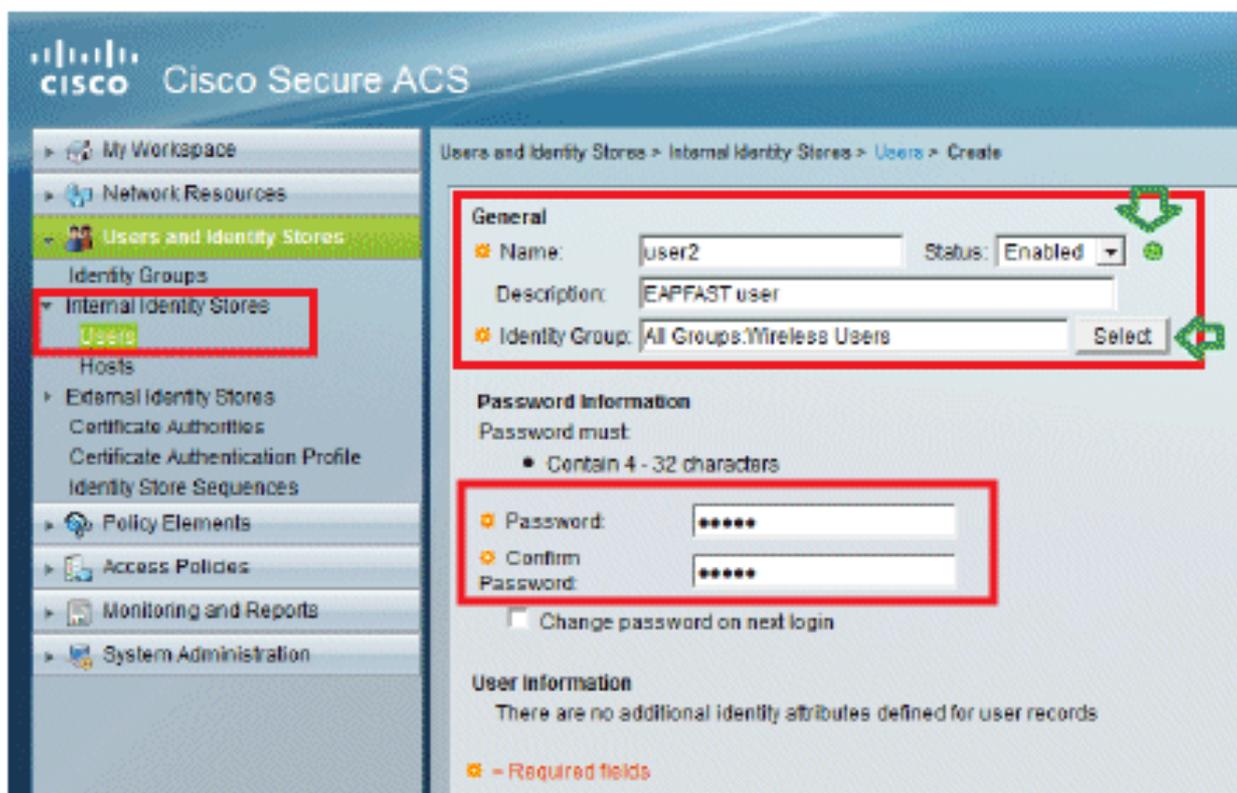


3. ユーザの user1 と user2 を作成して、それらを "Wireless Users" グループに割り当てます。

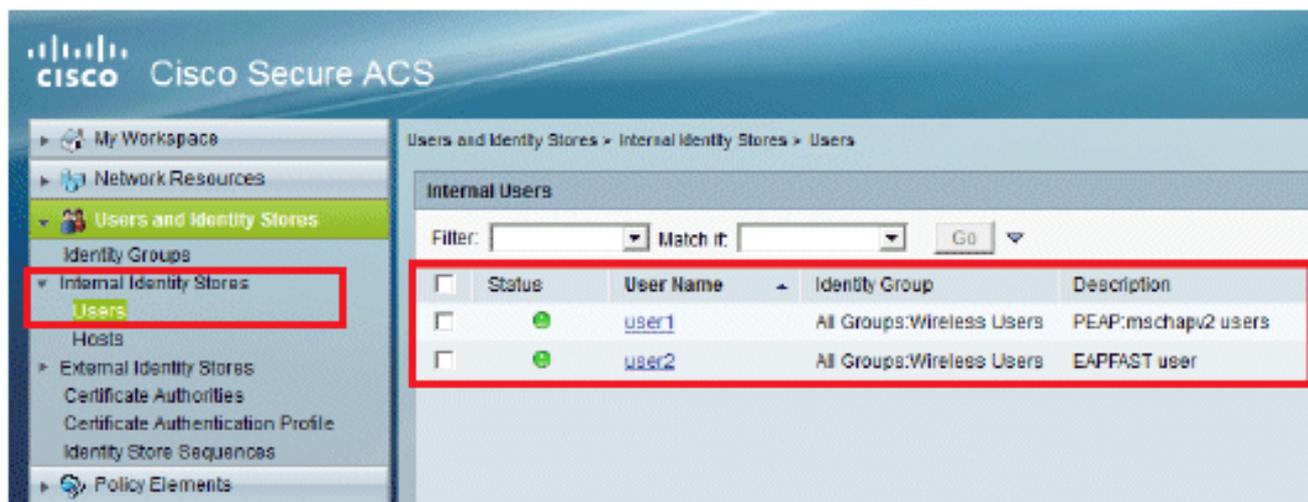
a. [Users and Identity Stores] > [Identity Groups] > [Users] > [Create] をクリックします。



b. 同様に、user2 を作成します。

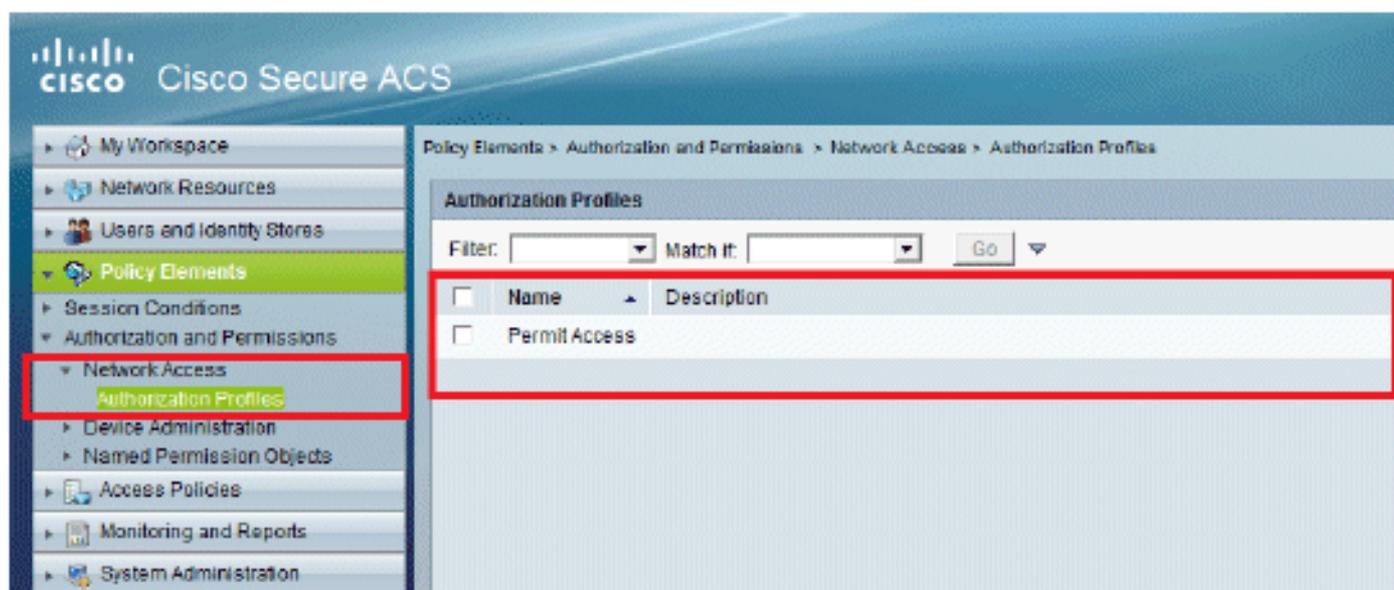


次のような画面が表示されます。



ポリシー要素の定義

[Permit Access] が設定されていることを確認します。

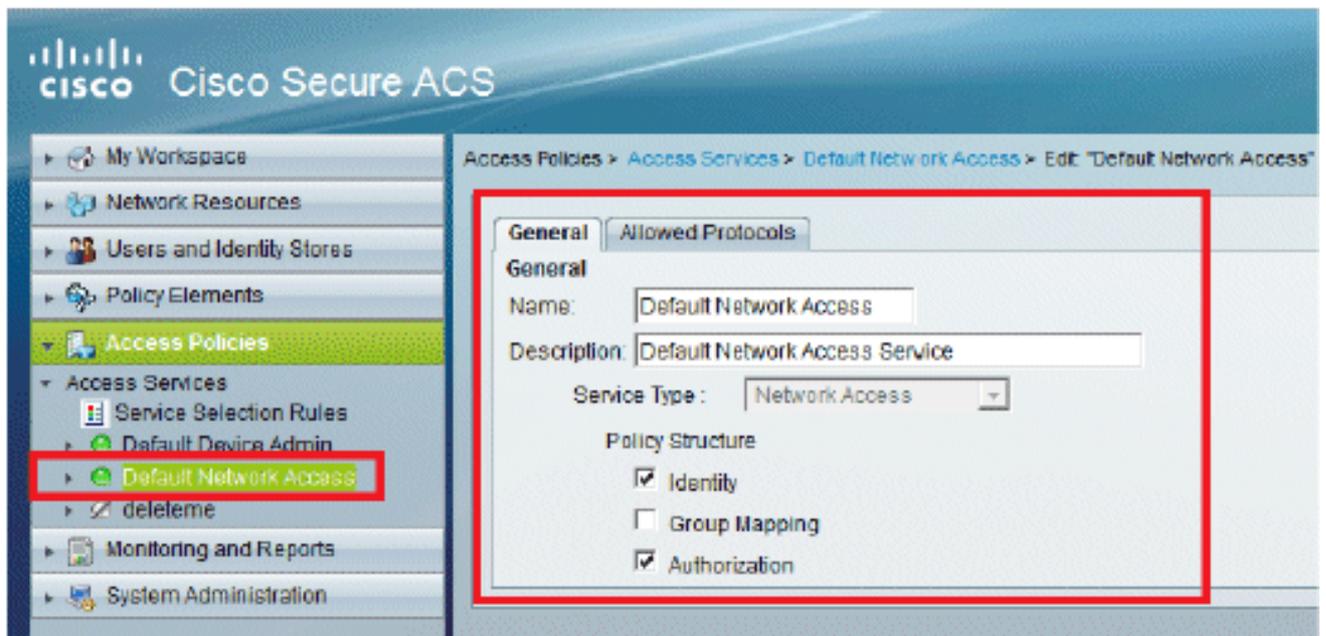


アクセス ポリシーの適用

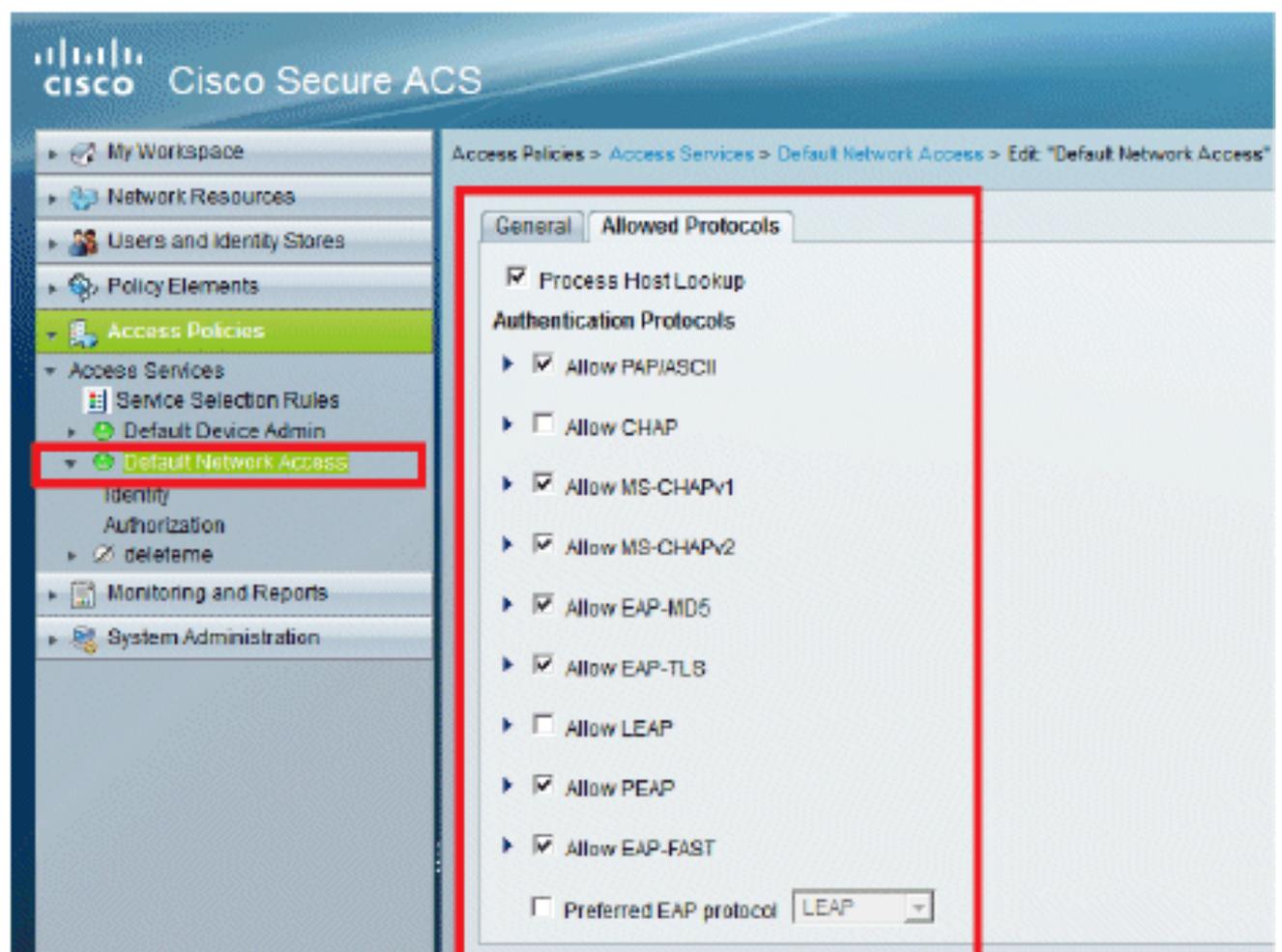
ここでは、使用する認証方式とルールの設定方法を選択します。これまでのステップに基づいてルールを作成します。

