AireOSコントローラを使用したDNAスペースキャプティブポータルの設定例

内容

概要

このドキュメントでは、AireOSコントローラでCisco DNAスペースを使用してキャプティブポータルを設定する方法について説明します。

著者：Cisco TACエンジニア、Andres Silva

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。

- ワイヤレスコントローラへのコマンドラインインターフェイス(CLI)またはグラフィックユーザインターフェイス(GUI)アクセス
- Cisco DNA Spaces

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。

- 5520ワイヤレスLANコントローラバージョン8.10.112.0

設定

ネットワーク図

設定

WLCをCisco DNA Spaceに接続する

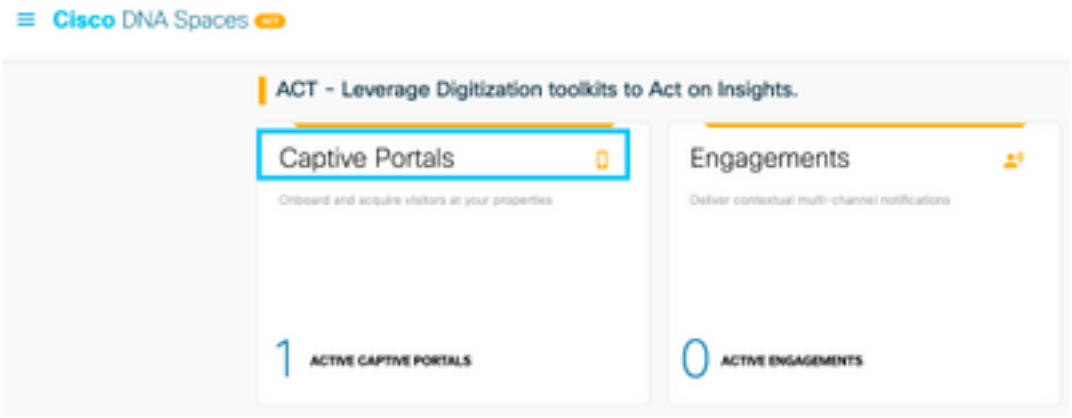
コントローラは、使用可能なセットアップ（Direct Connect、DNA Spaces Connector経由、またはCMXテザリングを使用）のいずれかを使用して、DNAスペースに接続する必要があります。

この例では、[Direct Connect]オプションが使用されていますが、キャプティブポータルはすべての設定に対して同じ方法で設定されています。

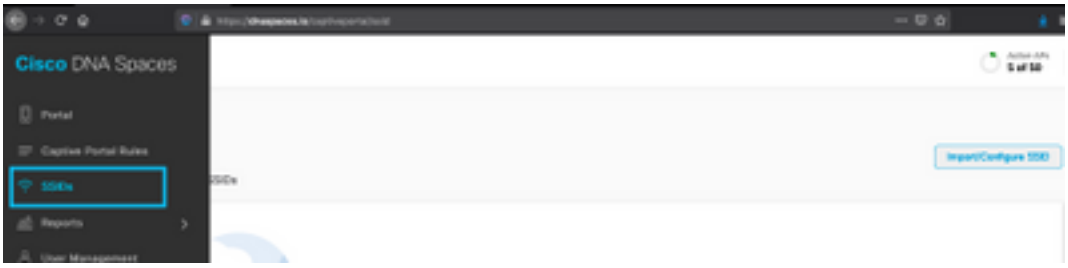
コントローラをCisco DNA Spacesに接続するには、HTTPS経由でCisco DNA Spacesクラウドに到達できる必要があります。コントローラをDNAスペースに接続する方法の詳細については、『DNAスペースダイレクトコネクトの設定例』を参照してください。

DNAスペースでのSSIDの作成

ステップ 1：DNA Spacesのダッシュボードで[Captive Portals] をクリックします。



ステップ 2：ページの左上隅にある3行のアイコンをクリックしてキャプティブポータルメニューを開き、[**SSIDs:**

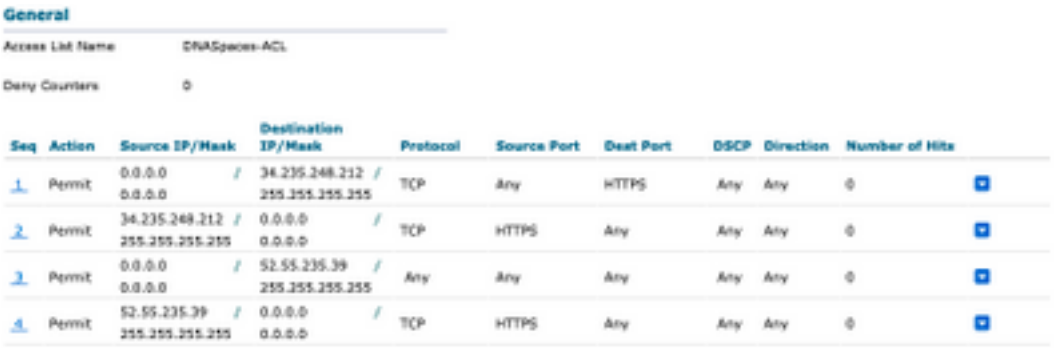


ステップ 3：[Import/Configure SSID] をクリックし、[Wireless Network]タイプとして[CUWN (CMX/WLC)] を選択し、SSID名を入力します。

コントローラでのACLの設定

Web認証SSIDであるため、事前認証ACLが必要です。ワイヤレスデバイスがSSIDに接続してIPアドレスを受け取るとすぐに、デバイスのPolicy Manager状態が**Webauth_Reqd**状態に移行し、ACLがクライアントセッションに適用されて、デバイスが到達できるリソースが制限されます。

ステップ 1：[Security] > [Access Control Lists] > [Access Control Lists] に移動し、[New] をクリックして、ワイヤレスクライアント間でDNA空間への通信を許可するルールを次のように設定します。IPアドレスを、使用中のアカウントのDNAスペースから与えられたIPアドレスに置き換えます。



