PEAP、ISE 2.1、およびWLC 8.3を使用した802.1X認証の設定

内容

はじめに

このドキュメントでは、802.1xセキュリティと仮想ローカルエリアネットワーク(VLAN)オーバーライドを使用してワイヤレスローカルエリアネットワーク(WLAN)をセットアップする方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- 802.1X
- Protected Extensible Authentication Protocol（PEAP）
- 認証局（CA）

- 証明書

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。

- WLC v8.3.102.0
- Identity Service Engine(ISE)v2.1
- Windows 10 ラップトップ

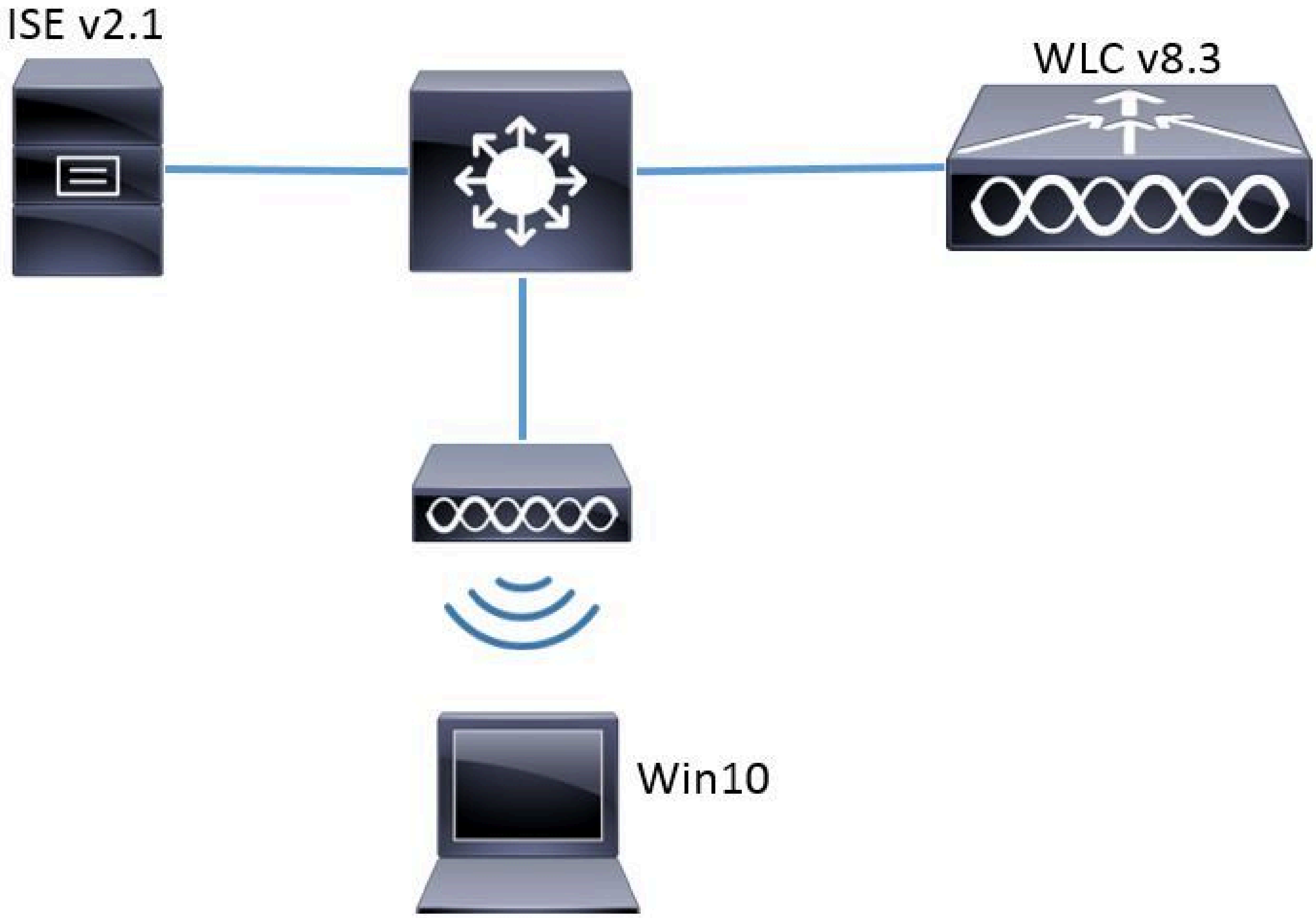
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

802.1xセキュリティとVLANを使用してWLANを設定する場合は、Protected Extensible Authentication Protocol(PEAP)をExtensible Authentication Protocol(EAP)として上書きできます。

設定

ネットワーク図



コンフィギュレーション

一般的な手順は以下のとおりです。

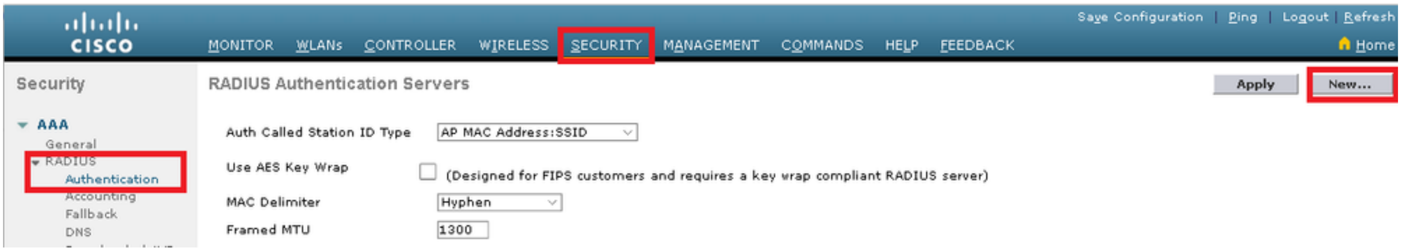
1. 相互の通信を可能にするには、WLC上でRADIUSサーバを宣言し、その逆も宣言します。
2. WLCでService Set Identifier(SSID)を作成します。
3. ISE の認証ルールの作成.
4. ISEで認可プロファイルを作成します。
5. ISE の認可ルールの作成.
6. エンドポイントの設定.

WLCでのRADIUSサーバの宣言

RADIUSサーバとWLC間の通信を可能にするには、RADIUSサーバをWLCに登録する必要があります（その逆も同様）。

GUI：

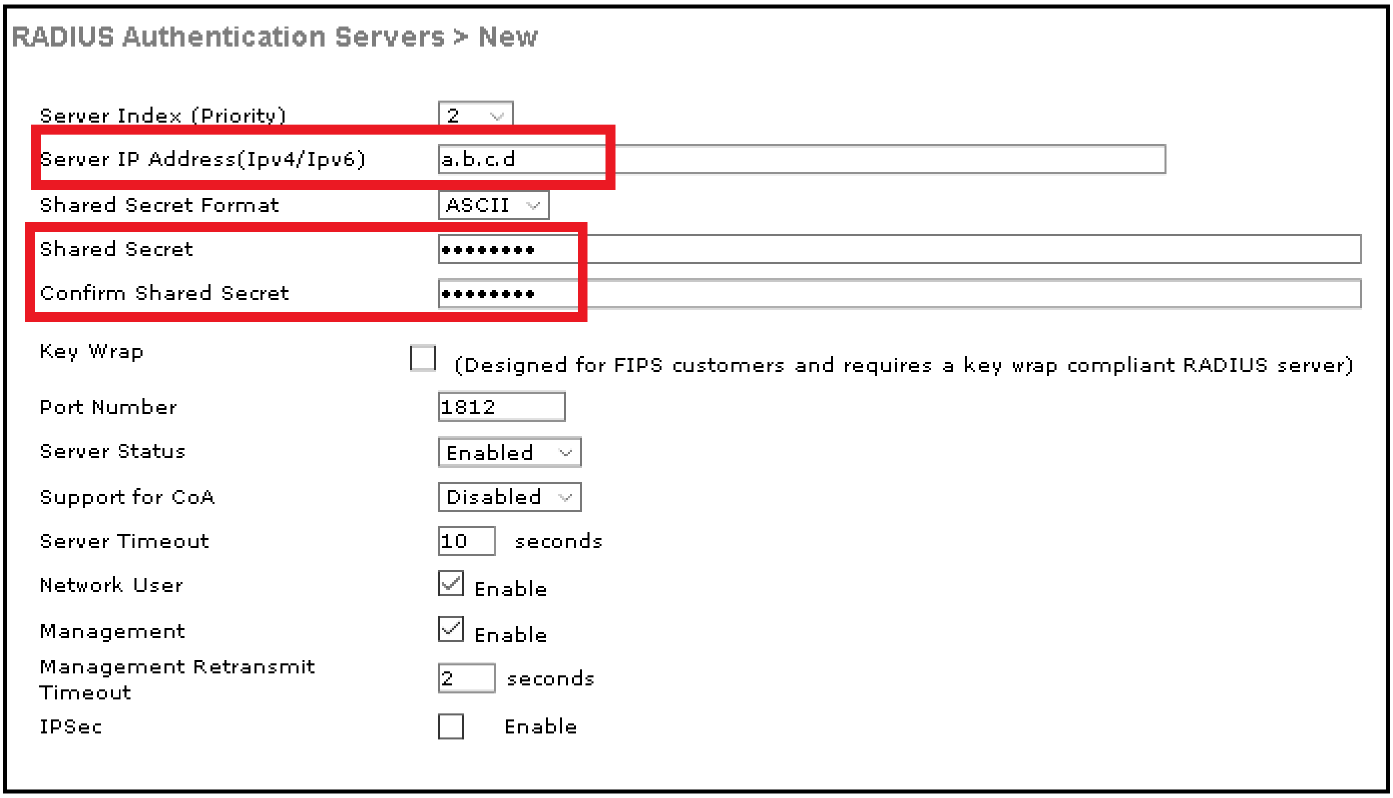
ステップ 1：図に示すように、WLCのGUIを開き、SECURITY > RADIUS > Authentication > Newの順に選択します。



RADIUS Authentication Servers

Auth Called Station ID Type	AP MAC Address:SSID
Use AES Key Wrap	□ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
MAC Delimiter	Hyphen
Framed MTU	1300

ステップ２：図に示すように、RADIUSサーバ情報を入力します。



RADIUS Authentication Servers > New

Server Index (Priority)	2
Server IP Address(Ipv4/Ipv6)	a.b.c.d
Shared Secret Format	ASCII
Shared Secret	••••••••
Confirm Shared Secret	••••••••
Key Wrap	□ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812
Server Status	Enabled
Support for CoA	Disabled
Server Timeout	10 seconds
Network User	☑ Enable
Management	☑ Enable
Management Retransmit Timeout	2 seconds
IPSec	□ Enable

CLI：

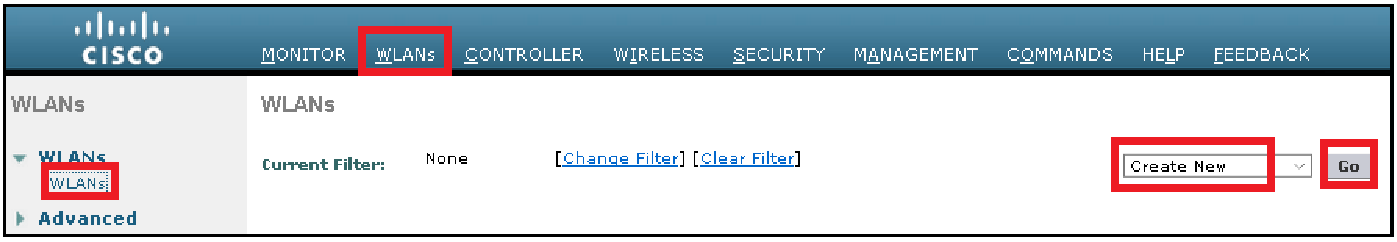
```
> config radius auth add <index> <a.b.c.d> 1812 ascii <shared-key>
> config radius auth disable <index>
> config radius auth retransmit-timeout <index> <timeout-seconds>
> config radius auth enable <index>
```