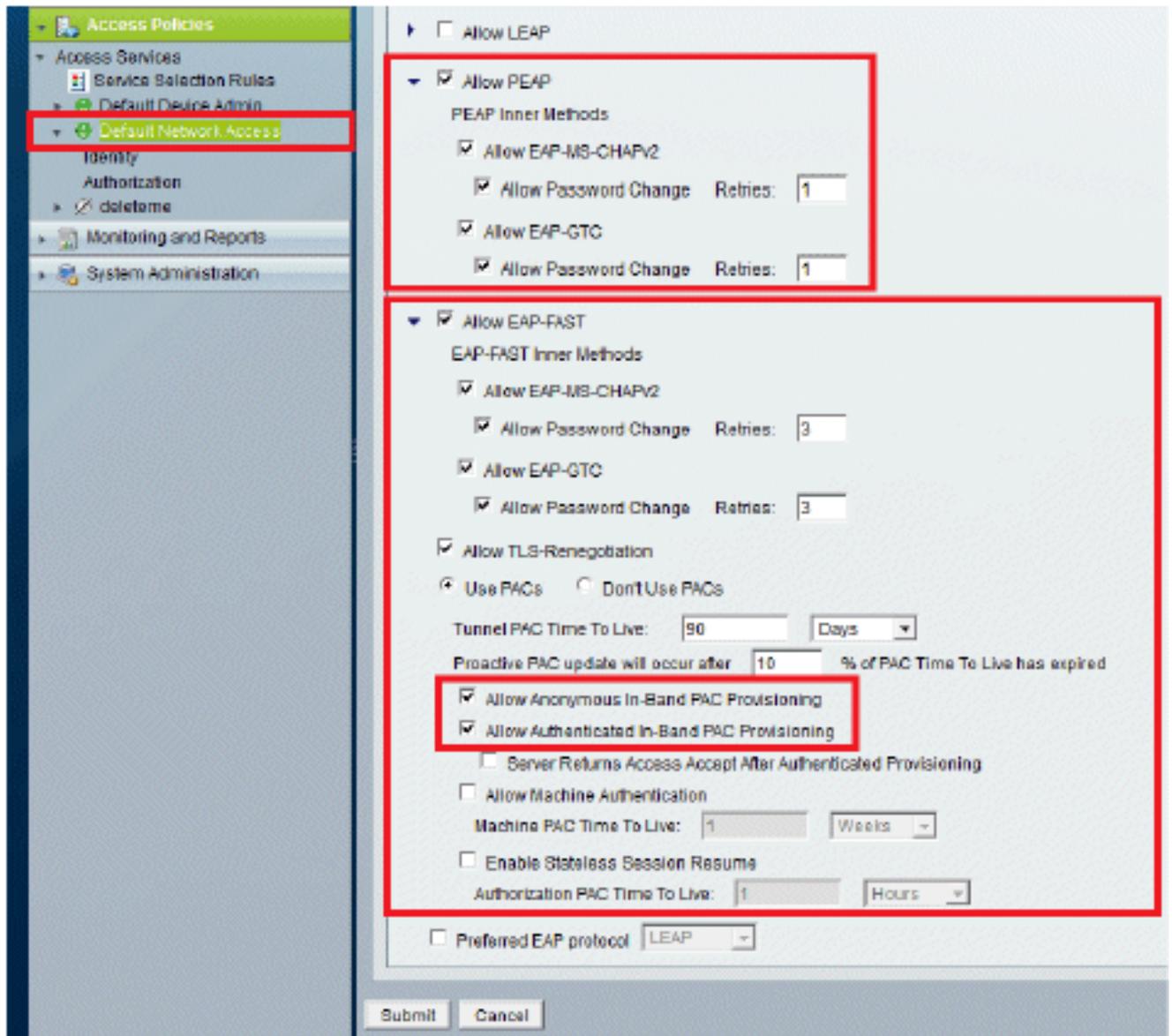
次のステップを実行します。

1. Access Policies > Access Services > Default Network Access > Edit: "Default Network Access"の順に選択します。



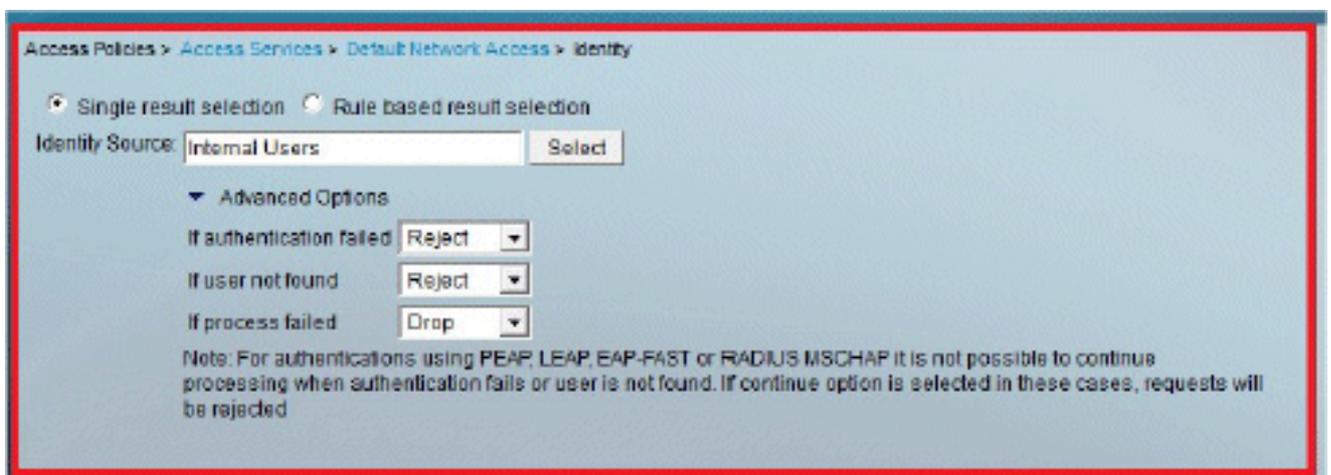
2. ワイヤレスクライアントを認証する EAP 方式を選択します。この例では、PEAP-MSCHAPv2 と EAP-FAST を使用します。





3. [Submit] をクリックします。

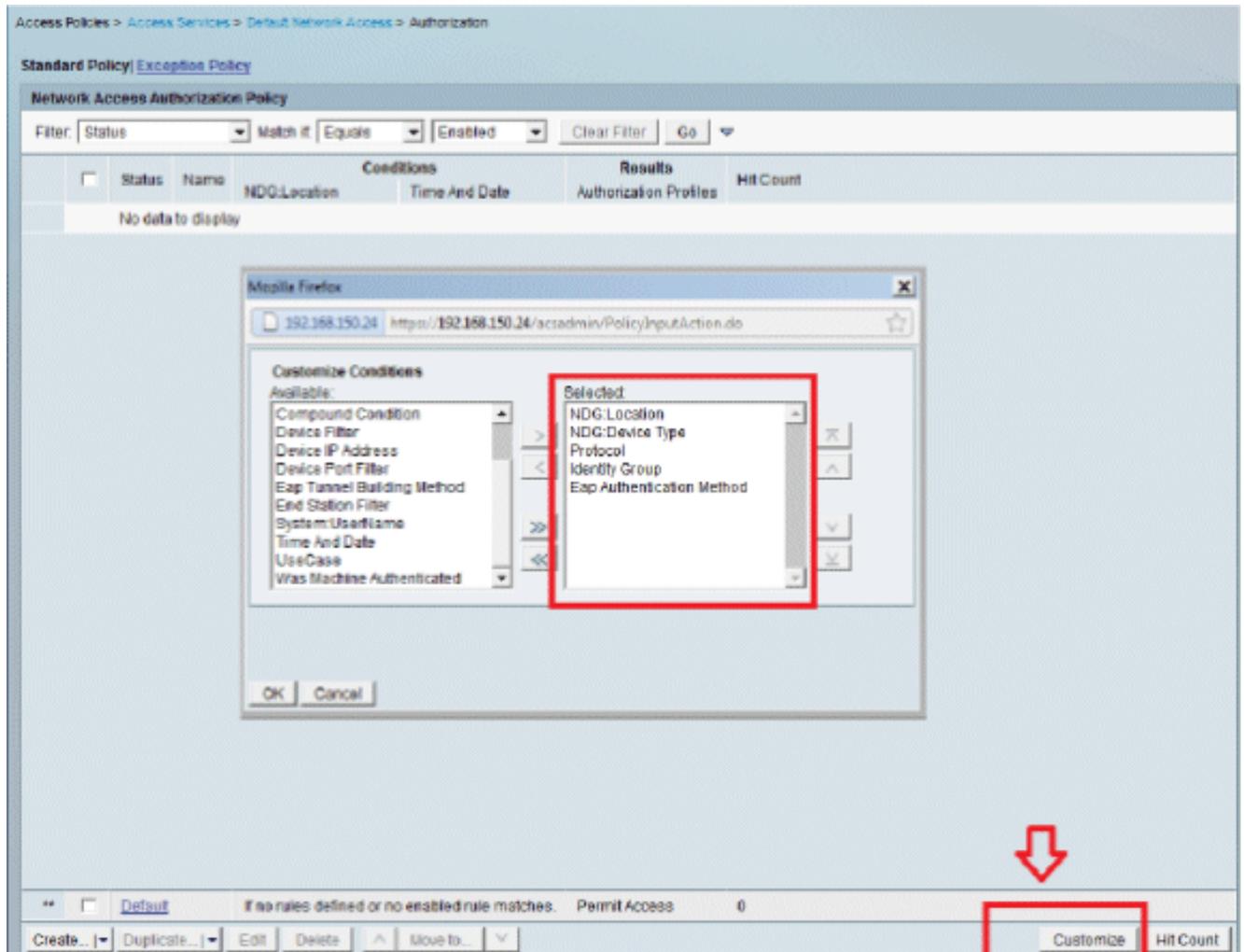
4. 選択した Identity グループを確認します。この例では、ACS 上に作成した [Internal Users] を使用し、変更を保存します。



5. 許可プロファイルを確認するには、[Access Policies] > [Access Services] > [Default Network

Access] > [Authorization] に移動します。

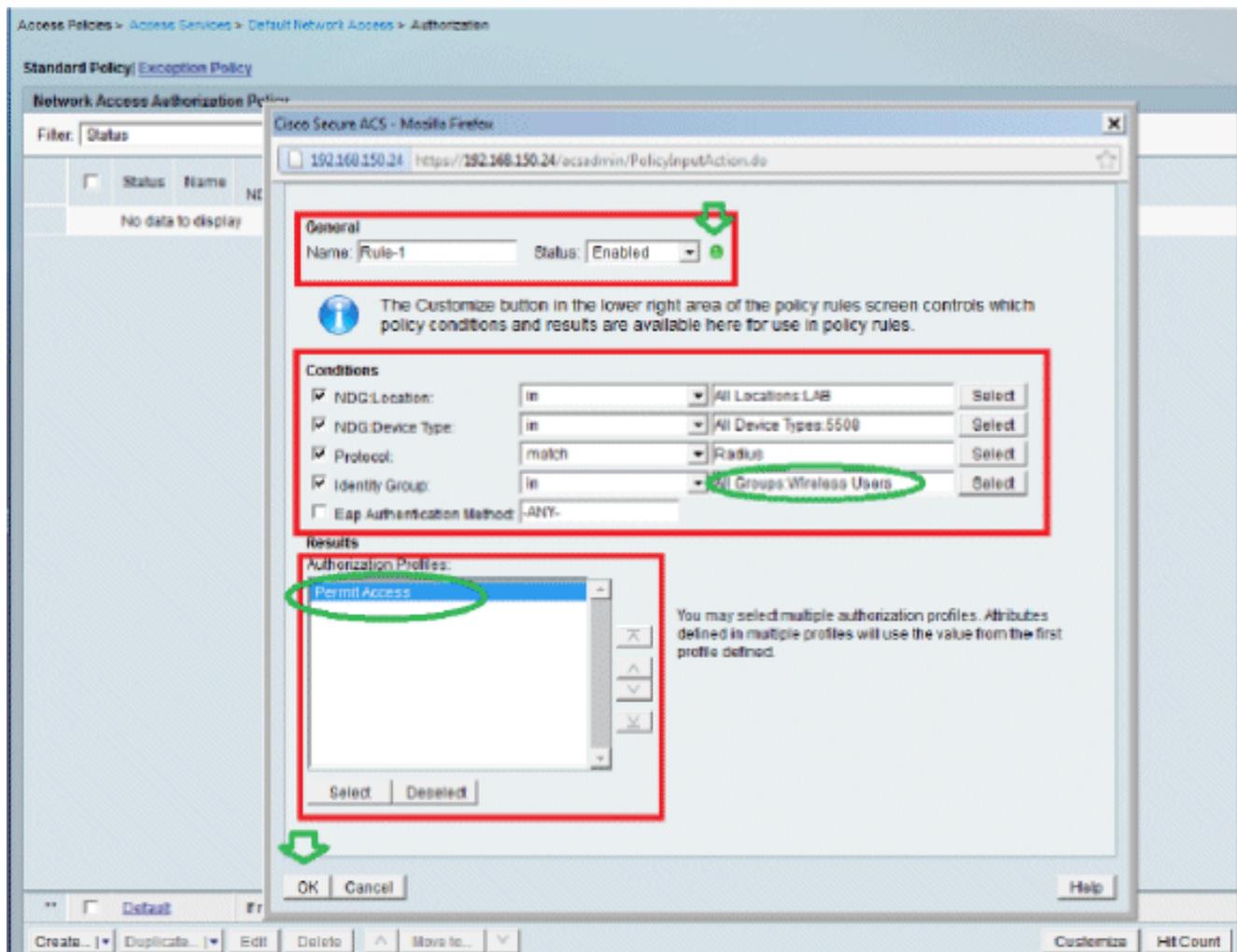
ユーザのネットワークに対するアクセス条件や、認証後に許可する許可プロファイル（属性）をカスタマイズできます。この精度は ACS 5.x でしか利用できません。この例では、[Location]、[Device Type]、[Protocol]、[Identity Group]、[EAP Authentication Method] を選択します。