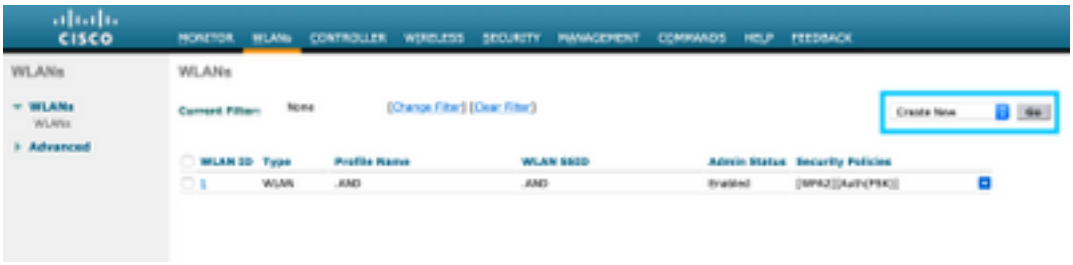
> **注**:ACLで許可されるDNAスペースのIPアドレスを取得するには、「ACL設定」セクションの「**DNAスペースでのSSIDの作成**」セクションのステップ3で作成したSSIDから、[Configure Manually] オプションをクリックします。

SSIDは、RADIUSサーバを使用するように設定することも、使用せずに設定することもできます。キャプティブポータルルール設定の[Actions] セクションで[Session Duration]、[Bandwidth Limit]、または[Seamently Provision Internet]が設定されている場合は、SSIDをRADIUSサーバで設定する必要があります。そうでない場合は、RADIUSサーバを使用する必要はありません。DNAスペース上のすべての種類のポータルは、両方の構成でサポートされています。

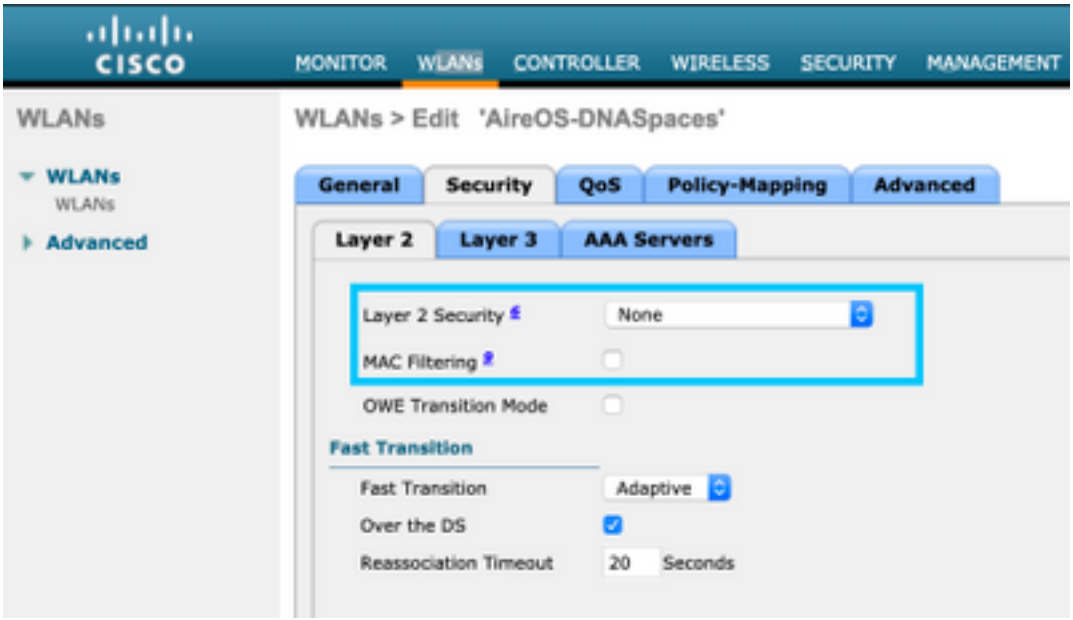
DNAスペース上のRADIUSサーバを使用しないキャプティブポータル

コントローラでのSSID設定

ステップ 1：[WLAN] > [WLANs] に移動します。新規 WLAN を作成してください。プロファイル名とSSIDを設定します。SSID名が、「**DNAスペースでのSSIDの作成**」セクションのステップ3で設定したものと同じであることを確認します。



ステップ 2：レイヤ2セキュリティを設定します。WLAN設定タブで**Security > Layer 2**タブに移動し、Layer 2 Securityのドロップダウンメニューから**None**を選択します。MACフィルタリングが無効になっていることを確認します。



ステップ 3：レイヤ3セキュリティを設定します。[WLAN configuration]タブで[Security] > [Layer 3] タブに移動し、レイヤ3セキュリティ方式として[Web **Policy]を設定し、[Enable]** パススルーを設定し、事前認証ACLを設定し、[Override Global Config] を[Web Auth Type] に[External] を設定し、リダイレクトURLを設定します。

注：リダイレクトURLを取得するには、[Configure Manually] オプションをクリックします。このオプションは、[SSID configuration]セクションの[Create the SSID on DNA Spaces] セクションのステップ3で作成したSSIDから選択します。

DNAスペース上のRADIUSサーバを使用したキャプティブポータル

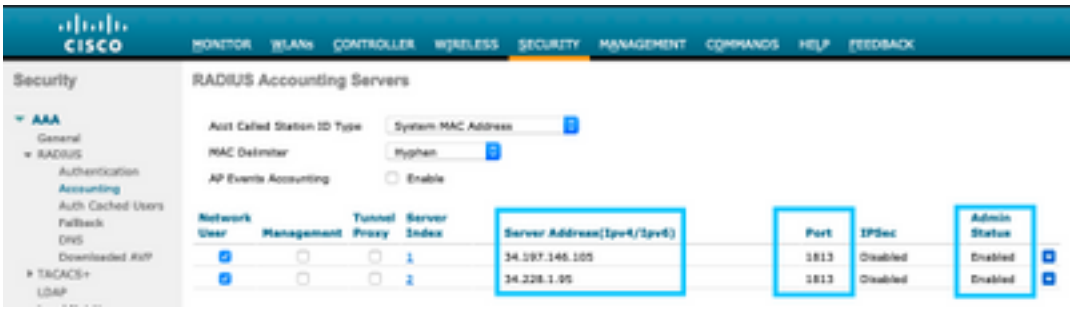
注:DNAスペースRADIUSサーバは、コントローラからのPAP認証のみをサポートします。

