

外部認証を使用したローカルWeb認証の設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[パラメータマップ](#)

[認証用のデータベース](#)

[設定](#)

[CLIでのローカル認証を使用したローカルWeb認証](#)

[ローカル認証の方式リスト](#)

[パラメータマップ](#)

[WLANセキュリティパラメータ](#)

[ポリシープロファイルの作成](#)

[ポリシータグの作成](#)

[APへのポリシータグの割り当て](#)

[ゲストユーザ名の作成](#)

[WebUI経由のローカル認証を使用したローカルWeb認証](#)

[確認](#)

[FlexConnectローカルスイッチングでのローカルWeb認証](#)

[確認](#)

[トラブルシュート](#)

はじめに

このドキュメントでは、9800ワイヤレスLANコントローラ(WLC)でローカル認証を使用してローカルWeb認証(LWA)を設定する方法について説明します。

前提条件

9800 WLC設定モデルに関する知識があることが推奨されます。

要件

次の項目に関する知識があることが推奨されます。

- Cisco WLC 9800シリーズ
- Web認証に関する包括的な知識。

使用するコンポーネント

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

- 9800-CL WLC Cisco IOS® XEバージョン17.12.5
- CiscoアクセスポイントC9117AXI

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

ローカルWeb認証(LWA)は、WLCで設定できるワイヤレスローカルエリアネットワーク(WLAN)の認証方法です。ユーザが使用可能なネットワークリストからWLANを選択すると、Webポータルにリダイレクトされます。このポータルでは、設定に応じて、ユーザ名とパスワードの入力、アクセプタブルユースポリシー(AUP)の受け入れ、またはその両方のアクションの組み合わせを求めるプロンプトが表示され、接続が完了します。

ログインプロセス中に表示される4種類のWeb認証ページの詳細については、『[ローカルWeb認証の設定](#)』ガイドを参照し、Web認証の種類に使用可能なオプションを確認してください。「認証のタイプ」セクションの『[外部認証を使用したローカルWeb認証の設定](#)』ガイドも参照してください。

パラメータマップ

パラメータマップは、Web認証をイネーブルにするWLCの重要な設定要素です。認証タイプ、リダイレクトURL、追加されたパラメータ、タイムアウト、カスタムWebページなど、Web認証プロセスのさまざまな側面を制御する一連の設定で構成されます。特定のSSIDのWebベース認証をアクティブ化および管理するには、このマップをWLANプロファイルにリンクする必要があります。

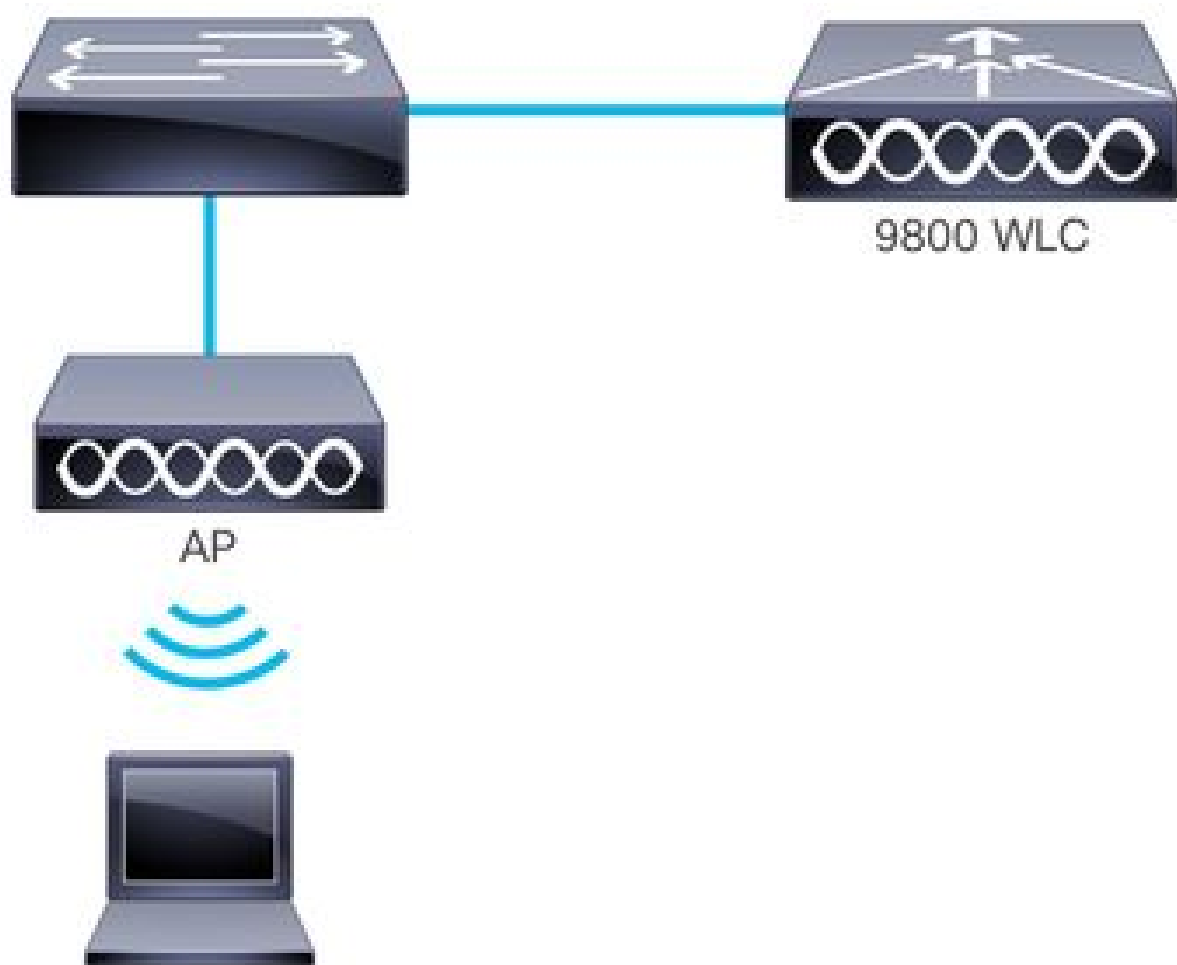
ワイヤレスLANコントローラ(WLC)にはデフォルトのグローバルパラメータマップが付属していますが、管理者はカスタムパラメータマップを作成して、特定のニーズに応じてWeb認証の動作をカスタマイズすることができます。

認証用のデータベース

ユーザ名とパスワードを使用するようにパラメータマップが設定されている場合は、WLC上にローカルに保存される認証クレデンシャルを定義する必要があります。GUIを使用してゲストユーザアカウントを作成する場合、ゲストアカウントごとに許可される同時ログインの最大数を設定できます。有効な値の範囲は0 ~ 64です。0は、そのゲストユーザに無制限の同時ログインが許可されることを示します。

LWAは主に小規模な導入を目的としています。これは他の認証方式との統合をサポートしています。詳細については、『[クライアントでサポートされる認証の組み合わせ](#)』を参照してください。