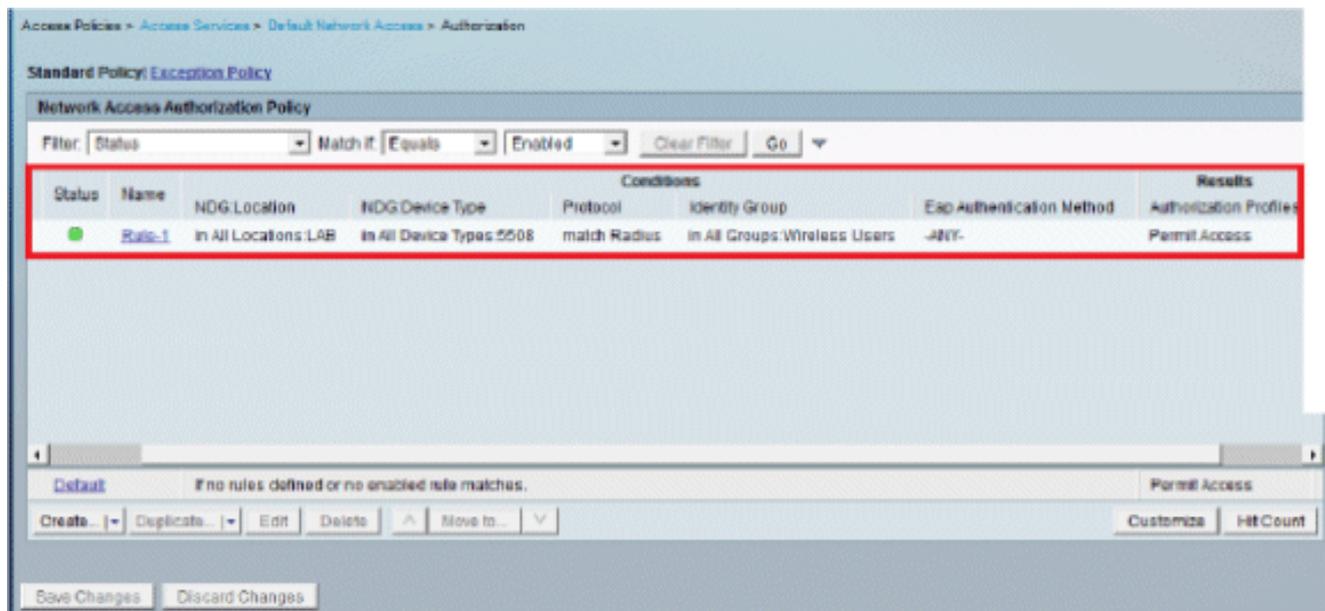
6. [OK] をクリックして変更を保存します。

7. 次に、ルールを作成します。ルールが定義されていない場合、クライアントは条件なしでアクセスが許可されます。

[Create] > [Rule-1] をクリックします。このルールは、グループ "Wireless Users" 内のユーザ向けです。



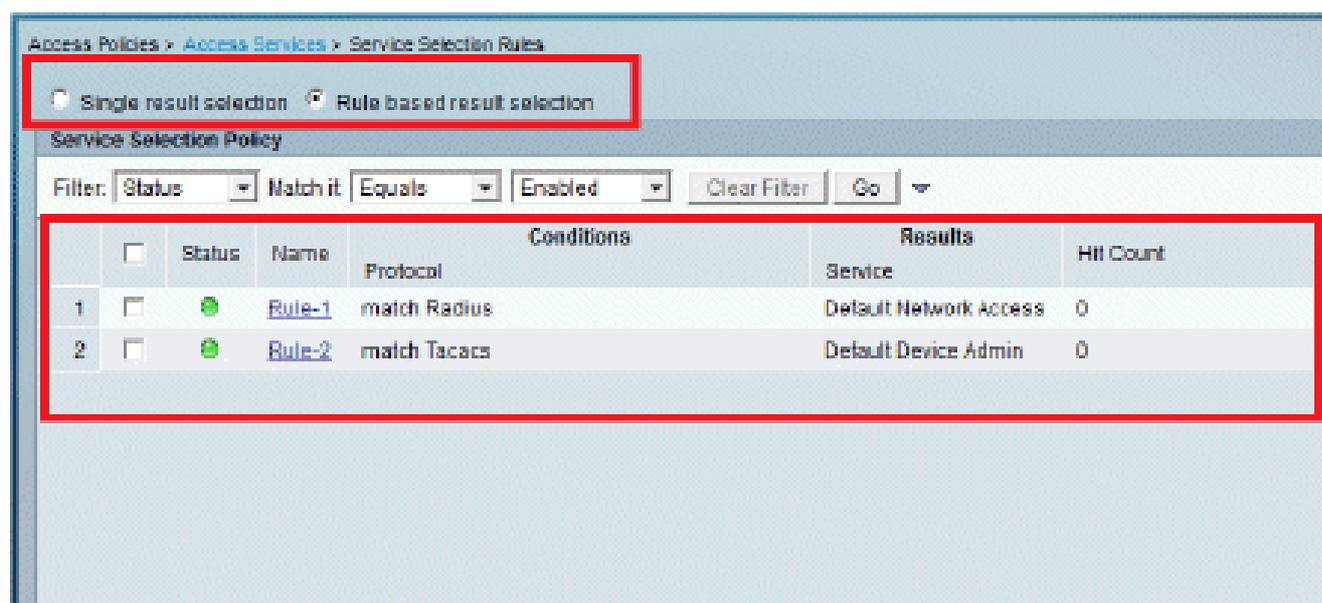
8. 変更を保存します。次のような画面が表示されます。



条件と一致しないユーザを拒否する場合は、デフォルトルールを "deny access" に編集します。

9. 次に、サービス選択ルールを定義します。このページは、着信要求に適用するサービスを決

定する単純なポリシーまたはルールベースのポリシーを設定する場合に使用します。この例では、ルールベースのポリシーを使用しています。



WLC の設定

設定には次の手順が必要です。

1. [WLC での認証サーバの詳細設定](#)
2. [ダイナミック インターフェイス \(VLAN \) の設定](#)
3. [WLAN \(SSID \) の設定](#)

WLC での認証サーバの詳細設定

WLC と RADIUS サーバの間でクライアントの認証やその他のトランザクションを行えるように、WLC を設定する必要があります。

次のステップを実行します。

1. コントローラの GUI で、[Security] をクリックします。
2. RADIUS サーバの IP アドレスと、RADIUS サーバと WLC の間で使用する共有秘密キーを入力します。

この共有秘密キーは、RADIUS サーバに設定されたキーと一致している必要があります。

The screenshot shows the Cisco WLC configuration interface. The top navigation bar includes MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY (highlighted), MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The left sidebar shows the Security menu with options like AAA, RADIUS, TACACS+, LDAP, Local EAP, Priority Order, Certificate, Access Control Lists, Wireless Protection Policies, Web Auth, and Advanced. The main content area is titled "RADIUS Authentication Servers > New" and contains the following configuration fields:

Server Index (Priority)	1
Server IP Address	192.168.150.24
Shared Secret Format	ASCII
Shared Secret	*****
Confirm Shared Secret	*****
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812
Server Status	Enabled
Support for RFC 3576	Enabled
Server Timeout	2 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable

ダイナミック インターフェイス (VLAN) の設定

この手順では、WLC でダイナミック インターフェイスを設定する方法について説明します。

次のステップを実行します。

1. ダイナミック インターフェイスは [Controller] > [Interfaces] ウィンドウのコントローラ GUI で設定します。

The screenshot shows the Cisco WLC configuration interface. The top navigation bar includes MONITOR, WLANs, CONTROLLER (highlighted), WIRELESS, SECURITY, and MANAGEMENT. The left sidebar shows the Controller menu with options like General, Inventory, Interfaces (highlighted), Interface Groups, Multicast, Network Routes, Internal DHCP Server, Mobility Management, Ports, NTP, CDP, and Advanced. The main content area is titled "Interfaces > New" and contains the following configuration fields:

Interface Name	vlan253
VLAN Id	253

2. [APPLY] をクリックします。

このダイナミック インターフェイス (この例では VLAN 253) の [Edit] ウィンドウが開きます。

3. このダイナミック インターフェイスの IP アドレスとデフォルト ゲートウェイを入力します。

The screenshot shows the Cisco Controller configuration page for a dynamic interface. The page is titled "Interfaces > Edit" and is divided into several sections. The "Interface Address" section is highlighted with a red box. The configuration details are as follows:

General Information	
Interface Name	vlan253
MAC Address	00:24:97:09:03:cf

Configuration	
Guest Lan	<input type="checkbox"/>
Quarantine	<input type="checkbox"/>
Quarantine Vlan Id	0

Physical Information	
The interface is attached to a LAG.	
Enable Dynamic AP Management	<input type="checkbox"/>

Interface Address	
VLAN Identifier	253
IP Address	192.168.153.81
Netmask	255.255.255.0
Gateway	192.168.153.1

DHCP Information	
Primary DHCP Server	192.168.130.25
Secondary DHCP Server	

Access Control List	
ACL Name	none

Note: Changing the Interface parameters causes the VLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.

4. [APPLY] をクリックします。

5. 設定したインターフェイスは、次のようになります。

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
management	75	192.168.75.44	Static	Enabled
service-port	N/A	0.0.0.0	Static	Not Supported
virtual	N/A	1.1.1.1	Static	Not Supported
vlan253	253	192.168.153.81	Dynamic	Disabled

WLAN (SSID) の設定

この手順では、WLC で WLAN を設定する方法について説明します。

次のステップを実行します。

1. 新規の WLAN を作成するには、コントローラの GUI で [WLANs] > [Create New] の順に選択します。新規の WLAN のウィンドウが表示されます。
2. WLAN ID と WLAN SSID 情報を入力します。

WLAN SSID には任意の名前を入力できます。この例では、WLAN SSID として goa を使用しています。

WLANs > New

Type: WLAN

Profile Name: goa

SSID: goa

ID: 1

3. [Apply] をクリックして、WLAN goa の [Edit] ウィンドウに移動します。

CISCO MONITOR **WLANs** CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

WLANs

- WLANs
- Advanced
 - AP Groups

WLANs > Edit 'goa'

General Security QoS Advanced

Profile Name: goa
Type: WLAN
SSID: goa
Status: Enabled

Security Policies: [WPA2][Auth(802.1X + CCKM)]
(Modifications done under security tab will appear after applying the changes.)

Radio Policy: All

Interface/Interface Group(G): vlan253

Multicast Vlan Feature: Enabled
Broadcast SSID: Enabled

CISCO MONITOR **WLANs** CONTROLLER WIRELESS SECURITY

WLANs

- WLANs
- Advanced

WLANs > Edit 'goa'

General **Security** QoS Advanced

Layer 2 Layer 3 AAA Servers

Layer 2 Security: WPA+WPA2

802.1X NAC Filtering

WPA+WPA2 Parameters

WPA Policy:

WPA2 Policy:

WPA2 Encryption: AES TKIP

Auth Key Mgmt: 802.1X+CCKM

WLANs > Edit 'goa'

The screenshot shows the 'Security' tab with the 'AAA Servers' sub-tab selected. A red box highlights the 'AAA Servers' sub-tab and the table below. The table has columns for 'Authentication Servers' and 'Accounting Servers'. The 'Server 1' row is highlighted with a red box, showing 'IP:192.168.150.24, Port:1812' for authentication and 'None' for accounting. Other servers are set to 'None'. There are also sections for 'Radius Servers' (with 'Radius Server Overrides interface' disabled) and 'LDAP Servers' (with three servers set to 'None').

Server	Authentication Servers	Accounting Servers
Server 1	IP:192.168.150.24, Port:1812	None
Server 2	None	None
Server 3	None	None

WLANs > Edit 'goa'

The screenshot shows the 'Advanced' sub-tab selected. A red box highlights the 'Advanced' sub-tab and several configuration options: 'Enable Session Timeout' (disabled), 'Client Exclusion' (disabled), 'DHCP Addr. Assignment' (Required), 'MFP Client Protection' (Disabled), and 'Client Load Balancing' (disabled). Other options include 'Allow AAA Override' (disabled), 'Coverage Hole Detection' (enabled), 'Aironet IE' (enabled), 'Diagnostic Channel' (disabled), 'IPv6 Enable' (disabled), 'Override Interface ACL' (None), 'P2P Blocking Action' (Disabled), 'Maximum Allowed Clients' (0), 'Static IP Tunneling' (disabled), 'DTIM Period' (1 for both 802.11a/n and 802.11b/g/n), 'NAC State' (None), and 'Load Balancing and Band Select' (both disabled).