コントローラでのRADIUSサーバの設定

ステップ 1：[Security] > [AAA] > [RADIUS] > [Authentication] に移動し、[New] をクリックしてRADIUSサーバ情報を入力します。Cisco DNA Spacesは、ユーザ認証のためにRADIUSサーバとして機能し、2つのIPアドレスで応答できます。両方のRADIUSサーバを設定します。

注：プライマリサーバとセカンダリサーバの両方のRADIUS IPアドレスと秘密キーを取得するには、「**DNAスペースでのSSIDの作成**」セクションのステップ3で作成したSSIDから [Configure Manually] オプションをクリックし、[RADIUS Server Configuration] セクションに移動します。

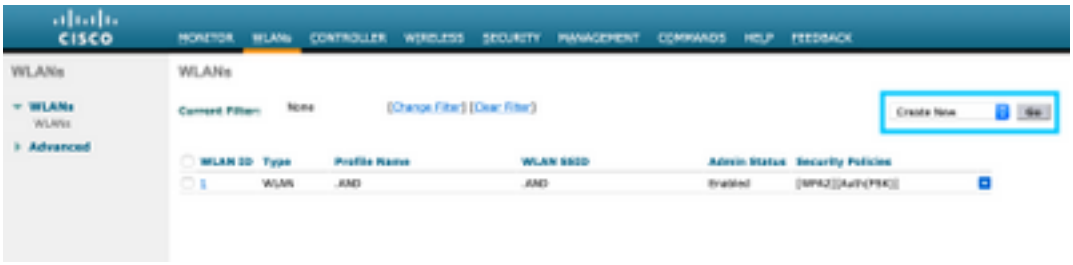
ステップ 2：アカウンティングRADIUSサーバを設定します。[Security] > [AAA] > [RADIUS] > [Accounting] に移動し、[New] をクリックします。同じ両方のRADIUSサーバを設定します。



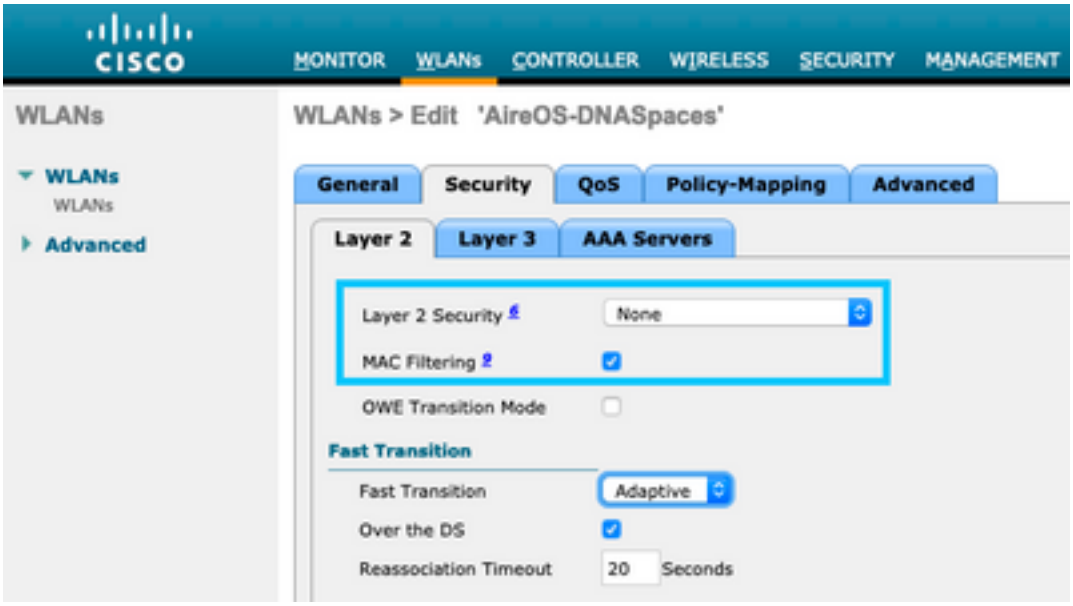
コントローラでのSSID設定

重要:SSID設定を開始する前に、[Controller] > [General]で[Web Radius Authentication] が[PAP]に設定されていることを確認してください。

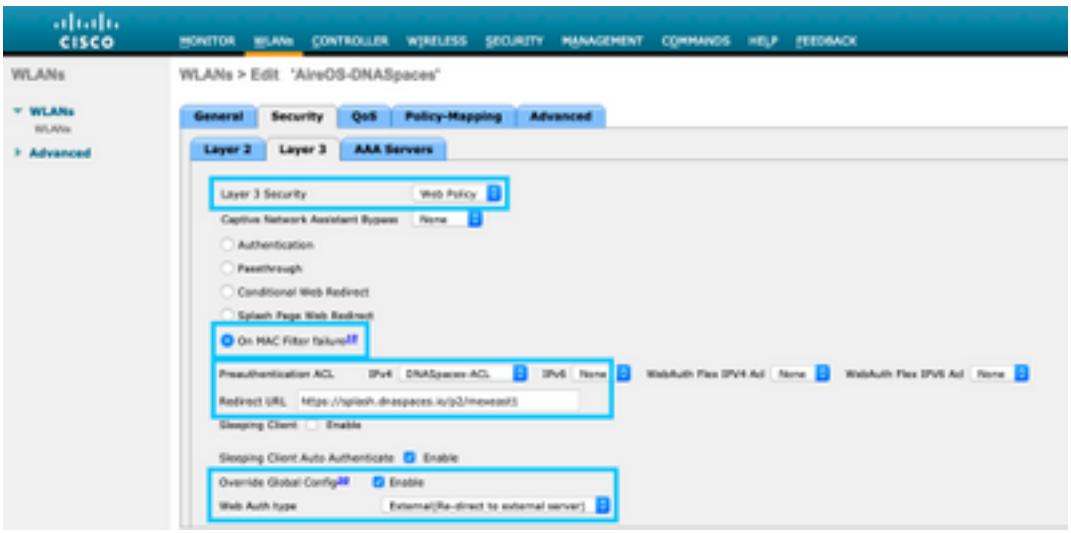
ステップ 1：[WLAN] > [WLANs] に移動します。新規 WLAN を作成してください。プロファイル名とSSIDを設定します。SSID名が、「**DNAスペースでのSSIDの作成**」セクションのステップ3で設定したものと同じであることを確認します。