<a.b.c.d> は、RADIUS サーバに対応しています。

SSIDの作成

GUI：

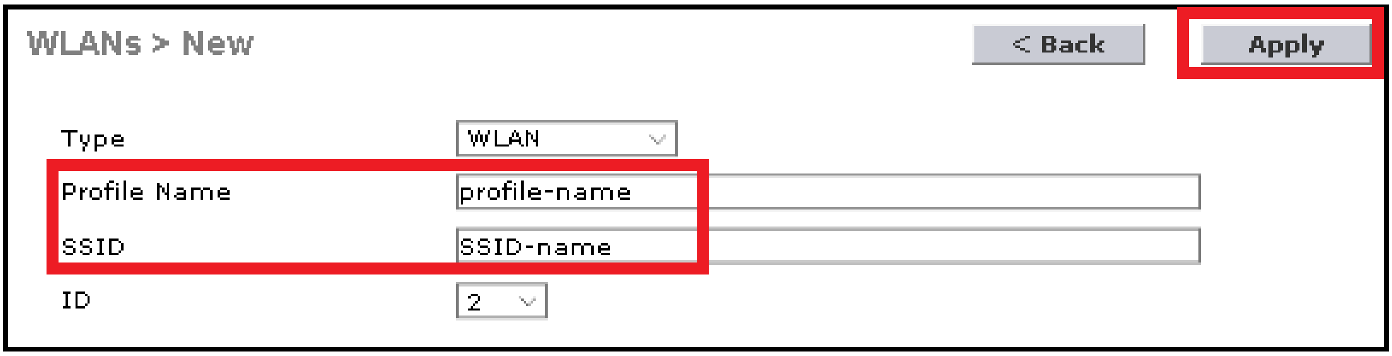
ステップ１：図に示すように、WLCのGUIを開き、WLANs > Create New > Goの順に移動します
。



Current Filter: None [Change Filter] [Clear Filter]

Create New Go

ステップ２：SSIDとプロファイルの名前を選択し、図に示すようにApplyをクリックします。



Type WLAN

Profile Name profile-name

SSID SSID-name

ID 2

CLI：

```
> config wlan create <id> <profile-name> <ssid-name>
```

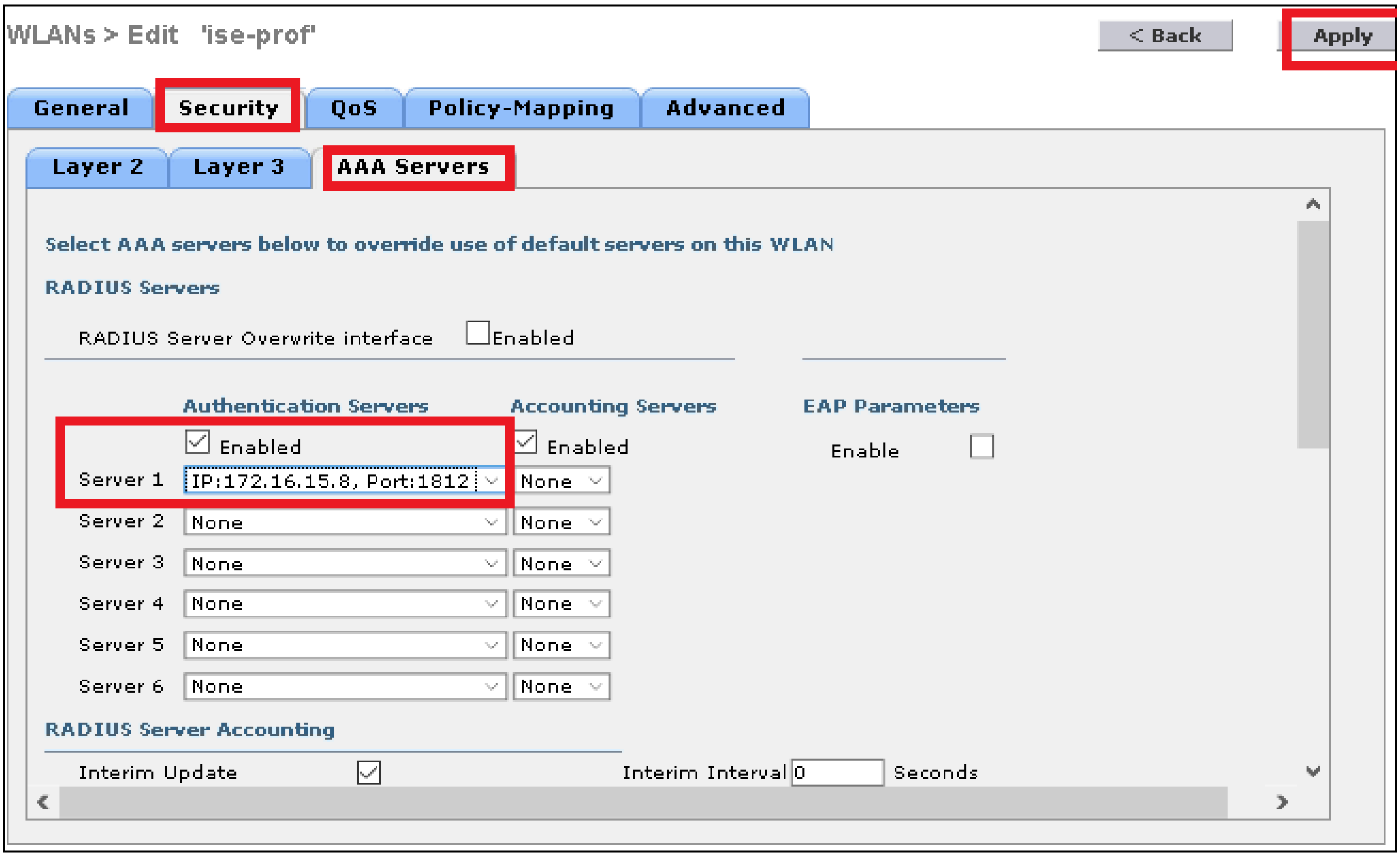
ステップ３：RADIUSサーバをWLANに割り当てます。

CLI：

```
> config wlan radius_server auth add <wlan-id> <radius-index>
```

GUI：

Security > AAA Serversに移動し、目的のRADIUSサーバを選択し、図に示すようにApplyをクリックします。



Select AAA servers below to override use of default servers on this WLAN

RADIUS Servers

RADIUS Server Overwrite interface □Enabled

	Authentication Servers	Accounting Servers	EAP Parameters
	☑ Enabled	☑ Enabled	Enable □
Server 1	IP:172.16.15.8, Port:1812	None	
Server 2	None	None	
Server 3	None	None	
Server 4	None	None	
Server 5	None	None	
Server 6	None	None	

RADIUS Server Accounting

Interim Update ☑ Interim Interval 0 Seconds

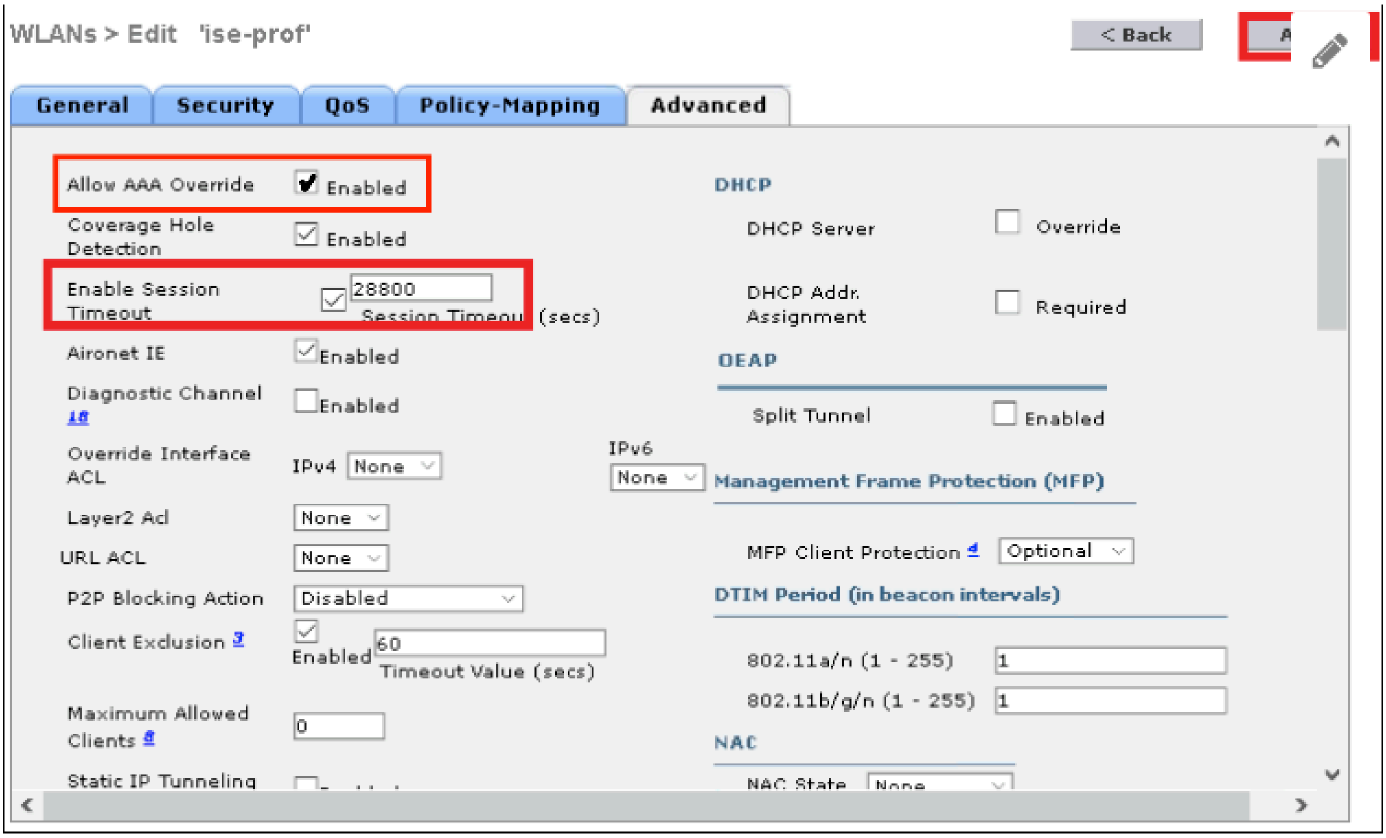
ステップ 4：Allow AAA Overrideを有効にし、オプションでセッションタイムアウトを増やします

CLI：

```
> config wlan aaa-override enable <wlan-id>
> config wlan session-timeout <wlan-id> <session-timeout-seconds>
```

GUI：

WLANs > WLAN ID > Advancedの順に選択し、Allow AAA Overrideをイネーブルにします。 オプションで、図に示すように、セッションタイムアウトを指定します。



WLANs > Edit 'ise-prof'

Allow AAA Override ☑ Enabled

Coverage Hole Detection ☑ Enabled

Enable Session Timeout ☑ 28800 Session Timeout (secs)

Aironet IE ☑ Enabled

Diagnostic Channel 18 □ Enabled

Override Interface ACL IPv4 None IPv6 None

Layer2 Acl None

URL ACL None

P2P Blocking Action Disabled

Client Exclusion 3 ☑ Enabled 60 Timeout Value (secs)

Maximum Allowed Clients 8 0

Static IP Tunneling □

DHCP

DHCP Server □ Override

DHCP Addr. Assignment □ Required

OEAP

Split Tunnel □ Enabled

Management Frame Protection (MFP)