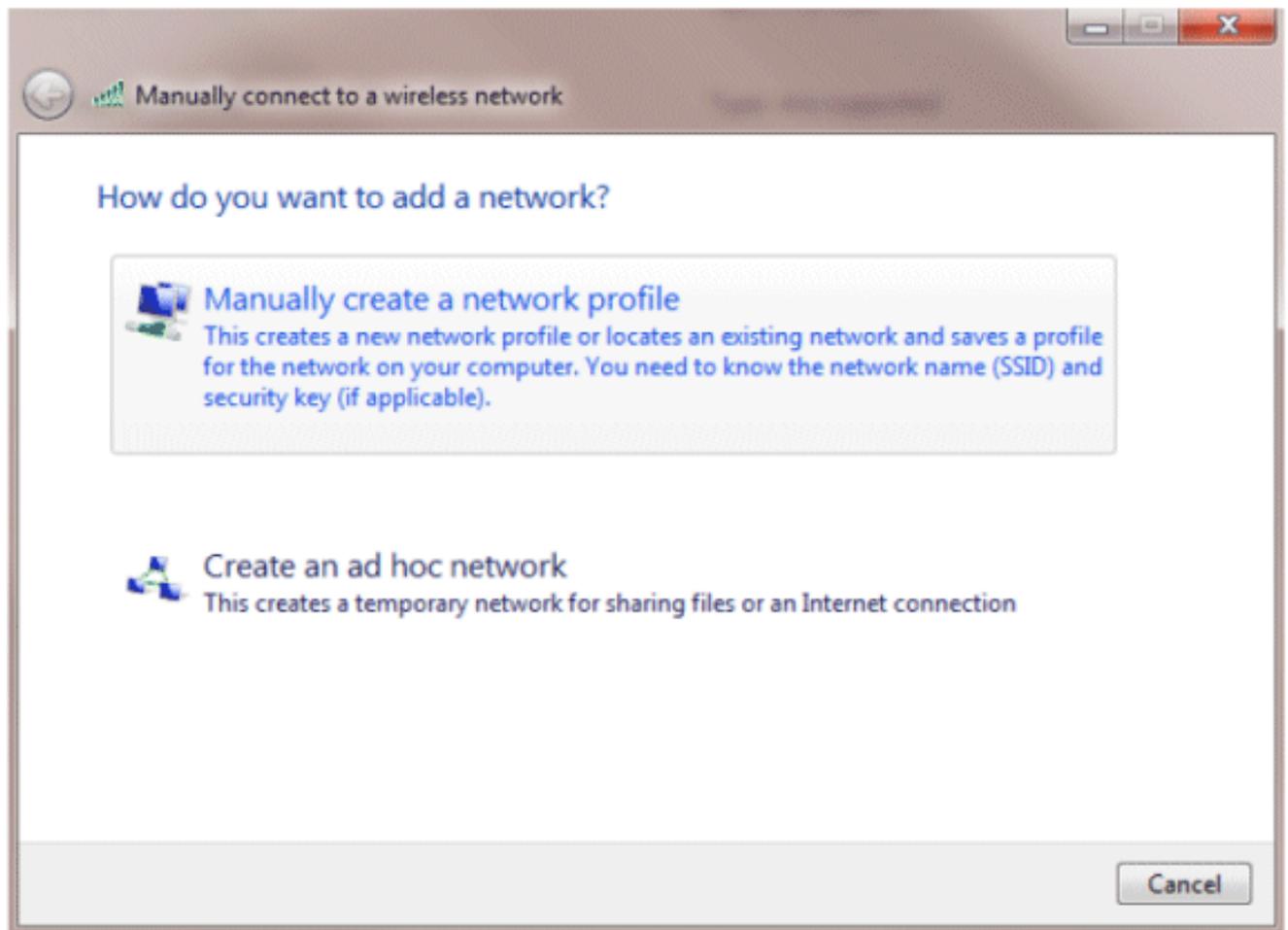
無線クライアント ユーティリティの設定

PEAP-MSCHAPv2 (user1)

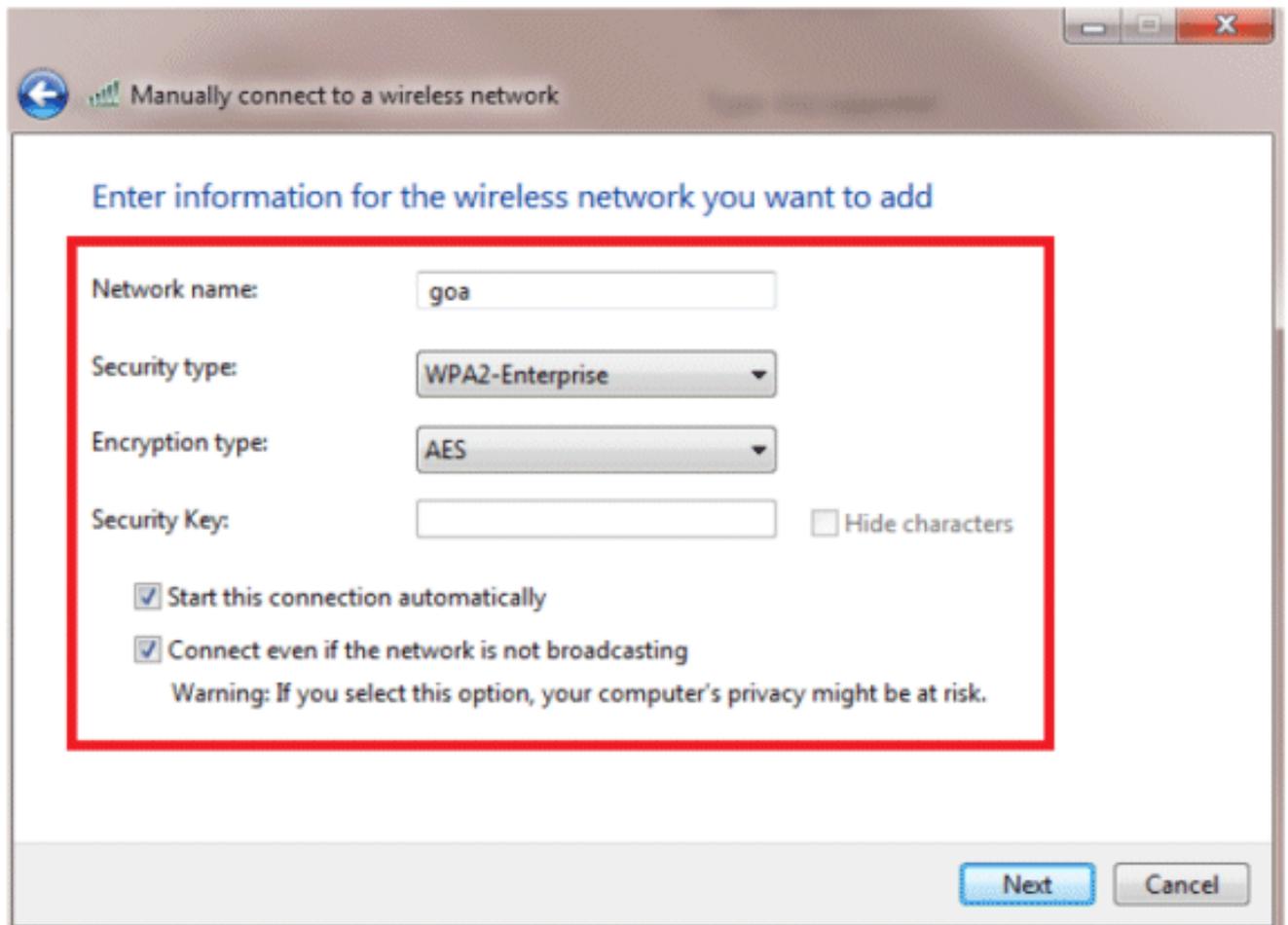
テスト クライアントでは、Intel 6300-N ドライバ バージョン 14.3 対応の Microsoft Windows 7 ネットワーク サプリカントを使用します。テストでは、ベンダーから最新のドライバを取得して使用することを推奨します。

次の手順を実行して、Windows Zero Config (WZC) のプロファイルを作成します。

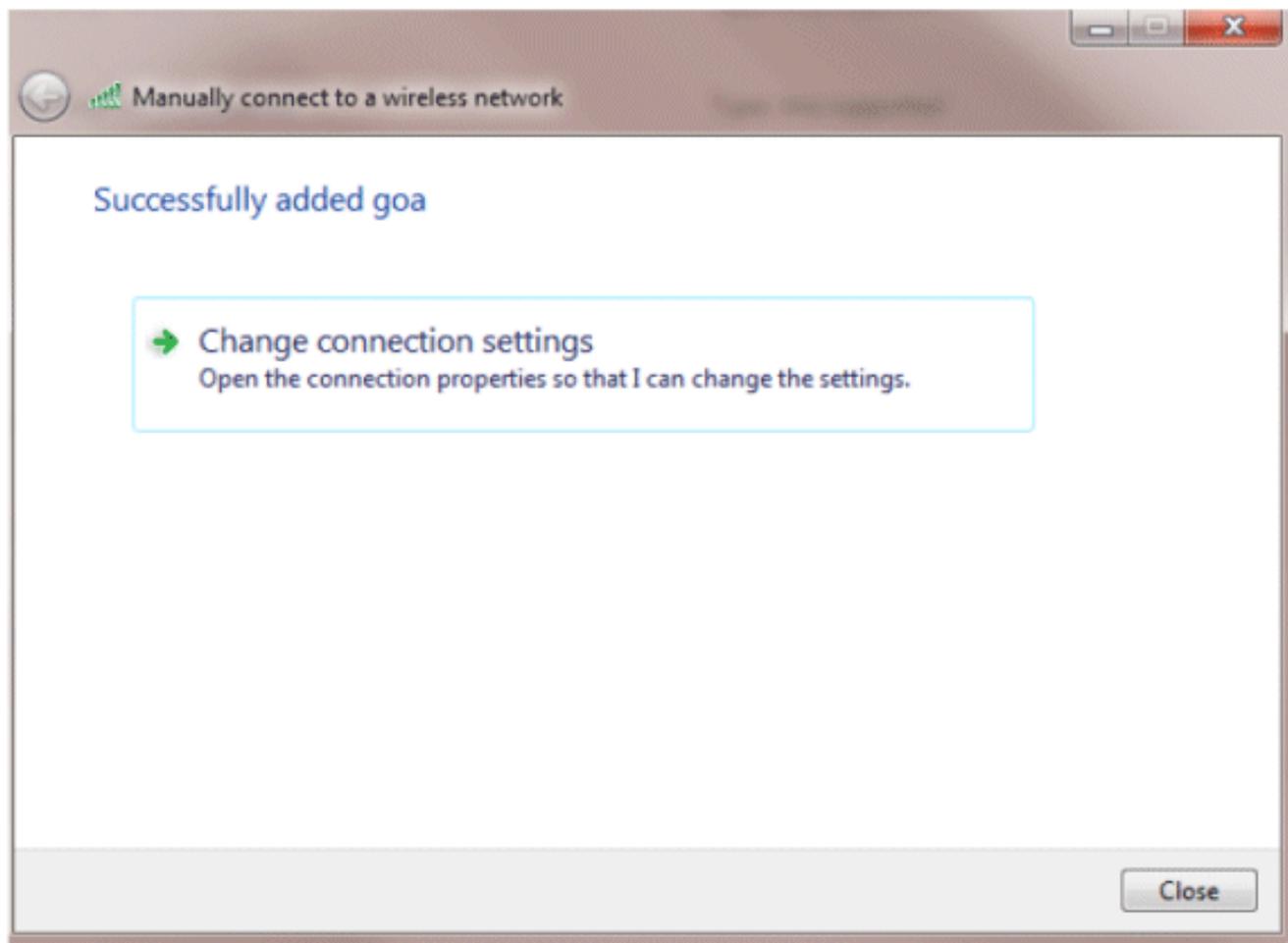
1. [Control Panel] > [Network and Internet] > [Manage Wireless Networks] に移動します。
2. [Add] タブをクリックします。
3. [Manually create a network profile] をクリックします。



4. WLC で設定したとおりに詳細を追加します。
注：SSIDでは大文字と小文字が区別されます。
5. [Next] をクリックします。



6. [Change connection settings] をクリックして設定を再度確認します。



7. PEAP が有効になっていることを確認します。

goa Wireless Network Properties



Connection

Security

Security type:

WPA2-Enterprise

Encryption type:

AES

Choose a network authentication method:

Microsoft: Protected EAP (PEAP)