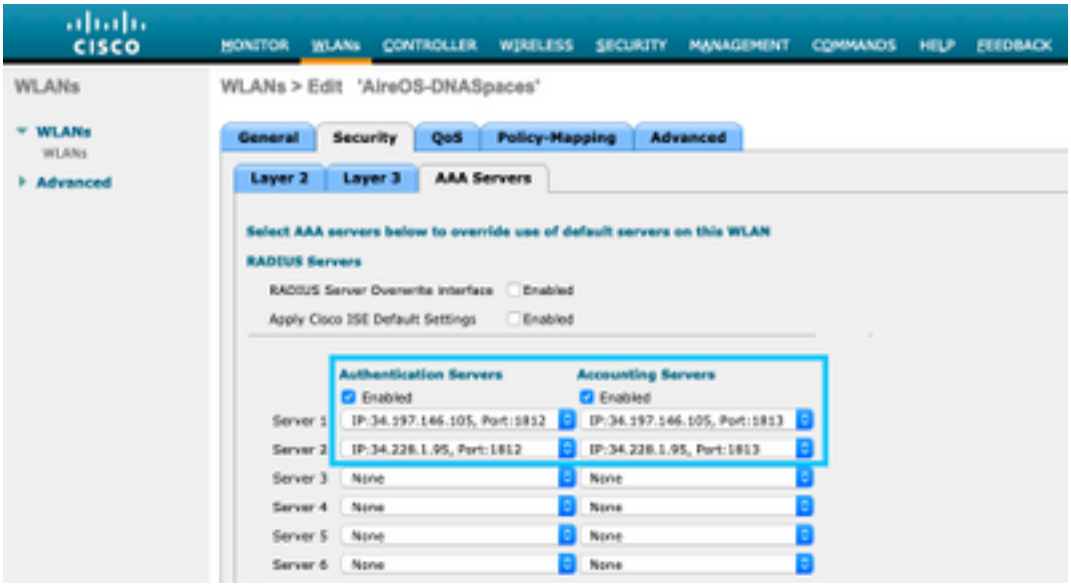
ステップ 2：レイヤ2セキュリティを設定します。[WLAN configuration]タブで[Security] > [Layer 2] タブに移動します。レイヤ2セキュリティを[None] に設定します。MAC フィルタリングの有効化.



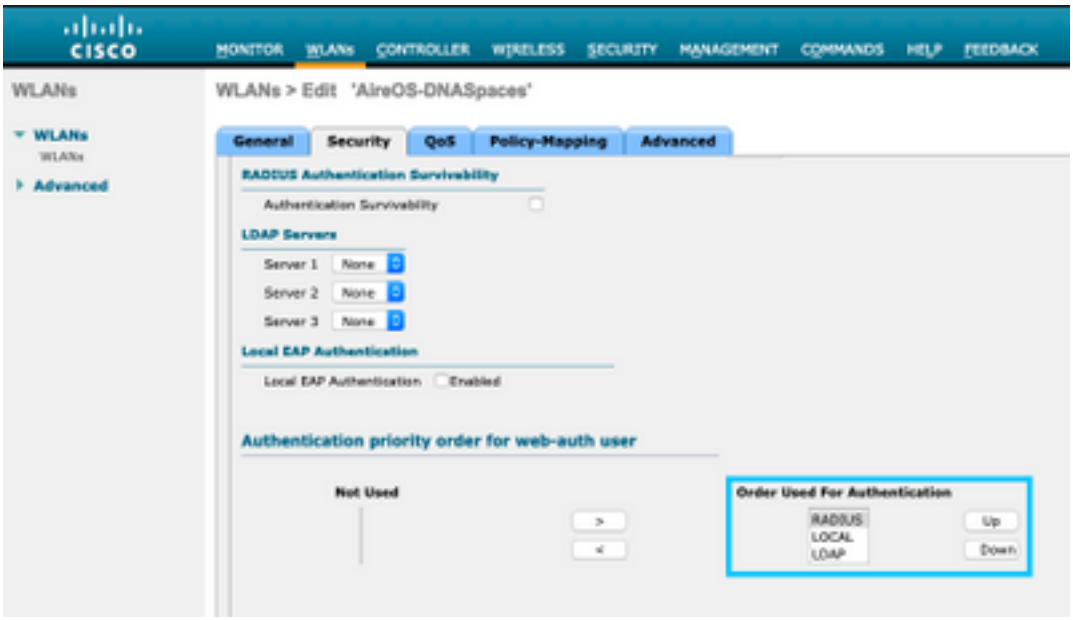
ステップ 3：レイヤ3セキュリティを設定します。[WLAN configuration]タブで[Security] > [Layer 3] タブに移動し、レイヤ3セキュリティ方式として[Web **Policy]を設定し、[Enable]** [On Mac Filter failure]を設定し、事前認証ACLを設定し、[Override Global Config] を[Web Auth Type] に[External]を設定し、リダイレクトURLを設定します。