次の図は、LWAの一般的なトポロジを表しています。



ローカル認証を使用するLWAの一般的なトポロジ

LWAのネットワークトポロジのデバイス：

- クライアント/サブリカント：WLANへの接続要求を開始し、後でDHCPサーバとDNSサーバに対して接続要求を開始し、WLCからの通信に応答します。
- アクセスポイント：スイッチに接続され、ゲストWLANをブロードキャストし、ゲストデバイスにワイヤレス接続を提供します。ゲストユーザが認証を完了する前に、有効なクレデンシャルを入力するか、AUPを受け入れるか、またはその両方のアクションを組み合わせ、DHCPおよびDNSトラフィックを許可します。
- WLC/オーセンティケーター：APとクライアントデバイスを管理します。WLCはリダイレクトURLをホストし、トラフィックを制御するアクセスコントロールリスト(ACL)を適用します。また、パラメータマップの設定時にデフォルトで作成されます。ゲストユーザからのHTTP要求を代行受信し、ユーザの認証が必要なWebポータル（ログインページ）にリダイレクトします。WLCは、ユーザクレデンシャルをキャプチャし、ゲストを認証し、クレデンシャルの有効性を確認するためにローカルデータベースを確認します。

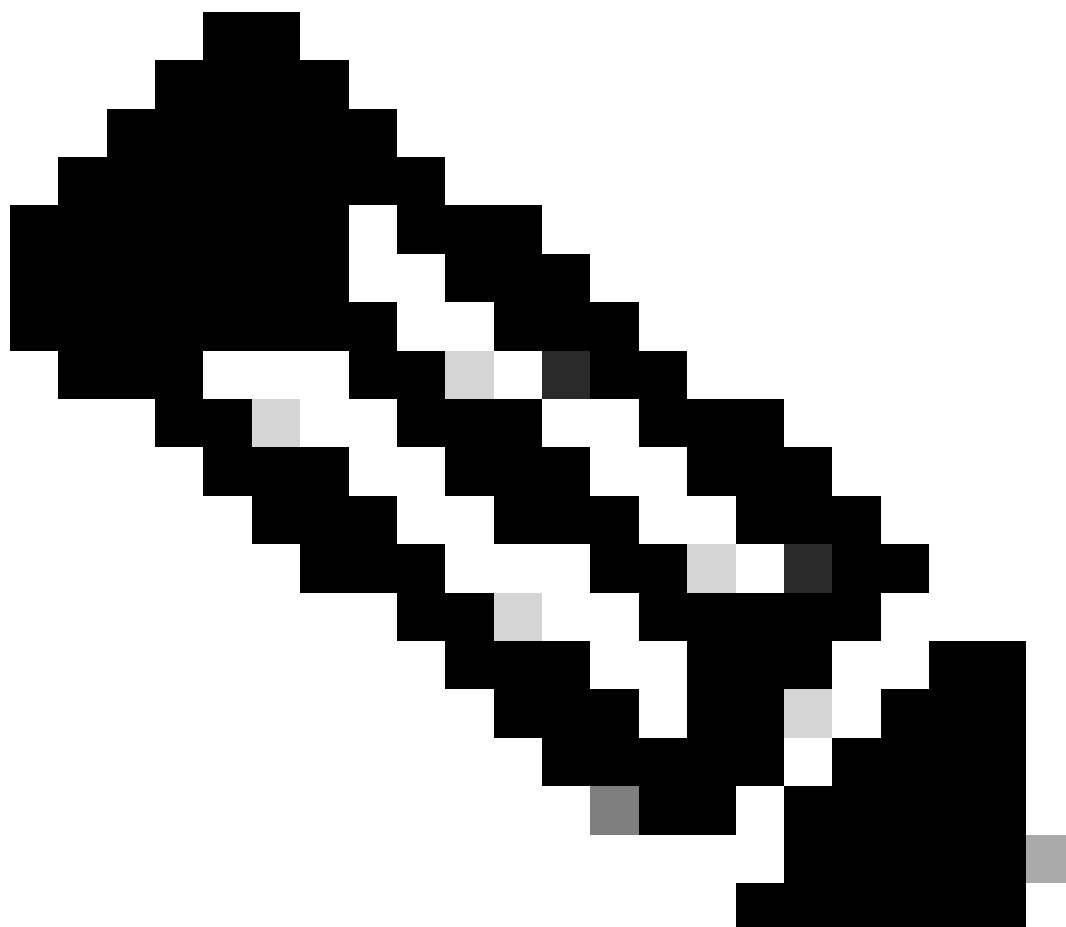
- 認証サーバ：このシナリオでは、WLCは認証サーバとして機能します。ゲストユーザクレデンシャルを検証し、それに応じてネットワークアクセスを許可または拒否します。

設定

CLIでのローカル認証を使用したローカルWeb認証

ローカル認証方式リスト

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#aaa new-model
9800WLC(config)#aaa authentication login LWA_AUTHENTICATION local
9800WLC(config)#aaa authorization network default local
9800WLC(config)#end
```



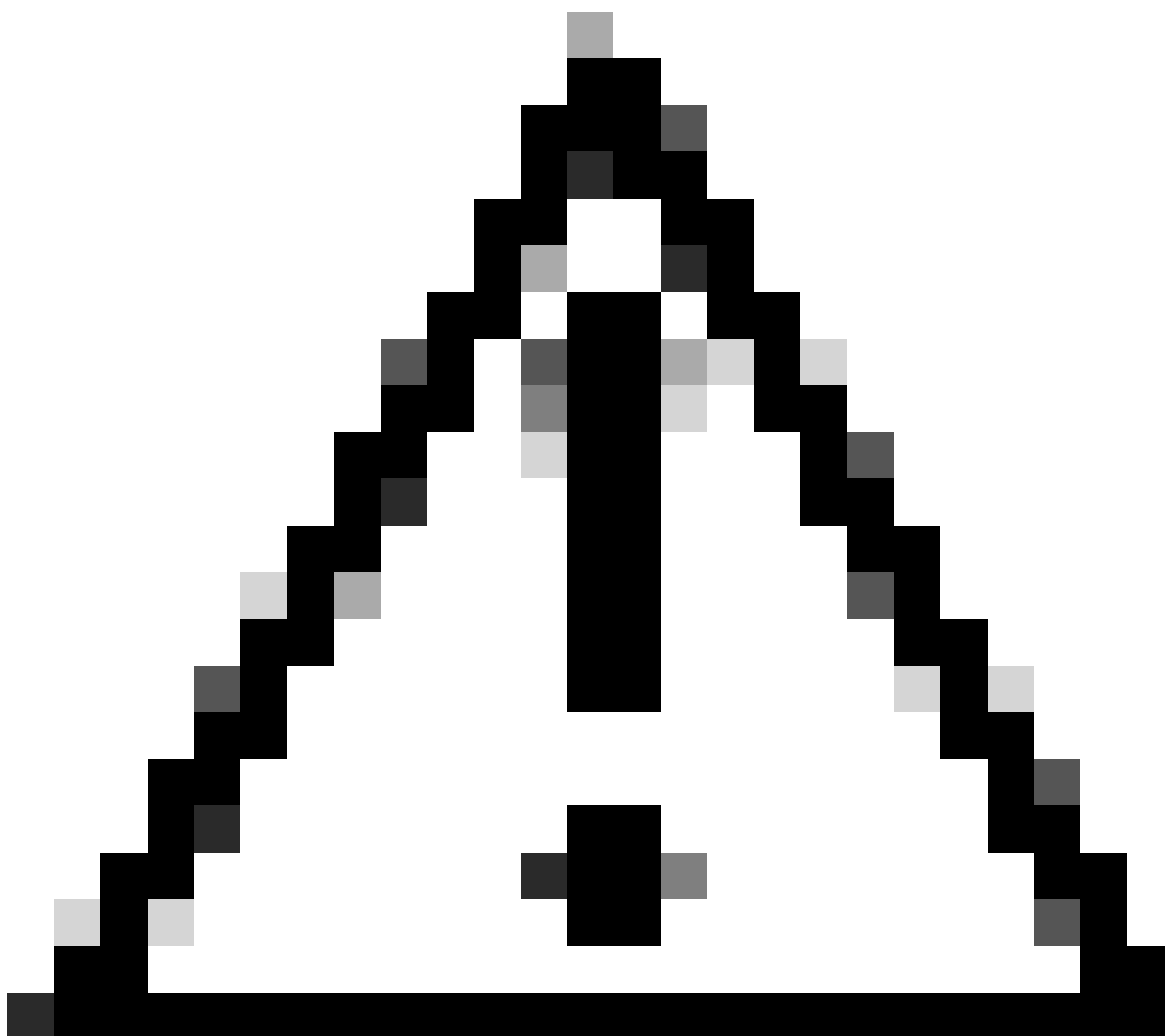
注:ローカルログイン方式リストが機能するためには、WLC上にaaa authorization network default localが設定されていることを確認してください。これは、WLCがネットワークへのユーザを承認するために必要です。

パラメータマップ

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#parameter-map type webauth global
9800WLC(config-params-parameter-map)#type webauth
9800WLC(config-params-parameter-map)#virtual-ip ipv4 192.0.2.1
9800WLC(config-params-parameter-map)#trustpoint
```

```
9800WLC(config-params-parameter-map)#webauth-http-enable
```

```
9800WLC(config-params-parameter-map)#end
```



