

Konfigurieren von DNA Spaces Captive Portal mit Catalyst 9800 WLC

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Verbinden des 9800 Controllers mit Cisco DNA Spaces](#)

[Erstellung der SSID auf DNA-Spaces](#)

[ACL- und URL-Filterkonfiguration auf dem Controller 9800](#)

[Captive Portal ohne RADIUS-Server auf DNA-Spaces](#)

[Konfiguration der Web Auth-Parameterzuordnung auf dem 9800-Controller](#)

[Erstellen der SSID auf dem 9800-Controller](#)

[Richtlinienprofil auf dem 9800-Controller konfigurieren](#)

[Konfigurieren der Richtlinien-Tag-Nummer auf dem 9800-Controller](#)

[Captive Portal mit RADIUS-Server auf DNA-Spaces](#)

[Konfiguration der Web Auth-Parameterzuordnung auf dem 9800-Controller](#)

[Konfiguration der RADIUS-Server auf dem Controller 9800](#)

[Erstellen der SSID auf dem 9800-Controller](#)

[Richtlinienprofil auf dem 9800-Controller konfigurieren](#)

[Konfigurieren der Richtlinien-Tag-Nummer auf dem 9800-Controller](#)

[Globale Parameterzuordnung konfigurieren](#)

[Portal zu DNA Spaces erstellen](#)

[Konfigurieren der Captive Portal-Regeln für DNA-Bereiche](#)

[Spezifische Informationen von DNA Spaces abrufen](#)

[Welche IP-Adressen verwenden DNA Spaces?](#)

[Welche URL verwendet das DNA Spaces-Anmeldeportal?](#)

[Was sind die RADIUS-Serverdetails für DNA Spaces?](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Häufige Probleme](#)

[Stets verfügbare Ablaufverfolgung](#)

[Bedingtes Debugging und Radio Active Tracing](#)

[Beispiel eines erfolgreichen Versuchs](#)

Einleitung

In diesem Dokument wird die Konfiguration von Captive Portals auf Cisco DNA Spaces

beschrieben.

Voraussetzungen

In diesem Dokument können Kunden auf dem Catalyst 9800 Wireless LAN Controller (C9800 WLC) DNA Spaces als externe Webauthentifizierungs-Anmeldeseite verwenden.

Anforderungen

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

- Zugriff auf die Wireless Controller 9800 über eine Kommandozeile oder eine grafische Benutzeroberfläche
- Cisco DNS-Räume

Verwendete Komponenten

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

- 9800-L Controller Version 16.12.2s

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

Die Web-Authentifizierung ist eine einfache Layer-3-Authentifizierungsmethode, ohne dass eine Komponente oder ein Client-Dienstprogramm erforderlich ist. Dies ist möglich

- a) Mit der internen Seite des C9800 WLC, entweder unverändert oder nach Änderungen
- b) Mit auf C9800 WLC hochgeladenem, angepasstem Anmeldebündel
- c) Benutzerdefinierte Anmeldeseite auf einem externen Server

Die Nutzung des von DNA Spaces bereitgestellten Captive Portals ist im Wesentlichen eine Möglichkeit, externe Web-Authentifizierung für Clients auf dem C9800 WLC zu implementieren.

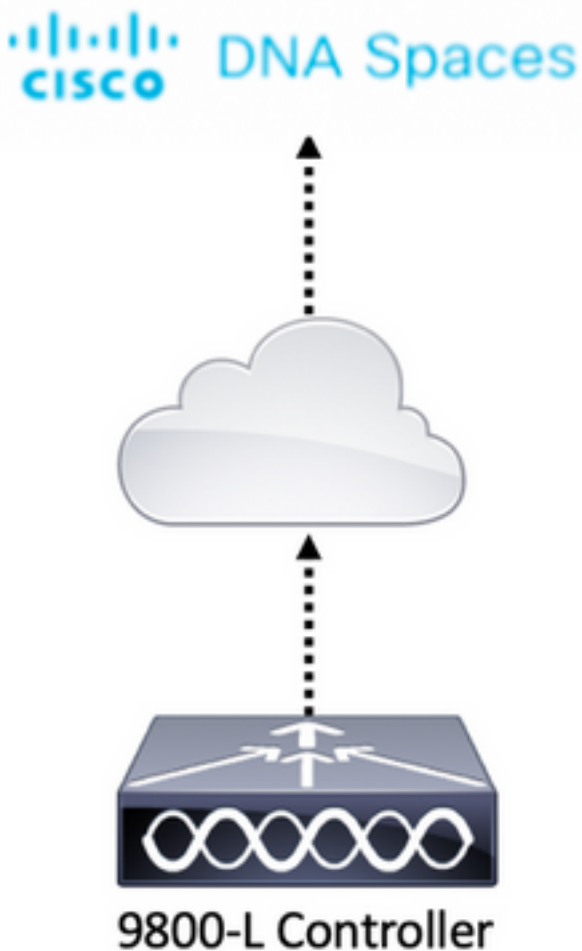
Ausführliche Informationen zum externen Webauthentifizierungsprozess finden Sie unter:

<https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/config-guide/web-authentication/b-configuring-web-based-authentication-on-cisco-catalyst-9800-series-controllers/m-external-web-authentication-configuration.html>

Auf dem C9800 WLC wird die virtuelle IP-Adresse als globale Parameterzuordnung definiert und lautet in der Regel 192.0.2.1

Konfigurieren

Netzwerkdiagramm



Verbinden des 9800 Controllers mit Cisco DNA Spaces

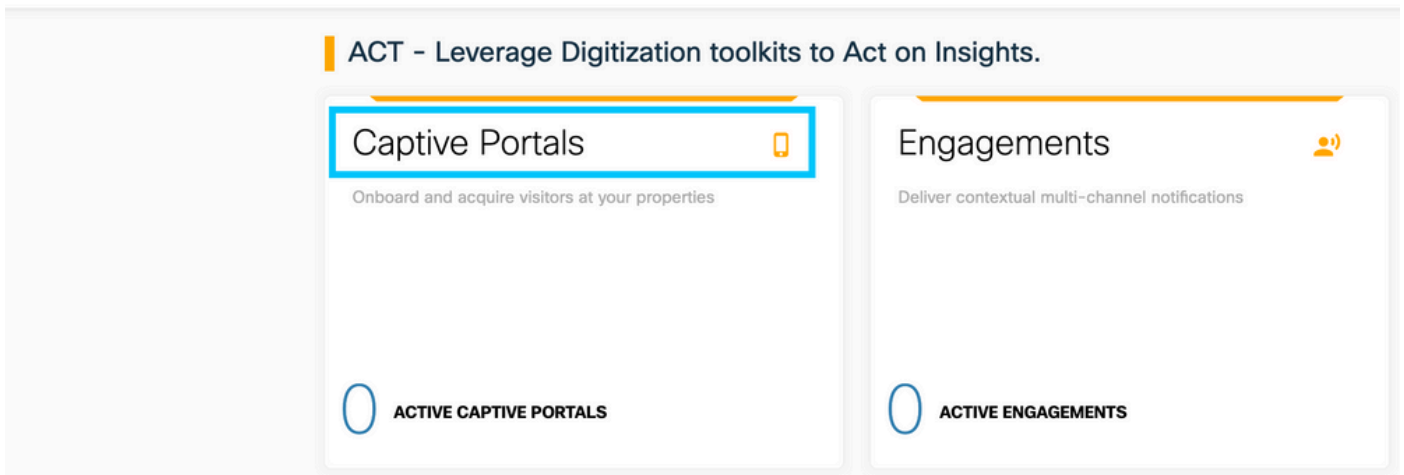
Der Controller muss mit DNA Spaces über eine der Optionen verbunden werden - Direct Connect, über DNA Spaces Connector oder mit CMX Tethering.

