# Konfigurationsbeispiel für DNA Spaces Captive Portal mit AireOS-Controller

## Inhalt



## Einleitung

In diesem Dokument wird beschrieben, wie Sie Captive Portals mithilfe von Cisco DNA Spaces mit einem AireOS-Controller konfigurieren.

Beitrag von Andres Silva Cisco TAC Engineer.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Zugriff auf die Wireless Controller über eine Kommandozeile oder eine grafische Benutzeroberfläche
- Cisco DNS-Räume

### Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- 5520 Wireless LAN Controller Version 8.10.112.0

# Konfigurieren

## Netzwerkdiagramm


## Konfigurationen

### Verbinden des WLC mit Cisco DNA Spaces

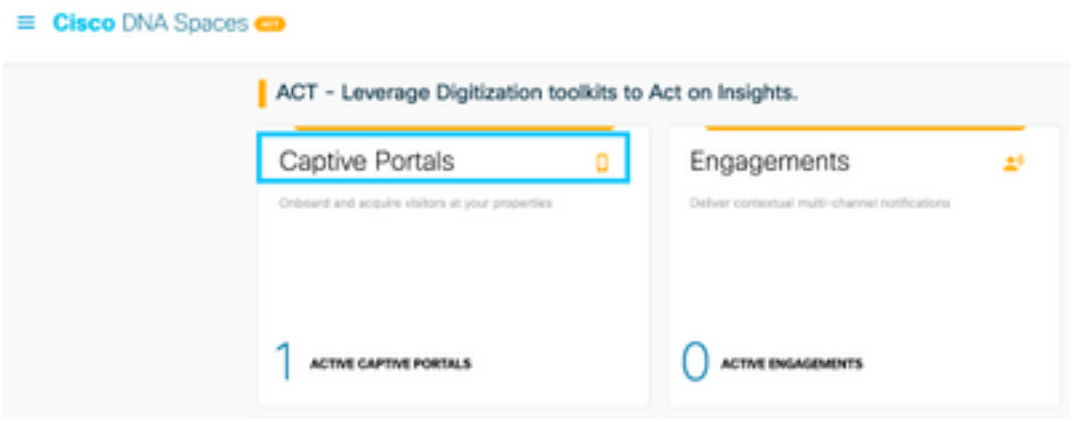
Der Controller muss über eine der verfügbaren Konfigurationen, Direct Connect, über den DNA Spaces Connector oder über CMX Tethering mit DNA Spaces verbunden werden.

In diesem Beispiel wird die Option "Direct Connect" verwendet, obwohl Captive-Portale für alle Setups auf die gleiche Weise konfiguriert sind.

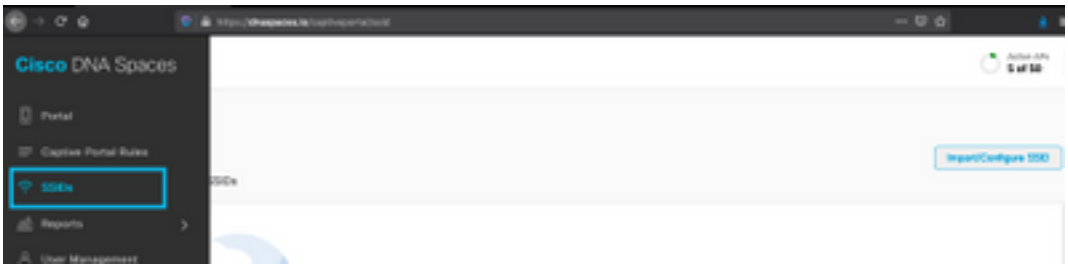
Um den Controller mit Cisco DNA Spaces zu verbinden, muss er über HTTPS auf die Cisco DNA Spaces-Cloud zugreifen können. Weitere Informationen zum Verbinden des Controllers mit DNA Spaces finden Sie unter diesem Link: DNA Spaces Direct Connect-Konfigurationsbeispiel

### Erstellung der SSID auf DNA-Spaces

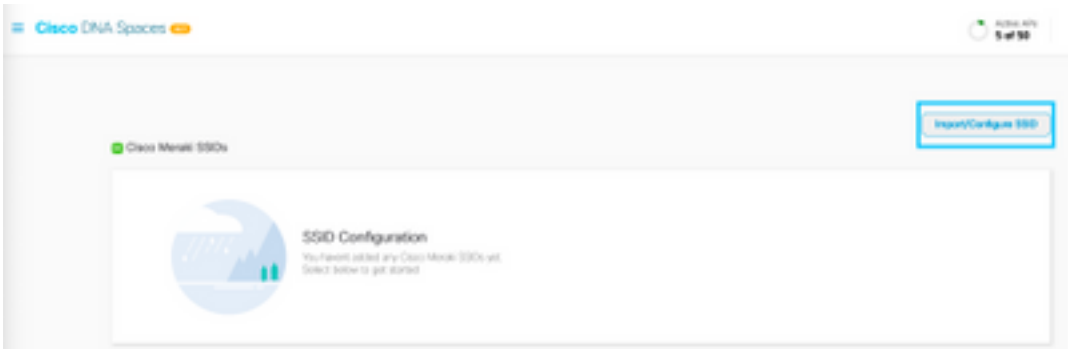
Schritt 1: Klicken Sie auf **Captive Portals** im Armaturenbrett von DNA Spaces:




Schritt 2: Öffnen Sie das Captive Portal-Menü, indem Sie auf das Symbol mit drei Zeilen in der oberen linken Ecke der Seite klicken und dann auf **SSIDs** klicken:



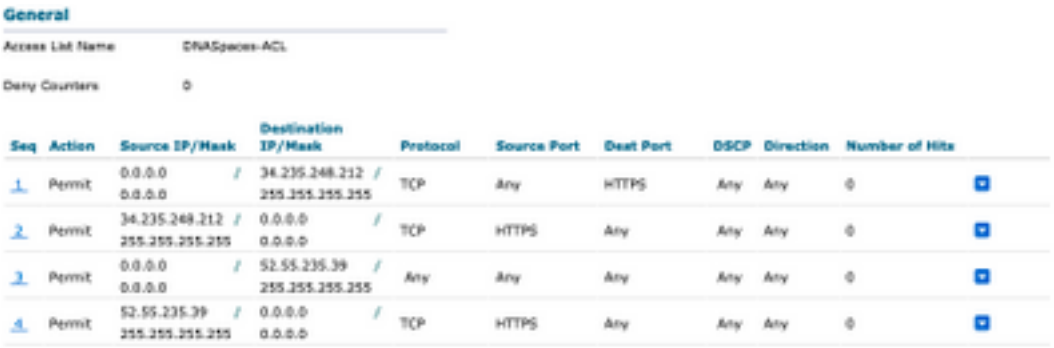

Schritt 3: Klicken Sie auf **Import/Configure SSID**, wählen Sie **CUWN (CMX/WLC)** als Typ "Wireless Network" aus, und geben Sie den SSID-Namen ein:




### ACL-Konfiguration auf dem Controller

Eine Vorauthentifizierungs-ACL ist erforderlich, da es sich um eine Webauthentifizierungs-SSID handelt. Sobald das Wireless-Gerät eine Verbindung mit der SSID herstellt und eine IP-Adresse empfängt, wechselt der Richtlinienmanager-Status des Geräts in den Status **Webauth_Reqd,** und die ACL wird auf die Client-Sitzung angewendet, um die Ressourcen zu beschränken, die das Gerät erreichen kann.

Schritt 1: Navigieren Sie zu **Security > Access Control Lists > Access Control Lists,** klicken Sie auf **New** und konfigurieren Sie die Regeln, um die Kommunikation zwischen den Wireless-Clients zu DNA Spaces wie folgt zuzulassen. Ersetzen Sie die IP-Adressen durch die IP-Adressen, die von DNA Spaces für das verwendete Konto angegeben wurden:




> **Hinweis:** Um die IP-Adressen der DNA-Spaces abzurufen, die in der ACL zugelassen werden sollen, klicken Sie auf die Option **Manuell konfigurieren** aus der SSID, die in Schritt 3 des Abschnitts **Erstellen der SSID auf DNA-Spaces** unter dem ACL-Konfigurationsabschnitt erstellt wurde.

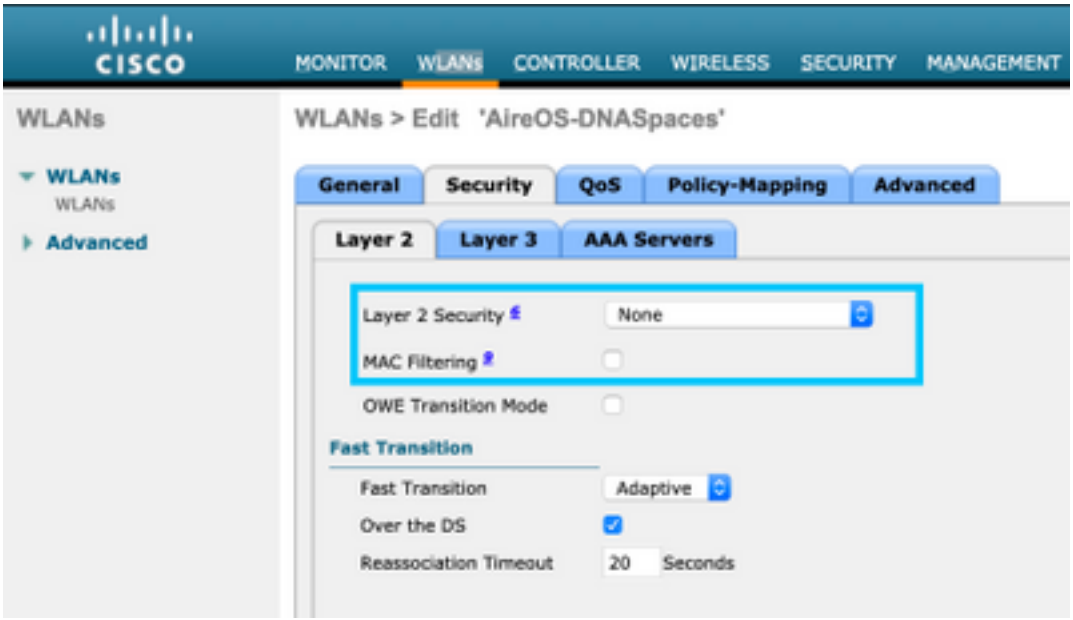
Die SSID kann für die Verwendung eines RADIUS-Servers oder ohne diesen konfiguriert werden. Wenn die Sitzungsdauer, das Bandbreitenlimit oder die nahtlose Internetbereitstellung im Abschnitt "**Aktionen**" der Captive Portal Rule-Konfiguration konfiguriert ist, muss die SSID mit einem RADIUS-Server konfiguriert werden. Andernfalls muss der RADIUS-Server nicht verwendet werden. Alle Arten von Portalen auf DNA Spaces werden auf beiden Konfigurationen unterstützt.

## Captive Portal ohne RADIUS-Server auf DNA-Spaces

### SSID-Konfiguration auf dem Controller

Schritt 1: Navigieren Sie zu **WLAN > WLANs.** Erstellen Sie ein neues WLAN. Konfigurieren des Profilnamens und der SSID Stellen Sie sicher, dass der SSID-Name mit dem in Schritt 3 des Abschnitts **Erstellen der SSID auf DNA-Spaces** konfigurierten Namen übereinstimmt**.**


Schritt 2: Konfigurieren der Layer-2-Sicherheit Navigieren Sie zur Registerkarte **Security > Layer 2** der Registerkarte WLAN Configuration, und wählen Sie im Dropdown-Menü von Layer 2 Security die Option **None** aus**.** Stellen Sie sicher, dass die MAC-Filterung deaktiviert ist.