注意:Virtual IP (VIP ; 仮想IP) は、RFC 5737で提案されているルーティング不能アドレスにする必要があります。デフォルトでは、IP 192.0.2.1が設定されます。仮想IPアドレスの詳細については、『[Cisco Catalyst 9800シリーズ設定のベストプラクティス](#)』を参照してください。AireOsでは、ほとんどの場合、IPは1.1.1.1を使用します。これはパブリックIPになったため、もはや推奨されません。

複数のパラメータマップを作成する機能により、カスタマイズされたWebページや各WLANの特定の表示パラメータなど、フローをカスタマイズできます。グローバルパラメータマップは、トラストポイント、つまりリダイレクトポータルでWLCがクライアントに提示する証明書を決定します。さらに、リダイレクトポータルのHTTP/HTTPS、仮想IPアドレスのドメインまたはホスト

名解決など、代行受信されるクライアントトラフィックのタイプも制御します。この分離により、グローバルマップは証明書の表示やトラフィックの代行受信などの包括的な設定を処理でき、ユーザ定義のパラメータマップはWLANごとのきめ細かなエクスペリエンスを提供します。

WLANセキュリティパラメータ

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#wlan LWA_LA 1 "LWA LA"
9800WLC(config-wlan)#no security wpa
9800WLC(config-wlan)#no security wpa wpa2
9800WLC(config-wlan)#no security wpa wpa2 ciphers aes
9800WLC(config-wlan)#no security wpa akm dot1x
9800WLC(config-wlan)#security web-auth
9800WLC(config-wlan)#security web-auth authentication-list LWA_AUTHENTICATION
9800WLC(config-wlan)#security web-auth parameter-map global
9800WLC(config-wlan)#no shutdown
9800WLC(config-wlan)#end
```

ポリシープロファイルの作成

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#wireless profile policy
```

```
9800WLC(config-wireless-policy)#vlan
```

```
9800WLC(config-wireless-policy)#no shutdown
```

```
9800WLC(config-wireless-policy)#end
```

ポリシータグの作成

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#wireless tag policy
```

```
9800WLC(config-policy-tag)#wlan LWA_LA policy
```

```
9800WLC(config-policy-tag)# end
```

APへのポリシータグの割り当て

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#ap
```

```
>
```

```
9800WLC(config-ap-tag)#policy-tag POLICY_TAG
```

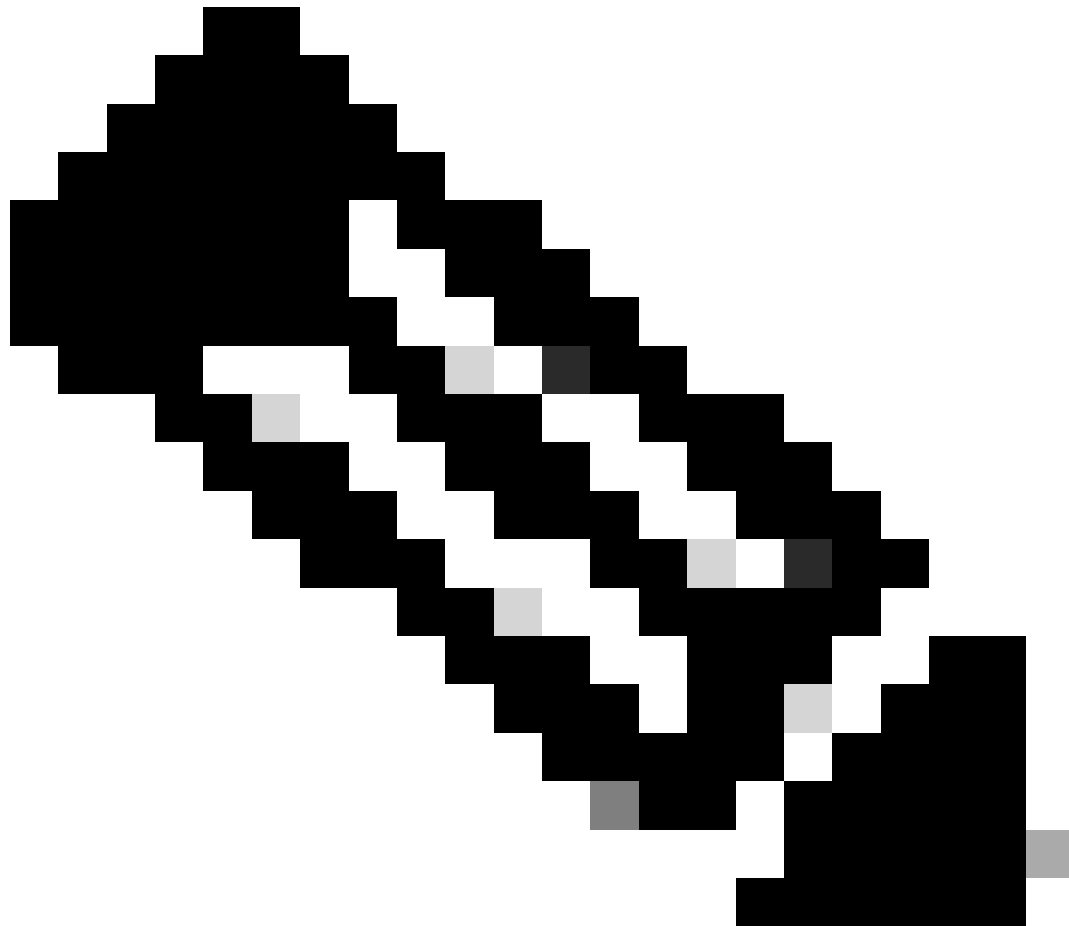
```
9800WLC(config-ap-tag)#end
```

ゲストユーザ名の作成

```
9800WLC>enable
9800WLC#configure terminal
9800WLC(config)#user-name johndoe
9800WLC(config-user-name)#description Guest-User
9800WLC(config-user-name)#password 0 Cisco123
9800WLC(config-user-name)#type network-user description
```

```
guest-user lifetime year 0 month 11 day 30 hour 23
```

```
9800WLC(config-user-name)#end
```

