

MACフィルタ失敗時のWeb認証の検証およびトラブルシューティングの設定

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](#)

[設定](#)

[ネットワーク図](#)

[コンフィギュレーション](#)

[Webパラメータの設定](#)

[ポリシープロファイルの設定](#)

[WLANプロファイルの設定](#)

[AAAの設定：](#)

[ISEの設定：](#)

[確認](#)

[コントローラ コンフィギュレーション](#)

[コントローラのクライアントポリシーの状態](#)

[トラブルシューティング](#)

[放射能トレースの収集](#)

[組み込みパケットキャプチャ：](#)

[関連情報](#)

はじめに

このドキュメントでは、外部認証にISEを使用した「MACフィルタ障害」機能でのローカルWeb認証の設定、トラブルシューティング、および確認について説明します。

前提条件

MAC認証用のISEの設定

ISE/Active Directoryで設定された有効なユーザクレデンシャル

要件

次の項目に関する知識があることが推奨されます。

コントローラのWeb UIをナビゲートするための基本的な知識

ポリシー、WLANプロファイル、およびポリシータグの設定

ISEでのサービスポリシーの設定

使用するコンポーネント

9800 WLCバージョン17.12.2

C9120 AXI AP (すべてのモデル)

9300 スイッチ

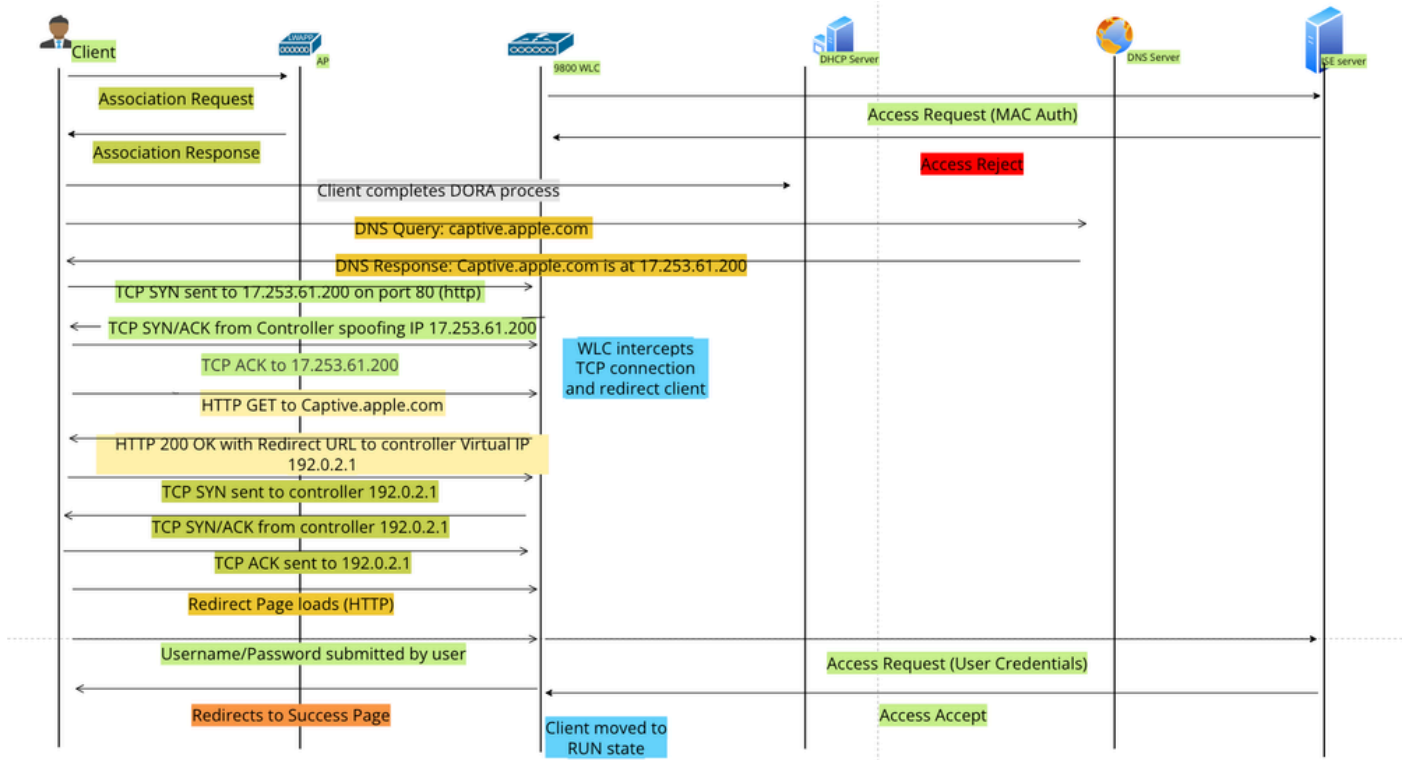
ISEバージョン3.1.0.518

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

Web Authの「On Mac Failure Filter」機能は、MAC認証とWeb認証の両方を使用するWLAN環境で、フォールバックメカニズムとして機能します。

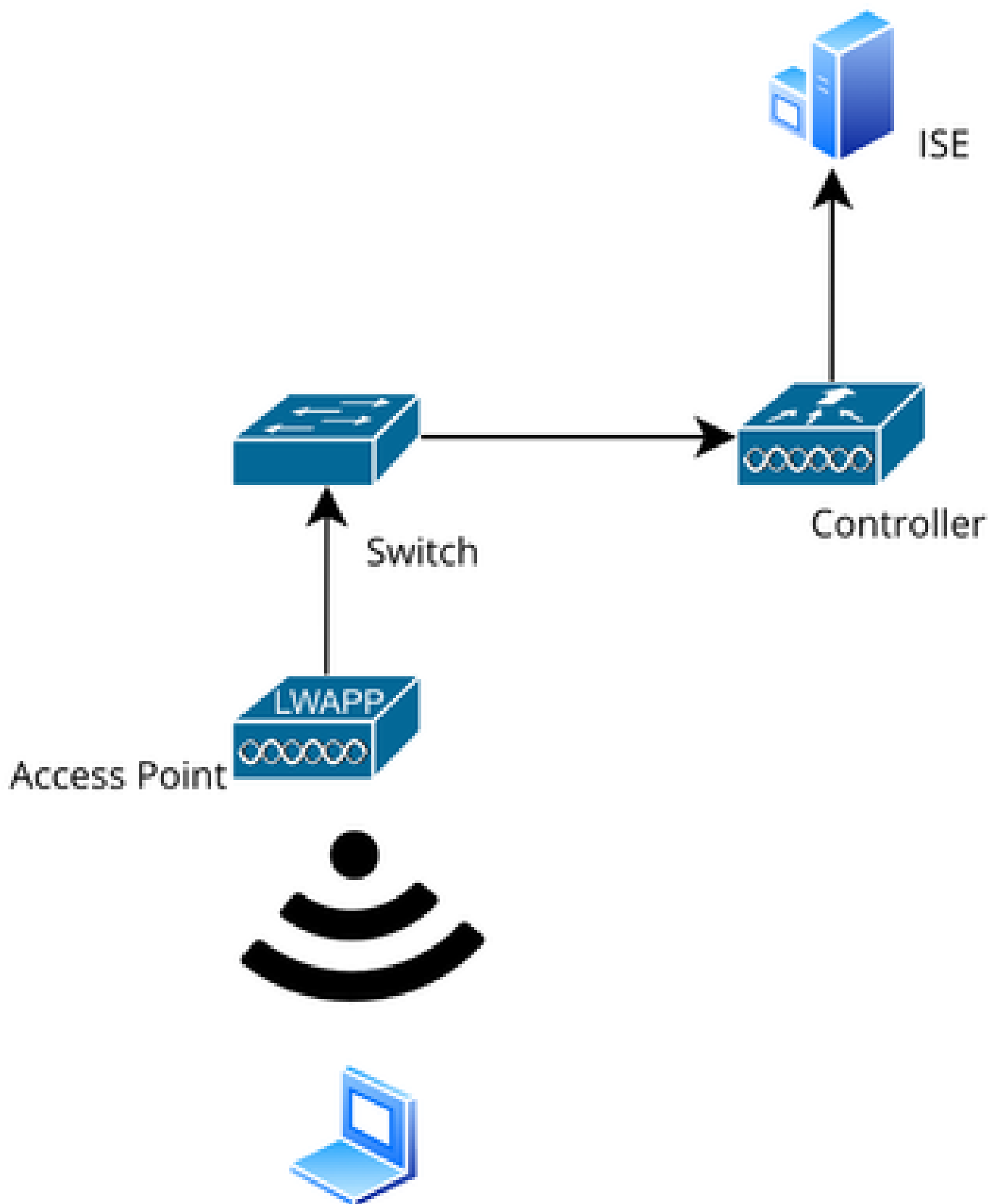
- フォールバックメカニズム：クライアントが外部RADIUSサーバ(ISE)またはローカルサーバに対してMACフィルタを使用してWLANに接続しようとして、認証に失敗した場合、この機能によってレイヤ3 Web認証が自動的に開始されます。
- 認証の成功：クライアントがMACフィルタを使用して正常に認証されると、Web認証がバイパスされ、クライアントはWLANに直接接続できます。
- 関連付け解除の回避：この機能を使用すると、MACフィルタ認証の失敗が原因で関連付け解除が行われるのを防ぐことができます。