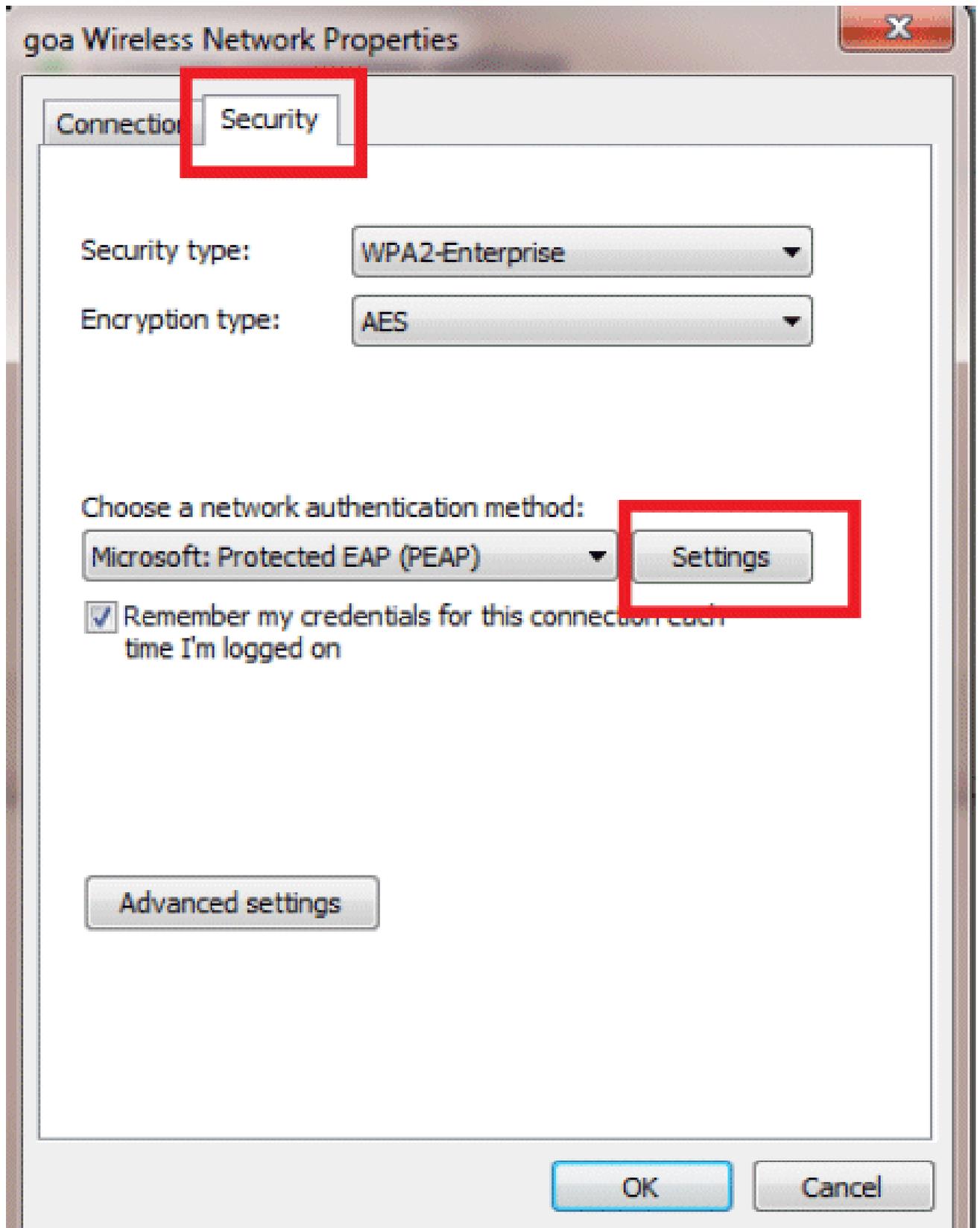
Settings

Remember my credentials for this connection each time I'm logged on

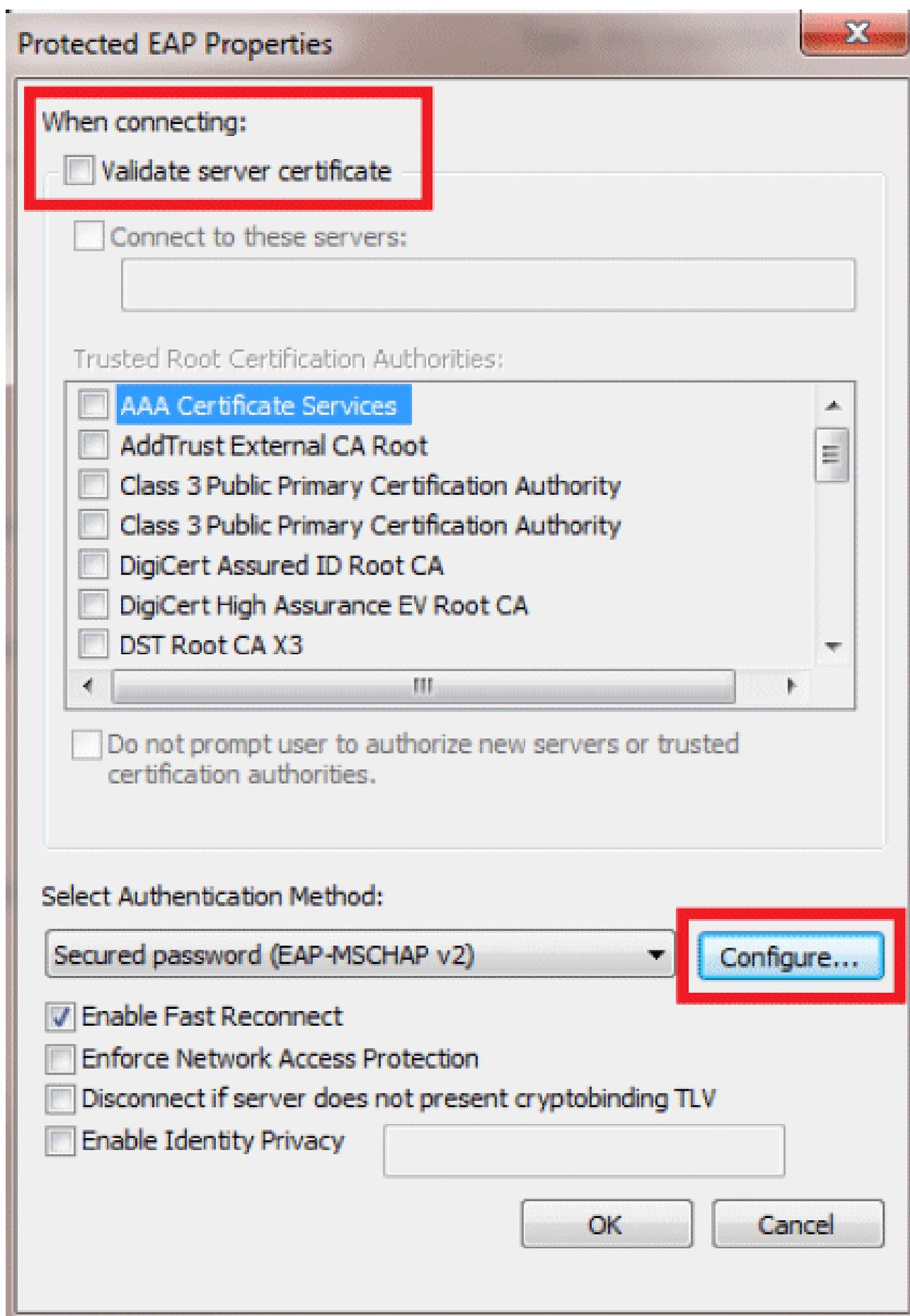
Advanced settings

OK

Cancel

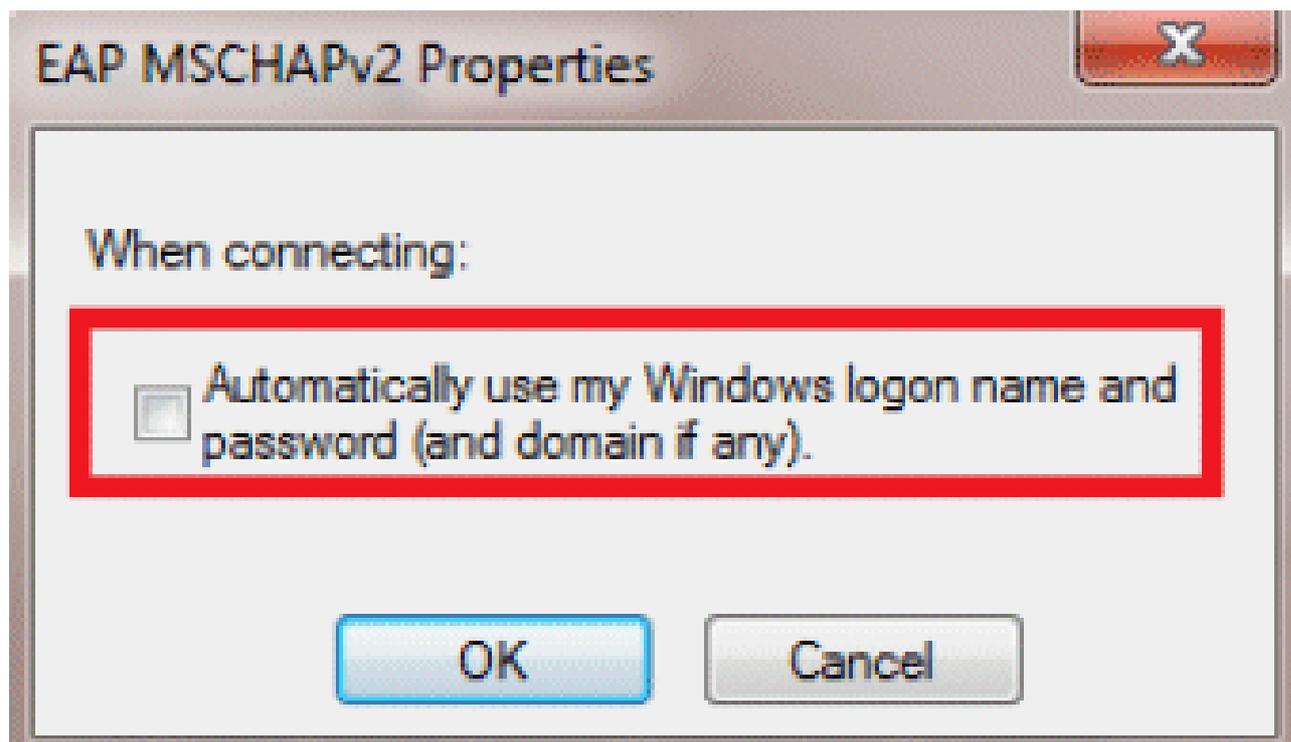


- この例では、サーバ証明書は検証しません。このチェックボックスをオンにしても接続できない場合は、機能を無効にしてから再度テストしてみてください。



9. ほかにも、Windows クレデンシャルでログインできます。ただし、この例ではその方法を

用いません。[OK] をクリックします。



10. [Advanced settings] をクリックしてユーザ名とパスワードを設定します。

goa Wireless Network Properties



Connection Security

Security type: WPA2-Enterprise

Encryption type: AES

Choose a network authentication method:

Microsoft: Protected EAP (PEAP)

Settings

Remember my credentials for this connection each time I'm logged on

Advanced settings

OK

Cancel

Advanced settings



802.1X settings

802.11 settings

Specify authentication mode:

User authentication



Save credentials

Delete credentials for all users

Enable single sign on for this network

Perform immediately before user logon

Perform immediately after user logon

Maximum delay (seconds):

10

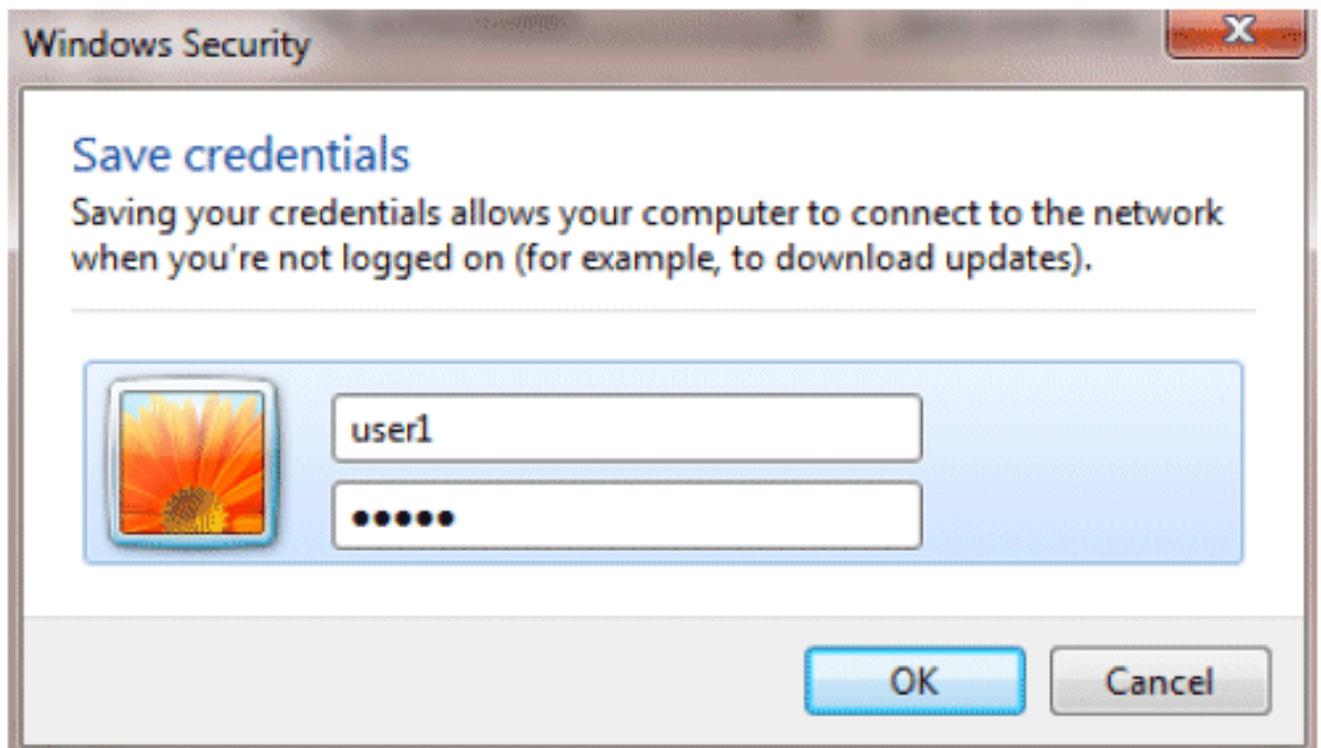


Allow additional dialogs to be displayed during single sign on

This network uses separate virtual LANs for machine and user authentication

OK

Cancel



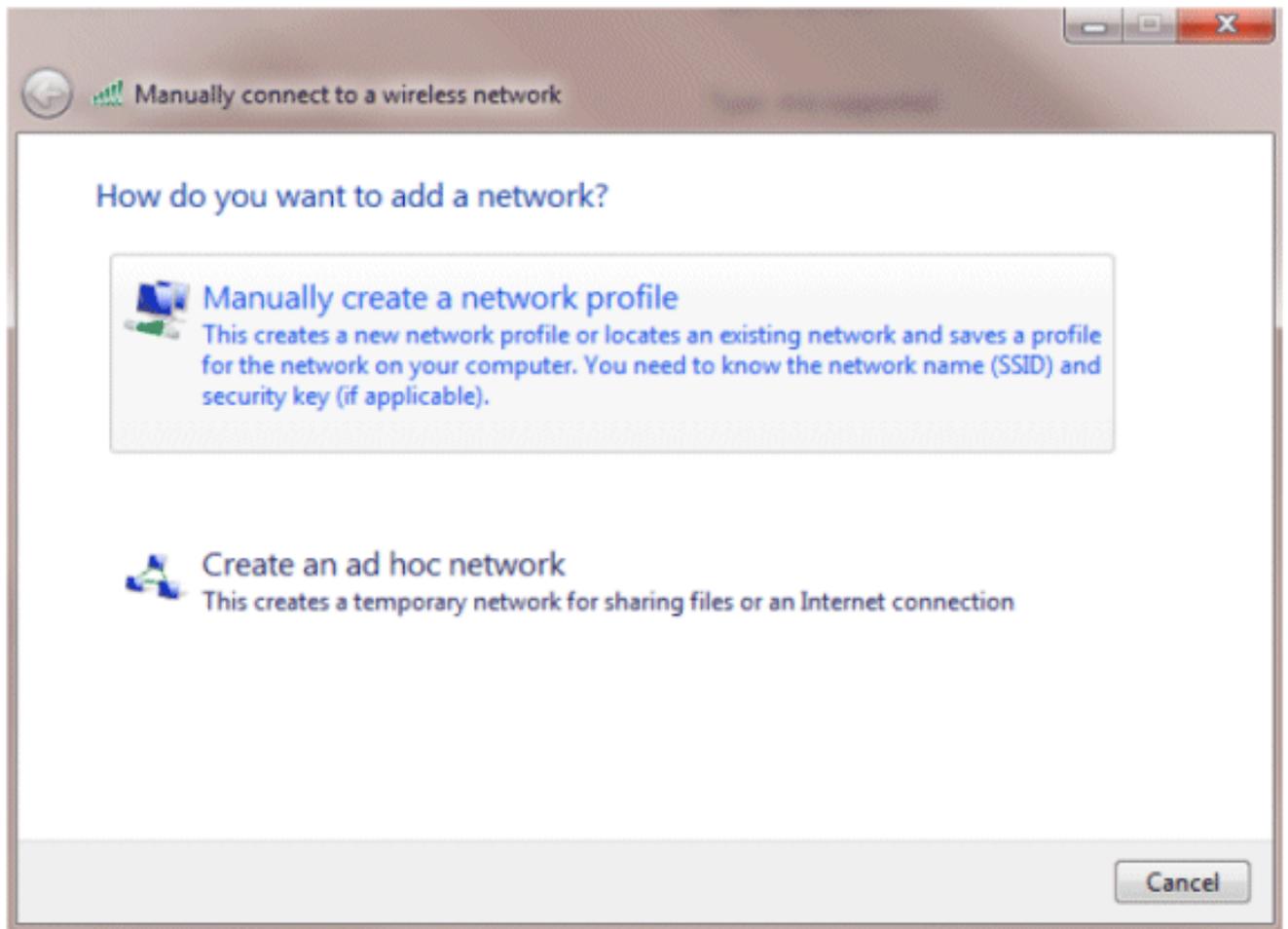
これで、クライアントユーティリティで接続する準備が整いました。

EAP-FAST (user2)