MFP Client Protection 4 Optional

DTIM Period (in beacon intervals)

802.11a/n (1 - 255) 1

802.11b/g/n (1 - 255) 1

NAC

NAC State None

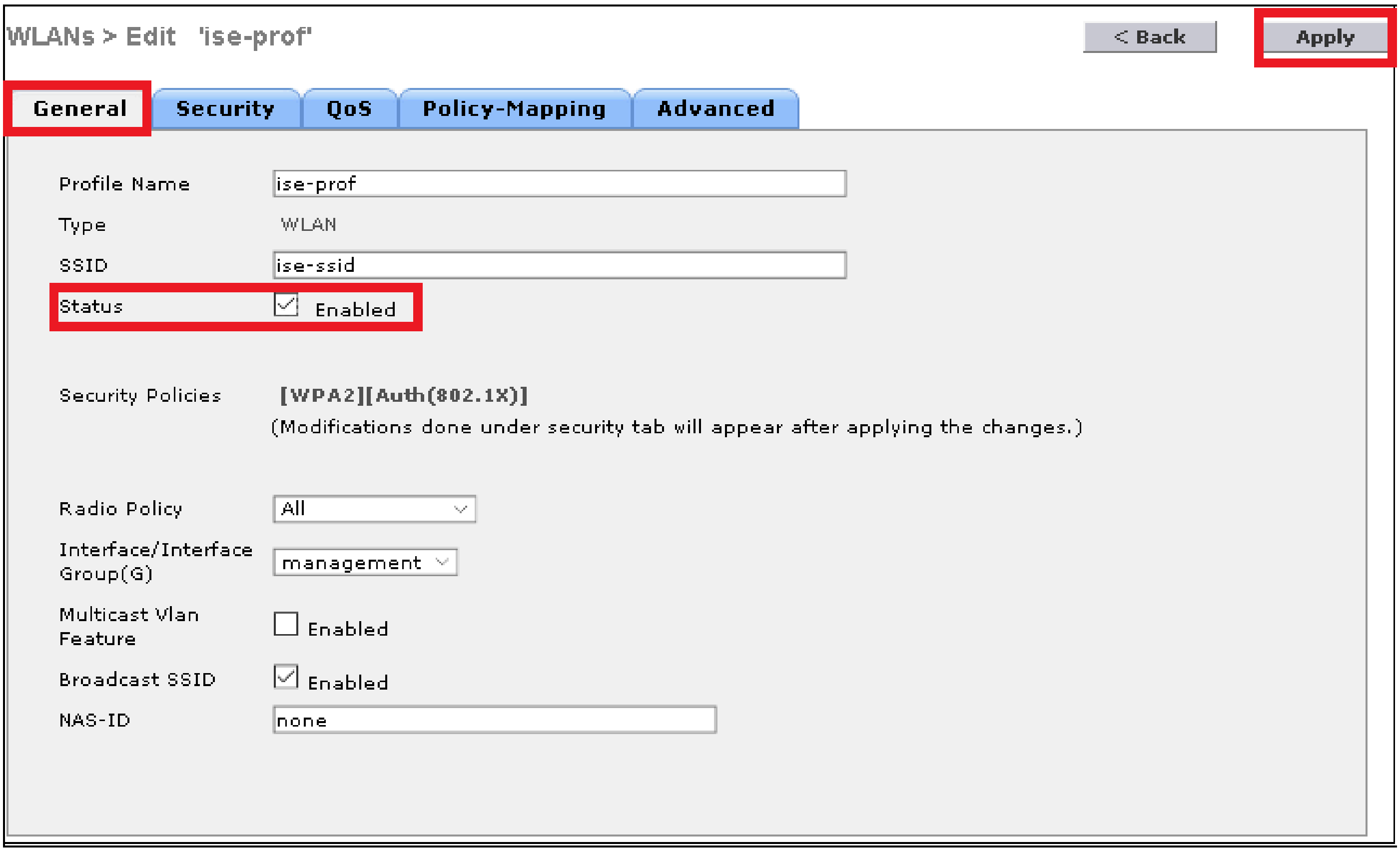
ステップ５：WLANを有効にします。

CLI：

```
> config wlan enable <wlan-id>
```

GUI：

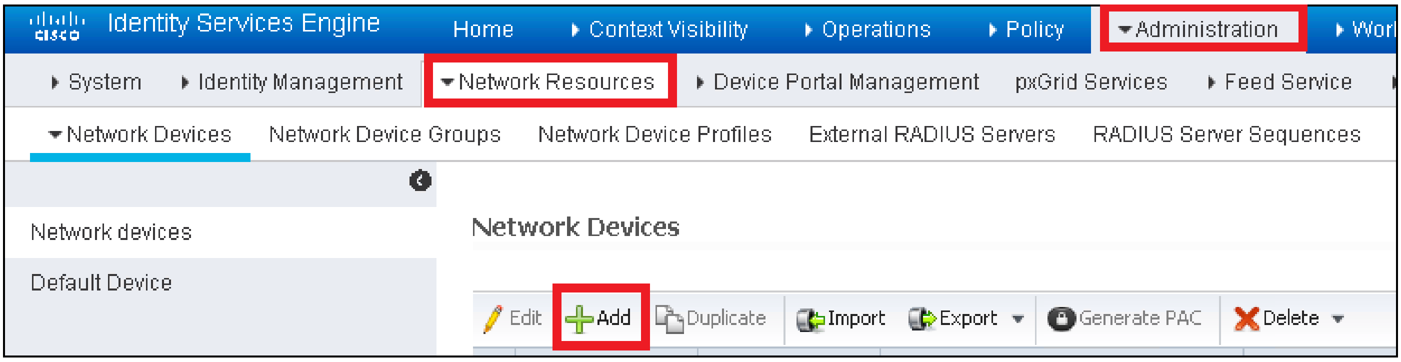
WLANs > WLAN ID > Generalの順に移動し、図に示すようにSSIDを有効にします。



Profile Name	ise-prof
Type	WLAN
SSID	ise-ssid
Status	☑ Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface/Interface Group(G)	management
Multicast Vlan Feature	□ Enabled
Broadcast SSID	☑ Enabled
NAS-ID	none

ISEでのWLCの宣言

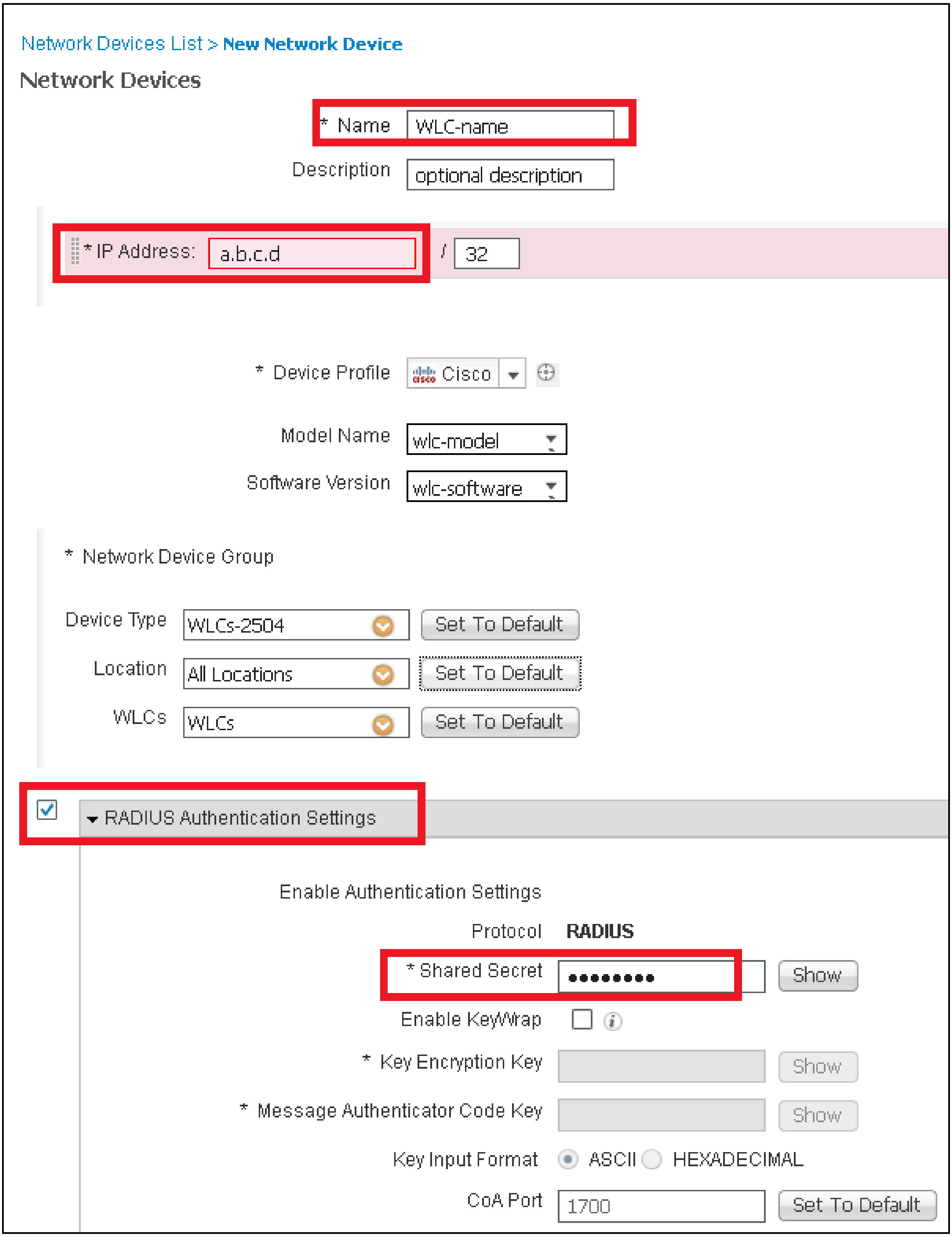
ステップ１：図に示すように、ISEコンソールを開き、Administration > Network Resources > Network Devices > Addの順に選択します。



ステップ２：値を入力します。

必要に応じて、モデル名、ソフトウェアバージョン、説明を指定し、デバイスタイプ、ロケーション、またはWLCに基づいてネットワークデバイスグループを割り当てることができます。