Web認証フロー

設定

ネットワーク図



Network Topology

コンフィギュレーション

Webパラメータの設定

Configuration > Security > Web Authの順に移動し、Globalパラメータマップを選択します

グローバルパラメータマップでVirtual IPとTrustpointの設定を確認します。すべてのカスタムWeb認証パラメータプロファイルは、グローバルパラメータマップから仮想IPとトラストポイントの設定を継承します。

Edit Web Auth Parameter	
Parameter-map Name	global
Maximum HTTP connections	100
Init-State Timeout(secs)	120
Type	webauth
Captive Bypass Portal	<input type="checkbox"/>
Disable Success Window	<input type="checkbox"/>
Disable Logout Window	<input type="checkbox"/>
Disable Cisco Logo	<input type="checkbox"/>
Sleeping Client Status	<input type="checkbox"/>
Virtual IPv4 Address	192.0.2.1
Trustpoint	TP-self-signed-3...
Virtual IPv4 Hostname	
Virtual IPv6 Address	xxxxxx
Web Auth intercept HTTPs	<input type="checkbox"/>
Enable HTTP server for Web Auth	<input checked="" type="checkbox"/>
Disable HTTP secure server for Web Auth	<input type="checkbox"/>
Banner Configuration	

グローバルWeb認証パラメータプロファイル

ステップ1：カスタムWeb認証パラメータマップを作成するには、[追加]を選択します。プロファイル名を入力し、タイプとして「Webauth」を選択します。

Configuration > Security > Web Auth

+ Add Delete

Parameter Map Name

global

1 10

Create Web Auth Parameter

Parameter-map Name* Web-Filter

Maximum HTTP connections 1-200

Init-State Timeout(secs) 60-3932100

Type webauth

Close Apply to Device

クライアントがIPv6アドレスも取得している場合は、パラメータマップに仮想IPv6アドレスも追加する必要があります。ドキュメント範囲2001:db8::/32のIPを使用します。

クライアントがIPv6アドレスを取得した場合は、V4ではなくV6でHTTP Web認証のリダイレクションを取得しようとする可能性が高いため、仮想IPv6も設定する必要があります。

CLI による設定：

```
parameter-map type webauth Web-Filter  
type webauth
```

ポリシープロファイルの設定

ステップ1：ポリシープロファイルの作成

[設定 (Configuration)] > [タグとプロファイル (Tags & Profiles)] > [ポリシー (Policy)] に移動します。「追加」を選択します。[一般]タブで、プロファイルの名前を指定し、ステータス切り替えを有効にします。

Configuration > Tags & Profiles > Policy

+ Add Add Policy Profile

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

Admin Status

General Access Policies QOS and AVC Mobility Advanced

Name* Web-Filter-Policy

Description Enter Description

Status ENABLED

Passive Client DISABLED

IP MAC Binding ENABLED

Encrypted Traffic Analytics DISABLED

CTS Policy

WLAN Switching Policy

Central Switching ENABLED

Central Authentication ENABLED

Central DHCP ENABLED

Flex NAT/PAT DISABLED

Inline Tagging

SGACL Enforcement

ポリシー プロファイル

ステップ2:

Access Policiesタブで、VLANセクションのドロップダウンリストからクライアントVLANを選択します。

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

RADIUS Profiling

HTTP TLV Caching

DHCP TLV Caching

WLAN Local Profiling

Global State of Device Classification ⓘ

Local Subscriber Policy Name Search or Select ↕

VLAN

VLAN/VLAN Group VLAN2074 ⓘ

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 ↕

Access Policyタブ

CLI による設定 :

```
wireless profile policy Web-Filter-Policy
vlan VLAN2074
no shutdown
```

WLANプロファイルの設定

ステップ1: Configuration > Tags and Profiles > WLANsの順に移動します。「追加」を選択して新しいプロファイルを作成します。プロファイル名とSSID名を定義し、ステータスフィールドを有効にします。

+ Add

× Delete

Clone

Enable WLAN

Disable WLAN

Add WLAN

General

Security

Advanced

Profile Name* Mac_Filtering_Wlan

SSID* Mac_Filtering_Wlan

WLAN ID* 9

Status ENABLED Broadcast SSID ENABLED

Radio Policy ⓘ

[Show slot configuration](#)

6 GHz

Status ENABLED ⓘ

- ✖ WPA3 Enabled
- ✔ Dot11ax Enabled

5 GHz

Status ENABLED

2.4 GHz

Status ENABLED

802.11b/g Policy 802.11b/g ▼

WLAN プロファイル

ステップ2:Securityタブで、Mac Filteringチェックボックスをオンにし、許可リスト（ISEまたはローカルサーバ）でRADIUSサーバを設定します。この設定では、MAC認証とWeb認証の両方にISEを使用します。