テストクライアントでは、Intel 6300-N ドライババージョン 14.3 対応の Microsoft Windows 7 ネットワーク サプリカントを使用します。テストでは、ベンダーから最新のドライバを取得して使用することを推奨します。

次の手順を実行して WZC でプロファイルを作成します。

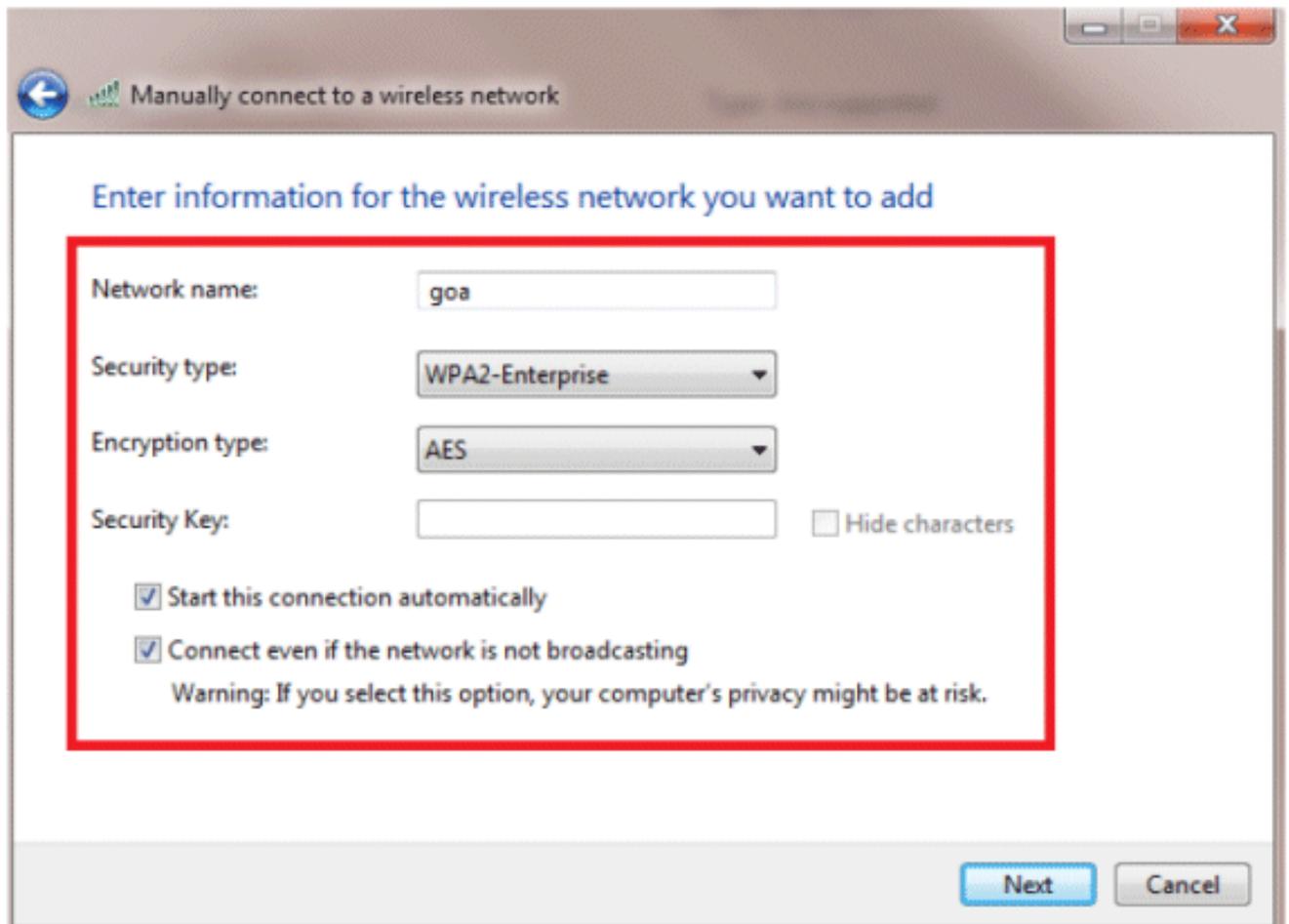
1. [Control Panel] > [Network and Internet] > [Manage Wireless Networks] に移動します。
2. [Add] タブをクリックします。
3. [Manually create a network profile] をクリックします。



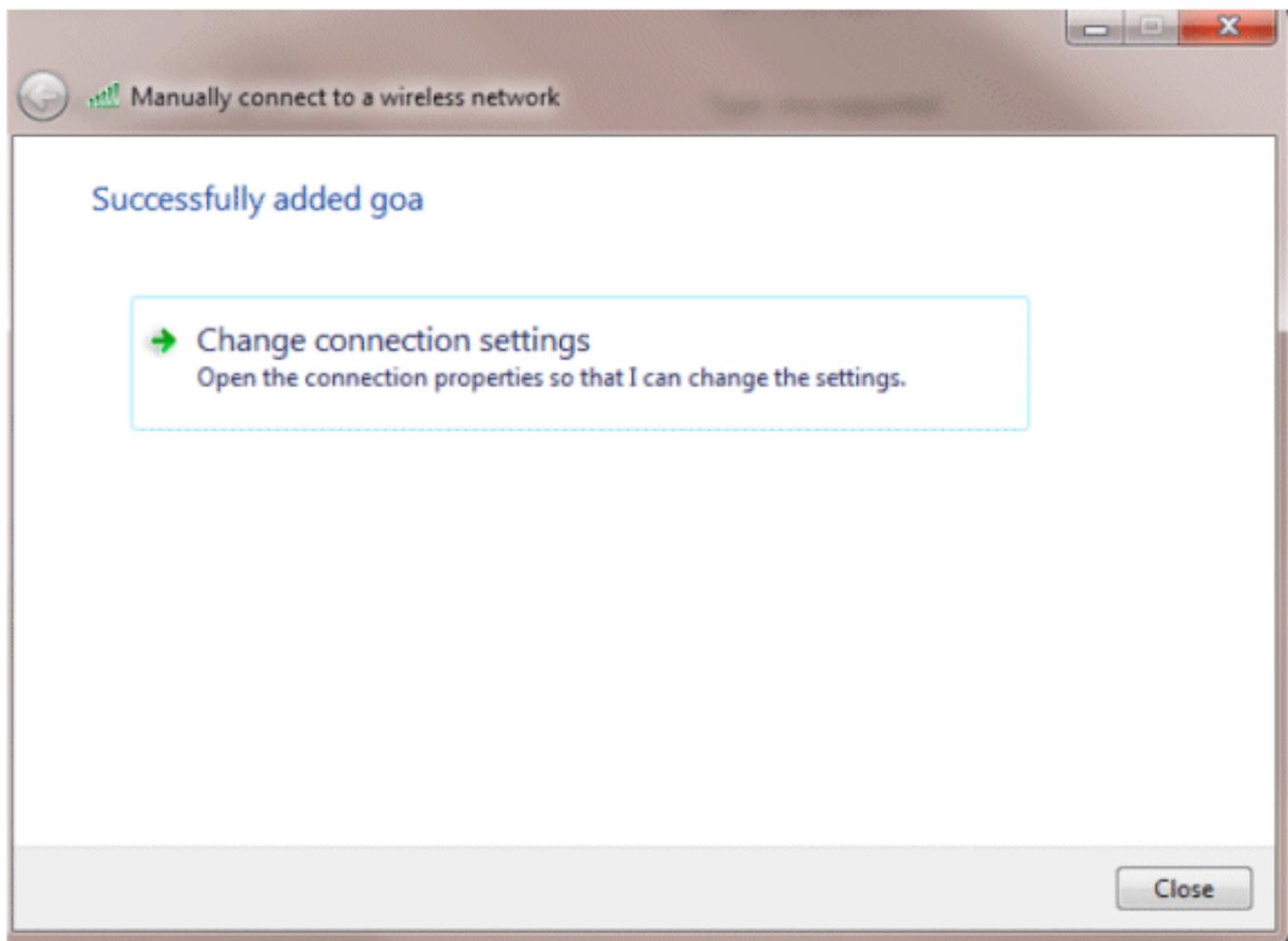
4. WLC で設定したとおりに詳細を追加します。

注：SSIDでは大文字と小文字が区別されます。

5. [Next] をクリックします。



6. [Change connection settings] をクリックして設定を再度確認します。



7. EAP-FAST が有効になっていることを確認します。

注：デフォルトでは、WZCの認証方式はEAP-FASTではありません。サードパーティベンダーからユーティリティをダウンロードする必要があります。この例では、Intel カードを使用するため、システムに Intel PROSet がインストールされています。

Connection

Security

Security type:

WPA2-Enterprise

Encryption type:

AES

Choose a network authentication method:

Cisco: EAP-FAST

Microsoft: Smart Card or other certificate

Microsoft: Protected EAP (PEAP)