a.b.c.dは、要求された認証を送信するWLCインターフェイスに対応します。デフォルトでは、次の図に示すように管理インターフェイスになります。



Network Devices List > **New Network Device**

Network Devices

* Name: WLC-name

Description: optional description

* IP Address: a.b.c.d / 32

* Device Profile: Cisco

Model Name: wlc-model

Software Version: wlc-software

* Network Device Group

Device Type: WLCs-2504 — Set To Default

Location: All Locations — Set To Default

WLCs: WLCs — Set To Default

☑ RADIUS Authentication Settings

Enable Authentication Settings

Protocol: **RADIUS**

* Shared Secret: ●●●●●●●●● — Show

Enable KeyWrap: □

* Key Encryption Key: — Show

* Message Authenticator Code Key: — Show

Key Input Format: ● ASCII ○ HEXADECIMAL

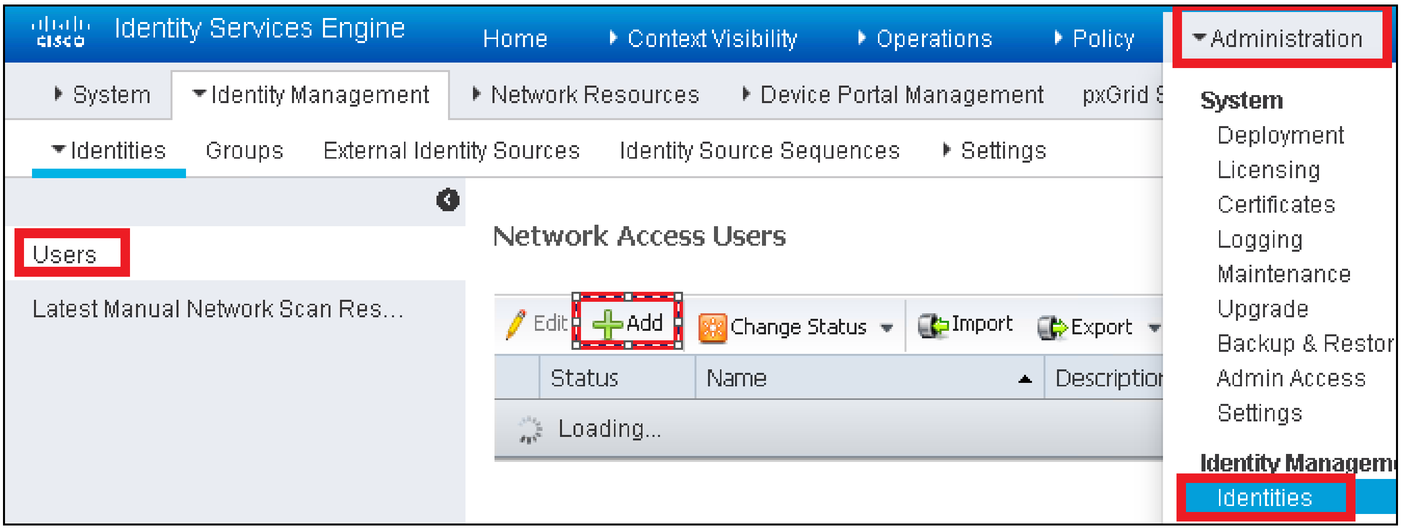
CoA Port: 1700 — Set To Default

ネットワークデバイスグループの詳細については、以下を参照してください。

ISE - ネットワーク デバイス グループ

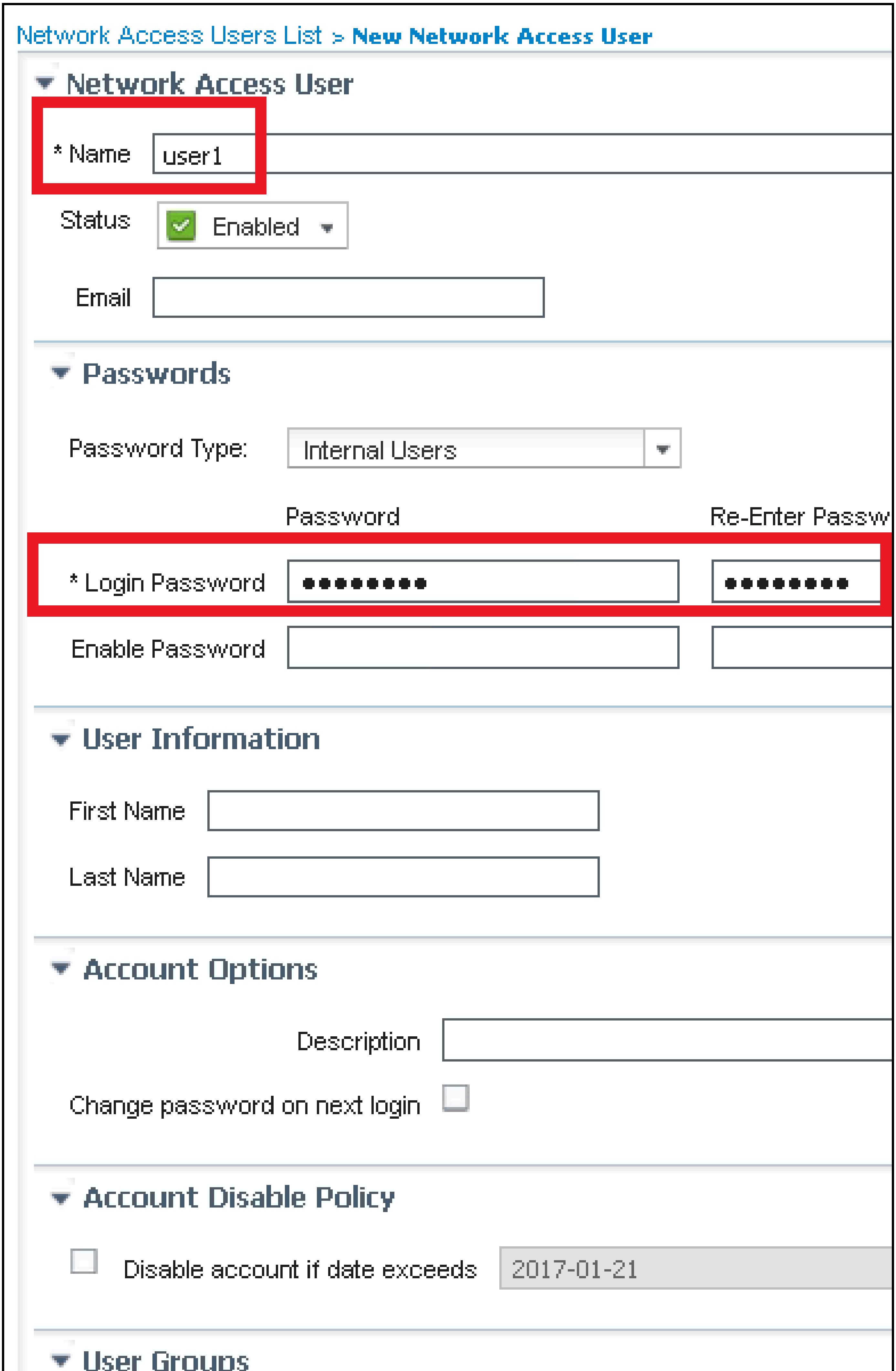
ISE での新しいユーザの作成

ステップ１：図に示すように、Administration > Identity Management > Identities > Users > Addの順に移動します。



ステップ２：情報を入力します。

この例では、このユーザはALL_ACCOUNTSというグループに属していますが、図に示すように、必要に応じて調整できます。



Network Access Users List > **New Network Access User**

▾ **Network Access User**

* Name	user1
Status	✓ Enabled ▾
Email	

▾ **Passwords**

Password Type: Internal Users ▾

	Password	Re-Enter Passw
* Login Password	●●●●●●●●●	●●●●●●●●●
Enable Password		

▾ **User Information**

First Name	
Last Name	

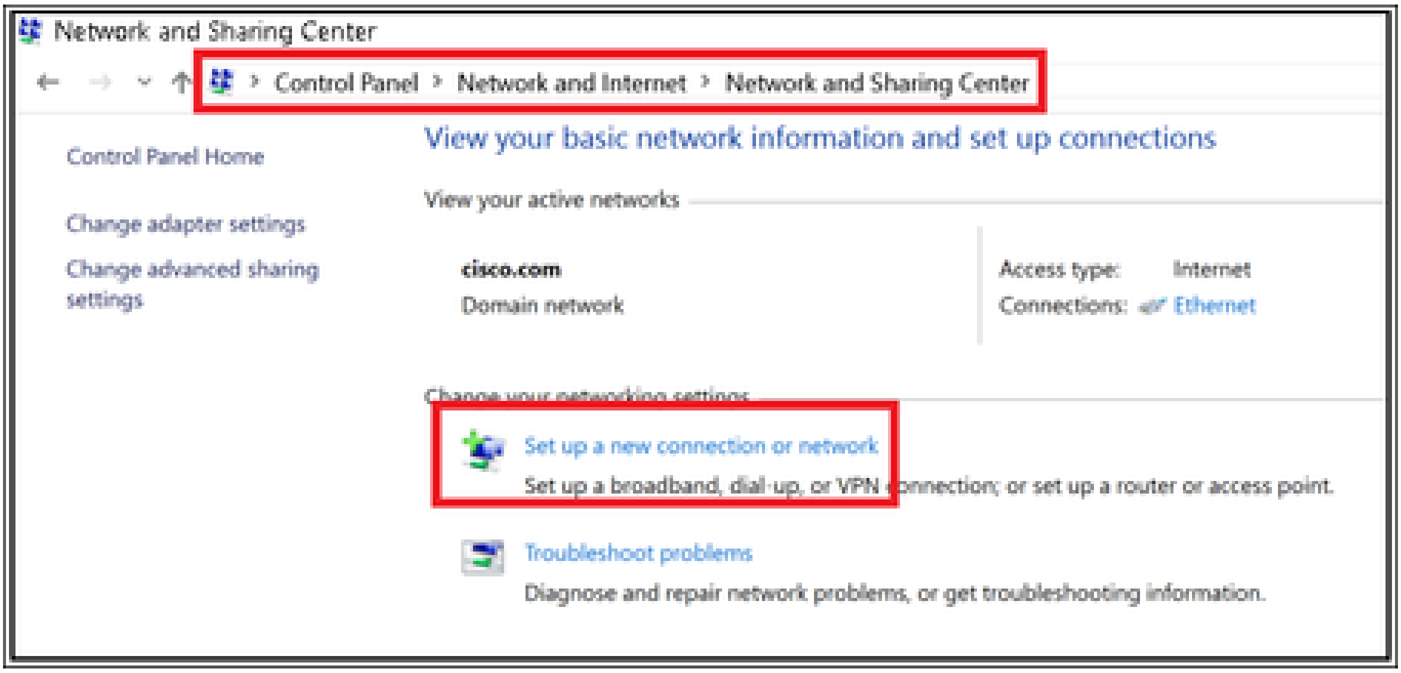
▾ **Account Options**

Description	
Change password on next login	□

▾ **Account Disable Policy**

□ Disable account if date exceeds 2017-01-21

▾ **User Groups**



Network and Sharing Center

Control Panel > Network and Internet > Network and Sharing Center

View your basic network information and set up connections

Control Panel Home

Change adapter settings

Change advanced sharing settings

View your active networks

cisco.com
Domain network

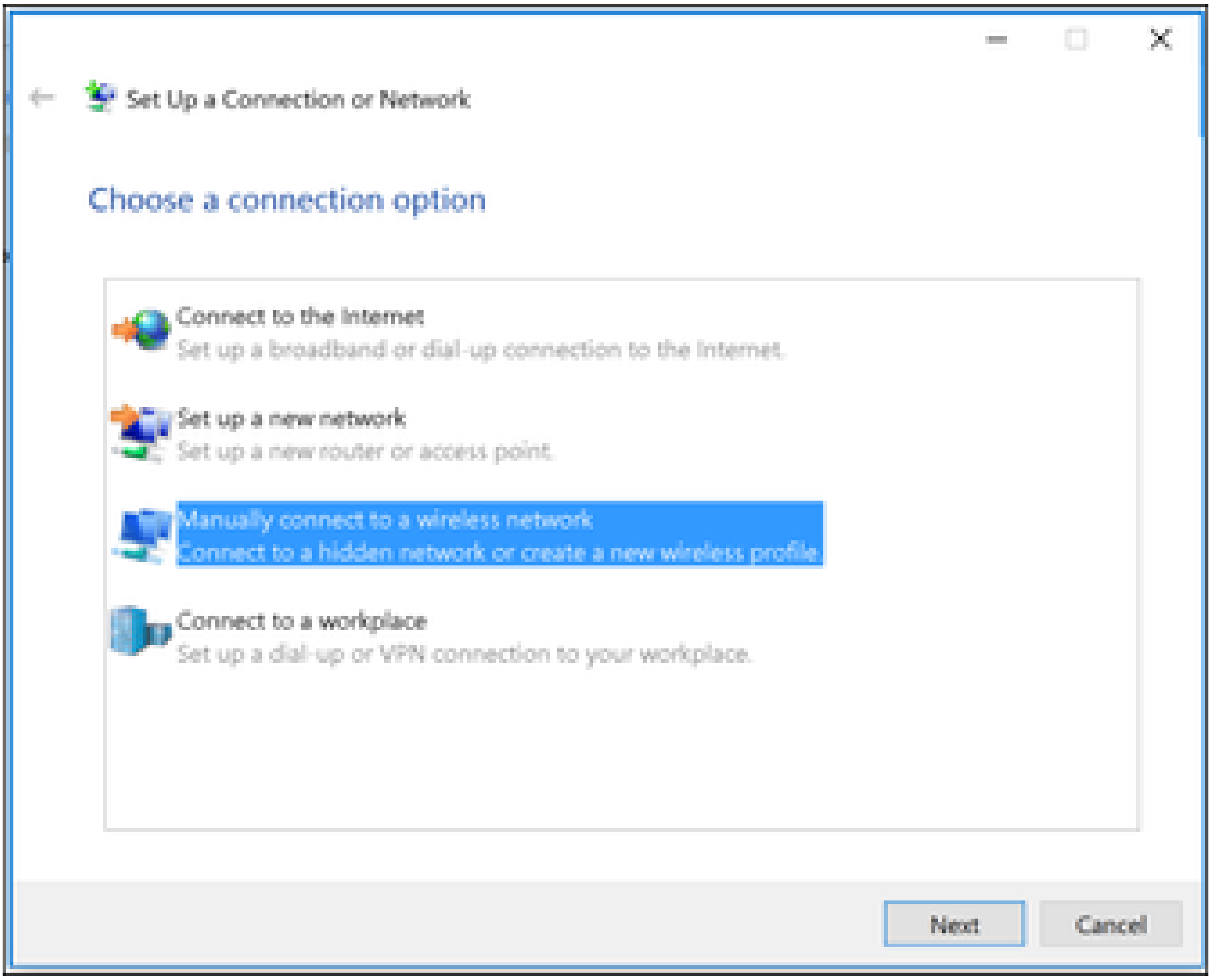
Access type: Internet
Connections: Ethernet