Schritt 3: Konfigurieren der Layer-3-Sicherheit Navigieren Sie zur Registerkarte Security > Layer 3 auf der Registerkarte WLAN configuration, konfigurieren Sie Web **Policy als die Sicherheitsmethode Layer 3, aktivieren Sie Passthrough, konfigurieren Sie die ACL für die Vorauthentifizierung, aktivieren Sie Override Global Config,** wenn Sie den **Web Auth Type** als **Extern** festlegen, und konfigurieren Sie die Umleitungs-URL.

> **Hinweis**: Um die Umleitungs-URL abzurufen, klicken Sie in Schritt 3 des Abschnitts **"Erstellen** der **SSID auf DNA-Spaces"** unter dem SSID-Konfigurationsabschnitt auf die Option **"Manuell konfigurieren".**

## Captive Portal mit RADIUS-Server auf DNA-Spaces

> **Hinweis:** Der RADIUS-Server DNA Spaces unterstützt nur die PAP-Authentifizierung, die vom Controller ausgeht.

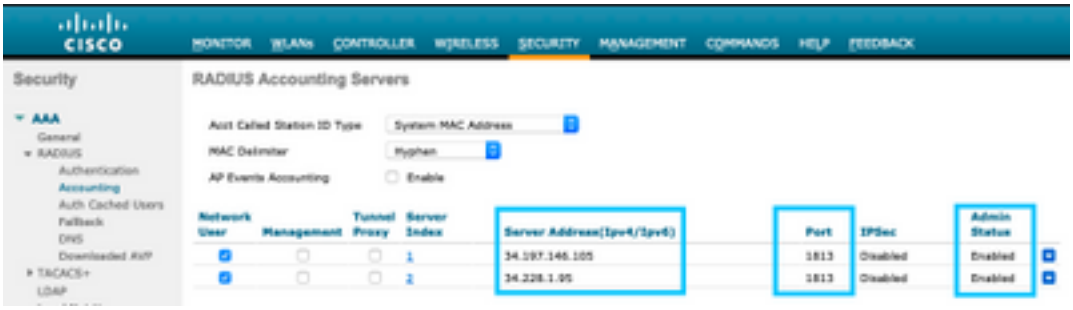
### Konfiguration der RADIUS-Server auf dem Controller

Schritt 1: Navigieren Sie zu **Security > AAA > RADIUS > Authentication,** klicken Sie auf **New**, und

geben Sie die RADIUS-Serverinformationen ein. Cisco DNA Spaces fungiert als RADIUS-Server für die Benutzerauthentifizierung und kann auf zwei IP-Adressen antworten. Konfigurieren Sie beide RADIUS-Server:

> **Hinweis:** Um die RADIUS-IP-Adresse und den geheimen Schlüssel für den primären und den sekundären Server abzurufen, klicken Sie auf die Option **Manuell konfigurieren** der in Schritt 3 des Abschnitts erstellten SSID. **Erstellen Sie die SSID auf DNA-Spaces,** und navigieren Sie zum Abschnitt **"RADIUS-Serverkonfiguration".**

Schritt 2: Konfigurieren Sie den Accounting-RADIUS-Server. Navigieren Sie zu **Security > AAA > RADIUS > Accounting,** und klicken Sie auf **New**. Beide RADIUS-Server konfigurieren:

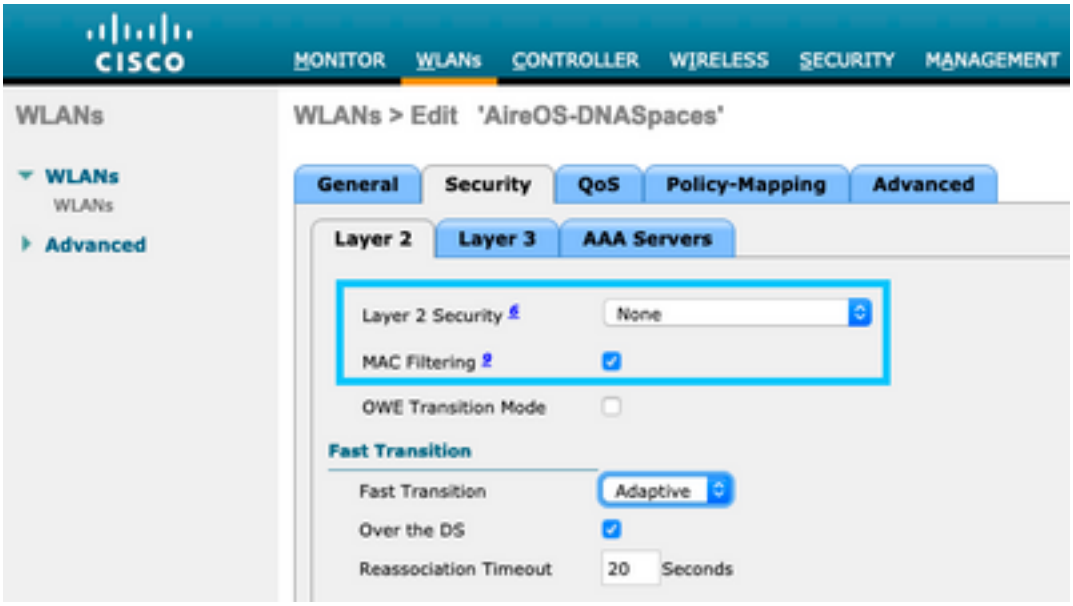


**SSID-Konfiguration auf dem Controller**

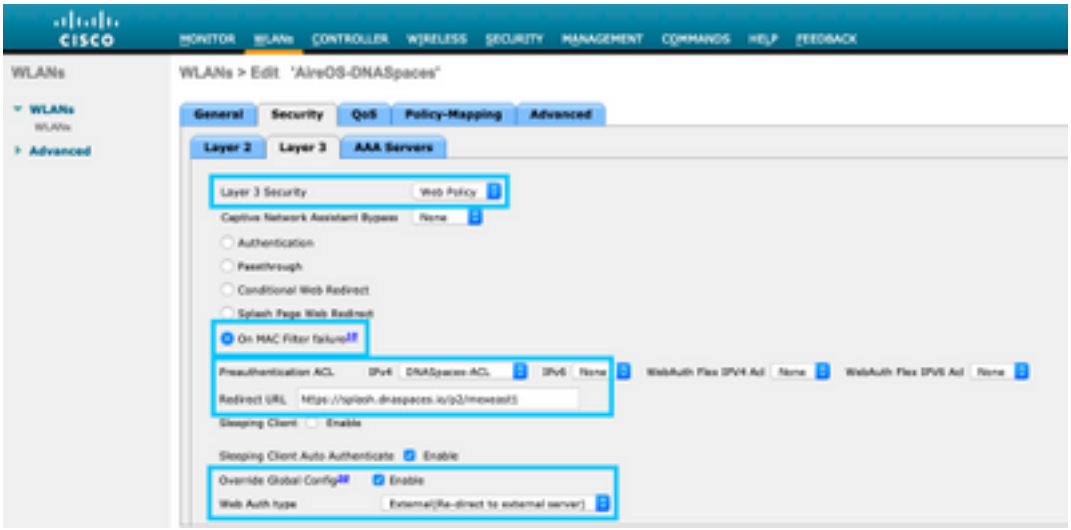
> **Wichtig**: Bevor Sie mit der SSID-Konfiguration beginnen, stellen Sie sicher, dass **Web Radius Authentication** unter Controller > General (Controller > Allgemein) auf "PAP" gesetzt ist.

Schritt 1: Navigieren Sie zu **WLAN > WLANs.** Erstellen Sie ein neues WLAN. Konfigurieren des Profilnamens und der SSID Stellen Sie sicher, dass der SSID-Name mit dem in Schritt 3 des Abschnitts **Erstellen der SSID auf DNA-Spaces** konfigurierten Namen übereinstimmt**.**

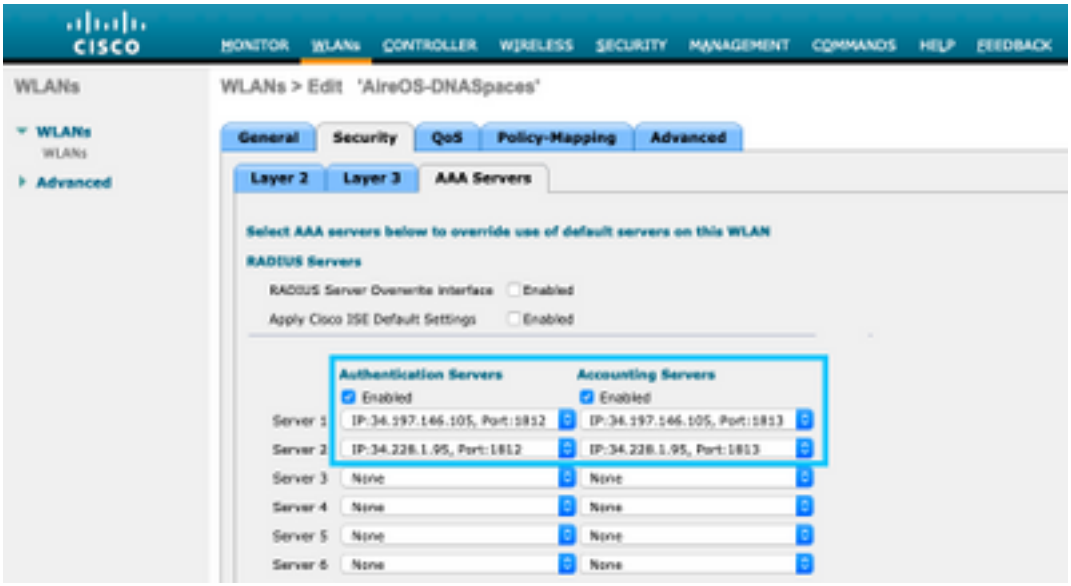
Schritt 2: Konfigurieren der Layer-2-Sicherheit Navigieren Sie auf der Registerkarte für die WLAN-Konfiguration zur Registerkarte **Security > Layer 2**. Konfigurieren Sie die Layer-2-Sicherheit als **None**. Mac-Filterung aktivieren.