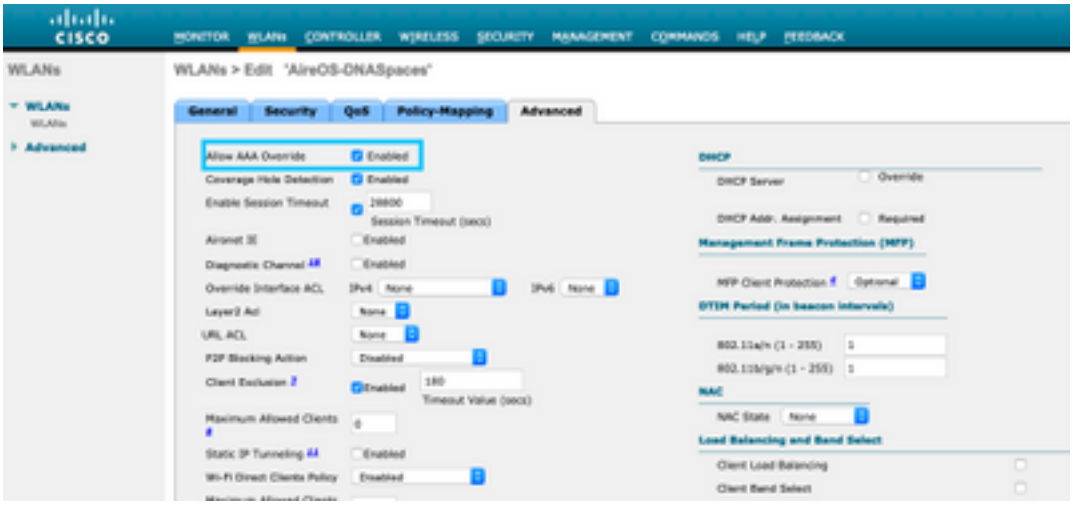
ステップ 4：AAAサーバを設定します。WLAN設定タブの[Security] > [AAA Servers] タブに移動し、[Authentication Servers] と[Accounting Servers] を有効にして、ドロップダウンメニューから2つのRADIUSサーバを選択します。



手順 6：**Web認証ユーザの認証の優先順位**を設定します。WLAN設定タブで[Security] > [AAA Servers] タブに移動し、RADIUSを順に最初に設定します。

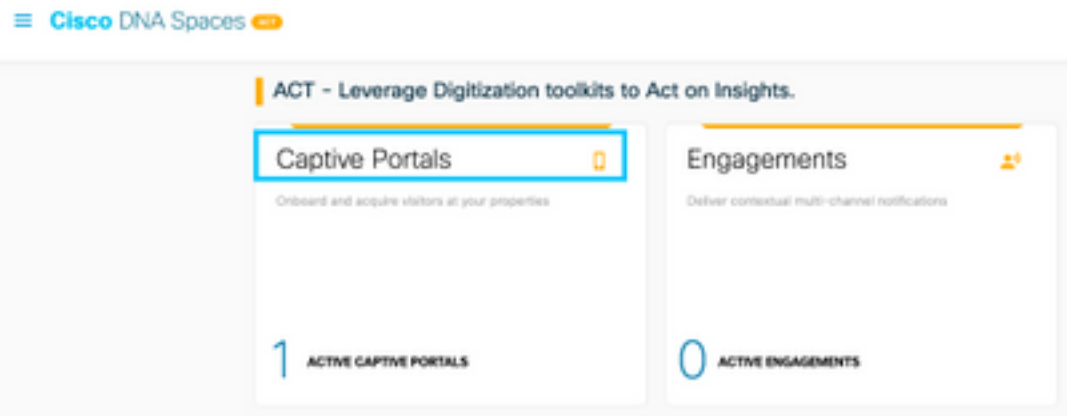


手順 7：WLAN設定タブの**Advanced**タブに移動し、**Allow AAA Override**を有効にします。

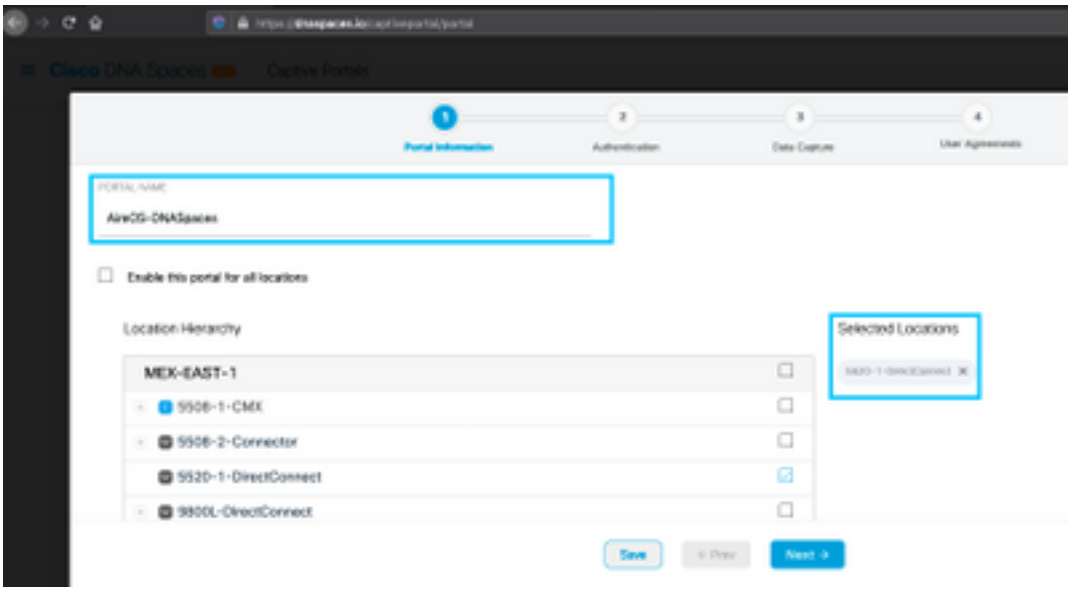


DNAスペースにポータルを作成する

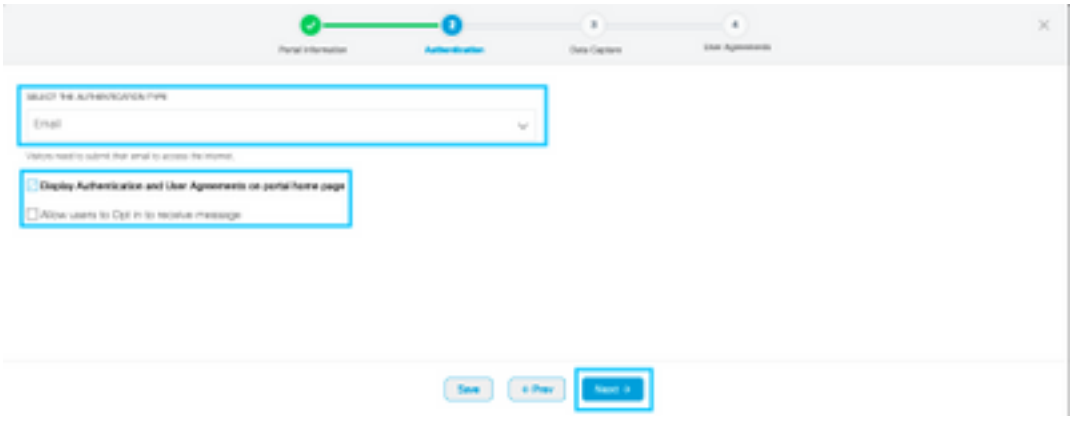
ステップ 1：DNA Spacesのダッシュボードで[Captive Portals] をクリックします。