Change your networking settings

Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

ステップ 3：図に示すように、Manually connect to a wireless networkを選択し、Nextをクリックします。



Choose a connection option

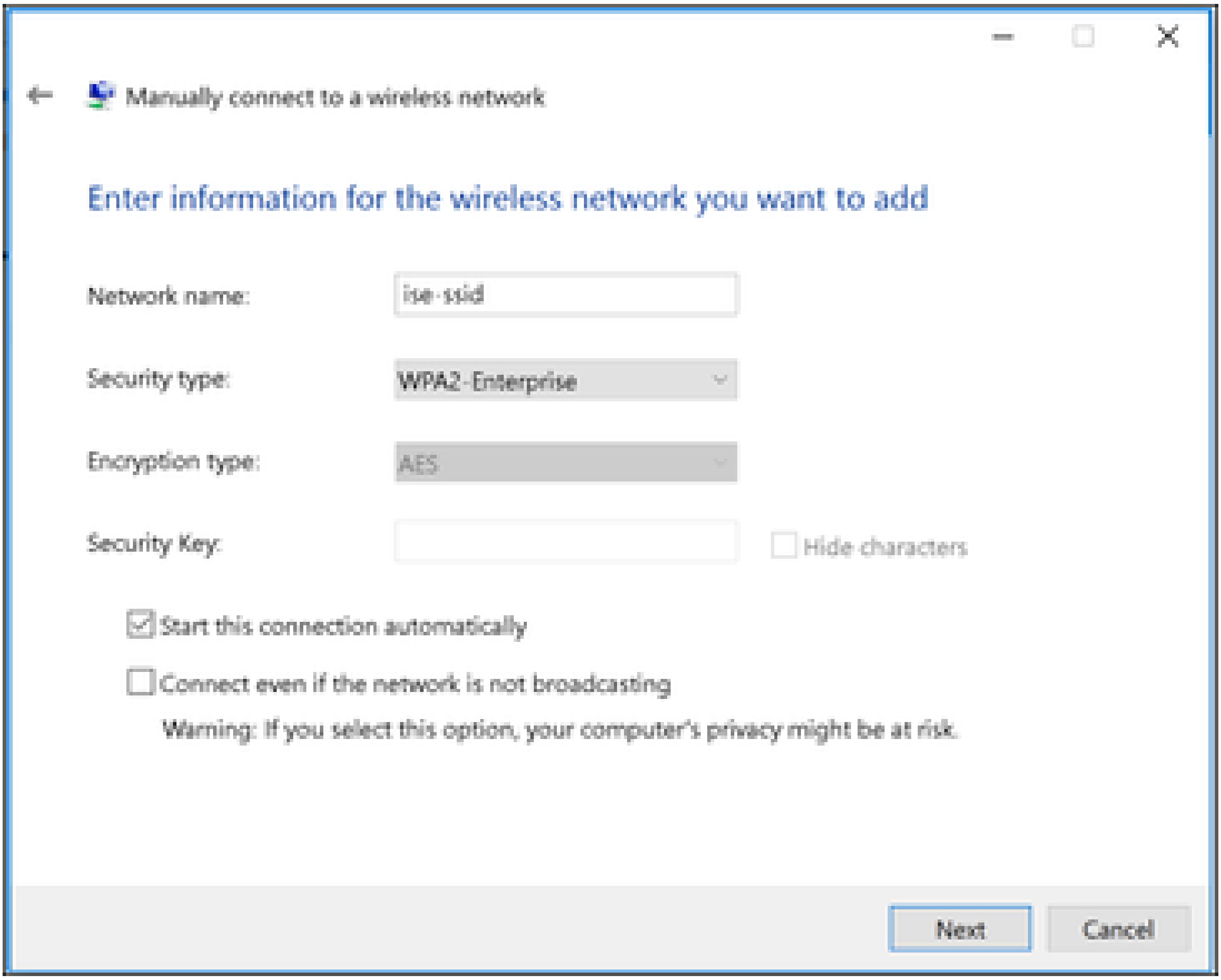
Connect to the Internet
Set up a broadband or dial-up connection to the Internet.

Set up a new network
Set up a new router or access point.

Manually connect to a wireless network
Connect to a hidden network or create a new wireless profile.

Connect to a workplace
Set up a dial-up or VPN connection to your workplace.

ステップ４：SSIDの名前とセキュリティタイプWPA2-Enterpriseを使用して情報を入力し、図に示すようにNextをクリックします。


Manually connect to a wireless network

Enter information for the wireless network you want to add

Network name: ise-ssid

Security type: WPA2-Enterprise

Encryption type: AES

Security Key:

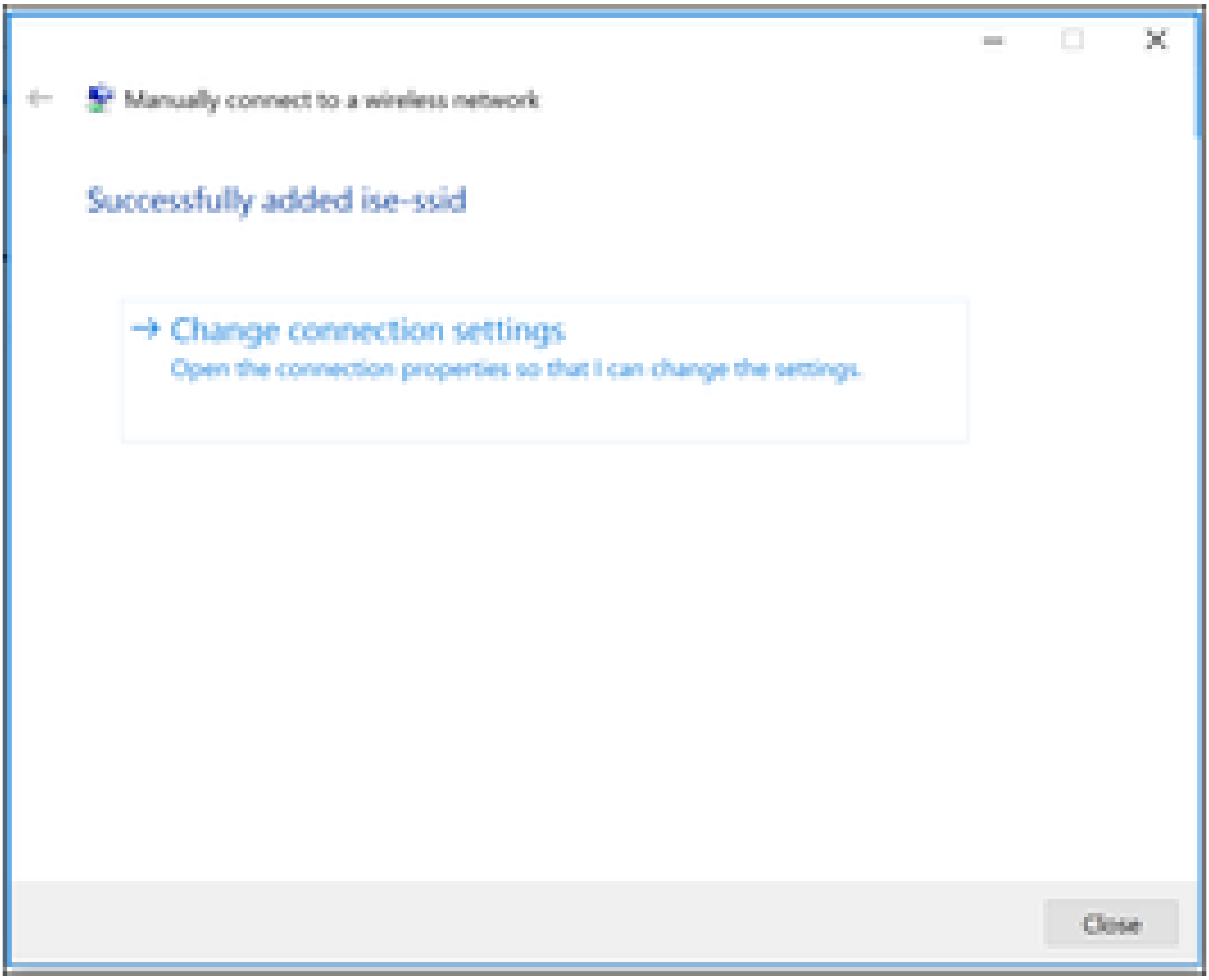
□ Hide characters

☑ Start this connection automatically

□ Connect even if the network is not broadcasting

Warning: If you select this option, your computer's privacy might be at risk.