注：ゲストユーザのライフタイムを設定する際に年を1に設定すると、最大ライフタイムが1年なので、それに続くパラメータ（月、日、時間、分）は指定できません。

WebUI経由のローカル認証を使用したローカルWeb認証

ローカル認証方式リスト

Configuration > Security > AAA > AAA Method List > Authentication > Addの順に移動し、後でWLAN設定で使用する方式リストを作成します。

Configuration > Security > AAA [Show Me How](#)

[+ AAA Wizard](#)

Servers / Groups **AAA Method List** AAA Advanced

Authentication

Authorization

Accounting

[+ Add](#) [- Delete](#)

Name	Type	Group Type	Group1	Group2
☐ default	login	local	N/A	N/A

Quick Setup: AAA Authentication

Method List Name*

LWA-AUTHENTICATION

Type*

login

i

Group Type

local

i

Available Server Groups

radius
ldap
tacacs+
AAA-group

>
<
>>
<<

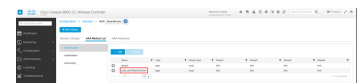
Assigned Server Groups

^
^
v
v

Cancel

Apply to Device

Apply to Deviceをクリックした後、AAA方式リストの作成を確認します。



ローカル認証方式リストがあることを確認します。これは、作成されたローカルログイン方式リストが機能するための要件です。

設定>セキュリティ> AAA > AAA方式リスト>許可>追加

Configuration > Security > AAA [Show Me How](#)

[+ AAA Wizard](#)

Servers / Groups **AAA Method List** AAA Advanced

Authentication

Authorization

Accounting

[+ Add](#) [- Delete](#)

Name	Type	Group Type	Group1	Group2
☐ default	exec	local	N/A	N/A

Quick Setup: AAA Authorization

Method List Name*

default

Type*

network

i

Group Type

local

i

Authenticated

☐

Available Server Groups

radius
ldap
tacacs+
AAA-group

Assigned Server Groups

Cancel

Apply to Device

Apply to Deviceをクリックした後、AAA方式リストの作成を確認します。

Configuration > Security > AAA

[+ AAA Wizard](#)

Servers / Groups **AAA Method List** AAA Advanced

Authentication

Authorization

Accounting

[+ Add](#) [- Delete](#)

Name	Type	Group Type	Group1	Group2	Group3	Group4
☐ default	exec	local	N/A	N/A	N/A	N/A
☐ default	network	local	N/A	N/A	N/A	N/A

1 - 2 of 2 items

パラメータマップ

Configuration > Security > Web Authでグローバルパラメータマップを編集します。

Configuration > Security > Web Auth

+ Add - Delete

Selected Rows: 0

Parameter Map Name
☐ global

1 10 items per page

Edit Web Auth Parameter

General Advanced

Parameter-map Name	global	Virtual IPv4 Address	192.0.2.1
Maximum HTTP connections	100	Trustpoint	TP-self-signed-...
Init-State Timeout(secs)	120	Virtual IPv4 Hostname	
Type	webauth	Virtual IPv6 Address	xxxxxx
Captive Bypass Portal	☐	Web Auth intercept HTTPs	☐
Disable Success Window	☐	Enable HTTP server for Web Auth	☒
Disable Logout Window	☐	Disable HTTP secure server for Web Auth	☐
Disable Cisco Logo	☐	Banner Configuration	
Sleeping Client Status	☐	Banner Title	
Sleeping Client Timeout (minutes)	720	Banner Type	☒ None ☐ Banner Text ☐ Read From File

使用するWeb認証のタイプ、仮想IP(VIP)、およびWLCがWebポータルで提示するトラストポイントを選択します。この場合、自己署名証明書(SSC)が選択されており、ローカルで有効な証明書(LSC)であり、インターネット上の認識可能なCAによって署名されていないため、「あなたの接続はプライベートネットではありません :ERR_CERT_AUTHORITY_INVALID」という種類の免責事項が発生する可能性があります。これを修正するには、サードパーティの署名付き証明書を使用します。詳細は、「[Catalyst 9800 WLCでのCSR証明書の生成とダウンロード](#)」に記載されています。また、アップロードとトラストポイント作成の「[Cisco 9800 WLCでのWebAuthとWebAdminの証明書の更新](#)」[セキュアワイヤレスLANコントローラの設定](#)」について説明するビデオオプションもあります。

Edit Web Auth Parameter



General

Advanced

Parameter-map Name

Maximum HTTP connections

Init-State Timeout(secs)

Type

Captive Bypass Portal ☐

Disable Success Window ☐

Disable Logout Window ☐

Disable Cisco Logo ☐

Sleeping Client Status ☐

Sleeping Client Timeout (minutes)