Cisco: LEAP

Cisco: PEAP

Cisco: EAP-FAST

Intel: EAP-SIM

Intel: EAP-TTLS

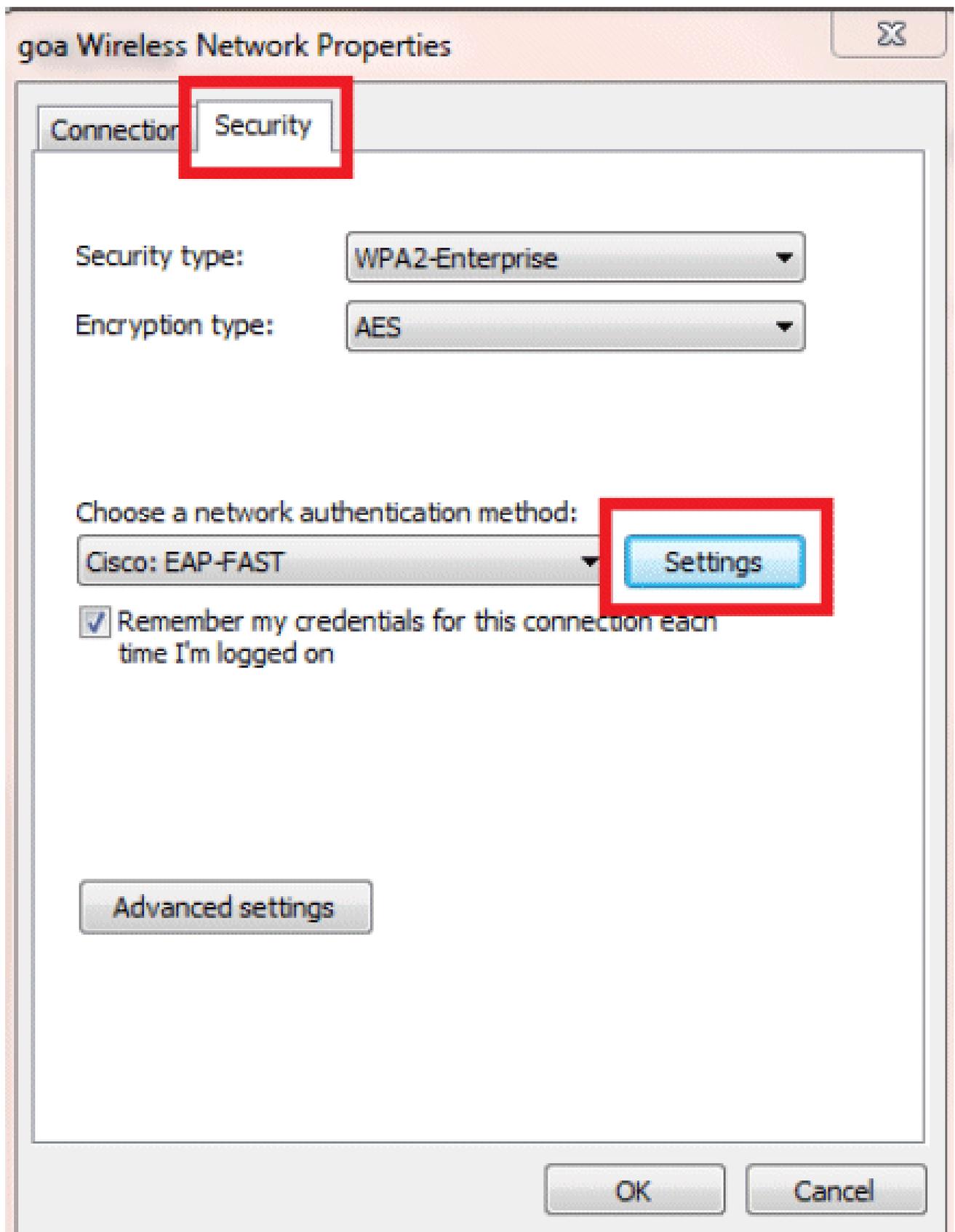
Intel: EAP-AKA

Settings

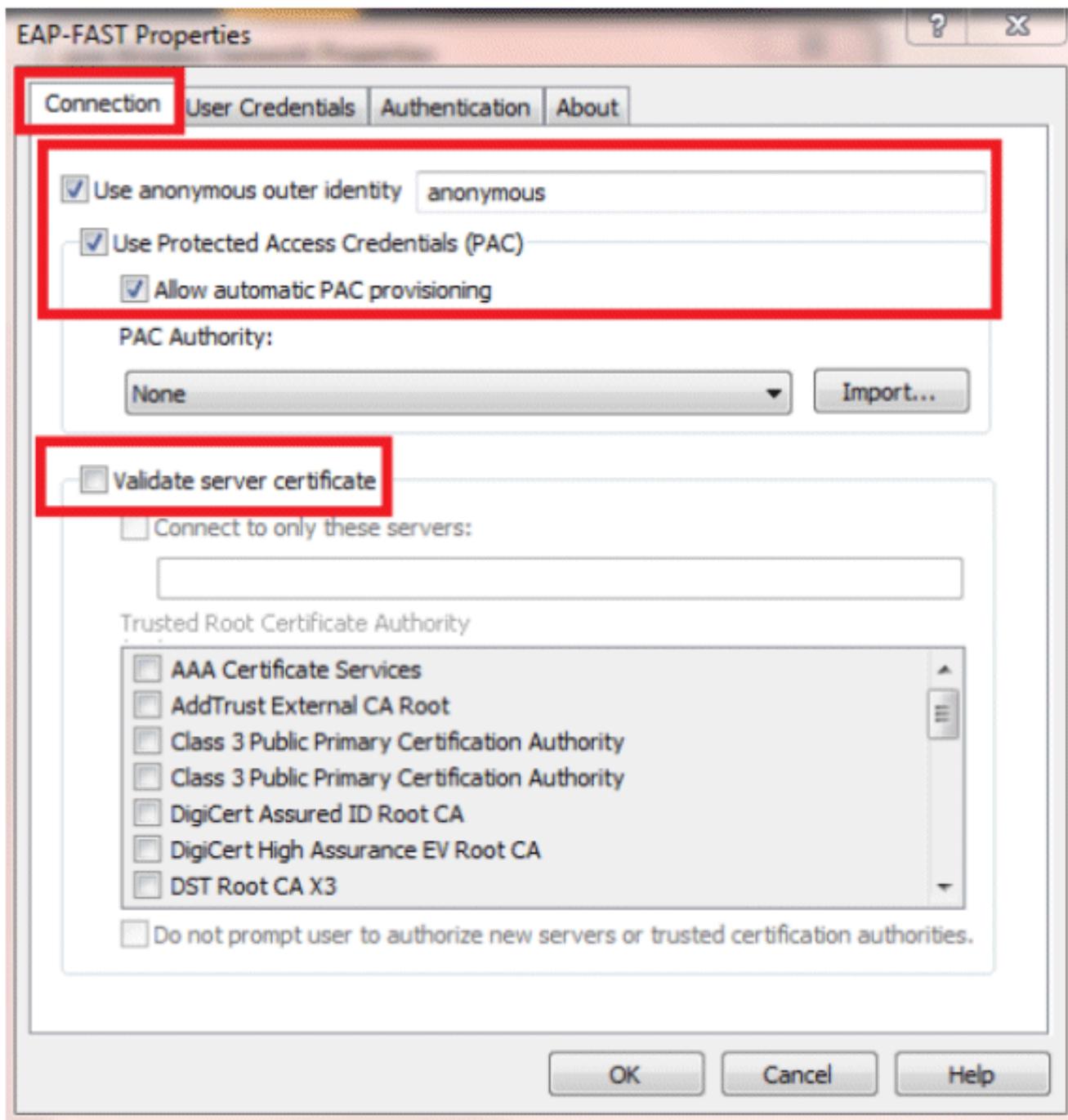
Advanced settings

OK

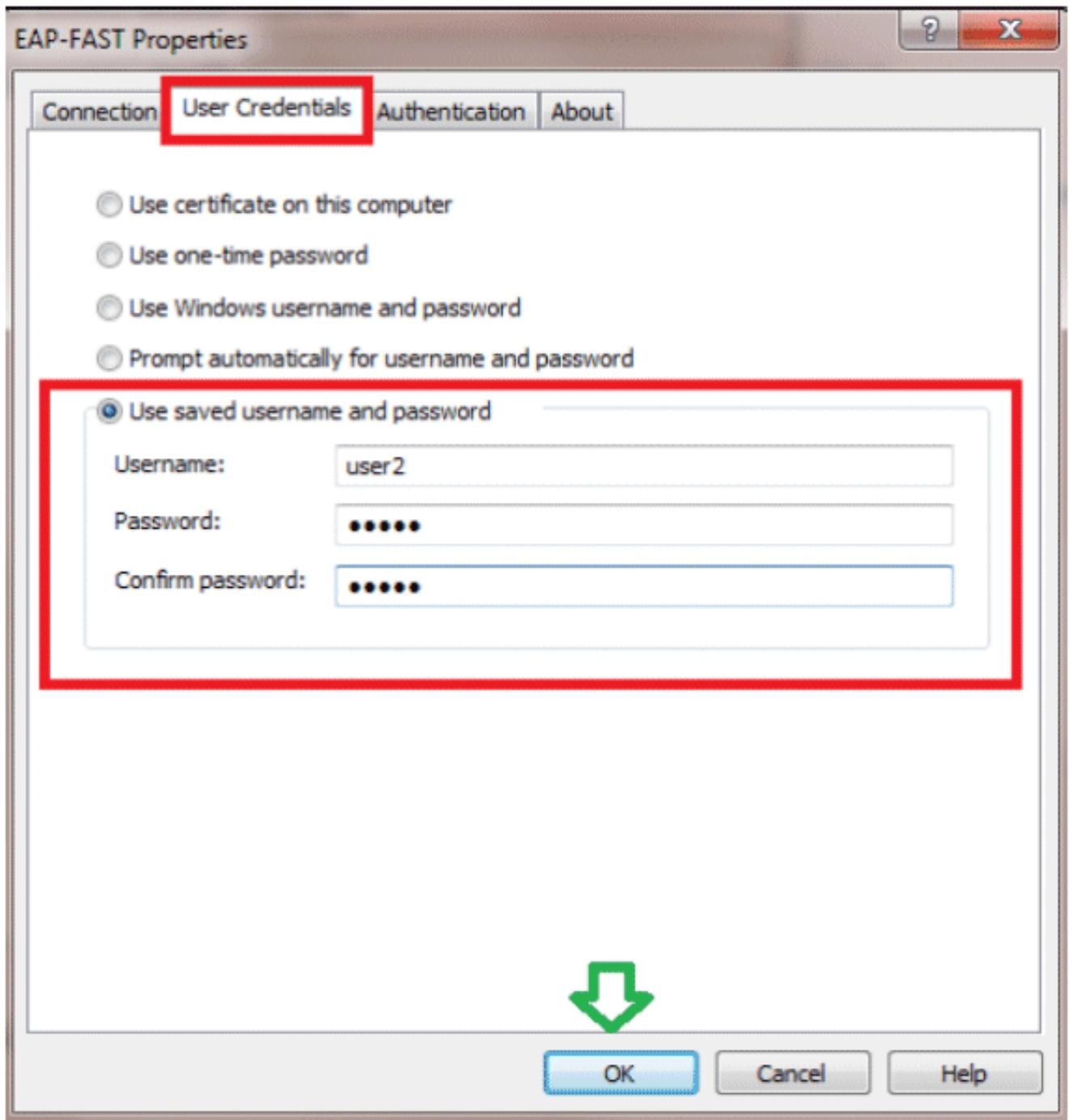
Cancel



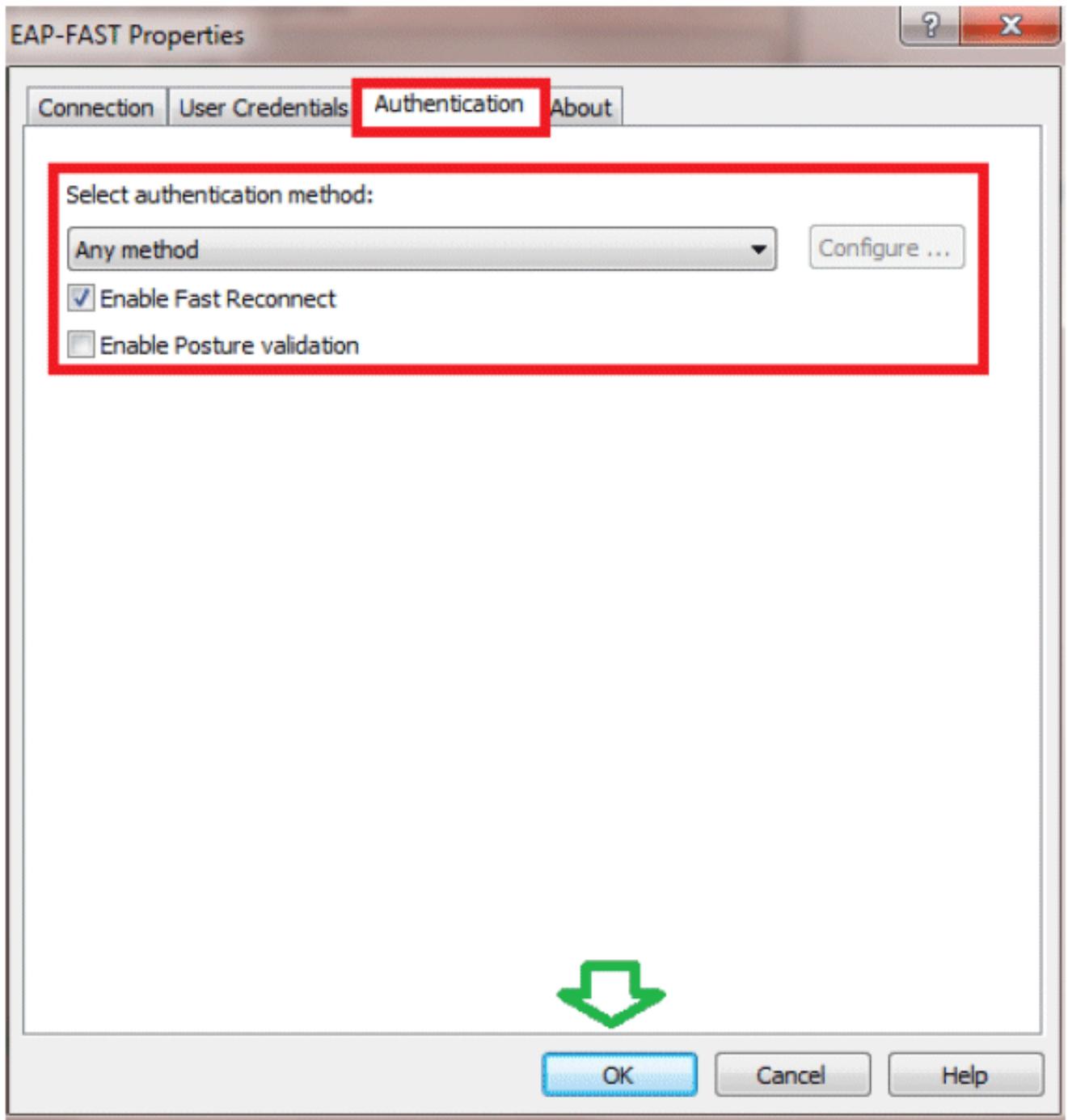
8. [Allow automatic PAC provisioning] をオンにして、[Validate server certificate] がオフになっていることを確認します。



9. [User Credentials] タブをクリックして、user2 のクレデンシャルを入力します。ほかにも、Windows クレデンシャルでログインできます。ただし、この例ではその方法を用いません。

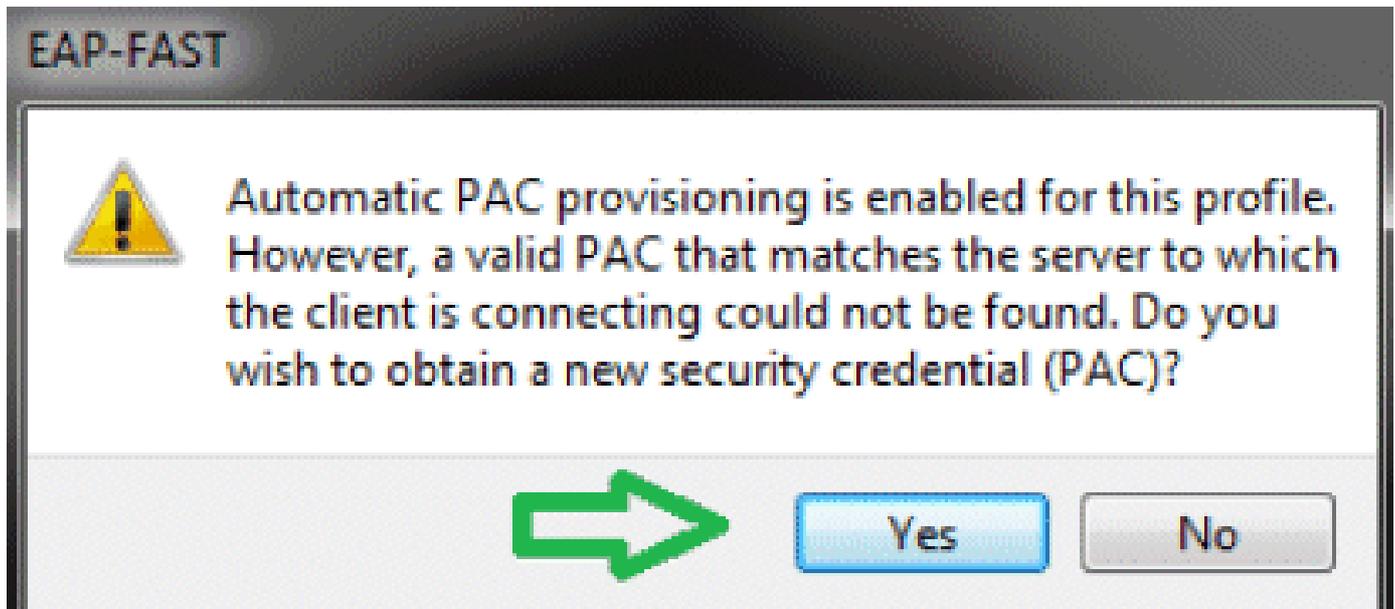


10. [OK] をクリックします。



これで、クライアントユーティリティで user2 に接続する準備が整いました。

注：user2が認証を試みると、RADIUSサーバはPACを送信します。PACを受け入れて認証を完了します。



確認

ここでは、設定が正常に機能しているかどうかを確認します。

[Output Interpreter Tool](#) (OIT) ([登録ユーザ専用](#)) では、特定の show コマンドがサポートされています。OIT を使用して show コマンド出力の解析を表示します。

user1 (PEAP-MSCHAPv2) の検証

WLC GUI から [Monitor] > [Clients] に移動して MAC アドレスを選択します。

Clients > Detail

Client Properties

MAC Address	00:24:d7:aa:f1:08
IP Address	192.168.153.107
Client Type	Regular
User Name	user1
Port Number	13
Interface	vlan253
VLAN ID	253
CCX Version	CCXv4
E2E Version	E2Ev1
Mobility Role	Local
Mobility Peer IP Address	N/A
Policy Manager State	RLN
Management Frame Protection	No
UpTime (Sec)	12
Power Save Mode	OFF
Current TxRateSet	6.0,9.0,12.0,18.0,24.0,36.0,48.0,54.0
Data RateSet	0