Add WLAN

General **Security** Advanced

Layer2 Layer3 AAA

WPA + WPA2 WPA2 + WPA3 WPA3 Static WEP None

MAC Filtering

Authorization List*

network

OWE Transition Mode

Lobby Admin Access

Fast Transition

Status

Disabled

Over the DS

Reassociation Timeout *

20

WLANレイヤ2セキュリティ

ステップ3:Security > Layer3の順に移動します。Webポリシーを有効にし、Web認証パラメータマッププロファイルに関連付けます。「On Mac Filter Failure」チェックボックスにチェックマークを入れて、認証リストのドロップダウンからRADIUSサーバを選択します。

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

Web-Filter

Authentication List

ISE-List

For Local Login Method List to work, please make sure

<< Hide

On MAC Filter Failure

Splash Web Redirect

DISABLED

Preauthentication ACL

WLAN Layer3 Securityタブ

CLIでの設定

```
wlan Mac_Filtering_Wlan 9 Mac_Filtering_Wlan
mac-filtering network
radio policy dot11 24ghz
radio policy dot11 5ghz
no security ft adaptive
no security wpa
no security wpa wpa2
no security wpa wpa2 ciphers aes
no security wpa akm dot1x
security web-auth
security web-auth authentication-list ISE-List
security web-auth on-macfilter-failure
security web-auth parameter-map Web-Filter
no shutdown
```

ステップ4：ポリシータグの設定、WLANプロファイルの作成、およびポリシープロファイルマッピング

Configuration > Tags & Profiles > Tags > Policyの順に移動します。[追加]をクリックして、ポリシータグの名前を定義します。WLAN-Policy MapsでAddを選択し、以前に作成したWLANとポリシープロファイルをマッピングします。

Policy Site RF AP

+ Add × Delete Clone

Add Policy Tag

Name* default-policy-tag

Description Enter Description

▼ WLAN-POLICY Maps: 0

+ Add × Delete

WLAN Profile	Policy Profile
No items to display	

Map WLAN and Policy

WLAN Profile* Search or Select Policy Profile* Search or Select

× ✓

ポリシータグマップ

CLIによる設定：

```
wireless tag policy default-policy-tag
description "default policy-tag"
wlan Mac_Filtering_Wlan policy Web-Filter-Policy
```

ステップ5: Configuration > Wireless > Access Pointの順に移動します。このSSIDのブロードキャストを担当するアクセスポイントを選択します。Edit APメニューで、作成したPolicy Tagを割り当てます。

The screenshot shows the 'Edit AP' configuration page in a web interface. The left sidebar displays a list of 'All Access Points' with a table containing columns for 'AP Name' and 'AP Model'. The main content area is titled 'Edit AP' and has several tabs: 'General', 'Interfaces', 'High Availability', 'Inventory', 'Geolocation', 'ICap', 'Advanced', and 'Support Bundle'. The 'General' tab is active, showing fields for 'AP Name*', 'Location*', 'Base Radio MAC', 'Ethernet MAC', 'Admin Status', 'AP Mode', 'Operation Status', 'Fabric Status', and 'CleanAir NSI Key'. The 'Tags' section is highlighted with a red box and contains a 'Policy' dropdown menu set to 'default-policy-tag', along with 'Site' and 'RF' dropdowns. The 'Version' section shows 'Primary Software Version' as 17.12.2.35.

APへのポリシータグのマッピング

AAAの設定 :

ステップ1: RADIUSサーバを作成します。

Configuration > Security > AAAの順に移動します。Server/Groupセクションの下にあるAddオプションをクリックします。[Create AAA Radius Server]ページで、サーバ名、IPアドレス、および共有秘密を入力します。

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

[+ AAA Wizard](#)

Servers / Groups AAA Method List AAA Advanced

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

RADIUS **Servers** Server Groups

Create AAA Radius Server

Name*	<input type="text"/>	Support for CoA ⓘ	ENABLED <input checked="" type="checkbox"/>
Server Address*	<input type="text" value="IPv4/IPv6/Hostname"/>	CoA Server Key Type	Clear Text ▼
PAC Key	<input type="checkbox"/>	CoA Server Key ⓘ	<input type="text"/>
Key Type	Clear Text ▼	Confirm CoA Server Key	<input type="text"/>
Key* ⓘ	<input type="text"/>	Automate Tester	<input type="checkbox"/>
Confirm Key*	<input type="text"/>		
Auth Port	<input type="text" value="1812"/>		
Acct Port	<input type="text" value="1813"/>		
Server Timeout (seconds)	<input type="text" value="1-1000"/>		
Retry Count	<input type="text" value="0-100"/>		

[Cancel](#) [Apply to Device](#)

サーバの設定

CLI での設定

```
radius server ISE-Auth
address ipv4 10.197.224.122 auth-port 1812 acct-port 1813
key *****
server name ISE-Auth
```

ステップ2:RADIUSサーバグループを作成します。

Server Groupsセクションの下のAddオプションを選択して、サーバグループを定義します。同じグループ設定に含めるサーバを切り替えます。

発信元インターフェイスを設定する必要はありません。デフォルトでは、9800はルーティングテーブルを使用して、RADIUSサーバに到達するために使用するインターフェイスを特定し、通常はデフォルトゲートウェイを使用します。

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

[+ AAA Wizard](#)

[Servers / Groups](#) [AAA Method List](#) [AAA Advanced](#)

[+ Add](#) [× Delete](#)

RADIUS

[Servers](#) **Server Groups**

Create AAA Radius Server Group

Name* ! Name is required

Group Type

MAC-Delimiter

MAC-Filtering

Dead-Time (mins)