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

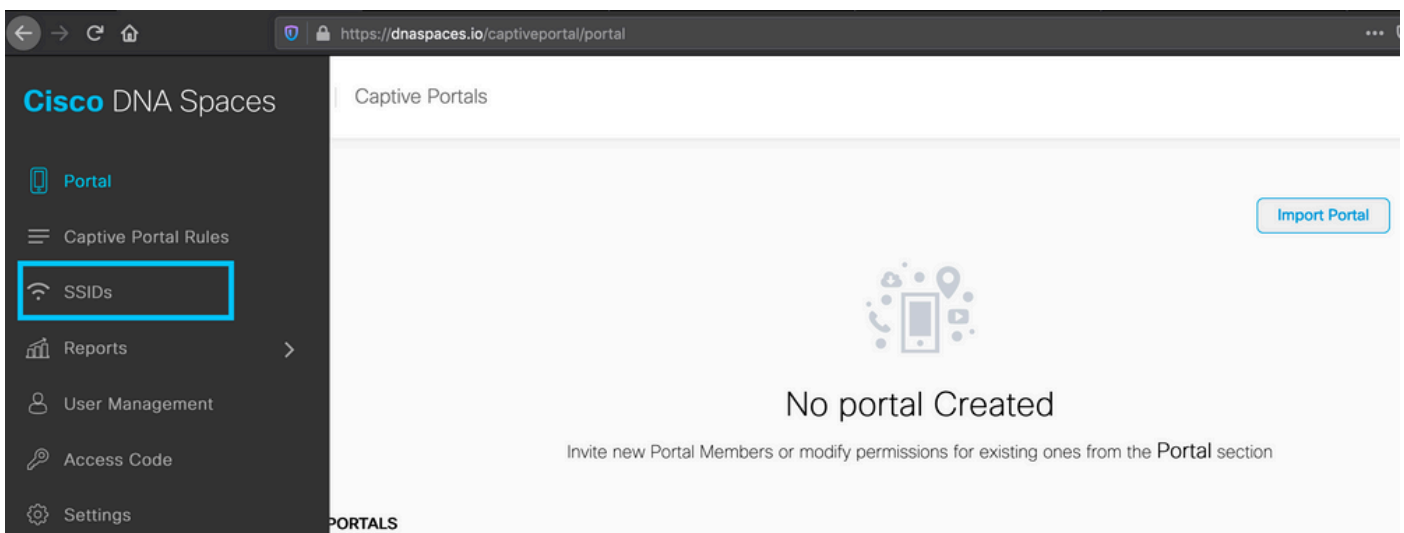
Um den Controller mit Cisco DNA Spaces zu verbinden, muss er über HTTPS in der Lage sein, Cisco DNA Spaces Cloud zu erreichen. Weitere Informationen zur Verbindung des 9800 Controllers mit DNA Spaces finden Sie unter diesem Link: [DNA Spaces - 9800 Controller Direct Connect](#)

Erstellung der SSID auf DNA-Spaces

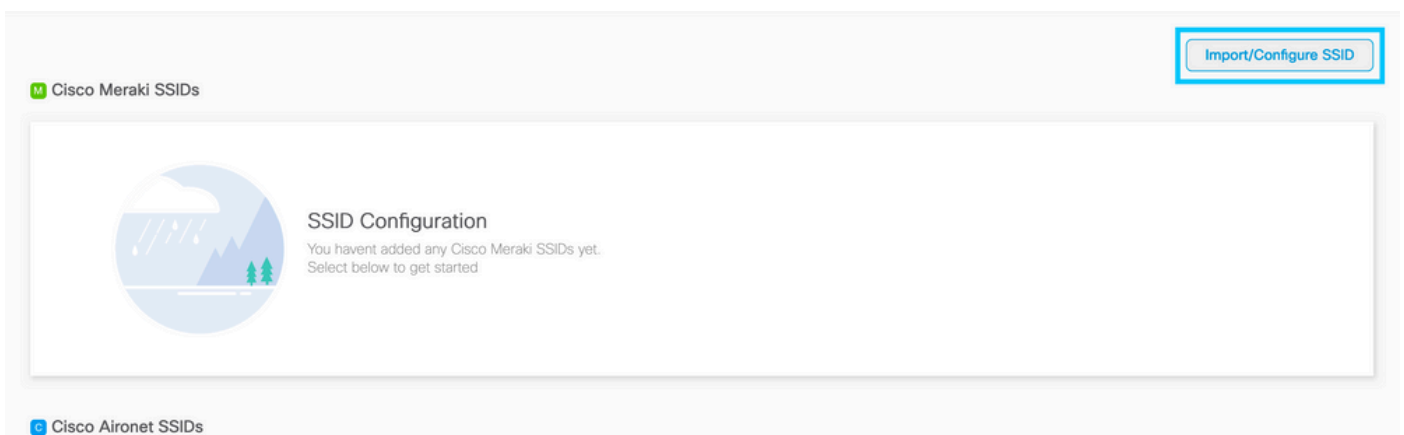
Schritt 1: Klicken Sie auf **Captive Portals** im Armaturenbrett von DNA Spaces:



Schritt 2: Öffnen Sie das spezifische Menü des Captive Portals, klicken Sie auf das Symbol mit den drei Zeilen in der oberen linken Ecke der Seite, und klicken Sie auf **SSIDs**:



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- und URL-Filterkonfiguration auf dem Controller 9800

Datenverkehr von einem Wireless-Client ist im Netzwerk erst nach Abschluss der Authentifizierung zulässig. Im Fall einer Webauthentifizierung stellt ein Wireless-Client zum

Abschließen eine Verbindung zu dieser SSID her, empfängt eine IP-Adresse und setzt den Client-Richtlinienmanager in den Zustand **Webauth_reqd**. Da der Client noch nicht authentifiziert ist, wird der gesamte Datenverkehr, der von der Client-IP-Adresse stammt, verworfen, mit Ausnahme von DHCP, DNS und HTTP (das abgefangen und umgeleitet wird).

Standardmäßig erstellt der 9800 vor der Authentifizierung hardcodierte Zugriffskontrolllisten, wenn ein Web-Auth-WLAN eingerichtet wird. Diese fest codierten ACLs ermöglichen DHCP, DNS und Datenverkehr zum externen Web-Authentifizierungsserver. Der Rest wird wie jeder HTTP-Datenverkehr umgeleitet.

Wenn Sie jedoch einen bestimmten Nicht-HTTP-Datenverkehrstyp zulassen müssen, können Sie eine Pre-Auth-ACL konfigurieren. Anschließend müssen Sie den Inhalt der bestehenden, hartcodierten ACLs vor der Authentifizierung (aus Schritt 1 in diesem Abschnitt) imitieren und an Ihre Anforderungen anpassen.

Schritt 1: Überprüfen der aktuellen hardcodierten ACLs

CLI-Konfiguration:

```
Andressi-9800L#show ip access list
```

```
Extended IP access list WA-sec-34.235.248.212
```

```
10 permit tcp any host 34.235.248.212 eq www
20 permit tcp any host 34.235.248.212 eq 443
30 permit tcp host 34.235.248.212 eq www any
40 permit tcp host 34.235.248.212 eq 443 any
50 permit tcp any any eq domain
60 permit udp any any eq domain
70 permit udp any any eq bootpc
80 permit udp any any eq bootps
90 deny ip any any
```

```
Extended IP access list WA-v4-int-34.235.248.212
```

```
10 deny tcp any host 34.235.248.212 eq www
20 deny tcp any host 34.235.248.212 eq 443
30 permit tcp any any eq www
40 permit tcp any host 192.0.2.1 eq 443
```

WA-sec-34.235.248.212 wird als solcher aufgerufen, da es sich um eine automatische Webauthentifizierungs-Sicherheitszugriffskontrollliste (WA) oder die Portal-IP "34.235.248.212" handelt. Sicherheits-ACLs definieren, was zulässig ist (bei Genehmigung) oder was abgelehnt wird (bei Ablehnung)

Wa-v4-int ist eine Intercept-ACL, d. h. eine Punkt-ACL oder eine Umleitungs-ACL, die definiert, was zur Umleitung an die CPU gesendet wird (bei Genehmigung) oder was an das Datenflugzeug gesendet wird (bei Ablehnung).

WA-v4-int34.235.248.212 wird zuerst auf den vom Client kommenden Datenverkehr angewendet und hält den HTTP(s)-Datenverkehr in Richtung des DNA Spaces-Portals IP 34.235.248.212 auf dem Datenflugzeug (noch keine Drop- oder Forward-Aktion, nur Übergabe an das Datenflugzeug). Er sendet den gesamten HTTP(s)-Verkehr an die CPU (für die Umleitung außer dem virtuellen IP-Verkehr, der vom Webserver bedient wird). Andere Arten von Datenverkehr werden an das Datenflugzeug weitergeleitet.

WA-sec-34.235.248.212 lässt HTTP- und HTTPS-Datenverkehr zum DNS-Raum zu IP 34.235.248.212, den Sie in der Web-Authentifizierungsparameterübersicht konfiguriert haben. Außerdem lässt er DNS- und DHCP-Datenverkehr zu und verwirft den Rest. Der abzufangende

HTTP-Datenverkehr wurde bereits abgefangen, bevor er diese ACL erreicht. Aus diesem Grund muss er nicht von dieser ACL abgedeckt werden.