Virtual IPv4 Address

Trustpoint

Virtual IPv4 Hostname

Virtual IPv6 Address

Web Auth intercept HTTPs ☐

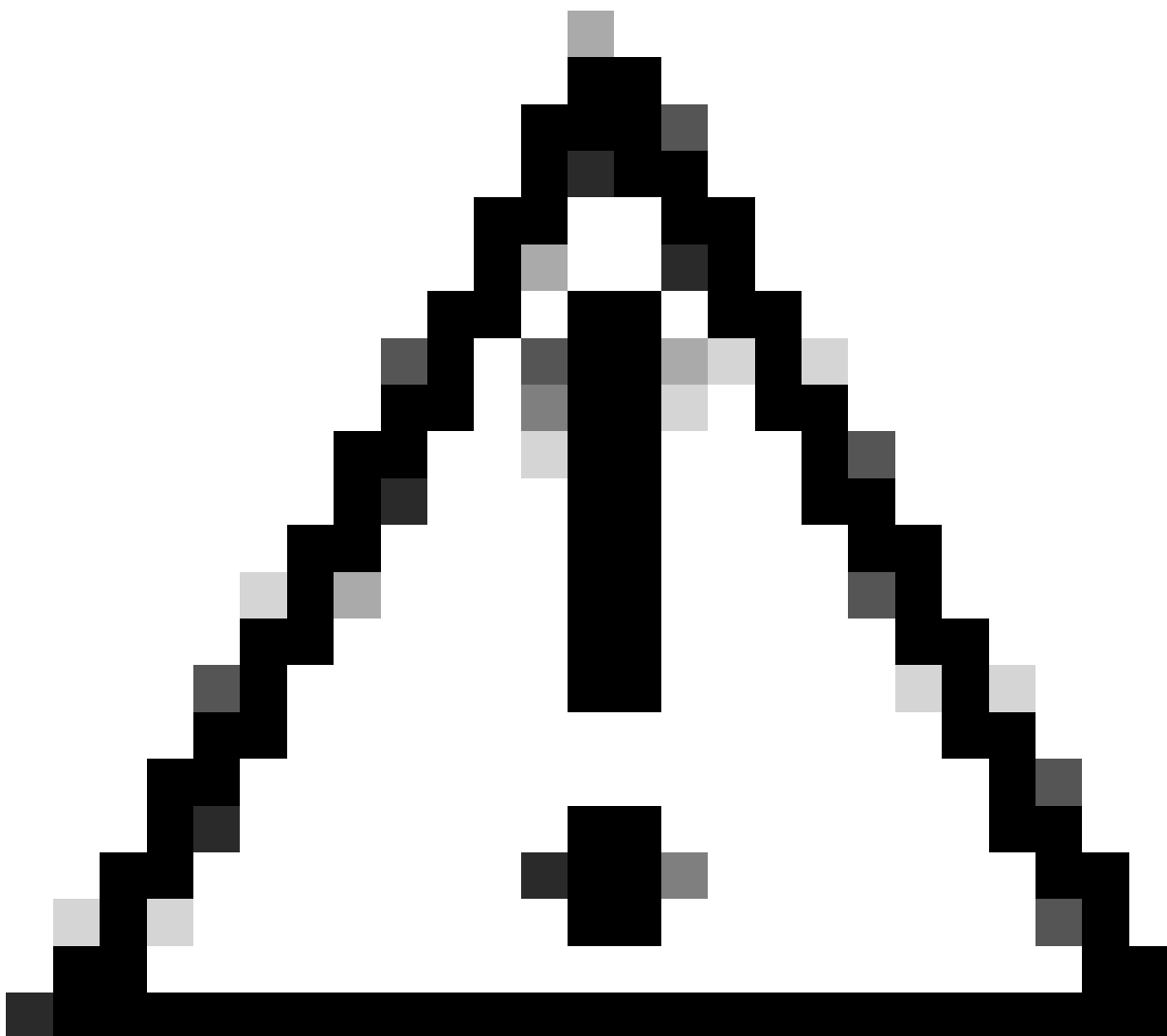
Enable HTTP server for Web Auth ☒

Disable HTTP secure server for Web Auth ☐

Banner Configuration

Banner Title

Banner Type ☒ None ☐ Banner Text ☐ Read From File



注意:9800でHTTPをグローバルで無効にしている場合は、Web認証用のEnable HTTP serverにチェックマークが付いていることを確認してください。これは、Ciscoによってこれらのプロセスの依存関係が分離されているためです。クライアントまたはサブリカントはHTTP接続プロセスを開始することが期待され、そのセッションはコントローラによってインターセプトされ、Webポータルを提示します。このため、絶対に必要でない限り、Web Auth Intercept HTTPSを有効にすることは推奨されません。この設定はほとんどの導入で不要であり、コントローラのCPU使用率を増加させて、パフォーマンスに影響を与える可能性があるためです。

WLANセキュリティパラメータ

Configuration > Tags & Profiles > WLANsの順に移動し、Addをクリックします。

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General

Security

Advanced

Add To Policy Tags

Profile Name*

LWA_LA

SSID*

LWA LA

WLAN ID*

1

Status

ENABLED ☒

Broadcast SSID

ENABLED ☒

Radio Policy ⓘ

6 GHz

Status

ENABLED ☒☒ Slot 2/3

✖ WPA3 Enabled

✔ Dot11ax Enabled

5 GHz

Status

ENABLED ☒☒ Slot 0☒ Slot 1☒ Slot 2

2.4 GHz

Status

ENABLED ☒☒ Slot 0802.11b/g
Policy

802.11b/g ▼

Securityタブで、Layer2に対してNoneを選択します。

Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General

Security

Advanced

Add To Policy Tags

Layer2

Layer3

AAA

⚠ To review the necessary considerations for ensuring WLAN compatibility with Wi-Fi 7 security [click here](#).

☐ WPA + WPA2

☐ WPA2 + WPA3

☐ WPA3

☐ Static WEP

☒ None

MAC Filtering

☐

OWE Transition Mode

☐

Lobby Admin Access

☐

Fast Transition

Status

Adaptive Ena...

Over the DS

☐

Reassociation Timeout *

20

Securityタブで、Layer3のWeb Policyボックスにチェックマークを入れて、ドロップダウンメニューとAuthentication Listから以前に設定したParameter Mapを選択します。

Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General

Security

Advanced

Add To Policy Tags

Layer2

Layer3

AAA

Web Policy

☒

Web Auth Parameter Map

global

Authentication List

LWA_AUTHENTI...

On MAC Filter Failure

☐

Splash Web Redirect

DISABLED

Preauthentication ACL

IPv4

None

IPv6

None

<< Hide

For Local Login Method List to work, please make sure the configuration 'aaa authorization network default local' exists on the device

ポリシープロファイルの作成

WLANプロファイルにリンクするポリシープロファイルを作成するには、Configuration > Tags & Profiles > Policyの順に選択します。

Edit Policy Profile ✕

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General

Access Policies

QOS and AVC

Mobility

Advanced

Name*

LWA_CentralSW

Description

Enter Description

Status

ENABLED ☒

Passive Client

☐ DISABLED

IP MAC Binding

ENABLED ☒

Encrypted Traffic Analytics

☐ DISABLED

CTS Policy

Inline Tagging

☐

SGACL Enforcement

☐

Default SGT

2-65519

WLAN Switching Policy

Central Switching

ENABLED ☒

Central Authentication

ENABLED ☒

Central DHCP

ENABLED ☒

Flex NAT/PAT

☐ DISABLED

Access Policiesタブで、クライアント/サブリカントがIPを要求するVLANを選択します。

Edit Policy Profile

⚠ Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.

General **Access Policies** QOS and AVC Mobility Advanced

RADIUS Profiling

☐

HTTP TLV Caching

☐

DHCP TLV Caching

☐

WLAN Local Profiling

Global State of Device Classification

Enabled ⓘ

Local Subscriber Policy Name

Search or Select ▼ ⓘ

VLAN

VLAN/VLAN Group

2622 ▼ ⓘ

Multicast VLAN

Enter Multicast VLAN

WLAN ACL

IPv4 ACL

Search or Select ▼ ⓘ

IPv6 ACL

Search or Select ▼ ⓘ

URL Filters ⓘ

Pre Auth

Search or Select ▼ ⓘ

Post Auth

Search or Select ▼ ⓘ

ポリシータグの作成

この設定ガイドでは、LWAという名前のカスタムポリシータグを作成しました。

Edit Policy Tag

⚠ Changes may result in loss of connectivity for some clients that are associated to APs with this Policy Tag.

Name*

LWA

Description

LWA_LA

▼ WLAN-POLICY Maps: 1

+ Add

× Delete

WLAN Profile



Policy Profile



☐ LWA_LA

LWA_CentralSW

1

10 ▼

1 - 1 of 1 items

WLANとポリシープロファイルの関連付け

ポリシープロファイルとWLANからスイッチングポリシーをリンクするには、Configuration >

Tags & Profiles > WLANsの順に移動し、WLANプロファイルを選択し、Add to Policy Tagsをクリックします。

Warning: Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General Security Advanced **Add To Policy Tags**

+ Add × Delete

☐	Policy Tag	Policy Profile
☐	LWA	LWA_CentralSW

1 10 1 - 1 of 1 items

APへのポリシータグの割り当て

作成したポリシータグを使用してAPにタグを付けるには、Configuration > Wireless > Access Pointsの順に移動し、APを選択します。Generalタブの右側に、APで使用されるタグがあります。

Edit AP

General

Interfaces

High Availability

Inventory

Geolocation

Advanced

Support Bundle

General

AP Name*

9117

Location*

default location

Base Radio MAC

cc0

Ethernet MAC

c00

Admin Status

ENABLED

AP Mode

Local

Operation Status

Registered

Fabric Status

Disabled

LED Settings

LED State

ENABLED

Brightness Level

8

Flash Settings

Flash State

DISABLED

Apply

Time Statistics

Up Time

8 days 15 hrs 26 mins 48 secs

Controller Association Latency

1 sec

Tags

Policy

LWA

Site

default-site-tag

RF

default-rf-tag

Write Tag Config to AP

Version

Primary Software Version

17.12.5.41

Predownloaded Status

N/A

Predownloaded Version

N/A

Next Retry Time

N/A

Boot Version

1.1.2.4

IOS Version

17.12.5.41

Mini IOS Version

0.0.0.0

IP Config

CAPWAP Preferred Mode

IPv4

DHCP IPv4 Address

172.16.60.40

Static IP (IPv4/IPv6)