Load Balance DISABLED

Source Interface VLAN ID

Available Servers Assigned Servers

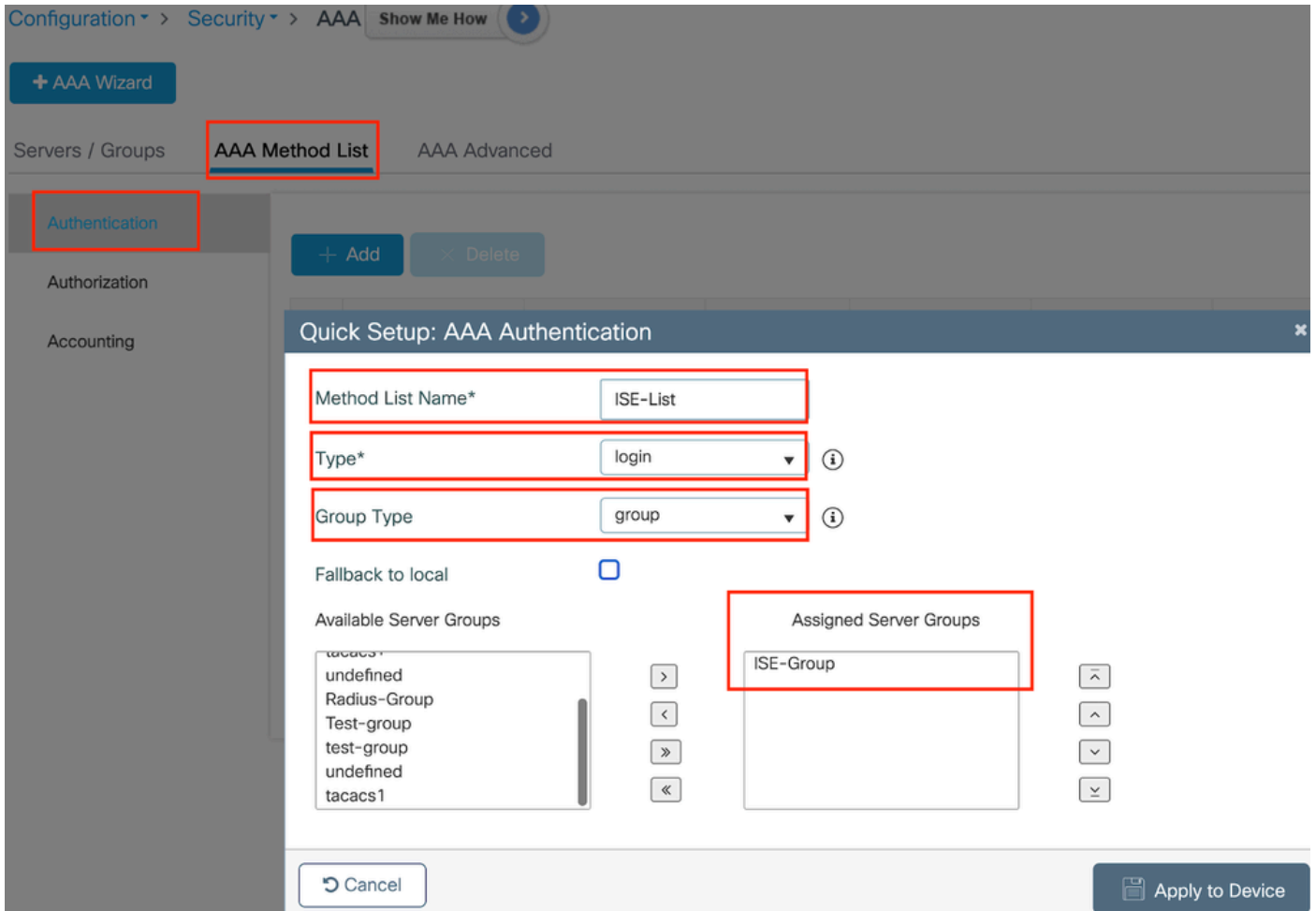
サーバグループ

CLI での設定

```
aaa group server radius ISE-Group
server name ISE-Auth
ip radius source-interface Vlan2074
deadtime 5
```

ステップ3:AAA方式リストを設定します。

AAA Method Listタブに移動します。Authenticationの下にあるAddをクリックします。Typeを「login」、Group typeを「Group」に設定して、方式リスト名を定義します。Assigned Server Groupセクションで、設定した認証サーバグループをマッピングします。



認証方式リスト

CLI での設定

```
aaa authentication login ISE-List group ISE-Group
```

Authorization Method Listセクションに移動し、Addをクリックします。方式リスト名を定義し、タイプを「network」に、グループタイプを「Group」に設定します。設定済みRADIUSサーバをAssigned Server Groupsセクションに切り替えます。

+ AAA Wizard

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

Authentication

Authorization

Accounting

+ Add × Delete

Quick Setup: AAA Authorization

Method List Name* network

Type* network ⓘ

Group Type group ⓘ

Fallback to local

Authenticated

Available Server Groups

- tacacs1
- undefined
- Radius-Group
- Test-group
- test-group
- undefined
- tacacs1

Assigned Server Groups

- ISE-Group

許可方式リスト

CLI での設定

```
aaa authorization network network group ISE-Group
```

ISE の設定 :

ISEのネットワークデバイスとしてのWLCの追加

ステップ1:Administration > Network Devicesの順に移動し、Addをクリックします。Radius Authentication Settingsで、コントローラのIPアドレス、ホスト名、および共有秘密を入力します

Network Devices

Name

Description

 IP Address * IP : / 32 

ネットワーク デバイスの追加

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol RADIUS

Shared Secret

Show

共有秘密

ステップ2 : ユーザエントリの作成

Identity Management > Identitiesの下で、Addオプションを選択します。

クライアントがWeb認証に使用する必要があるユーザ名とパスワードを設定します

✓ Network Access User

* Username

Status Enabled

Email

✓ Passwords

Password Type:

* Login Password

ユーザー資格情報の追加

ステップ3:Administration > Identity Management > Groups > Registered Devicesの順に移動し、Addをクリックします。

デバイスのMACアドレスを入力して、サーバ上にエントリを作成します。

Identities **Groups** External Identity Sources Identity Source Sequences Settings

Endpoint Identity Group List > RegisteredDevices

Endpoint Identity Group

* Name RegisteredDevices

Description Asset Registered Endpoints Identity Group

Parent Group

Identity Group Endpoints Select

+ Add Remove

MAC Address Static Group Assignment Endpoint Profile

デバイスのMACアドレスの追加

ステップ4：サービスポリシーの作成

Policy > Policy setsに移動し、「+」記号を選択して新しいポリシーセットを作成します

このポリシーセットはユーザWeb認証用で、クライアントのユーザ名とパスワードはアイデンティティ管理で作成されます

Policy Sets → User-Webauth Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	User-Webauth		Wireless_802.1X	Default Network Access	0

✓ Authentication Policy (1)

Status	Rule Name	Conditions	Use	Hits	Actions
✓	Default		Internal Users	0	

Web認証サービスポリシー

同様に、MABサービスポリシーを作成し、認証ポリシーの下に内部エンドポイントをマッピングします。

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✔	Test-MAB		Normalised Radius-RadiusFlowType EQUALS WirelessMAB	Default Network Access	0

Authentication Policy (1)

Status	Rule Name	Conditions	Use	Hits	Actions
✔	Default		Internal Endpoints	0	Options

MAB認証サービスポリシー

確認

コントローラ コンフィギュレーション

<#root>

show wireless tag policy detailed

default-policy-tag

Policy Tag Name : default-policy-tag

Description : default policy-tag

Number of WLAN-POLICY maps: 1

WLAN Profile Name	Policy Name
-------------------	-------------

Mac_Filtering_Wlan

Web-Filter-Policy

<#root>

show wireless profile policy detailed

Web-Filter-Policy

Policy Profile Name :

Web-Filter-Policy

Description :

Status :
ENABLED
VLAN :
2074
Multicast VLAN : 0

<#root>

show wlan name

Mac_Filtering_Wlan

WLAN Profile Name :

Mac_Filtering_Wlan

=====
Identifier : 9
Description :
Network Name (SSID) :

Mac_Filtering_Wlan

Status :

Enabled

Broadcast SSID :

Enabled

Mac Filter Authorization list name :

network

Webauth On-mac-filter Failure :

Enabled

Webauth Authentication List Name :

ISE-List

Webauth Authorization List Name : Disabled

Webauth Parameter Map :

Web-Filter

<#root>

show parameter-map type webauth name Web-Filter

Parameter Map Name :

Web-Filter

Type :

webauth

Auth-proxy Init State time : 120 sec
Webauth max-http connection : 100
Webauth logout-window :

Enabled

Webauth success-window :

Enabled

Consent Email : Disabled
Activation Mode : Replace
Sleeping-Client : Disabled
Webauth login-auth-bypass:

<#root>

show ip http server status

HTTP server status:

Enabled

HTTP server port:

80

HTTP server active supplementary listener ports: 21111
HTTP server authentication method: local
HTTP server auth-retry 0 time-window 0
HTTP server digest algorithm: md5
HTTP server access class: 0
HTTP server IPv4 access class: None
HTTP server IPv6 access class: None
HTTP server base path:
HTTP File Upload status: Disabled
HTTP server upload path:
HTTP server help root:
Maximum number of concurrent server connections allowed: 300
Maximum number of secondary server connections allowed: 50
Server idle time-out: 180 seconds
Server life time-out: 180 seconds
Server session idle time-out: 600 seconds
Maximum number of requests allowed on a connection: 25
Server linger time : 60 seconds
HTTP server active session modules: ALL
HTTP secure server capability: Present
HTTP secure server status:

Enabled

HTTP secure server port:

443

show ap name AP2-AIR-AP3802I-D-K9-2 tag detail


Policy tag mapping

WLAN Profile Name	Policy Name	VLAN	Flex
Mac_Filtering_Wlan	Web-Filter-Policy	2074	ENAB

コントローラのクライアントポリシーの状態


Dashboard > Clientsセクションに移動し、接続されたクライアントのステータスを確認します。
クライアントは現在Web認証保留状態です

Clients Sleeping Clients Excluded Clients

× Delete 

Selected 0 out of 1 Clients

<input type="checkbox"/>	Client MAC Address	IPv4 Address	IPv6 Address	AP Name	Slot ID	SSID	WLAN ID	Client Type	State	Protocol	User Name	Device Type
<input type="checkbox"/>	6c7e.67e3.6db9	10.76.6.150	fe80::10eb:ede2:23fe:75c3	AP2-AIR-AP3802I-D-K9-2	1	Mac_Filtering_Wlan	9	WLAN	Web Auth Pending	11ac	6c7e67e36db9	N/A

1 - 1 of 1 clients 

クライアントの詳細

```
show wireless client summary
```

```
Number of Clients: 1
```

MAC Address	AP Name	Type	ID	State	Protocol	Method
6c7e.67e3.6db9	AP2-AIR-AP3802I-D-K9-2	WLAN	9	Webauth Pending	11ac	Web

```
<#root>
```

```
show wireless client mac-address 6c7e.67e3.6db9 detail
```

```
Client MAC Address :
```

```
6c7e.67e3.6db9
```

```
Client MAC Type : Universally Administered Address
```

```
Client DUID: NA
```

```
Client IPv4 Address :
```

```
10.76.6.150
```

```
Client IPv6 Addresses : fe80::10eb:ede2:23fe:75c3
```

```
Client Username :
```

```
6c7e67e36db9
```

```
AP MAC Address : 1880.902b.05e0
```

```
AP Name: AP2-AIR-AP3802I-D-K9-2
```

```
AP slot : 1
```

```
Client State : Associated
```

```
Policy Profile :
```

```
Web-Filter-Policy
```

```
Flex Profile : N/A
```

```
Wireless LAN Id: 9
WLAN Profile Name:

Mac_Filtering_Wlan

Wireless LAN Network Name (SSID): Mac_Filtering_Wlan
BSSID : 1880.902b.05eb

Client ACLs : None
Mac authentication :

Failed

Policy Manager State:

Webauth Pending

Last Policy Manager State :

IP Learn Complete

Client Entry Create Time : 88 seconds
Policy Type : N/A
Encryption Cipher : None

Auth Method Status List
    Method: Web Auth
        Webauth State      :

Get Redirect

        Webauth Method    :

Webauth
```

Web認証に成功すると、クライアントポリシーマネージャの状態はRUNに移行します

```
<#root>
```

```
show wireless client mac-address 6c7e.67e3.6db9 detail
```

```
Client ACLs : None
Mac authentication : Failed
Policy Manager State:

Run

Last Policy Manager State :

Webauth Pending

Client Entry Create Time : 131 seconds
Policy Type : N/A
```

トラブルシューティング

MAC障害時のWeb認証機能の機能は、MABの障害時にWeb認証をトリガーするコントローラ機能に依存しています。主な目的は、トラブルシューティングと分析のためにコントローラからRAT

レースを効率的に収集することです。

放射能レースの収集

CLIで指定したMACアドレスのクライアントデバッグレースを生成するには、無線アクティブレースをアクティブにします。

放射性レースを有効にする手順：

すべての条件付きデバッグが無効になっていることを確認します

```
clear platform condition all
```

指定したMACアドレスのデバッグを有効にする

```
debug wireless mac <H.H.H> monitor-time <Time in seconds>
```

問題を再現したら、デバッグを無効にしてRAレース収集を停止します。

```
no debug wireless mac <H.H.H>
```

RAレースが停止すると、コントローラブートフラッシュにデバッグファイルが生成されます。

```
show bootflash: | include ra_trace  
2728          179 Jul 17 2024 15:13:54.0000000000 +00:00 ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_Da
```

ファイルを外部サーバにコピーします。

```
copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://<IP address>
```

デバッグログを表示します。

```
more bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```


GUIでRAトレースを有効にします。

ステップ1：トラブルシューティング>放射性トレースに移動します。新しいエントリを追加するオプションを選択し、指定されたAdd MAC/IP AddressタブにクライアントのMACアドレスを入力します。

The screenshot shows the 'Radioactive Trace' interface. At the top, it says 'Troubleshooting > Radioactive Trace'. Below that, a status bar indicates 'Conditional Debug Global State: Started'. There are four buttons: '+ Add' (highlighted with a red box), '× Delete', '✓ Start', and '■ Stop'. To the right, there is a 'Wireless Deb' gear icon and a 'Last Run' label. A dialog box titled 'Add MAC/IP Address' is open, with a red box around the 'MAC/IP Address*' label. The dialog contains a text area with the instruction 'Enter a MAC/IP Address every newline'. At the bottom of the dialog, there is a 'Cancel' button and an 'Apply to Device' button (highlighted with a red box).

ラジオアクティブトレース

組み込みパケットキャプチャ：

Troubleshooting > Packet Captureに移動します。キャプチャ名を入力し、クライアントのMACアドレスを内部フィルタMACとして指定します。バッファサイズを100に設定し、着信パケットと発信パケットを監視するアップリンクインターフェイスを選択します。

+ Add × Delete

Create Packet Capture

Capture Name* TestPCap

Filter* any

Monitor Control Plane

Inner Filter Protocol DHCP

Inner Filter MAC

Buffer Size (MB)* 100

Limit by* Duration 3600 secs ≈ 1.00 hour

Available (12) Search

- Tw0/0/1
- Tw0/0/2
- Tw0/0/3
- Te0/1/0

Selected (1)

- Tw0/0/0



注：システムCPUにリダイレクトされ、データプレーンに再注入されたトラフィックを表示するには、「コントロールトラフィックの監視」オプションを選択します。

パケットをキャプチャするにはStartを選択します

Capture Name	Interface	Monitor Control Plane	Buffer Size	Filter by	Limit	Status	Action
<input type="checkbox"/> TestPCap	TwoGigabitEthernet0/0/0	No	0%	any	3600 secs	Inactive	<input type="button" value="Start"/>

キャプチャの開始

CLI での設定

```
monitor capture TestPCap inner mac <H.H.H>
monitor capture TestPCap buffer size 100
monitor capture TestPCap interface twoGigabitEthernet 0/0/0 both
monitor capture TestPCap start
```

<Reproduce the issue>