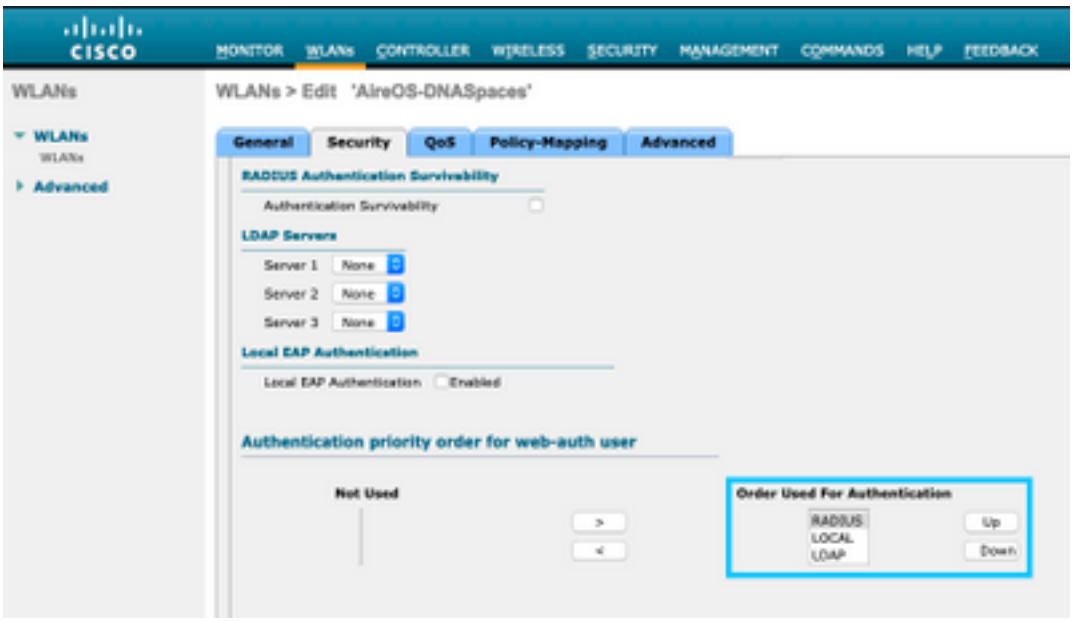

Schritt 3: Konfigurieren der Layer-3-Sicherheit Navigieren Sie zur Registerkarte Security > Layer 3 auf der Registerkarte WLAN configuration, konfigurieren Sie Web **Policy als die Layer 3-Sicherheitsmethode, aktivieren Sie bei einem MAC-Filterfehler die ACL für die Vorauthentifizierung, aktivieren Sie Override Global Config,** wenn Sie den **Web Auth Type** als **Extern** festlegen, und konfigurieren Sie die Umleitungs-URL.



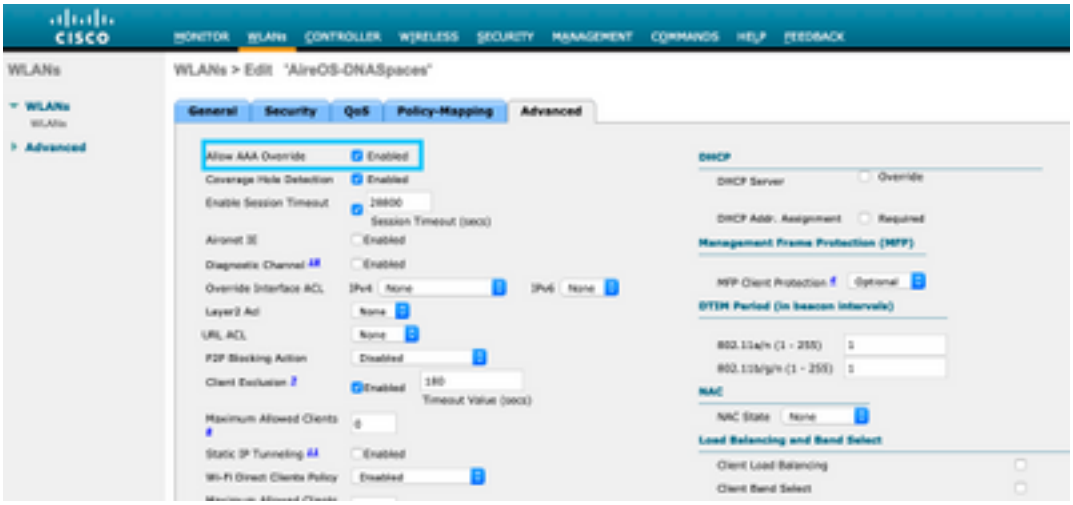
Schritt 4: Konfigurieren von AAA-Servern Navigieren Sie zur Registerkarte **Security > AAA Servers** (Sicherheit > AAA-Server) auf der Registerkarte WLAN configuration (WLAN-Konfiguration), aktivieren Sie **Authentication Servers** and **Accounting Servers (Authentifizierungsserver** und **Abrechnungsserver)**, und wählen Sie aus dem Dropdown-Menü die beiden RADIUS-Server aus:




Schritt 6: Konfigurieren Sie die **Reihenfolge der Authentifizierungspriorität für Web-Authentifizierungsbenutzer**. Navigieren Sie zur Registerkarte **Security > AAA Servers** (Sicherheit > AAA-Server) auf der Registerkarte WLAN configuration (WLAN-Konfiguration), und legen Sie RADIUS in der Reihenfolge als Erstes fest.

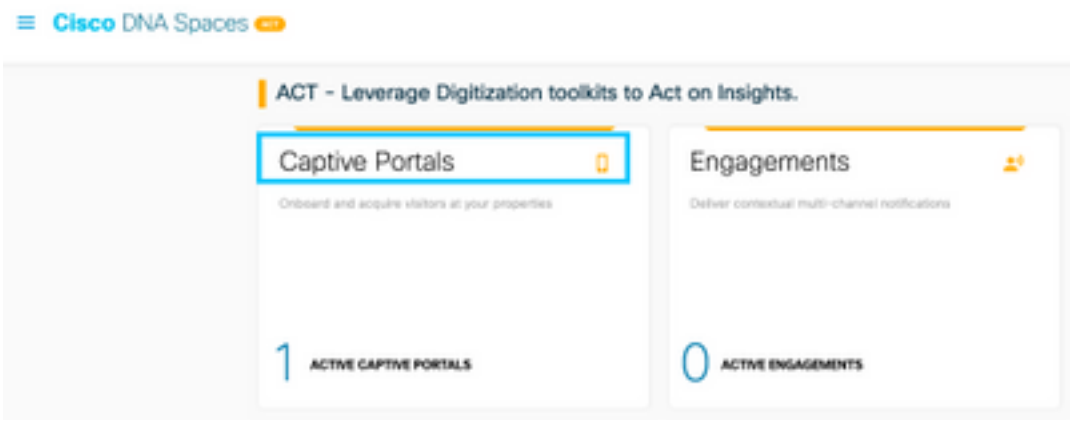



Schritt 7. Navigieren Sie zur Registerkarte **Advanced (Erweitert)** auf der Registerkarte WLAN Configuration (WLAN-Konfiguration), und aktivieren Sie **Allow AAA Override (AAA-Außerkraftsetzung zulassen).**