Cancel

Update & Apply to Device

ゲストユーザ名の作成

パラメータマップでwebauthタイプを選択した場合は、Guest User-Nameが必要です。これを作成するには、Configuration > Security > Guest Userの順に選択します。

ユーザの最大有効期間は1年です。使用可能なオプションを使用して、それ以外のオプションを指定できます。

[+ Add](#) [- Delete](#)

Selected Rows: 0

- ☐
- User Name
-
- ☐
- johndoe

1 10 items per page

Edit Guest User

General

Enter User Name* johndoe

Password* 

☐ Generate password

Confirm Password

Description* Guest-User

AAA Attribute list 

No. of Simultaneous User Logins*
Enter 0 for unlimited users

Start Time 15:21:19 UTC Aug 26 2025

Expiry Time 15:21:19 UTC Aug 21 2026

Remaining Time 0 years 11 months 29 days 23 hours 34 mins 24 secs

Lifetime

Years*

Months*

Days*

Hours*

Mins*

確認

GUI 経由

Cisco Catalyst 9800-CL Wireless Controller 17.12.5 Welcome admin

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

[Delete](#) 

Selected 0 out of 1 Clients

☐	Client MAC Address	IPv4 Address	IPv6 Address	AP Name	Slot ID	SSID	WLAN ID	Client Type	State	Protocol	User Name	Device Type	Role	6E Capable
☐	9ef2.4b16.a507	172.16.74.83	fe80:9c72:4b16:fe16:a507	9117	0	LWA LA	1	WLAN	Run	11ax(2.4)	johndoe	N/A	Local	No

1 10 1 - 1 of 1 clients

Monitoring > Wireless > Clients

Clients
Sleeping Clients
Excluded Clients

Delete
Refresh

Selected 0 out of 1 Clients

	Client MAC Address	IPv4 Address	IPv6 Address	AP Name	Slot ID	SSID
☐	507	172.16.74.83	fe80::9cf2:4bff:fe16:a507	-9117	0	LWA LA

1
10

Client
360 View
General
QoS Statistics
ATF Statistics
Mobility History
Call Statistics

Client Properties
AP Properties
Security Information
Client Statistics
QoS Properties
EoGRE

MAC Address
Client MAC Type
Client DUID
IPv4 Address
IPv6 Address
User Name
Policy Profile
Flex Profile
Wireless LAN Id
WLAN Profile Name
Wireless LAN Network Name (SSID)
BSSID
Uptime(sec)
Idle state timeout
Session Timeout
Session Warning Time
Client Active State
Power Save mode
Current TxRateSet
Supported Rates
QoS Average Data Rate Upstream
QoS Realtime Average Data Rate Upstream
QoS Burst Data Rate Upstream
QoS Realtime Burst Data Rate Upstream
QoS Average Data Rate Downstream
QoS Realtime Average Data Rate Downstream
QoS Burst Data Rate Downstream
QoS Realtime Burst Data Rate Downstream
Join Time Of Client
Policy Manager State
Last Policy Manager State
Transition Disable Bitmap
User Defined (Private) Network
User Defined (Private) Network Drop
Unicast

y507
Locally Administered Address
NA
172.16.74.83
fe80::9cf2:4bff:fe16:a507
johndoe
LWA_CentralSW
N/A
1
LWA_LA
LWA LA
0cd0.f897.acc0
151 seconds
N/A
28800 sec (Remaining time: 28678 sec)
Timer not running
Active
ON
1.0
1.0,2.0,5.5,6.0,9.0,11.0,12.0,18.0,24.0,36.0,48.0,54.0
0 (kbps)
0 (kbps)
0 (kbps)
0 (kbps)
0 (kbps)
0 (kbps)
0 (kbps)
0 (kbps)
0 (kbps)
0 (kbps)
0 (kbps)
0 (kbps)
09/10/2025 21:26:11 UTC
Run
Webauth Pending
0x00
Disabled
Disabled

OK

CLI の場合

```

9800WLC>enable
9800WLC#show wireless client summary
Number of Clients: 1
MAC Address      AP Name          Type ID State Protocol Method  Role
-----
9ef2.4b16.a507   xxxxx-9117 WLAN 1 Run   11ax(2.4) Web Auth Local
9800WLC#show wireless client mac-address

```

detail

Client MAC Address : 9ef2.4b16.a507

Client MAC Type : Locally Administered Address

Client DUID: NA

Client IPv4 Address : 172.16.74.83

Client IPv6 Addresses : fe80::9cf2:4bff:fe16:a507

Client Username : johndoe

AP MAC Address : 0cd0.f897.acc0

AP Name: xxxxx-9117

AP slot : 0

Client State : Associated

Policy Profile : LWA_CentralSW

Flex Profile : N/A

Wireless LAN Id: 1

WLAN Profile Name: LWA_LA

Wireless LAN Network Name (SSID): LWA LA

BSSID : 0cd0.f897.acc0

Connected For : 392 seconds

Protocol : 802.11ax - 2.4 GHz

Channel : 11

Client IIF-ID : 0xa0000002

Association Id : 1

Authentication Algorithm : Open System

Idle state timeout : N/A

Session Timeout : 28800 sec (Remaining time: 28455 sec)

Session Warning Time : Timer not running

Input Policy Name : None

Input Policy State : None

Input Policy Source : None

Output Policy Name : None

Output Policy State : None

Output Policy Source : None

WMM Support : Enabled

U-APSD Support : Disabled

Fastlane Support : Disabled

Client Active State : Active

Power Save : ON

Current Rate : m0 ss2

Supported Rates : 1.0,2.0,5.5,6.0,9.0,11.0,12.0,18.0,24.0,36.0,48.0,54.0

AAA QoS Rate Limit Parameters:

QoS Average Data Rate Upstream : 0 (kbps)

QoS Realtime Average Data Rate Upstream : 0 (kbps)

QoS Burst Data Rate Upstream : 0 (kbps)

QoS Realtime Burst Data Rate Upstream : 0 (kbps)

QoS Average Data Rate Downstream : 0 (kbps)

QoS Realtime Average Data Rate Downstream : 0 (kbps)

QoS Burst Data Rate Downstream : 0 (kbps)

QoS Realtime Burst Data Rate Downstream : 0 (kbps)

Mobility:

Move Count : 0

Mobility Role : Local

Mobility Roam Type : None

Mobility Complete Timestamp : 09/10/2025 21:41:11 UTC

Client Join Time:

Join Time Of Client : 09/10/2025 21:41:11 UTC

Client State Servers : None

Client ACLs : None

Policy Manager State: Run

Last Policy Manager State : Webauth Pending

Client Entry Create Time : 392 seconds

Policy Type : N/A

Encryption Cipher : None

Transition Disable Bitmap : 0x00

User Defined (Private) Network : Disabled

User Defined (Private) Network Drop Unicast : Disabled

Encrypted Traffic Analytics : No

Protected Management Frame - 802.11w : No

EAP Type : Not Applicable

VLAN Override after Webauth : No

VLAN : 2667

Multicast VLAN : 0

VRF Name : N/A

WiFi Direct Capabilities:

WiFi Direct Capable : No

Central NAT : DISABLED

Session Manager:

Point of Attachment : capwap_90400005

IIF ID : 0x90400005

Authorized : TRUE

Session timeout : 28800

Common Session ID: 044A10AC0000000F359351E3

Acct Session ID : 0x00000000

Auth Method Status List

Method : Web Auth

Webauth State : Authz

Webauth Method : Webauth

Local Policies:

Service Template : IP-Adm-V4-LOGOUT-ACL (priority 100)