```
monitor capture TestPCap stop
```

```
show monitor capture TestPCap
```

Status Information for Capture TestPCap

Target Type:

Interface: TwoGigabitEthernet0/0/0, Direction: BOTH

Status : Inactive

Filter Details:

Capture all packets

Inner Filter Details:

Mac: 6c7e.67e3.6db9

Continuous capture: disabled

Buffer Details:

Buffer Type: LINEAR (default)

Buffer Size (in MB): 100

Limit Details:

Number of Packets to capture: 0 (no limit)

Packet Capture duration: 3600

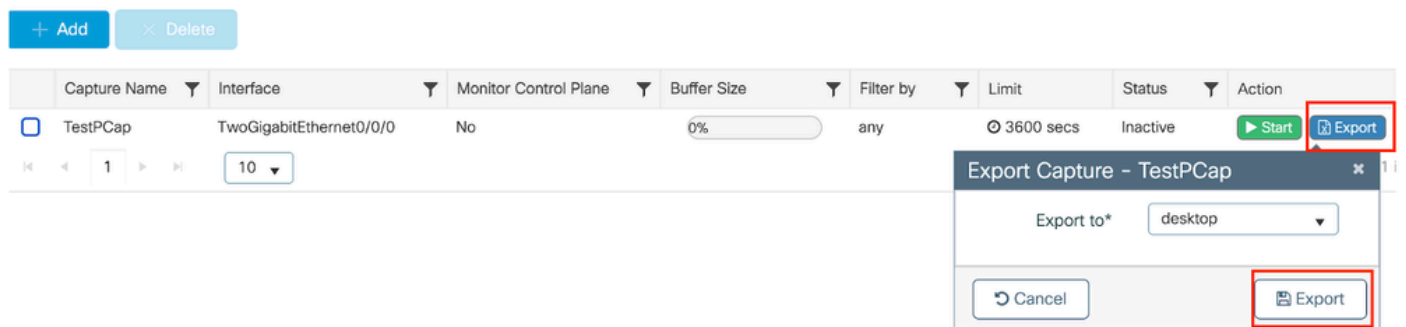
Packet Size to capture: 0 (no limit)

Maximum number of packets to capture per second: 1000

Packet sampling rate: 0 (no sampling)

外部TFTPサーバへのパケットキャプチャのエクスポート

```
monitor capture TestPCap export tftp://<IP address>/ TestPCap.pcap
```



パケットキャプチャのエクスポート

サンプルシナリオMAC認証が成功すると、クライアントデバイスがネットワークに接続し、そのMACアドレスが設定されたポリシーを通じてRADIUSサーバによって検証され、検証の際にネットワークアクセスデバイスによってアクセスが許可されて、ネットワーク接続が可能になります。

クライアントが関連付けられると、コントローラはISEサーバにアクセス要求を送信します。

User nameはクライアントのMACアドレスで、これはMAB認証です。

```
2024/07/16 21:12:52.711298748 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Send Access-Request t
2024/07/16 21:12:52.711310730 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: authenticator 19 c6
2024/07/16 21:12:52.711326401 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: User-Name
2024/07/16 21:12:52.711329615 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: User-Password
2024/07/16 21:12:52.711337331 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Service-Type
2024/07/16 21:12:52.711340443 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Vendor, Cisco
2024/07/16 21:12:52.711344513 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Cisco AVpair
2024/07/16 21:12:52.711349087 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Framed-MTU
2024/07/16 21:12:52.711351935 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Message-Authenticato
2024/07/16 21:12:52.711377387 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: EAP-Key-Name
2024/07/16 21:12:52.711382613 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Vendor, Cisco
2024/07/16 21:12:52.711385989 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Cisco AVpair
```

有効なユーザエントリがあるため、ISEはAccess-Acceptを送信します。

```
2024/07/16 21:12:52.779147404 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Received from id 1812
2024/07/16 21:12:52.779156117 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: authenticator 5d dc
2024/07/16 21:12:52.779161793 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: User-Name
2024/07/16 21:12:52.779165183 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Class
2024/07/16 21:12:52.779219803 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Message-Authenticato
```

```
2024/07/16 21:12:52.779417578 {wncd_x_R0-0}{1}: [mab] [17765]: (info): [6c7e.67b7.2d29:capwap_90000005]
2024/07/16 21:12:52.779436247 {wncd_x_R0-0}{1}: [mab] [17765]: (info): [6c7e.67b7.2d29:capwap_90000005]
```

クライアントポリシーの状態がMac認証に移行しました

```
2024/07/16 21:12:52.780181486 {wncd_x_R0-0}{1}: [client-auth] [17765]: (info): MAC: 6c7e.67b7.2d29 Cli
2024/07/16 21:12:52.780238297 {wncd_x_R0-0}{1}: [client-orch-sm] [17765]: (debug): MAC: 6c7e.67b7.2d29
```

MAB認証が成功した後、クライアントがIPラーニングステートになる

```
2024/07/16 21:12:55.791404789 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: 6c7e.67b7.2d29
2024/07/16 21:12:55.791739386 {wncd_x_R0-0}{1}: [client-iplearn] [17765]: (info): MAC: 6c7e.67b7.2d29
```