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. Ein Beispiel finden Sie im Abschnitt "What are the IP address that DNA Spaces use" am Ende des Dokuments.

DNA Spaces verwendet 2 IP-Adressen, und der Mechanismus in Schritt 1 lässt nur die Zulassung einer Portal-IP zu. Um den Zugriff vor der Authentifizierung auf weitere HTTP-Ressourcen zu ermöglichen, müssen Sie URL-Filter verwenden, die dynamisch Lücken in den Abfangrahmen- (Umleitung) und Sicherheits- (Vorauth)-ACLs für die IPs der Website erzeugen, deren URL Sie in den URL-Filter eingeben. DNS-Anfragen werden dynamisch für den 9800 abgefragt, um die IP-Adresse dieser URLs zu ermitteln und sie den ACLs dynamisch hinzuzufügen.

Schritt 2: Konfigurieren Sie den URL-Filter so, dass die DNS-Spaces-Domäne zugelassen wird. Navigieren Sie zu Konfiguration > Sicherheit > URL-Filter, klicken Sie auf **+Hinzufügen**, und konfigurieren Sie den Listennamen, wählen Sie **PRE-AUTH** als Typ, Aktion als **PERMIT** und die URL **splash.dnaspaces.io** (oder ".eu", wenn Sie das EMEA-Portal verwenden):

The screenshot shows the 'Add URL Filter' configuration window. The 'List Name*' field is set to 'DNASpaces'. The 'Type' dropdown is set to 'PRE-AUTH'. The 'Action' is set to 'PERMIT' with a checked checkbox. The 'URLs' field contains the text 'splash.dnaspaces.io'. The window has a 'Cancel' button on the bottom left and an 'Apply to Device' button on the bottom right.

CLI-Konfiguration:

```
Andressi-9800L(config)#urlfilter list
```

Andressi-9800L(config-urlfilter-params)#action permit

Andressi-9800L(config-urlfilter-params)#url splash.dnaspaces.io

Die SSID kann für die Verwendung eines RADIUS-Servers oder ohne diesen konfiguriert werden. Wenn die Sitzungsdauer, die Bandbreitenbeschränkung 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

Konfiguration der Web Auth-Parameterzuordnung auf dem 9800-Controller

Schritt 1: Navigieren Sie zu **Configuration > Security > Web Auth**, und klicken Sie auf **+Add**, um eine neue Parameterzuordnung zu erstellen. Konfigurieren Sie in dem sich öffnenden Fenster den Namen der Parameterzuordnung, und wählen Sie **Zustimmung** als Typ:

Parameter-map name*	DNASpaces-PM
Maximum HTTP connections	1-200
Init-State Timeout(secs)	60-3932100
Type	consent

Close Apply to Device

Schritt 2: Klicken Sie auf die im vorherigen Schritt konfigurierte Parameterzuordnung, navigieren Sie zur Registerkarte **Advanced (Erweitert)**, und geben Sie die Umleitung für die Anmelde-URL, Append für die AP-MAC-Adresse, Append für die Client-MAC-Adresse, Append für die WLAN-SSID und die Portal-IPv4-Adresse ein. Klicken Sie auf **Aktualisieren und Übernehmen**:

General

Advanced

Redirect to external server

Redirect for log-in

Redirect On-Success

Redirect On-Failure

Redirect Append for AP MAC Address


Redirect Append for Client MAC Address

Redirect Append for WLAN SSID

Portal IPV4 Address

Portal IPV6 Address

Customized page


Login Failed Page 

Login Page 

Logout Page 

Login Successful Page 

✕ Cancel

 Update & Apply

Hinweis: Um die URL der Splash-Seite und die IPv4-Umleitungsadresse abzurufen, klicken Sie auf der SSID-Seite von DNA Spaces auf die Option **Configure Manually (Manuell konfigurieren)**. Dies wird im Abschnitt "Welche URL verwendet das DNA Spaces-Portal?" am Ende des Dokuments veranschaulicht.

Hinweis: Das Cisco DNA Spaces-Portal kann in zwei IP-Adressen aufgelöst werden. Der 9800 Controller lässt jedoch nur die Konfiguration einer IP-Adresse zu. Wählen Sie eine dieser IP-Adressen, und konfigurieren Sie sie in der Parameterzuordnung als IPv4-Adresse des Portals.