URL Redirect ACL : IP-Adm-V4-LOGOUT-ACL

Service Template : wlan_svc_LWA_CentralSW_local (priority 254)

VLAN : 2667

Absolute-Timer : 28800

Server Policies:

Resultant Policies:

URL Redirect ACL : IP-Adm-V4-LOGOUT-ACL

VLAN Name : xxxxx

VLAN : 2667

Absolute-Timer : 28800

DNS Snooped IPv4 Addresses : None

DNS Snooped IPv6 Addresses : None

Client Capabilities

CF Pollable : Not implemented

CF Poll Request : Not implemented

Short Preamble : Not implemented

PBCC : Not implemented

Channel Agility : Not implemented

Listen Interval : 0

Fast BSS Transition Details :

Reassociation Timeout : 0

11v BSS Transition : Implemented

11v DMS Capable : No

QoS Map Capable : Yes

FlexConnect Data Switching : N/A

FlexConnect Dhcp Status : N/A

FlexConnect Authentication : N/A

Client Statistics:

Number of Bytes Received from Client : 111696

Number of Bytes Sent to Client : 62671

Number of Packets Received from Client : 529

Number of Packets Sent to Client : 268

Number of Data Retries : 136

Number of RTS Retries : 0

Number of Tx Total Dropped Packets : 1

Number of Duplicate Received Packets : 0

Number of Decrypt Failed Packets : 0

Number of Mic Failed Packets : 0

Number of Mic Missing Packets : 0

Number of Policy Errors : 0

Radio Signal Strength Indicator : -61 dBm

Signal to Noise Ratio : 4 dB

Fabric status : Disabled

Radio Measurement Enabled Capabilities

Capabilities: Link Measurement, Neighbor Report, Repeated Measurements, Passive Beacon Measurement, Act

Client Scan Report Time : Timer not running

Client Scan Reports

Assisted Roaming Neighbor List

Nearby AP Statistics:

EoGRE : Pending Classification

Max Client Protocol Capability: Wi-Fi6 (802.11ax)

WiFi to Cellular Steering : Not implemented

Cellular Capability : N/A

Advanced Scheduling Requests Details:

Apple Specific Requests(ASR) Capabilities/Statistics:

Regular ASR support: DISABLED

FlexConnectローカルスイッチングでのローカルWeb認証

このシナリオでは、APはFlexConnectモードであると想定されます。APをFlexConnectモードにするには、SiteTagに関連付けられたFlex Profileが必要です。Enable Local Siteチェックボックスは無効です。このサイトタグは、default-ap-joinとカスタムフレックスプロファイル名 Flex_LWAを使用します。

Configuration > Tags & Profiles > Tags

Policy
Site
RF
AP

Add
Delete
Clone
Reset APs

Site Tag Name

☐ FlexConnect
☐ default-site-tag

1
10

Edit Site Tag

Name*
FlexConnect

Description
Enter Description

AP Join Profile
default-ap-profile

Flex Profile
Flex_LWA

Fabric Control Plane Name

Enable Local Site
☐

Load*
0

APへのポリシータグの割り当て

Configuration > Wireless > Access Pointsの順に移動し、APを選択します。Generalタブの右側に、APで使用されるタグがあります。

Edit AP

General
Interfaces
High Availability
Inventory
Geolocation
Advanced
Support Bundle

General

AP Name*
9117

Location*
default location

Base Radio MAC

Ethernet MAC

Admin Status
ENABLED

AP Mode
Local

Operation Status
Registered

Fabric Status
Disabled

LED Settings

LED State
DISABLED

Flash Settings

Flash State
DISABLED

Apply

Time Statistics

Up Time
8 days 15 hrs 51 mins 4 secs

Controller Association Latency
1 sec

Tags

Policy
LWA

Site
FlexConnect

RF
default-rf-tag

Write Tag Config to AP

Version

Primary Software Version
17.12.5.41

Predownloaded Status
N/A

Predownloaded Version
N/A

Next Retry Time
N/A

Boot Version
1.1.2.4

IOS Version
17.12.5.41

Mini IOS Version
0.0.0.0

IP Config

CAPWAP Preferred Mode
Not Configured

DHCP IPv4 Address
172.16.60.40

Static IP (IPv4/IPv6)



警告：タグを変更すると、APがWLCから切断されます。

Configuration > Wireless > Access Points

▼ All Access Points

Total APs: 1

Misconfigured APs
Tag: 0 Country Code: 0 LSC Fallback: 0 Select an Action

Multiple APs can be configured at once from [Bulk AP Provisioning](#) feature

AP Name	AP Model	Slots	Admin Status	Up Time	IP Address	Base Radio MAC	Ethernet MAC	AP Mode	Power Derate Capable	Operation Status	Configuration Status	Country Code Misconfigured	LSC Fallback Misconfigure
9117	C9117AXI-A	2		8 days 15 hrs 54 mins 53 secs	172.16.60.40	cc0	c00	Flex	No	Registered	Healthy	No	No

WLANに関連付けられているポリシープロファイルはローカルスイッチングです

Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General
Security
Advanced
Add To Policy Tags

+ Add
Delete

☐ Policy Tag
☐ Policy Profile

☐ LWA
LWA_LocalSW

1
10
1 - 1 of 1 items

Configuration > Tags & Profiles > Policy

Add
Delete
Clone

Policy Profile Name "is equal to" LWA_LocalSW

Admin Status	Associated Policy Tags	Policy Profile Name
☒		LWA_LocalSW

1
10

Edit Policy Profile

⚠ Disabling a Policy or configuring it in "Enabled" state, will result in loss of connectivity for clients associated with this Policy profile.

General
Access Policies
QOS and AVC
Mobility
Advanced

Name*
LWA_LocalSW
WLAN Switching Policy

Description
Enter Description
Central Switching
DISABLED

Status
ENABLED
Central Authentication
ENABLED

Passive Client
DISABLED
Central DHCP
ENABLED

IP MAC Binding
ENABLED
Flex NAT/PAT
DISABLED

Encrypted Traffic Analytics
DISABLED

CTS Policy

Inline Tagging
SGACL Enforcement
Default SGT
2-65519

確認

```

9800WLC>enable
9800WLC#show wireless client summary
Number of Clients: 1
MAC Address      AP Name      Type ID  State Protocol  Method  Role
-----
9ef2.4b16.a507  xxxxx-9117  WLAN 1  Run  11ax(2.4)  Web Auth Local

9800WLC#show wireless client mac-address

```

detail

Client MAC Address :

Client MAC Type : Locally Administered Address

Client DUID: NA

Client IPv4 Address : 172.16.74.83

Client IPv6 Addresses : fe80::9cf2:4bff:fe16:a507

Client Username : johndoe

AP MAC Address : xxxx.xxxx.xcc0

AP Name: xxxxxx-9117

AP slot : 0

Client State : Associated

Policy Profile : LWA_LocalSW

Flex Profile : Flex_LWA

Wireless LAN Id: 1

WLAN Profile Name: LWA_LA

Wireless LAN Network Name (SSID): LWA LA

BSSID : 0cd0.f897.acc0

Connected For : 315 seconds

Protocol : 802.11ax - 2.4 GHz

Channel : 6

Client IIF-ID : 0xa0000004

Association Id : 1

Authentication Algorithm : Open System

Idle state timeout : N/A

Session Timeout : 28800 sec (Remaining time: 28525 sec)