```
2024/07/16 21:12:55.794130301 {iosrp_R0-0}{1}: [buginf] [4440]: (debug): AUTH-FEAT-SISF-EVENT: IP updat
```

クライアントポリシーマネージャの状態がRUNに更新され、MAB認証を完了するクライアントのWeb認証がスキップされる

2024/07/16 21:13:11.210786952 {wncd_x_R0-0}{1}: [errmsg] [17765]: (info): %CLIENT_ORCH_LOG-6-CLIENT_ADD

組み込みパケットキャプチャを使用した検証

No.	Time	Source	Destination	Length	Protocol	Info
53	02:42:52.710961	10.76.6.156	10.197.224.122		RADIUS	Access-Request id=0
54	02:42:52.778951	10.197.224.122	10.76.6.156		RADIUS	Access-Accept id=0

Frame 53: 464 bytes on wire (3712 bits), 464 bytes captured (3712 bits)
Ethernet II, Src: Cisco_58:42:4b (f4:bd:9e:58:42:4b), Dst: Cisco_34:90:e7 (6c:5e:3b:34:90:e7)
Internet Protocol Version 4, Src: 10.76.6.156, Dst: 10.197.224.122
User Datagram Protocol, Src Port: 65433, Dst Port: 1812
RADIUS Protocol
Code: Access-Request (1)
Packet identifier: 0x0 (0)
Length: 422
Authenticator: 19c6635633a7e6b6f30070b02a7f753c
[\[The response to this request is in frame 54\]](#)
Attribute Value Pairs
AVP: t=User-Name(1) l=14 val=6c7e67b72d29
AVP: t=User-Password(2) l=18 val=Encrypted
AVP: t=Service-Type(6) l=6 val=Call-Check(10)
AVP: t=Vendor-Specific(26) l=31 vnd=ciscoSystems(9)
AVP: t=Framed-MTU(12) l=6 val=1485

Radiusパケット

クライアントデバイスのMAC認証が失敗する例

アソシエーションが成功した後にクライアントに対して開始されたMAC認証

2024/07/17 03:20:59.842211775 {wncd_x_R0-0}{1}: [mab] [17765]: (info): [6c7e.67e3.6db9:capwap_90000005]
2024/07/17 03:20:59.842280253 {wncd_x_R0-0}{1}: [ewlc-infra-evq] [17765]: (note): Authentication Success
2024/07/17 03:20:59.842284313 {wncd_x_R0-0}{1}: [client-auth] [17765]: (info): MAC: 6c7e.67e3.6db9 Cl
2024/07/17 03:20:59.842320572 {wncd_x_R0-0}{1}: [mab] [17765]: (info): [6c7e.67e3.6db9:capwap_90000005]

このデバイスエントリがISEに存在しないため、ISEはアクセス拒否を送信します

2024/07/17 03:20:59.842678322 {wncd_x_R0-0}{1}: [mab] [17765]: (info): [6c7e.67e3.6db9:capwap_90000005]
2024/07/17 03:20:59.842877636 {wncd_x_R0-0}{1}: [auth-mgr] [17765]: (info): [6c7e.67e3.6db9:capwap_9000

MABが失敗したため、クライアントデバイスに対して開始されたWeb認証

2024/07/17 03:20:59.843728206 {wncd_x_R0-0}{1}: [client-auth] [17765]: (info): MAC: 6c7e.67e3.6db9 Cl

クライアントがHTTP GET要求を開始すると、対応するTCPセッションがコントローラによってスプーフィングされるため、リダイレクトURLがクライアントデバイスにプッシュされます。

2024/07/17 03:21:37.817434046 {wncd_x_R0-0}{1}: [webauth-httpd] [17765]: (info): capwap_90000005[6c7e.6
2024/07/17 03:21:37.817459639 {wncd_x_R0-0}{1}: [webauth-httpd] [17765]: (debug): capwap_90000005[6c7e.
2024/07/17 03:21:37.817466483 {wncd_x_R0-0}{1}: [webauth-httpd] [17765]: (debug): capwap_90000005[6c7e.
2024/07/17 03:21:37.817482231 {wncd_x_R0-0}{1}: [webauth-state] [17765]: (info): capwap_90000005[6c7e.6

クライアントはリダイレクトURLへのHTTP Getを開始し、ページがロードされるとログインクレデンシャルが送信されます。

コントローラがISEにアクセス要求を送信します

これは、Access-Acceptパケットで有効なユーザ名が確認されるWeb認証です

2024/07/17 03:22:51.132347799 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Send Access-Request t
2024/07/17 03:22:51.132362949 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: authenticator fd 40
2024/07/17 03:22:51.132368737 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Calling-Station-Id
2024/07/17 03:22:51.132372791 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: User-Name
2024/07/17 03:22:51.132376569 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Vendor, Cisco

ISEから受信したAccess-Accept

2024/07/17 03:22:51.187040709 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Received from id 1812
2024/07/17 03:22:51.187050061 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: authenticator d3 ac
2024/07/17 03:22:51.187055731 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: User-Name
2024/07/17 03:22:51.187059053 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Class
2024/07/17 03:22:51.187102553 {wncd_x_R0-0}{1}: [radius] [17765]: (info): RADIUS: Message-Authenticato

Web認証が成功し、クライアントの状態がRUN状態に移行します。

2024/07/17 03:22:51.193775717 {wncd_x_R0-0}{1}: [errmsg] [17765]: (info): %CLIENT_ORCH_LOG-6-CLIENT_ADD
2024/07/17 03:22:51.194009423 {wncd_x_R0-0}{1}: [client-orch-state] [17765]: (note): MAC: 6c7e.67e3.6db

EPCキャプチャによる検証

クライアントはコントローラの仮想IPアドレスを使用してTCPハンドシェイクを完了し、クライ

アントはリダイレクトポータルページをロードします。ユーザがユーザ名とパスワードを送信すると、コントローラ管理IPアドレスからのRADIUSアクセス要求を確認できます。

認証が成功すると、クライアントのTCPセッションが閉じられ、コントローラ上でクライアントがRUN状態に移行します。

15649	08:52:51.122979	10.76.6.150	192.0.2.1	TCP	58832 → 443 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1250 WS=64 TSval=4022788869 TSecr=0 SACK_PERM
15650	08:52:51.123986	192.0.2.1	10.76.6.150	TCP	443 → 58832 [SYN, ACK, ECE] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3313564363 TSecr=402
15651	08:52:51.125985	10.76.6.150	192.0.2.1	TCP	58832 → 443 [ACK] Seq=1 Ack=1 Win=131200 Len=0 TSval=4022788871 TSecr=3313564363
15652	08:52:51.126992	10.76.6.150	192.0.2.1	512	TLV1.2 Client Hello
15653	08:52:51.126992	192.0.2.1	10.76.6.150	TCP	443 → 58832 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=3313564366 TSecr=4022788871
15654	08:52:51.126992	192.0.2.1	10.76.6.150	85,1,64	TLV1.2 Server Hello, Change Cipher Spec, Encrypted Handshake Message
15655	08:52:51.129982	10.76.6.150	192.0.2.1	TCP	58832 → 443 [ACK] Seq=518 Ack=166 Win=131008 Len=0 TSval=4022788876 TSecr=3313564367
15656	08:52:51.129982	10.76.6.150	192.0.2.1	1,64	TLV1.2 Change Cipher Spec, Encrypted Handshake Message
15657	08:52:51.130989	10.76.6.150	192.0.2.1	640	TLV1.2 Application Data
15658	08:52:51.130989	10.76.6.150	192.0.2.1	160	TLV1.2 Application Data
15659	08:52:51.130989	192.0.2.1	10.76.6.150	TCP	443 → 58832 [ACK] Seq=166 Ack=1403 Win=64000 Len=0 TSval=3313564371 TSecr=4022788876
15660	08:52:51.131981	10.76.6.156	10.197.224.122	RADIUS	Access-Request id=3
15663	08:52:51.186986	10.197.224.122	10.76.6.156	RADIUS	Access-Accept id=3
15665	08:52:51.191976	192.0.2.1	10.76.6.150	TCP	443 → 58832 [ACK] Seq=166 Ack=1403 Win=64128 Len=948 TSval=3313564432 TSecr=4022788876 [TCP segment o
15666	08:52:51.191976	192.0.2.1	10.76.6.150	TCP	443 → 58832 [ACK] Seq=1114 Ack=1403 Win=64128 Len=948 TSval=3313564432 TSecr=4022788876 [TCP segment i
15667	08:52:51.191976	192.0.2.1	10.76.6.150	2496	TLV1.2 Application Data
15668	08:52:51.192983	192.0.2.1	10.76.6.150	48	TLV1.2 Encrypted Alert
15673	08:52:51.196980	10.76.6.150	192.0.2.1	TCP	58832 → 443 [ACK] Seq=1403 Ack=2667 Win=128512 Len=0 TSval=4022788942 TSecr=3313564432
15674	08:52:51.196980	10.76.6.150	192.0.2.1	TCP	58832 → 443 [ACK] Seq=1403 Ack=2721 Win=128512 Len=0 TSval=4022788942 TSecr=3313564432
15675	08:52:51.196980	10.76.6.150	192.0.2.1	TCP	[TCP Window Update] 58832 → 443 [ACK] Seq=1403 Ack=2721 Win=131072 Len=0 TSval=4022788942 TSecr=331356
15676	08:52:51.197987	10.76.6.150	192.0.2.1	48	TLV1.2 Encrypted Alert
15677	08:52:51.197987	10.76.6.150	192.0.2.1	TCP	58832 → 443 [FIN, ACK] Seq=1456 Ack=2721 Win=131072 Len=0 TSval=4022788942 TSecr=3313564432
15678	08:52:51.197987	192.0.2.1	10.76.6.150	TCP	443 → 58832 [RST] Seq=2721 Win=0 Len=0
15679	08:52:51.197987	192.0.2.1	10.76.6.150	TCP	443 → 58832 [RST] Seq=2721 Win=0 Len=0

RADIUSパケットを使用したTCPフロー

15660	08:52:51.131981	10.76.6.156	10.197.224.122	RADIUS	Access-Request id=3
15663	08:52:51.186986	10.197.224.122	10.76.6.156	RADIUS	Access-Accept id=3

Frame 15660: 499 bytes on wire (3992 bits), 499 bytes captured (3992 bits)
 Ethernet II, Src: Cisco_58:42:4b (f4:bd:9e:58:42:4b), Dst: Cisco_34:90:e7 (6c:5e:3b:34:90:e7)
 Internet Protocol Version 4, Src: 10.76.6.156, Dst: 10.197.224.122
 User Datagram Protocol, Src Port: 65433, Dst Port: 1812
 RADIUS Protocol

- Code: Access-Request (1)
- Packet identifier: 0x3 (3)
- Length: 457
- Authenticator: fd400f7e3567dc5a63cfefaef379eaa
- [The response to this request is in frame 15663]
- Attribute Value Pairs
 - AVP: t=Calling-Station-Id(31) l=19 val=6c-7e-67-e3-6d-b9
 - AVP: t=User-Name(1) l=10 val=testuser
 - AVP: t=Vendor-Specific(26) l=49 vnd=ciscoSystems(9)
 - AVP: t=Framed-IP-Address(8) l=6 val=10.76.6.150
 - AVP: t=Message-Authenticator(80) l=18 val=501b124c30216ef5973086d99f3a185
 - > AVP: t=Service-Type(6) l=6 val=Dialout-Framed-User(5)
 - > AVP: t=Vendor-Specific(26) l=29 vnd=ciscoSystems(9)
 - > AVP: t=Vendor-Specific(26) l=22 vnd=ciscoSystems(9)
 - > AVP: t=User-Password(2) l=18 val=Encrypted

ユーザクレデンシャルとともにISEに送信されるRADIUSパケット

クライアントトラフィックを検証するためのクライアント側のWiresharkキャプチャがポータルページにリダイレクトされ、コントローラの仮想IPアドレス/WebサーバへのTCPハンドシェイクを検証します。

Time	Source	Destination	Length	Protocol	Info
105	08:51:34.203945	10.76.6.150	10.76.6.145	HTTP	GET /auth/discovery?architecture=9 HTTP/1.1
108	08:51:34.206602	10.76.6.145	10.76.6.150	HTTP	HTTP/1.1 200 OK (text/html)
234	08:51:39.028084	10.76.6.150	7.7.7.7	HTTP	GET / HTTP/1.1
236	08:51:39.031420	7.7.7.7	10.76.6.150	HTTP	HTTP/1.1 200 OK (text/html)

Frame 108: 703 bytes on wire (5624 bits), 703 bytes captured (5624 bits) on interface en0, id 0
 Ethernet II, Src: Cisco_34:90:e7 (6c:5e:3b:34:90:e7), Dst: Apple_e3:6d:b9 (6c:7e:67:e3:6d:b9)
 Internet Protocol Version 4, Src: 10.76.6.145, Dst: 10.76.6.150
 Transmission Control Protocol, Src Port: 80, Dst Port: 58811, Seq: 1, Ack: 107, Len: 637

Hypertext Transfer Protocol

Line-based text data: text/html (9 lines)