AP Properties

AP Address	2c:3f:38:c1:3c:f0
AP Name	3502e
AP Type	802.11an
WLAN Profile	gsm
Status	Associated
Association ID	1
802.11 Authentication	Open System
Reason Code	1
Status Code	0
CF Pollable	Not Implemented
CF Poll Request	Not Implemented
Short Preamble	Not Implemented
PBCC	Not Implemented
Channel Agility	Not Implemented
Re-authentication timeout	86365
Remaining Re-authentication timeout	0
WEP State	WEP Enable

Security Information

Security Policy Completed	Yes
Policy Type	REN (WPA2)
Encryption Cipher	CCMP (AES)
EAP Type	PEAP
SNMP NAC State	Access
Radius NAC State	RLN

WLC RADIUS のステータス :

```
<#root>
```

```
(Cisco Controller) >
```

```
show radius auth statistics
```

```
Authentication Servers:
```

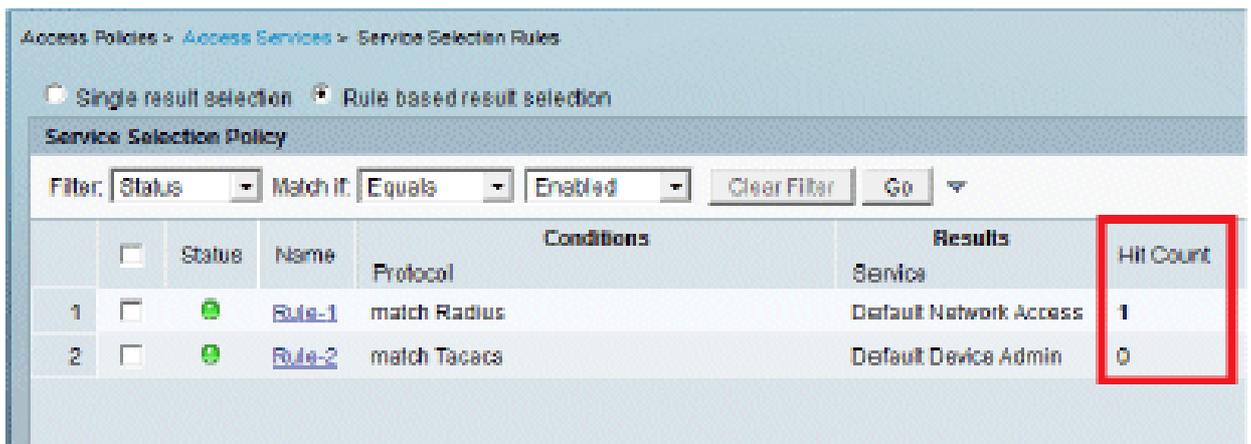
```
Server Index..... 1
Server Address..... 192.168.150.24
Msg Round Trip Time..... 1 (msec)
First Requests..... 8
Retry Requests..... 0
Accept Responses..... 1
Reject Responses..... 0
Challenge Responses..... 7
Malformed Msgs..... 0
Bad Authenticator Msgs..... 0
```

Pending Requests..... 0
Timeout Requests..... 0
Unknowntype Msgs..... 0
Other Drops..... 0

ACS ログ :

1. 次の手順を実行してヒット カウントを表示します。

- a. 認証から 15 分以内にログを確認するときは、必ずヒット カウントを更新してください。



Access Policies > Access Services > Service Selection Rules

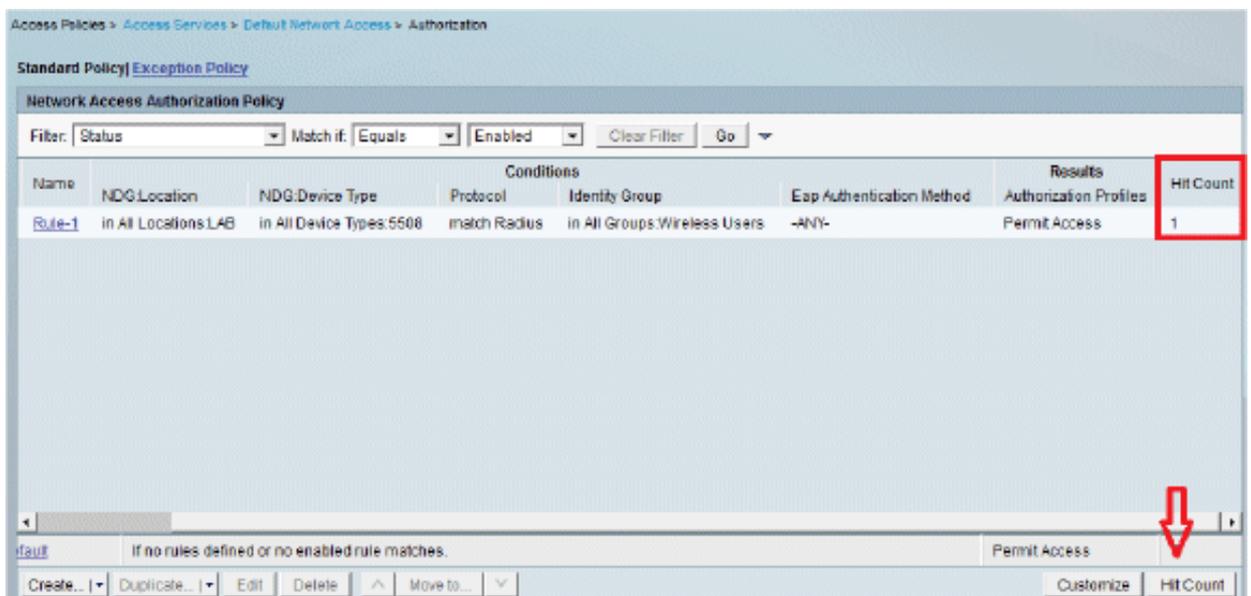
Single result selection Rule based result selection

Service Selection Policy

Filter: Status Match if: Equals Enabled Clear Filter Go

	<input type="checkbox"/>	Status	Name	Protocol	Conditions	Results	Hit Count
1	<input type="checkbox"/>		Rule-1	match Radius		Default Network Access	1
2	<input type="checkbox"/>		Rule-2	match Tacacs		Default Device Admin	0

- b. 同じページの最下部に [Hit Count] のタブがあります。



Access Policies > Access Services > Default Network Access > Authorization

Standard Policy | Exception Policy

Network Access Authorization Policy

Filter: Status Match if: Equals Enabled Clear Filter Go

Name	NDG:Location	NDG:Device Type	Protocol	Identity Group	Eap Authentication Method	Results	Hit Count
Rule-1	In All Locations:LAB	In All Device Types:5508	match Radius	In All Groups:Wireless Users	-ANY-	Permit Access	1

default If no rules defined or no enabled rule matches. Permit Access

Create... Duplicate... Edit Delete Move to... Customize Hit Count

2. [Monitoring and Reports] をクリックすると、新たにポップアップ ウィンドウが表示されます。[Authentications] – [Radius] – [Today] に移動します。このほか、どのサービス選択ルールが適用されたかについては、[Details] をクリックすると確認できます。

Showing Page 1 of 1 Go to Page: Go

AAA Protocol > RADIUS Authentication

Authentication Status : Pass or Fail
 Date : January 29, 2012 05:49 PM - January 29, 2012 05:10 PM (Last 30 Minutes) | [Last Hour](#) | [Last 12 Hours](#) | [Today](#) | [Yesterday](#) | [Last 7 Days](#) | [Last 30 Days](#)

Generated on January 29, 2012 6:10:42 PM EST

Selected

Pass
 Fail
 Click for details
 Mouse over item for additional information

Logged At	RADIUS Status	NAS Failure	Details	Username	MAC/IP Address	Access Service	Authentication Method	Network Device	NAS IP Address	NAS Port ID	CTS Security Group	ACS Instance
Jan 29, 12 6:07:37 943 PM				user1	00:24:7a:af:ff:56	Default_Network_Access	PEAP (EAP-MSCHAPv2)	WLC5508	192.168.75.44			SAUL-ACS02

user2 (EAP-FAST) の検証

WLC GUI から [Monitor] > [Clients] に移動して MAC アドレスを選択します。

Clients > Detail

Client Properties

MAC Address	00:24:7a:af:ff:56
IP Address	192.168.153.111
Client Type	Regular
User Name	user2
Port Number	13
Interface	vlan253
VLAN ID	253
CCX Version	CCXv4
E2E Version	E2Ev1
Mobility Role	Local
Mobility Peer IP Address	N/A
Policy Manager State	RUN
Management Frame Protection	No
UpTime (Sec)	29
Power Save Mode	OFF
Current TxRateSet	m13
Data RateSet	6.0,9.0,12.0,18.0,24.0,36.0,48.0,54.0

AP Properties

AP Address	2c13f1381c113c1f0
AP Name	3502a
AP Type	802.11an
WLAN Profile	g0a
Status	Associated
Association ID	1
802.11 Authentication	Open System
Reason Code	1
Status Code	0
CF Pollable	Not Implemented
CF Poll Request	Not Implemented
Short Preamble	Not Implemented
PBCC	Not Implemented
Channel Agility	Not Implemented
Re-authentication timeout	86302
Remaining Re-authentication timeout	0
WEP State	WEP Enable

Security Information

Security Policy Completed	Yes
Policy Type	RSN (WPA2)
Encryption Cipher	CCMP (AES)
EAP Type	EAP-FAST
SNMP NAC State	Access
Radius NAC State	RUN

ACS ログ :

1. 次の手順を実行してヒット カウントを表示します。

- a. 認証から 15 分以内にログを確認するときは、必ずヒット カウントを更新してください。

Access Policies > Access Services > Service Selection Rules

Single result selection
 Rule based result selection

Service Selection Policy

Filter: Status Match it: Equals Enabled Clear Filter Go

	<input type="checkbox"/>	Status	Name	Conditions	Results	Hit Count
				Protocol	Service	
1	<input type="checkbox"/>		Rule-1	match Radius	Default Network Access	3
2	<input type="checkbox"/>		Rule-2	match Tacacs	Default Device Admin	0

- b. 同じページの最下部に [Hit Count] のタブがあります。

Access Policies > Access Services > Default Network Access > Authorization

Standard Policy | [Exception Policy](#)

Network Access Authorization Policy

Filter: Status Match it: Equals Enabled Clear Filter Go

Name	NDG:Location	NDG:Device Type	Conditions	Results	Hit Count
			Protocol Identity Group	Eap Authentication Method Authorization Profiles	
Rule-1	in All Locations:LAB	in All Device Types:5508	match Radius in All Groups:Wireless Users	-ANY- Permit Access	2

2. [Monitoring and Reports] をクリックすると、新たにポップアップ ウィンドウが表示されます。[Authentications] – [Radius] – [Today] に移動します。このほか、どのサービス選択ルールが適用されたかについては、[Details] をクリックすると確認できます。

Showing Page 1 of 1

AAA Protocol > RADIUS Authentication

Authentication Status: Pass or Fail

Date: January 29, 2012 01:53 PM - January 29, 2012 06:23 PM (Last 30 Minutes | Last Hour | Last 12 Hours | Today | Yesterday | Last 7 Days | Last 30 Days)

Generated on January 29, 2012 6:23:17 PM EST

Legend: Pass Fail Click for details Mouse over items for additional information

Logged At	RADIUS Status	NAS Failure	Details	Username	MAC/IP Address	Access Service	Authentication Method	Network Device	NAS IP Address	NAS Port ID	CTS Security Group	ACS Ins
Jan 29 12 6 19 27 0 PM				user2	00-26-d7-ae-f1-08	Default Network Access	EAP-FAST (EAP-MSCHAPv2)	WLC-5508	192.168.75.44			SALLA
Jan 29 12 6 07 37 943 PM				user1	00-26-d7-ae-f1-08	Default Network Access	PEAP (EAP-MSCHAPv2)	WLC-5508	192.168.75.44			SALLA

トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を紹介します。

トラブルシューティングのためのコマンド

[Output Interpreter Tool](#) (OIT) ([登録](#) ユーザ専用) では、特定の show コマンドがサポートされています。OIT を使用して show コマンド出力の解析を表示します。

注 : [debug](#) コマンドを使用する前に、『[debug コマンドの重要な情報](#)』を参照してください。

1. 問題が発生した場合は、WLC で次のコマンドを発行します。

- debug client <mac add of the client>
- debug aaa all enable
- show client detail <mac addr> : ポリシー マネージャの状態を確認します。
- show radius auth statistics : 失敗の原因を確認します。
- debug disable-all : デバッグをオフにします。
- clear stats radius auth all : WLC 上の RADIUS 統計情報を削除します。

2. ACS のログを確認して失敗の原因を探します。

関連情報

- [テクニカル サポートとドキュメント - Cisco Systems](#)

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。