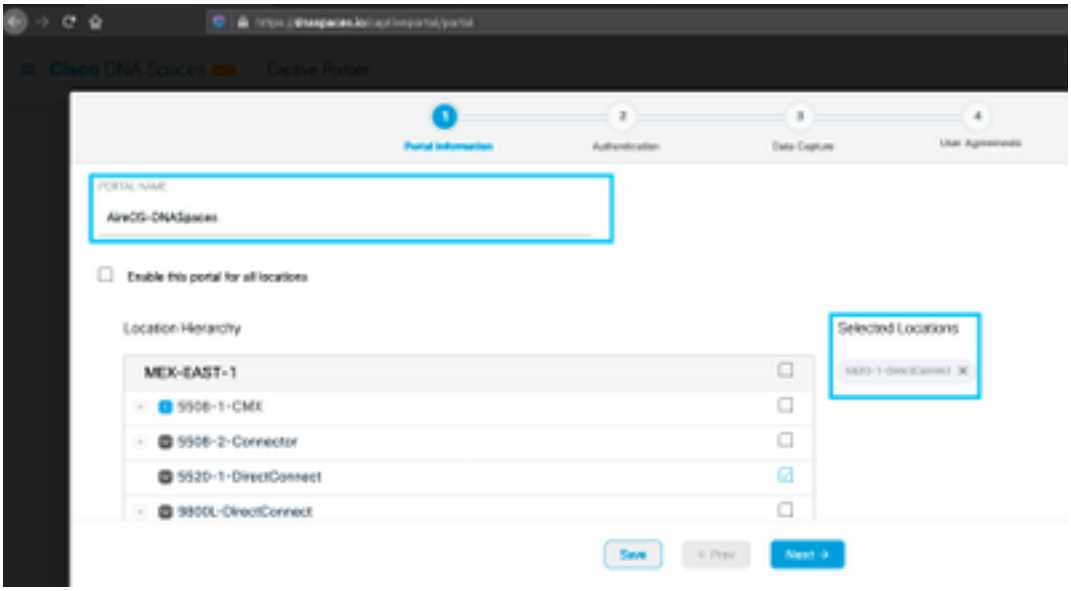



## Portal zu DNA Spaces erstellen

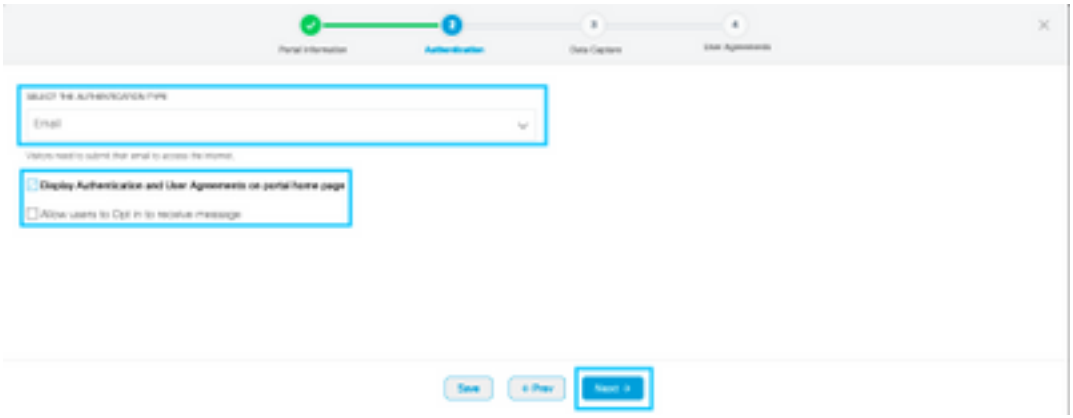
Schritt 1: Klicken Sie auf **Captive Portals** im Armaturenbrett von DNA Spaces:



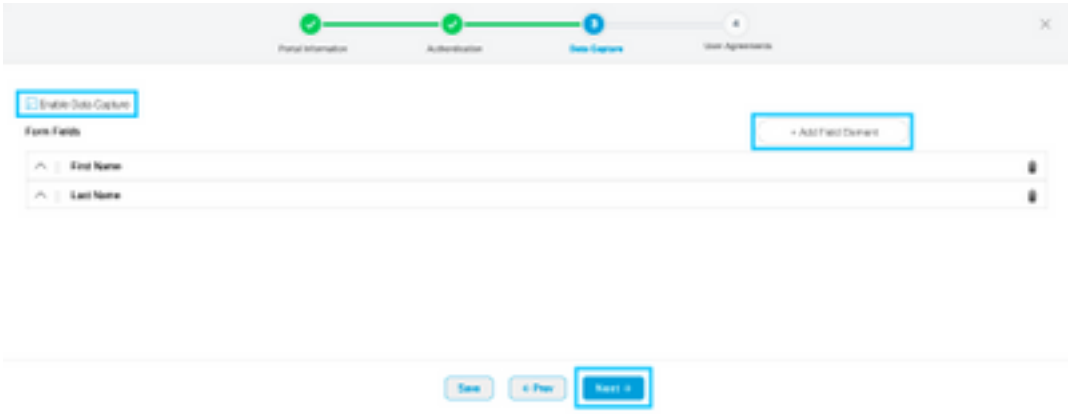

Schritt 2: Klicken Sie auf **Create New (Neu erstellen),** geben Sie den Portalnamen ein, und wählen Sie die Standorte aus, die das Portal verwenden können:



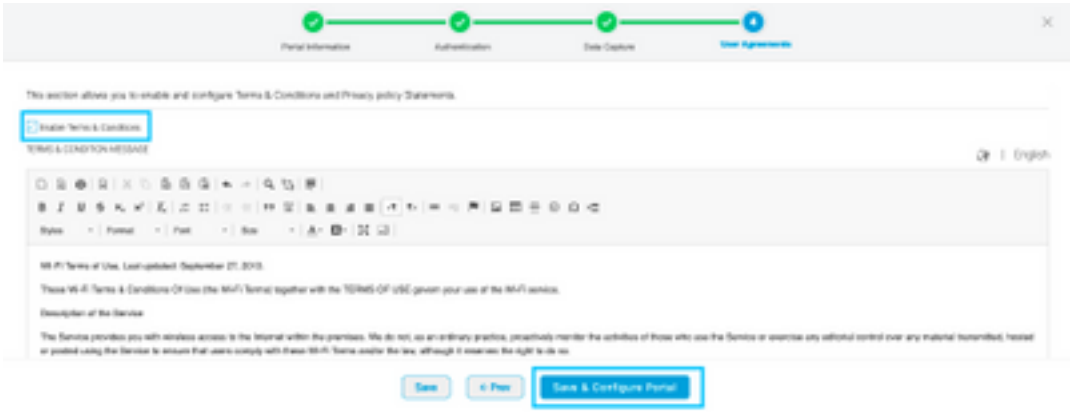

Schritt 3: Wählen Sie den Authentifizierungstyp aus, und wählen Sie aus, ob Sie Datenerfassung und Benutzervereinbarungen auf der Portal-Startseite anzeigen möchten und ob Benutzer sich anmelden dürfen, um eine Nachricht zu erhalten. Klicken Sie auf **Weiter**:



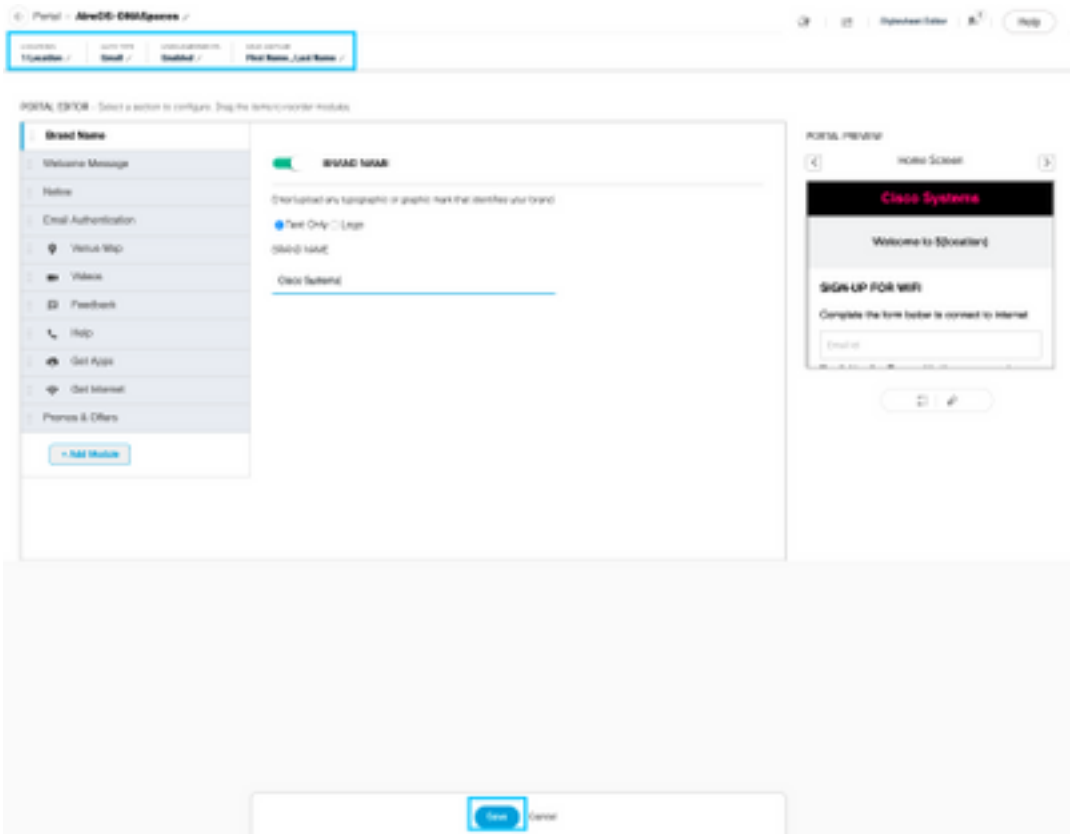
Schritt 4: Konfigurieren von Datenerfassungselementen Wenn Sie Daten von Benutzern erfassen möchten, aktivieren Sie das Feld **Datenerfassung aktivieren,** und klicken Sie auf **+Feldelement hinzufügen,** um die gewünschten Felder hinzuzufügen. Klicken Sie auf **Weiter**:



Schritt 5: Aktivieren Sie die Option **Enable Terms &** Conditions, und klicken Sie auf **Save & Configure Portal**:



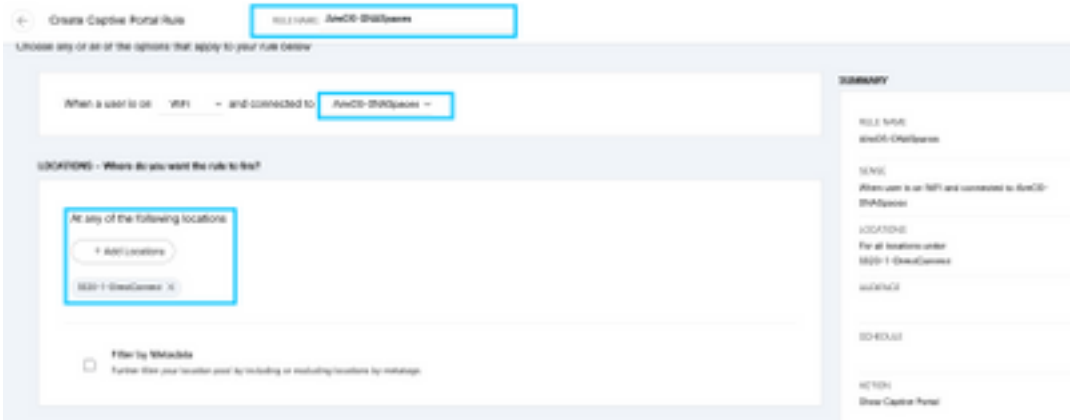
Schritt 6: Bearbeiten Sie das Portal nach Bedarf, und klicken Sie auf **Speichern:**