ステップ 5：Change connection settingsを選択して、図に示すようにWLANプロファイルの設定をカスタマイズします。

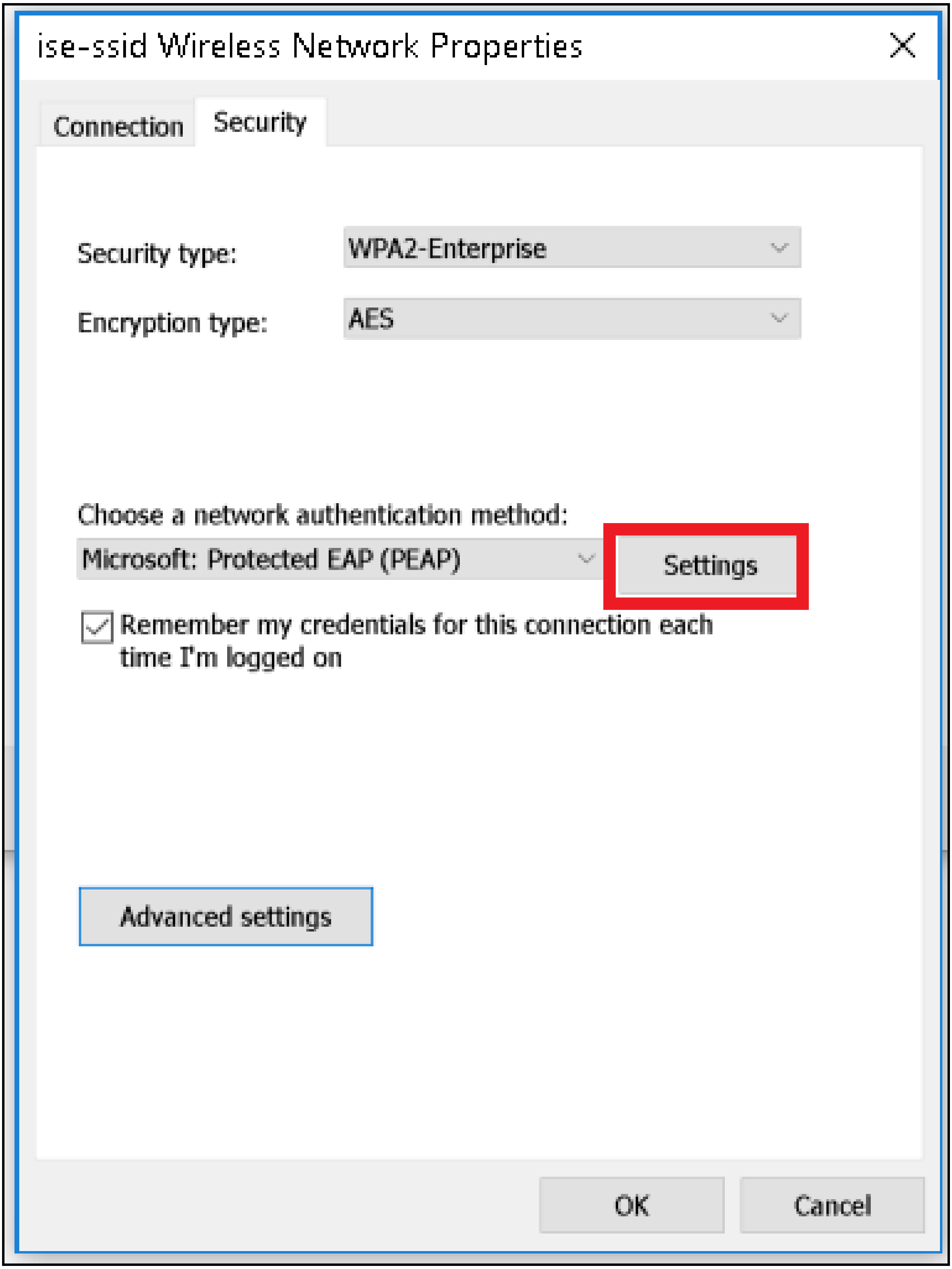


Manually connect to a wireless network

Successfully added ise-ssid

→ Change connection settings
Open the connection properties so that I can change the settings.

手順 6：Securityタブに移動し、図に示すようにSettingsをクリックします。



ise-ssid Wireless Network Properties

Security type: WPA2-Enterprise

Encryption type: AES

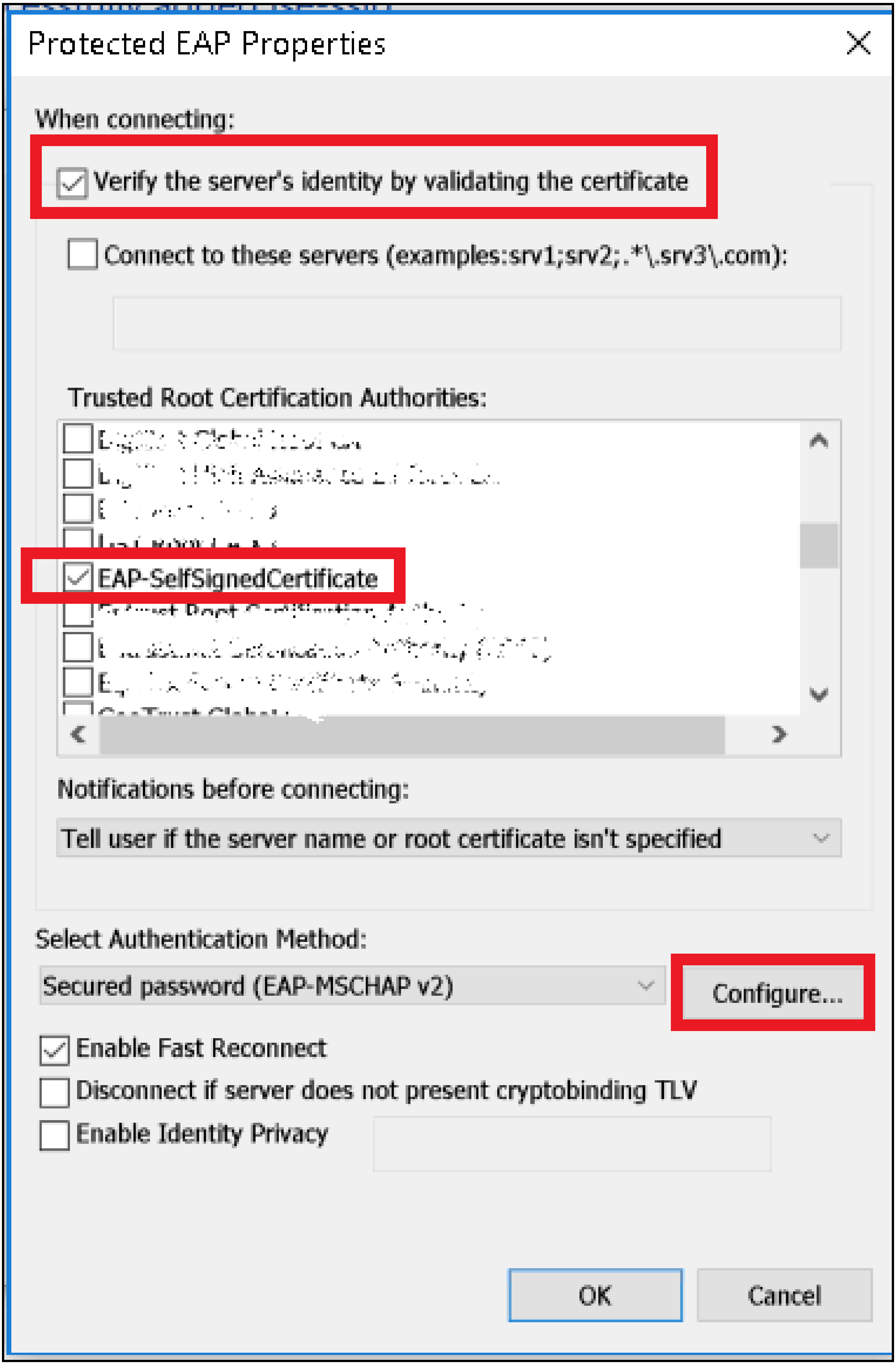
Choose a network authentication method:
Microsoft: Protected EAP (PEAP)

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

手順 7： RADIUSサーバを検証するかどうかを選択します。

存在する場合は、Verify the server identity by validating the certificateを有効にし、Trusted Root Certification Authorities:リストで、ISEの自己署名証明書を選択します。

その後、Configureを選択してAutomatically use my Windows logon name and password...をディセーブルにし、次に図に示すようにOKをクリックします。



Protected EAP Properties

When connecting:

☑ Verify the server's identity by validating the certificate

□ Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):

Trusted Root Certification Authorities:

□ [redacted]
□ [redacted]
□ [redacted]
□ [redacted]
☑ EAP-SelfSignedCertificate
□ [redacted]
□ [redacted]
□ [redacted]
□ [redacted]

Notifications before connecting:

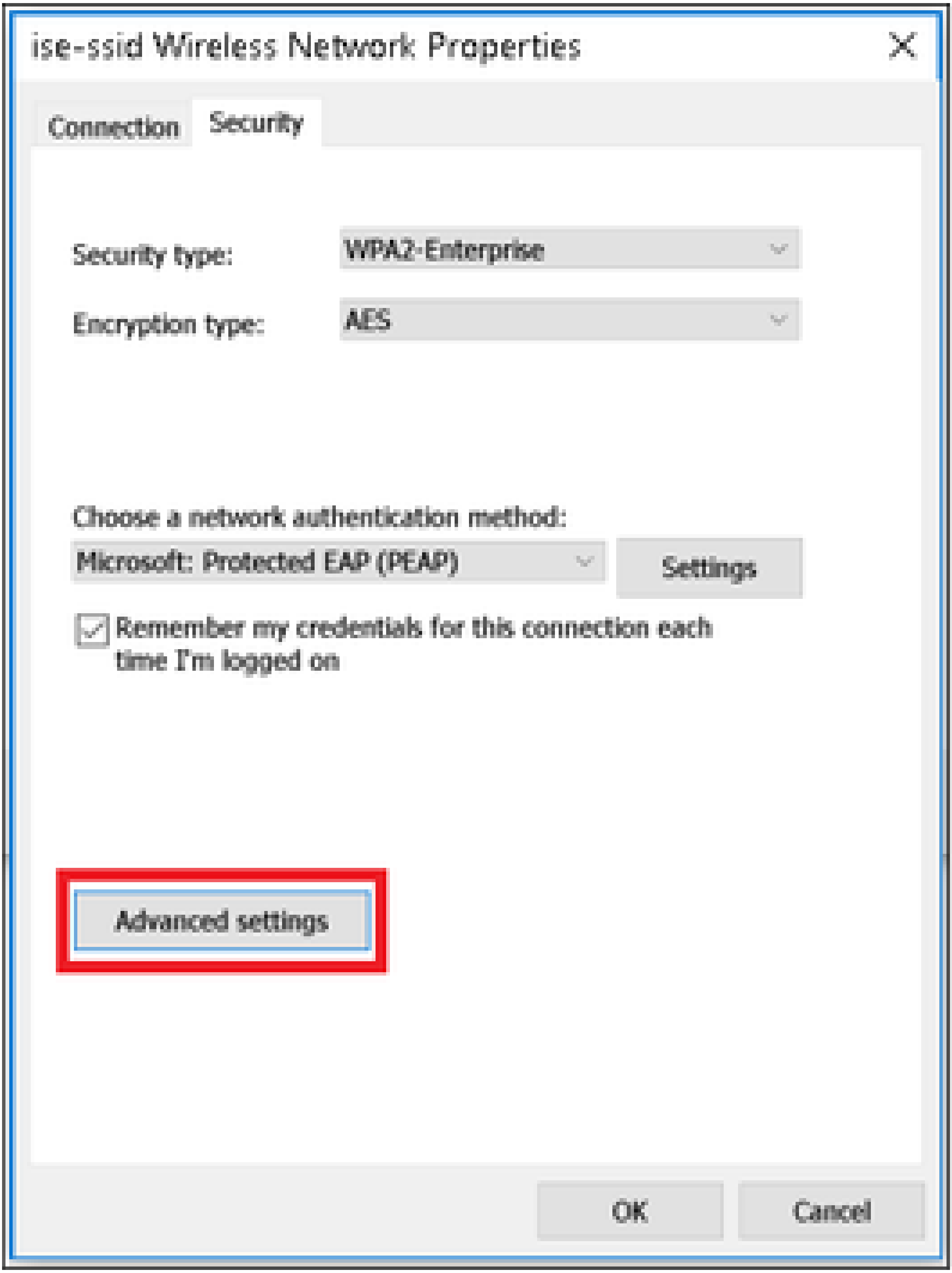
Tell user if the server name or root certificate isn't specified

Select Authentication Method:

Secured password (EAP-MSCHAP v2)

☑ Enable Fast Reconnect
□ Disconnect if server does not present cryptobinding TLV
□ Enable Identity Privacy

Securityタブに戻り、Advanced settingsを選択して、User authenticationとして認証モードを指定し、図に示すようにユーザを認証するためにISEで設定されたクレデンシャルを保存します。