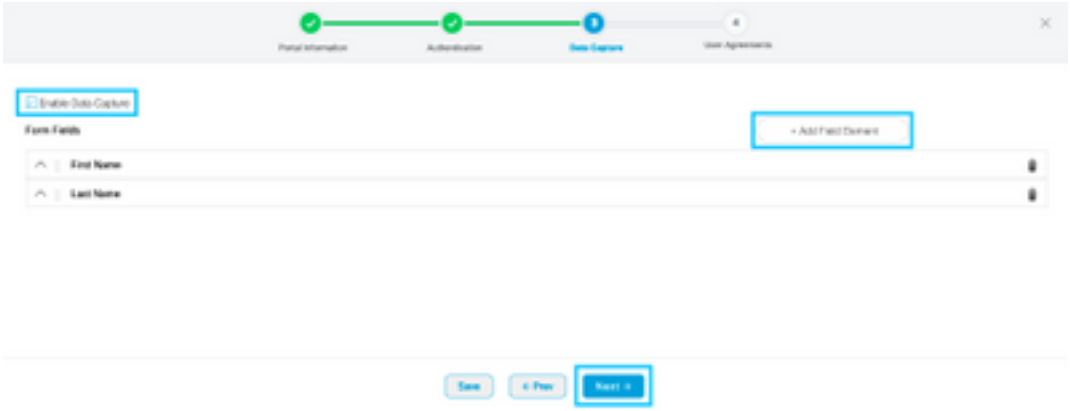
ステップ 2：[Create New] をクリックし、ポータル名を入力して、ポータルを使用できる場所を選択します。



ステップ 3：認証タイプを選択し、ポータルホームページにデータの取り込みとユーザ契約を表示するかどうか、およびユーザがメッセージを受信することを許可するかどうかを選択します。[Next] をクリックします。

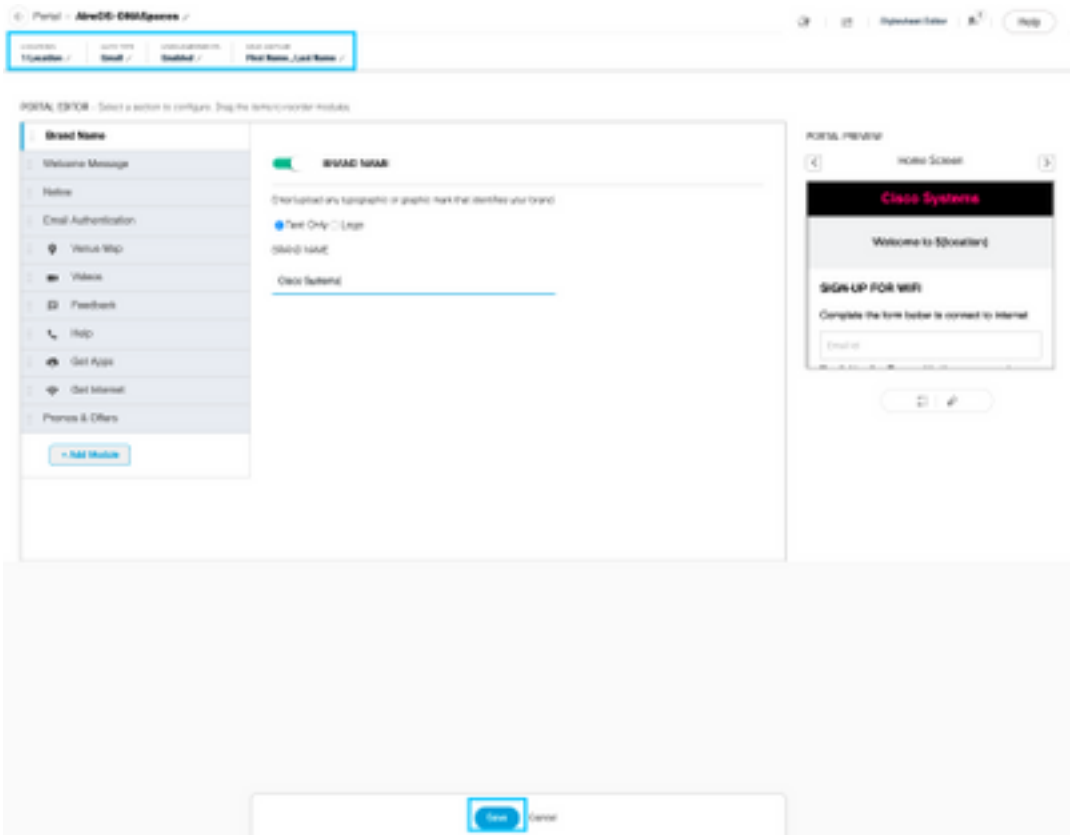


ステップ 4：データキャプチャ要素を構成します。ユーザからデータをキャプチャする場合は、[Enable Data Capture] ボックスをオンにし、[Add Field Element] をクリックして目的のフィールドを追加します。[Next] をクリックします。



ステップ 5：[Enable Terms & Conditions] にチェックマークを入れ、[Save & Configure Portal] をクリックします。