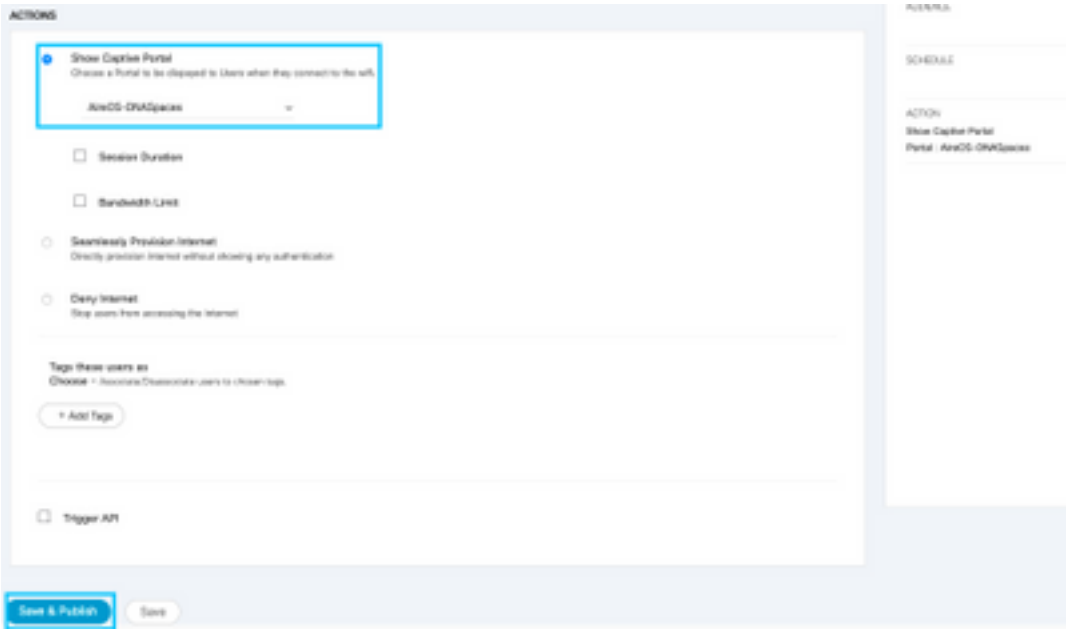
## Konfigurieren der Captive Portal-Regeln für DNA-Bereiche

Schritt 1: Öffnen Sie das Captive Portal-Menü, und klicken Sie auf **Captive Portal Rules:**


Schritt 2: Klicken Sie auf **+ Neue Regel erstellen**. Geben Sie den Regelnamen ein, wählen Sie die zuvor konfigurierte SSID aus, und wählen Sie die Standorte aus, für die diese Portalregel verfügbar ist:

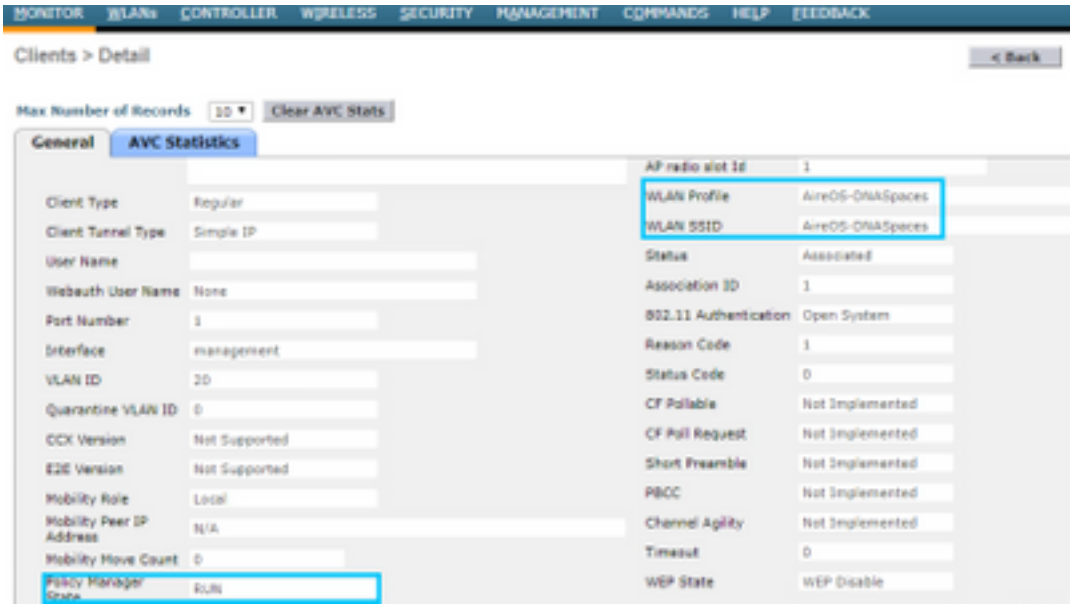


Schritt 3: Wählen Sie die Aktion des Captive Portals aus. In diesem Fall wird das Portal angezeigt, wenn die Regel getroffen wird. Klicken Sie auf **Speichern und veröffentlichen.**




# Überprüfung

Um den Status eines mit der SSID verbundenen Clients zu bestätigen, navigieren Sie zu **Monitor > Clients,** klicken Sie auf die MAC-Adresse, und suchen Sie nach Policy Manager State:




# Fehlerbehebung

Der folgende Befehl kann vor dem Testen im Controller aktiviert werden, um den Zuordnungs- und Authentifizierungsprozess des Clients zu bestätigen.

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

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

Dies ist die Ausgabe eines erfolgreichen Versuchs, jede der Phasen während des Assoziierungs-/Authentifizierungsprozesses zu identifizieren, während eine Verbindung zu einer SSID ohne RADIUS-Server hergestellt wird:

802.11-Zuordnung/Authentifizierung:

```
*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- und Layer 3-Authentifizierung:

```
*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
```

Layer-3-Authentifizierung erfolgreich. Verschieben Sie den Client in den RUN-Status:

```
*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
```

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.