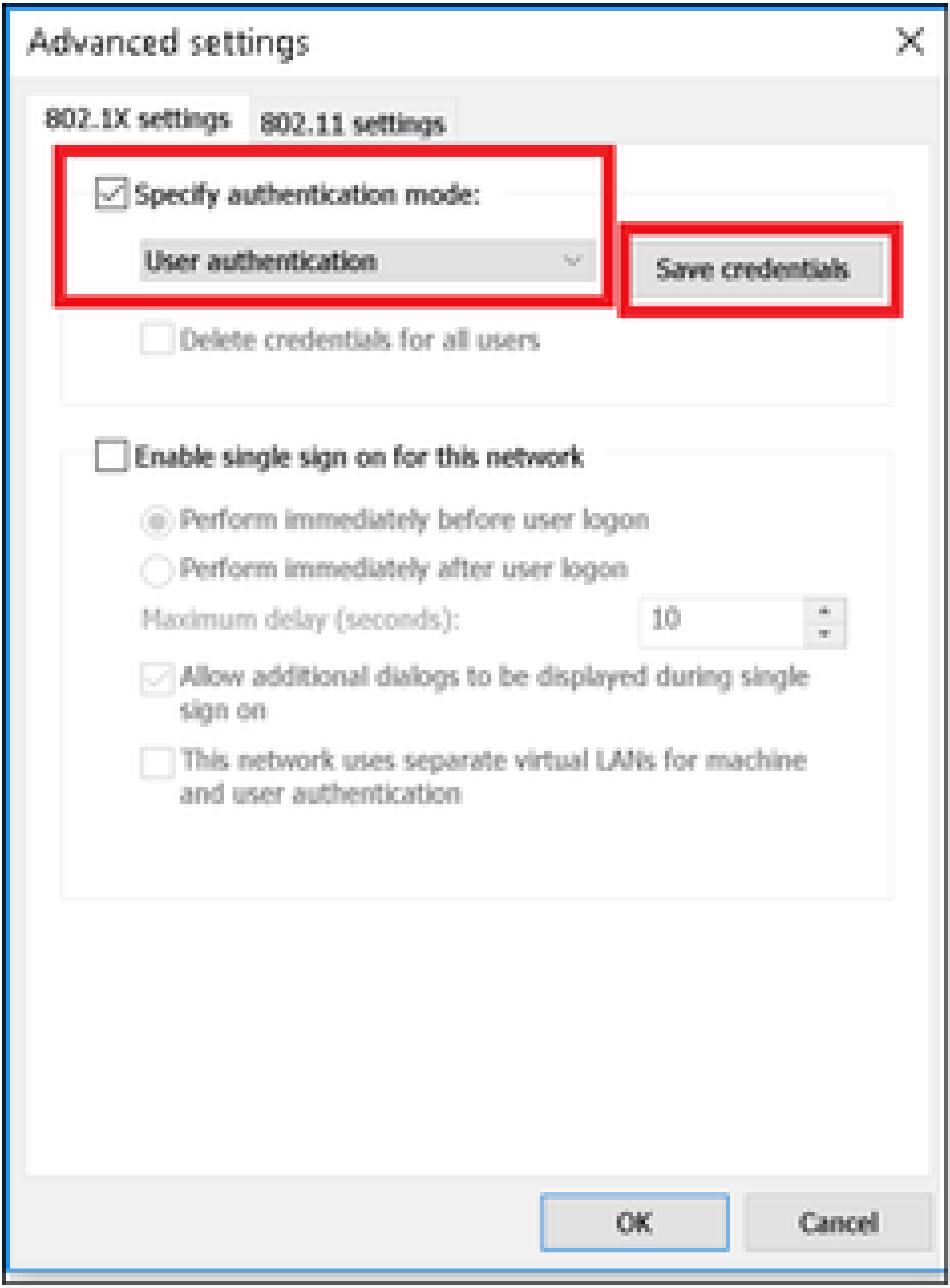
ise-ssid Wireless Network Properties

Security type: WPA2-Enterprise

Encryption type: AES

Choose a network authentication method: Microsoft: Protected EAP (PEAP)

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



☑ Specify authentication mode:

User authentication

□ Delete credentials for all users

□ Enable single sign on for this network

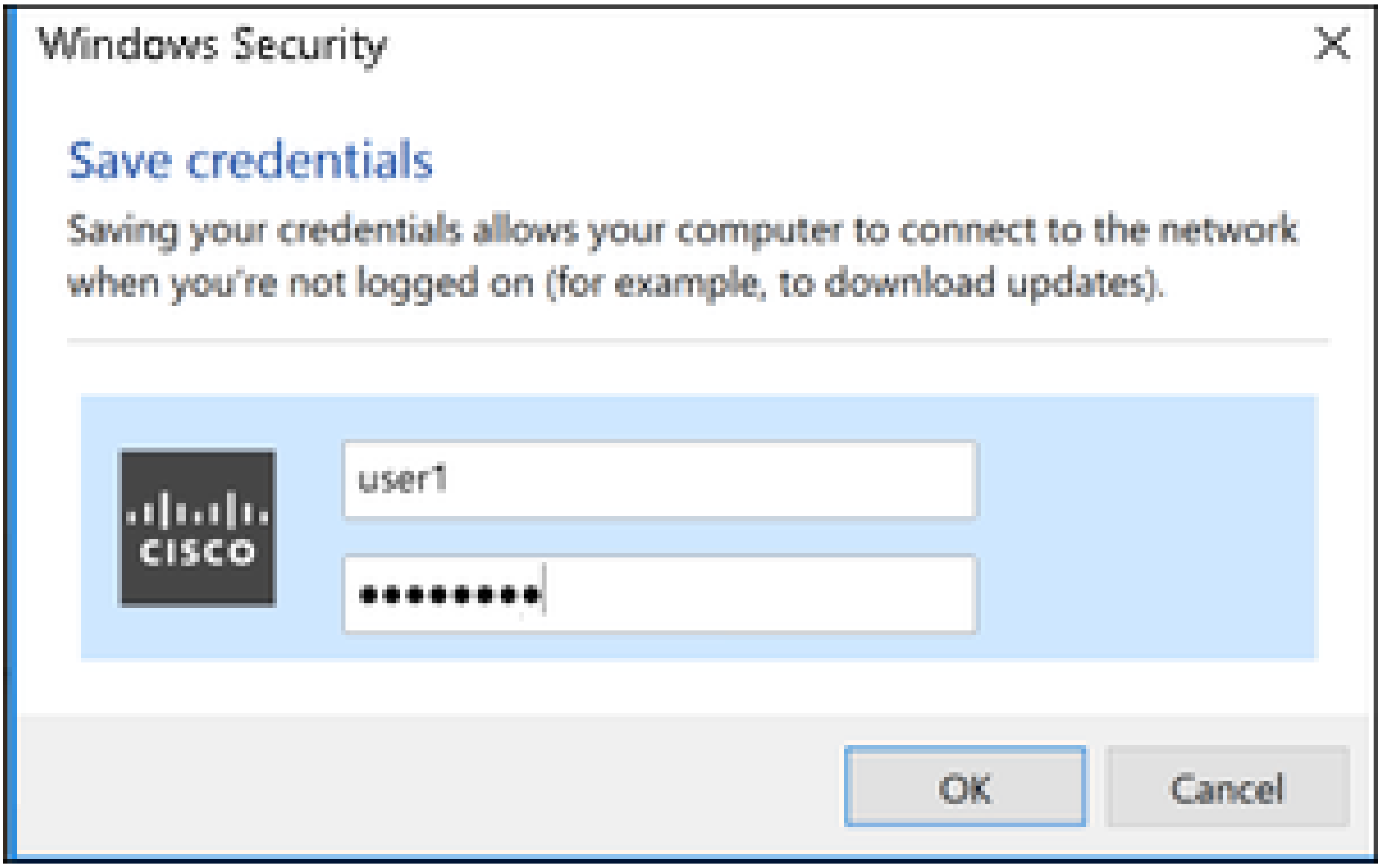
● Perform immediately before user logon

○ 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



Windows Security

Save credentials

Saving your credentials allows your computer to connect to the network when you're not logged on (for example, to download updates).

user1

••••••••

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。

認証フローは WLC または ISE の観点から確認できます。

WCL での認証プロセス

特定のユーザの認証プロセスをモニタするため、次のコマンドを実行します。

```
> debug client <mac-add-client>
> debug dot1x event enable
> debug dot1x aaa enable
```

認証の成功例（出力を一部省略しています）:

<#root>

```
*apfMsConnTask_1: Nov 24 04:30:44.317:

e4:b3:18:7c:30:58 Processing assoc-req station:e4:b3:18:7c:30:58 AP:00:c8:8b:26:2c:d0-00

 thread:1a5cc288
*apfMsConnTask_1: Nov 24 04:30:44.317: e4:b3:18:7c:30:58 Reassociation received from mobile on BSSID 00
*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Applying Interface(management) policy on Mobil
```

```
*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Applying site-specific Local Bridging override
*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Applying Local Bridging Interface Policy for st
*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 RSN Capabilities:  60
*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Marking Mobile as non-
```

e4:b3:18:7c:30:58 Received 802.11i 802.1X key management suite, enabling dot1x Authentication

```
11w Capable
*apfMsConnTask_1: Nov 24 04:30:44.318: e4:b3:18:7c:30:58 Received RSN IE with 1 PMKIDs from mobile e4:b
*apfMsConnTask_1: Nov 24 04:30:44.319: Received PMKID:  (16)
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 Searching for PMKID in MSCB PMKID cache for mob
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 No valid PMKID found in the MSCB PMKID cache fo
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 0.0.0.0 START (0) Initializing policy
*apfMsConnTask_1: Nov 24 04:30:44.319:
```

e4:b3:18:7c:30:58 0.0.0.0 START (0) Change state to AUTHCHECK (2) last state START (0)

```
*apfMsConnTask_1: Nov 24 04:30:44.319:
```

e4:b3:18:7c:30:58 0.0.0.0 AUTHCHECK (2) Change state to 8021X_REQD (3) last state AUTHCHECK (2)

```
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 0.0.0.0 8021X_REQD (3) Plumbed mobile LWAPP rul
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 apfMsAssoStateInc
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 apfPemAddUser2 (apf_policy.c:437) Changing stat
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 apfPemAddUser2:session timeout forstation e4:b
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 Stopping deletion of Mobile Station: (callerId
*apfMsConnTask_1: Nov 24 04:30:44.319: e4:b3:18:7c:30:58 Func: apfPemAddUser2, Ms Timeout = 0, Session T
*apfMsConnTask_1: Nov 24 04:30:44.320: e4:b3:18:7c:30:58 Sending Assoc Response to station on BSSID 00:
*spamApTask2: Nov 24 04:30:44.323: e4:b3:18:7c:30:58 Successful transmission of LWAPP Add-Mobile to AP 
*spamApTask2: Nov 24 04:30:44.325: e4:b3:18:7c:30:58 Received ADD_MOBILE ack - Initiating 1x to STA e4:
*spamApTask2: Nov 24 04:30:44.325: e4:b3:18:7c:30:58
```