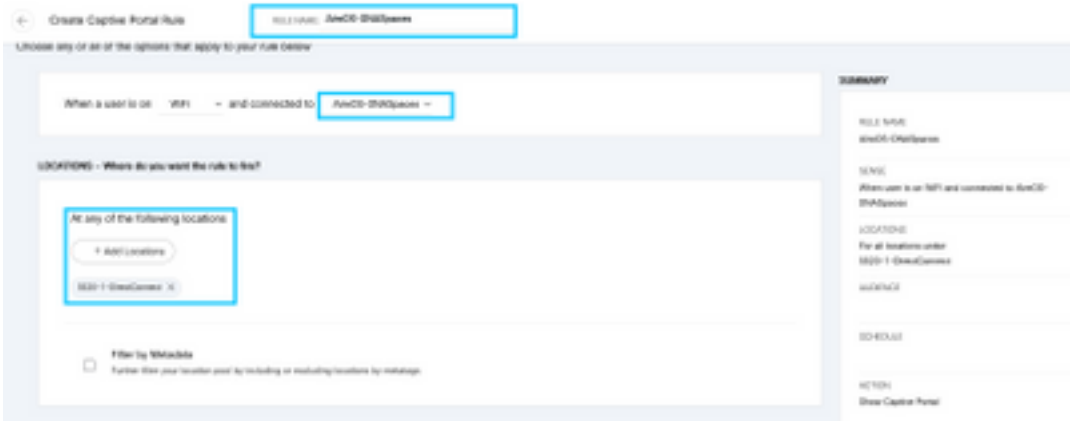
手順 6：必要に応じてポータルを編集し、[Save] をクリックします。



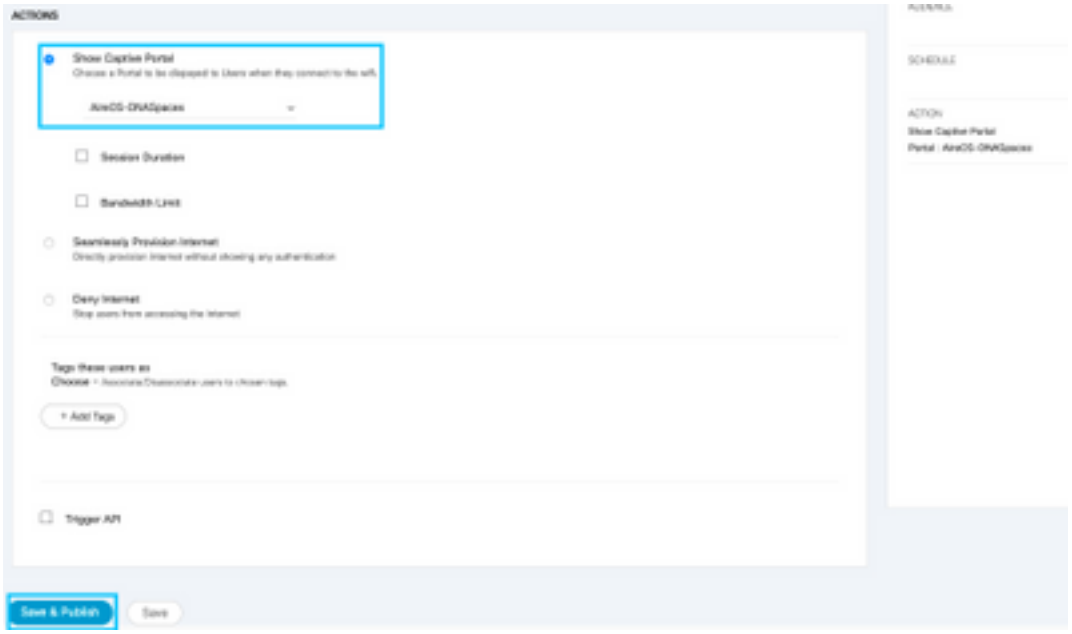
DNAスペースでのキャプティブポータルルールの設定

ステップ 1：キャプティブポータルメニューを開き、[Captive Portal Rules] をクリックします。

ステップ 2：+ [Create New Rule]をクリックします。ルール名を入力し、以前に設定したSSIDを選択し、このポータルルールを使用できる場所を選択します。

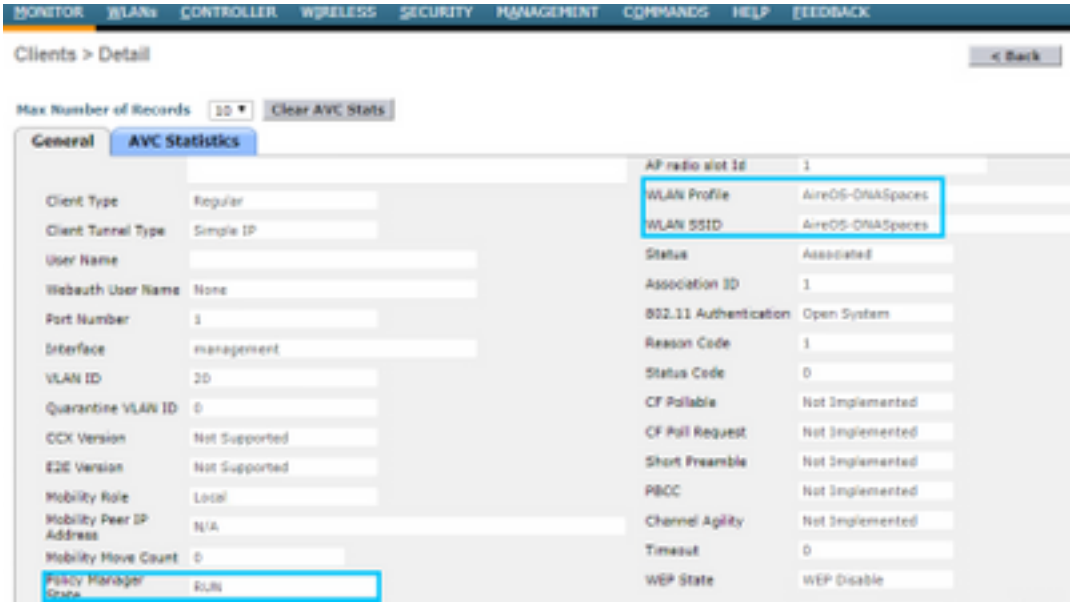


ステップ 3：キャプティブポータルのアクションを選択します。この場合、ルールがヒットすると、ポータルが表示されます。[Save & Publish] をクリックします。