Session Warning Time : Timer not running

Input Policy Name : None

Input Policy State : None

Input Policy Source : None

Output Policy Name : None

Output Policy State : None

Output Policy Source : None

WMM Support : Enabled

U-APSD Support : Disabled

Fastlane Support : Disabled

Client Active State : Active

Power Save : ON

Current Rate : m11 ss2

Supported Rates : 1.0,2.0,5.5,6.0,9.0,11.0,12.0,18.0,24.0,36.0,48.0,54.0

AAA QoS Rate Limit Parameters:

QoS Average Data Rate Upstream : 0 (kbps)

QoS Realtime Average Data Rate Upstream : 0 (kbps)

QoS Burst Data Rate Upstream : 0 (kbps)

QoS Realtime Burst Data Rate Upstream : 0 (kbps)

QoS Average Data Rate Downstream : 0 (kbps)

QoS Realtime Average Data Rate Downstream : 0 (kbps)

QoS Burst Data Rate Downstream : 0 (kbps)

QoS Realtime Burst Data Rate Downstream : 0 (kbps)

Mobility:

Move Count : 0

Mobility Role : Local

Mobility Roam Type : None

Mobility Complete Timestamp : 09/11/2025 17:38:26 UTC

Client Join Time:

Join Time Of Client : 09/11/2025 17:38:26 UTC

Client State Servers : None

Client ACLs : None

Policy Manager State: Run

Last Policy Manager State : Webauth Pending

Client Entry Create Time : 315 seconds

Policy Type : N/A

Encryption Cipher : None

Transition Disable Bitmap : 0x00

User Defined (Private) Network : Disabled

User Defined (Private) Network Drop Unicast : Disabled

Encrypted Traffic Analytics : No

Protected Management Frame - 802.11w : No

EAP Type : Not Applicable

VLAN Override after Webauth : No

VLAN : 2667

Multicast VLAN : 0

VRF Name : N/A

WiFi Direct Capabilities:

WiFi Direct Capable : No

Central NAT : DISABLED

Session Manager:

Point of Attachment : capwap_90400005

IIF ID : 0x90400005

Authorized : TRUE

Session timeout : 28800

Common Session ID: 044A10AC0000002A39DB6F52

Acct Session ID : 0x00000000

Auth Method Status List

Method : Web Auth

Webauth State : Authz

Webauth Method : Webauth

Local Policies:

Service Template : IP-Adm-V4-LOGOUT-ACL (priority 100)

URL Redirect ACL : IP-Adm-V4-LOGOUT-ACL

Service Template : wlan_svc_LWA_LocalSW (priority 254)

VLAN : 2667

Absolute-Timer : 28800

Server Policies:

Resultant Policies:

URL Redirect ACL : IP-Adm-V4-LOGOUT-ACL

VLAN Name : xxxxx

VLAN : 2667

Absolute-Timer : 28800

DNS Snooped IPv4 Addresses : None

DNS Snooped IPv6 Addresses : None

Client Capabilities

CF Pollable : Not implemented

CF Poll Request : Not implemented

Short Preamble : Not implemented

PBCC : Not implemented

Channel Agility : Not implemented

Listen Interval : 0

Fast BSS Transition Details :

Reassociation Timeout : 0

11v BSS Transition : Implemented

11v DMS Capable : No

QoS Map Capable : Yes

FlexConnect Data Switching : Local

FlexConnect Dhcp Status : Central

FlexConnect Authentication : Central

Client Statistics:

Number of Bytes Received from Client : 295564

Number of Bytes Sent to Client : 90146

Number of Packets Received from Client : 1890

Number of Packets Sent to Client : 351

Number of Data Retries : 96

Number of RTS Retries : 0

Number of Tx Total Dropped Packets : 0

Number of Duplicate Received Packets : 0

Number of Decrypt Failed Packets : 0

Number of Mic Failed Packets : 0

Number of Mic Missing Packets : 0

Number of Policy Errors : 0

Radio Signal Strength Indicator : -34 dBm

Signal to Noise Ratio : 31 dB

Fabric status : Disabled

Radio Measurement Enabled Capabilities

Capabilities: Link Measurement, Neighbor Report, Repeated Measurements, Passive Beacon Measurement, Act

Client Scan Report Time : Timer not running

Client Scan Reports

Assisted Roaming Neighbor List

Nearby AP Statistics:

EoGRE : Pending Classification

Max Client Protocol Capability: Wi-Fi6 (802.11ax)

WiFi to Cellular Steering : Not implemented

Cellular Capability : N/A

Advanced Scheduling Requests Details:

Apple Specific Requests(ASR) Capabilities/Statistics:

Regular ASR support: DISABLED

The screenshot displays the Cisco WLC interface. On the left, the 'Clients' tab is active, showing a list of clients. One client is selected, and its details are shown in the 'Client Properties' window on the right. The 'Client Properties' window has several tabs: 'General', 'QoS Statistics', 'ATF Statistics', 'Mobility History', 'Call Statistics', 'AP Properties', 'Security Information', 'Client Statistics', 'QoS Properties', and 'EoGRE'. The 'General' tab is selected, showing various client attributes. The 'Policy Profile' and 'Flex Profile' fields are highlighted with a red box, indicating they are set to 'LWA_LocalSW' and 'Flex_LWA' respectively.

Client Properties	Value
MAC Address	9ef2.4b16.a507
Client MAC Type	Locally Administered Address
Client DUID	NA
IPv4 Address	172.16.74.83
IPv6 Address	fe80::9cf2:4b16:fe16:a507
User Name	john.doe
Policy Profile	LWA_LocalSW
Flex Profile	Flex_LWA
Wireless LAN Id	1
WLAN Profile Name	LWA_LA
Wireless LAN Network Name (SSID)	LWA_LA
BSSID	cc0
Uptime(sec)	103 seconds
Idle state timeout	N/A
Session Timeout	28800 sec (Remaining time: 28737 sec)
Session Warning Time	Timer not running
Client Active State	Active
Power Save mode	OFF
Current TxRateSet	m11 ss2
Supported Rates	1.0,2.0,5.5,6.0,9.0,11.0,12.0,18.0,24.0,36.0,48.0,54.0
QoS Average Data Rate Upstream	0 (kbps)
QoS Realtime Average Data Rate Upstream	0 (kbps)
QoS Burst Data Rate Upstream	0 (kbps)
QoS Realtime Burst Data Rate Upstream	0 (kbps)
QoS Average Data Rate Downstream	0 (kbps)
QoS Realtime Average Data Rate Downstream	0 (kbps)
QoS Burst Data Rate Downstream	0 (kbps)
QoS Realtime Burst Data Rate Downstream	0 (kbps)
Join Time Of Client	09/11/2025 17:38:26 UTC
Policy Manager State	Run
Last Policy Manager State	Webauth Pending
Transition Disable Bitmap	0x00
User Defined (Private) Network	Disabled
User Defined (Private) Network Drop Unicast	Disabled

トラブルシューティング

「Web Auth Pending」ステータスは、クライアントがアクセスポイントに関連付けられているものの、まだWeb認証プロセスを完了していないことを示します。この状態の間、コントローラはクライアントのHTTPトラフィックを代行受信し、ユーザログインまたは条件の受け入れのためにWeb認証ポータルにリダイレクトします。クライアントは、Web認証が正常に完了するまでこの状態を維持します。その後、クライアントポリシーマネージャの状態は「Run」に移行し、フルネットワークアクセスが許可されます。

クライアント接続のフローを目視で確認するには、「[外部認証を使用したローカルWeb認証の設定](#)」でLWAのフローを確認します。

クライアントの観点からクライアントが受ける段階は、「[9800 WLCでのLWAの一般的な問題のトラブルシューティング](#)」で説明されています。

- [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。