Sent dot1x auth initiate message for mobile e4:b3:18:7c:30:58

```
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 reauth_sm state transition 0 ---> 1 for mob
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 EAP-PARAM Debug - eap-params for Wlan-Id :2
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 Disable re-auth, use PMK lifetime.
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 Station e4:b3:18:7c:30:58 setting dot1x rea
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 Stopping reauth timeout for e4:b3:18:7c:30:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326: e4:b3:18:7c:30:58 dot1x - moving mobile e4:b3:18:7c:30:58 int
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.326:
```

e4:b3:18:7c:30:58 Sending EAP-Request/Identity to mobile e4:b3:18:7c:30:58 (EAP Id 1)

```
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Received EAPOL EAPPKT from mobile e4:b3:18:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Received Identity Response (count=1) from m
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Resetting reauth count 1 to 0 for mobile e4
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 EAP State update from Connecting to Authent
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 dot1x - moving mobile e4:b3:18:7c:30:58 int
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Entering Backend Auth Response state for mo
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.380: e4:b3:18:7c:30:58 Created Acct-Session-ID (58366cf4/e4:b3:18:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.386: e4:b3:18:7c:30:58 Processing Access-Challenge for mobile e4:b
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.387: e4:b3:18:7c:30:58 Entering Backend Auth Req state (id=215) fo
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.387: e4:b3:18:7c:30:58 WARNING: updated EAP-Identifier 1 ===> 215 
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.387: e4:b3:18:7c:30:58 Sending EAP Request from AAA to mobile e4:b
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.387: e4:b3:18:7c:30:58 Allocating EAP Pkt for retransmission to mo
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.390: e4:b3:18:7c:30:58 Received EAPOL EAPPKT from mobile e4:b3:18:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.390: e4:b3:18:7c:30:58 Received EAP Response from mobile e4:b3:18:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.390: e4:b3:18:7c:30:58 Resetting reauth count 0 to 0 for mobile e4
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.390: e4:b3:18:7c:30:58 Entering Backend Auth Response state for mo
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.393: e4:b3:18:7c:30:58 Processing Access-Challenge for mobile e4:b
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.393: e4:b3:18:7c:30:58 Entering Backend Auth Req state (id=216) fo
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.393: e4:b3:18:7c:30:58 Sending EAP Request from AAA to mobile e4:b
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.393: e4:b3:18:7c:30:58 Reusing allocated memory for  EAP Pkt for r
.
```

```
.
.
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530:

e4:b3:18:7c:30:58 Processing Access-Accept for mobile e4:b3:18:7c:30:58

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 Resetting web IPv4 acl from 255 to 255
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 Resetting web IPv4 Flex acl from 65535 to 6
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530:

e4:b3:18:7c:30:58 Username entry (user1) created for mobile, length = 253

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530:

e4:b3:18:7c:30:58 Found an interface name:'vlan2404' corresponds to interface name received: vlan2404

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 override for default ap group, marking intg
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 Applying Interface(management) policy on Mo
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.530: e4:b3:18:7c:30:58 Re-applying interface policy for client
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 apfApplyWlanPolicy: Apply WLAN Policy over
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531:

e4:b3:18:7c:30:58 Inserting AAA Override struct for mobile

        MAC: e4:b3:18:7c:30:58, source 4
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Applying override policy from source Overri
*Dot1x_NW_MsgTask_0: Nov 24

04:30:44.531: e4:b3:18:7c:30:58 Found an interface name:'vlan2404' corresponds to interface name receive

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Applying Interface(vlan2404) policy on Mobi
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Re-applying interface policy for client
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Setting re-auth timeout to 0 seconds, got f
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Station e4:b3:18:7c:30:58 setting dot1x rea
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Stopping reauth timeout for e4:b3:18:7c:30:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Creating a PKC PMKID Cache entry for statio
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Resetting MSCB PMK Cache Entry 0 for statio
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Adding BSSID 00:c8:8b:26:2c:d1 to PMKID cac
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: New PMKID: (16)
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531:      [0000] cc 3a 3d 26 80 17 8b f1 2d c5 cd fd a0 8a c4 39
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 unsetting PmkIdValidatedByAp
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Updating AAA Overrides from local for stati
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Adding Audit session ID payload in Mobility
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 0 PMK-update groupcast messages sent
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 PMK sent to mobility group
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Disabling re-auth since PMK lifetime can ta
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.531: e4:b3:18:7c:30:58 Sending EAP-Success to mobile e4:b3:18:7c:3
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Freeing AAACB from Dot1xCB as AAA auth is d
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 key Desc Version FT - 0
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Found an cache entry for BSSID 00:c8:8b:26:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: Including PMKID in M1  (16)
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532:      [0000] cc 3a 3d 26 80 17 8b f1 2d c5 cd fd a0 8a c4 39
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: M1 - Key Data: (22)
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532:      [0000] dd 14 00 0f ac 04 cc 3a 3d 26 80 17 8b f1 2d c5
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532:      [0016] cd fd a0 8a c4 39
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532:

e4:b3:18:7c:30:58 Starting key exchange to mobile e4:b3:18:7c:30:58, data packets will be dropped

*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532:

e4:b3:18:7c:30:58 Sending EAPOL-Key Message to mobile e4:b3:18:7c:30:58

state INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Reusing allocated memory for  EAP Pkt for r
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Entering Backend Auth Success state (id=223
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 Received Auth Success while in Authenticati
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.532: e4:b3:18:7c:30:58 dot1x - moving mobile e4:b3:18:7c:30:58 int
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.547: e4:b3:18:7c:30:58 Received EAPOL-Key from mobile e4:b3:18:7c:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.547: e4:b3:18:7c:30:58 Ignoring invalid EAPOL version (1) in EAPOL
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.547: e4:b3:18:7c:30:58 key Desc Version FT - 0
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.547:
```

e4:b3:18:7c:30:58 Received EAPOL-key in PTK_START state (message 2) from mobile

```
 e4:b3:18:7c:30:58
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Successfully computed PTK from PMK!!!
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Received valid MIC in EAPOL Key Message M2!
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Not Flex client. Do not distribute PMK Key
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Stopping retransmission timer for mobile e4
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 key Desc Version FT - 0
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Sending EAPOL-Key Message to mobile e4:b3:1
state PTKINITNEGOTIATING (message 3), replay counter 00.00.00.00.00.00.00.01
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.548: e4:b3:18:7c:30:58 Reusing allocated memory for  EAP Pkt for r
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Received EAPOL-Key from mobile e4:b3:18:7c:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Ignoring invalid EAPOL version (1) in EAPOL
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 key Desc Version FT - 0
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555:
```

e4:b3:18:7c:30:58 Received EAPOL-key in PTKINITNEGOTIATING state (message 4)

```
 from mobile e4:b3:18:7c:30:58
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Stopping retransmission timer for mobile e4
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Freeing EAP Retransmit Bufer for mobile e4:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 apfMs1xStateInc
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 apfMsPeapSimReqCntInc
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 apfMsPeapSimReqSuccessCntInc
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555:
```

e4:b3:18:7c:30:58 0.0.0.0 8021X_REQD (3) Change state to L2AUTHCOMPLETE (4) last state 8021X_REQD (3)

```
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Mobility query, PEM State: L2AUTHCOMPLETE
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.555: e4:b3:18:7c:30:58 Building Mobile Announce :
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58   Building Client Payload:
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58     Client Ip: 0.0.0.0
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58     Client Vlan Ip: 172.16.0.134, Vlan mask
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58     Client Vap Security: 16384
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58     Virtual Ip: 10.10.10.10
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58     ssid: ise-ssid
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58   Building VlanIpPayload.
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 Not Using WMM Compliance code qosCap 00
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 L2AUTHCOMPLETE (4) Plumbed mobile L
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556:
```

e4:b3:18:7c:30:58 0.0.0.0 L2AUTHCOMPLETE (4) Change state to DHCP_REQD (7) last state L2AUTHCOMPLETE (4

```
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) pemAdvanceState2 6677
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Adding Fast Path rule
  type = Airespace AP - Learn IP address
  on AP 00:c8:8b:26:2c:d0, slot 0, interface = 1, QOS = 0
  IPv4 ACL ID = 255, IPv
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Successfully plumbed
*Dot1x_NW_MsgTask_0: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 Successfully Plumbed PTK session Keysfor mo
*spamApTask2: Nov 24 04:30:44.556: e4:b3:18:7c:30:58 Successful transmission of LWAPP Add-Mobile to AP
*pemReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 Added NPU entry of type 9, dtlFlags 0x0
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) mobility role update requ
  Peer = 0.0.0.0, Old Anchor = 0.0.0.0, New Anchor = 172.16.0.3
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) State Update from Mobilit
```

```
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) pemAdvanceState2 6315, Ad
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Replacing Fast Path rule
  IPv4 ACL ID = 255,
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd...)
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Fast Path rule (contd...)
*apfReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 0.0.0.0 DHCP_REQD (7) Successfully plumbed mobi
*pemReceiveTask: Nov 24 04:30:44.557: e4:b3:18:7c:30:58 Sent an XID frame
*dtlArpTask: Nov 24 04:30:47.932: e4:b3:18:7c:30:58 Static IP client associated to interface vlan2404 wh
*dtlArpTask: Nov 24 04:30:47.933: e4:b3:18:7c:30:58 apfMsRunStateInc
*dtlArpTask: Nov 24 04:30:47.933:

e4:b3:18:7c:30:58 172.16.0.151 DHCP_REQD (7) Change state to RUN (20)

 last state DHCP_REQD (7)
```

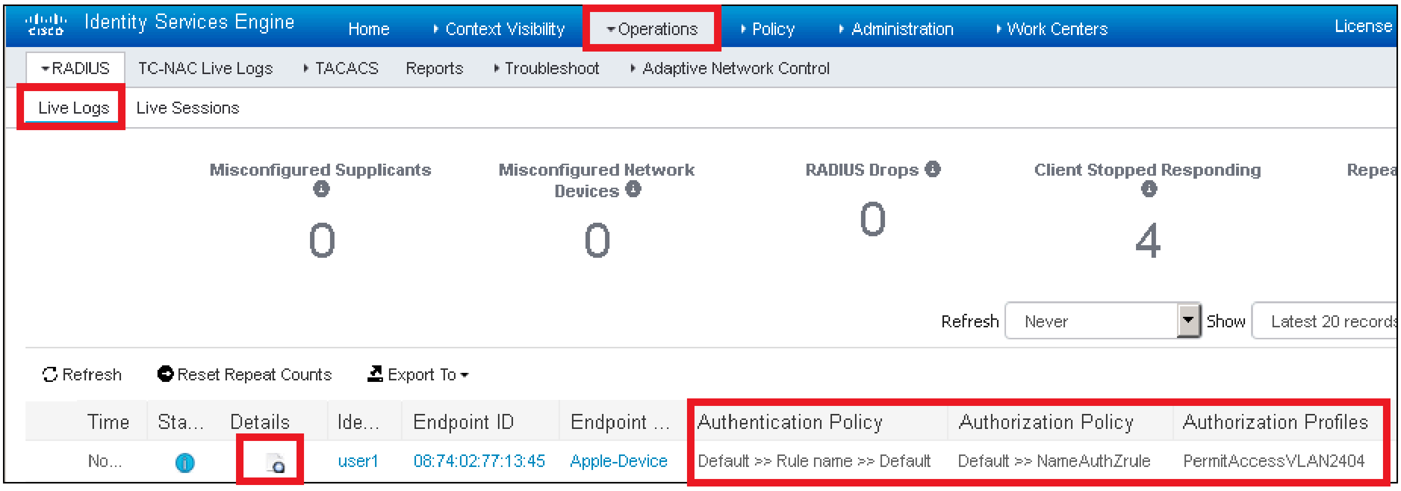
デバッグ クライアントの出力を簡単に読むための手段として、ワイヤレス デバッグ アナライザ ツールを使用します。

[ワイヤレス デバッグ アナライザ]

ISE の認証プロセス

Operations > RADIUS > Live Logsの順に移動し、ユーザに割り当てられている認証ポリシー、認可ポリシー、および認可プロファイルを確認します。

詳細については、Detailsをクリックして、図に示すように認証プロセスの詳細を確認してください。



Misconfigured Supplicants 0 | Misconfigured Network Devices 0 | RADIUS Drops 0 | Client Stopped Responding 4 | Repea

Refresh: Never | Show: Latest 20 records

Time	Sta...	Details	Ide...	Endpoint ID	Endpoint ...	Authentication Policy	Authorization Policy	Authorization Profiles
No...			user1	08:74:02:77:13:45	Apple-Device	Default >> Rule name >> Default	Default >> NameAuthZrule	PermitAccessVLAN2404

トラブルシュート

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

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。