確認

SSIDに接続されているクライアントのステータスを確認するには、[Monitor] > [Clients] に移動し、MACアドレスをクリックして[Policy Manager State]を探します。



トラブルシュート

クライアントの関連付けと認証プロセスを確認するためにテストを行う前に、コントローラで次のコマンドを有効にできます。

```
(5520-Andressi) >debug client
```

```
(5520-Andressi) >debug web-auth redirect enable mac
```

次に、RADIUSサーバを使用せずにSSIDに接続しているときに、関連付け/認証プロセス中に各フェーズを識別する試みが成功したときの出力を示します。

802.11アソシエーション/認証：

```
*apfOpenDtlSocket: Apr 09 21:49:06.227: 34:e1:2d:23:a6:68 Received management frame ASSOCIATION
REQUEST on BSSID 70:d3:79:dd:d2:0f destination addr 70:d3:79:dd:d2:0f slotid 1
*apfMsConnTask_5: Apr 09 21:49:06.227: 34:e1:2d:23:a6:68 Updating the client capabiility as 4
*apfMsConnTask_5: Apr 09 21:49:06.227: 34:e1:2d:23:a6:68 Processing assoc-req
station:34:e1:2d:23:a6:68 AP:70:d3:79:dd:d2:00-01 ssid : AireOS-DNASpaces thread:bd271d6280
*apfMsConnTask_5: Apr 09 21:49:06.227: 34:e1:2d:23:a6:68 CL_EVENT_ASSOC_START (1), reasonCode
(1), Result (0), Ssid (AireOS-DNASpaces), ApMac (70:d3:79:dd:d2:00), RSSI (-72), SNR (22)
*apfMsConnTask_5: Apr 09 21:49:06.228: 34:e1:2d:23:a6:68 Sending assoc-resp with status 0
station:34:e1:2d:23:a6:68 AP:70:d3:79:dd:d2:00-01 on apVapId 1
```

DHCPおよびレイヤ3認証：

```
*apfMsConnTask_5: Apr 09 21:49:06.228: 34:e1:2d:23:a6:68 Mobility query, PEM State: DHCP_REQD
*webauthRedirect: Apr 09 21:49:51.949: captive-bypass detection enabled, checking for wispr in
HTTP GET, client mac=34:e1:2d:23:a6:68
*webauthRedirect: Apr 09 21:49:51.949: captiveNetworkMode enabled, mac=34:e1:2d:23:a6:68
```

```
user_agent = AnyConnect Agent 4.7.04056
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Preparing redirect URL according to
configured Web-Auth type
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- unable to get the hostName for virtual
IP, using virtual IP =192.0.2.1
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Checking custom-web config for WLAN
ID:1
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Global status is 0 on WLAN
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- checking on WLAN web-auth type
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Web-auth type External, using
URL:https://splash.dnaspaces.io/p2/mexeast1
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Added switch_url, redirect URL is now
https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Added ap_mac (Radio ), redirect URL is
now
https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79:
dd:d2:00
*webauthRedirect: Apr 09 21:49:51.949: 34:e1:2d:23:a6:68- Added client_mac , redirect URL is now
https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79:
dd:d2:00&client_mac=34:e1:2d:23:a6
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- Added wlan, redirect URL is now
https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79:
dd:d2:00&client_mac=34:e1:2d:23:a6:68&wla
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- http_response_msg_body1 is
<HTML><HEAD><TITLE> Web Authentication Redirect</TITLE><META http-equiv="Cache-control"
content="no-cache"><META http-equiv="Pragma" content="
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- added redirect=, URL is now
https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79:
dd:d2:00&client_mac=34:e1:2d:23:a6:68&wlan=Ai
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- str1 is now
https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79:
dd:d2:00&client_mac=34:e1:2d:23:a6:68&wlan=AireOS-DNASpaces&r

*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- Message to be sent is
HTTP/1.1 200 OK
Location:
https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79:
dd:d2:00&client_mac=34:
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- 200 send_data =HTTP/1.1 200 OK
Location:
https://splash.dnaspaces.io/p2/mexeast1?switch_url=https://192.0.2.1/login.html&ap_mac=70:d3:79:
dd:d2:00&client_mac=34:e1:2d:23
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- send data length=688
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68-
Url:https://splash.dnaspaces.io/p2/mexeast1
*webauthRedirect: Apr 09 21:49:51.950: 34:e1:2d:23:a6:68- cleaning up after send
```

レイヤ3認証に成功し、クライアントをRUN状態に移行します。

```
*emWeb: Apr 09 21:49:57.633: Connection created for MAC:34:e1:2d:23:a6:68
*emWeb: Apr 09 21:49:57.634:
ewaURLHook: Entering:url=/login.html, virtIp = 192.0.2.1, ssl_connection=0, secureweb=1

*ewmwebWebauth1: Apr 09 21:49:57.634: 34:e1:2d:23:a6:68 10.10.30.42 WEBAUTH_NOL3SEC (14) Change
state to RUN (20) last state WEBAUTH_NOL3SEC (14)
*ewmwebWebauth1: Apr 09 21:49:57.634: 34:e1:2d:23:a6:68 CL_EVENT_WEB_AUTH_DONE (8), reasonCode
(0), Result (0), ServerIp (), UserName ()
*ewmwebWebauth1: Apr 09 21:49:57.634: 34:e1:2d:23:a6:68 CL_EVENT_RUN (9), reasonCode (0), Result
(0), Role (1), VLAN/VNID (20), Ipv4Addr (10.10.30.42), Ipv6Present (No)
*ewmwebWebauth1: Apr 09 21:49:57.634: 34:e1:2d:23:a6:68 10.10.30.42 RUN (20) Successfully
plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255,URL ACL ID 255,URL ACL
Action 0)
```

```
*emWeb: Apr 09 21:49:57.634: User login successful, presenting login success page to user
```

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。