```
<HTML><meta http-equiv="Content-Type" content="text/html; charset=utf-8" name="viewport" content="width=device-width, initial-scale=1">\n
<HEAD>\n
<TITLE> Web Authentication Redirect</TITLE>\n
<META http-equiv="Cache-control" content="no-cache">\n
<META http-equiv="Pragma" content="no-cache">\n
<META http-equiv="Expires" content="-1">\n
<META http-equiv="refresh" content="1; URL=https://192.0.2.1/login.html?redirect=http://10.76.6.145/auth/discovery?architecture=9">\n
</HEAD>\n
</HTML>
```

リダイレクトURLを検証するためのクライアント側キャプチャ

クライアントがコントローラの仮想IPアドレスへのTCPハンドシェイクを確立する

Time	Source	Destination	Length	Protocol	Info
115	08:51:34.208377	10.76.6.150	192.0.2.1	TCP	58812 → 443 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=3224314628 TSecr=0 SACK_PERM
117	08:51:34.211190	192.0.2.1	10.76.6.150	TCP	443 → 58812 [SYN, ACK, ECE] Seq=0 Ack=1 Win=65160 Len=0 MSS=1250 SACK_PERM TSval=3313491061 TSecr=0
118	08:51:34.211275	10.76.6.150	192.0.2.1	TCP	58812 → 443 [ACK] Seq=1 Ack=1 Win=131200 Len=0 TSval=3224314631 TSecr=3313491061
120	08:51:34.212673	10.76.6.150	192.0.2.1	512	TLSv1.2 Client Hello
122	08:51:34.217896	192.0.2.1	10.76.6.150	TCP	443 → 58812 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=3313491066 TSecr=3224314632
124	08:51:34.220834	192.0.2.1	10.76.6.150	89,830	TLSv1.2 Server Hello, Certificate
125	08:51:34.220835	192.0.2.1	10.76.6.150	783,4	TLSv1.2 Server Key Exchange, Server Hello Done

クライアントとWebサーバ間のTCPハンドシェイク

Web認証が成功した後、セッションが閉じられました。

144	08:51:34.235915	10.76.6.150	192.0.2.1	TCP	[TCP Window Update] 58812 → 443 [ACK] Seq=1145 Ack=10183 Win=131072 Len=0 TSval=3224314655 TSecr=0
145	08:51:34.235996	10.76.6.150	192.0.2.1	52	TLSv1.2 Encrypted Alert
146	08:51:34.236029	10.76.6.150	192.0.2.1	TCP	58812 → 443 [FIN, ACK] Seq=1202 Ack=10183 Win=131072 Len=0 TSval=3224314655 TSecr=3313491084
147	08:51:34.238965	192.0.2.1	10.76.6.150	52	TLSv1.2 Encrypted Alert
148	08:51:34.238966	192.0.2.1	10.76.6.150	TCP	443 → 58812 [FIN, ACK] Seq=10240 Ack=1203 Win=64256 Len=0 TSval=3313491089 TSecr=3224314655

クライアントがWeb認証を完了した後にTCPセッションが閉じられた

関連情報

[Catalyst 9800ワイヤレスLANコントローラでのワイヤレスデバッグとログ収集について](#)

[9800でのWebベース認証](#)

[9800でのローカルWeb認証の設定](#)

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。