Hinweis: Stellen Sie sicher, dass Sowohl virtuelle IPv4- als auch IPv6-Adressen werden in der globalen Web-Authentifizierungsparameterzuordnung konfiguriert. Wenn das virtuelle IPv6 nicht konfiguriert ist, werden die Clients manchmal zum internen Portal umgeleitet, anstatt zum konfigurierten DNA Spaces-Portal. Aus diesem Grund muss immer eine virtuelle IP konfiguriert werden. "192.0.2.1" kann als virtuelles IPv4 und FE80:0:0:903A::11E4 als virtuelles IPV6 konfiguriert werden. Es gibt wenig bis gar keine Gründe, andere IPs als diese zu verwenden.

CLI-Konfiguration:

```
Andressi-9800L(config)#parameter-map type webauth
Andressi-9800L(config-params-parameter-map)#type consent
Andressi-9800L(config-params-parameter-map)#timeout init-state sec 600
Andressi-9800L(config-params-parameter-map)#redirect for-login
```

```
Andressi-9800L(config-params-parameter-map)#redirect append ap-mac tag ap_mac
Andressi-9800L(config-params-parameter-map)#redirect append wlan-ssid tag wlan
Andressi-9800L(config-params-parameter-map)#redirect append client-mac tag client_mac
Andressi-9800L(config-params-parameter-map)#redirect portal ipv4
```

```
Andressi-9800L(config-params-parameter-map)#logout-window-disabled
Andressi-9800L(config-params-parameter-map)#success-window-disabled
```

Erstellen der SSID auf dem 9800-Controller

Schritt 1: Navigieren Sie zu **Konfiguration > Tags & Profile > WLANs**, und klicken Sie auf **+Hinzufügen**. Konfigurieren Sie den Profilnamen und die SSID, und aktivieren Sie das WLAN. Stellen Sie sicher, dass der SSID-Name mit dem in Schritt 3 des Abschnitts **Erstellen der SSID auf DNA-Spaces** konfigurierten Namen übereinstimmt.

Add WLAN ✕

General **Security** Advanced

Profile Name* Radio Policy

SSID* Broadcast SSID **ENABLED**

WLAN ID*

Status **ENABLED**

Schritt 2: Navigieren Sie zu **Sicherheit > Schicht 2**. Setzen Sie den Layer 2-Sicherheitsmodus auf **"None" (Keine)**, und stellen Sie sicher, dass die MAC-Filterung deaktiviert ist.

Add WLAN ✕

General **Security** Advanced

Layer2 Layer3 AAA

Layer 2 Security Mode Fast Transition

MAC Filtering Over the DS

Transition Mode WLAN ID Reassociation Timeout

Schritt 3: Navigieren Sie zu **Sicherheit > Layer 3**. Aktivieren Sie die Webrichtlinie, und konfigurieren Sie die Webauthentifizierungsparameterzuordnung. Klicken Sie auf **Auf Gerät anwenden**.

Edit WLAN ✕

General
Security
Advanced
Add To Policy Tags

Layer2
Layer3
AAA

[Show Advanced Settings >>>](#)

Web Policy

Web Auth Parameter Map DNASpacesPM ▼

Authentication List Select a value ▼ ⓘ

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

Richtlinienprofil auf dem 9800-Controller konfigurieren

Schritt 1: Navigieren Sie zu **Configuration > Tags & Profiles > Policy**, und erstellen Sie ein neues Richtlinienprofil, oder verwenden Sie das standardmäßige Richtlinienprofil. Konfigurieren Sie auf der Registerkarte Access Policies (Zugriffsrichtlinien) das Client-VLAN, und fügen Sie den URL-Filter hinzu.

Edit Policy Profile ✕

General
Access Policies
QOS and AVC
Mobility
Advanced

RADIUS Profiling

Local Subscriber Policy Name Search or Select ▼

WLAN Local Profiling

Global State of Device Classification Disabled ⓘ

HTTP TLV Caching

DHCP TLV Caching

VLAN

VLAN/VLAN Group VLAN2672 ▼

Multicast VLAN Enter Multicast VLAN

WLAN ACL

IPv4 ACL Search or Select ▼

IPv6 ACL Search or Select ▼

URL Filters

Pre Auth DNASpaces ▼

Post Auth Search or Select ▼

Konfigurieren der Richtlinien-Tag-Nummer auf dem 9800-Controller

Schritt 1: Navigieren Sie zu **Konfiguration > Tags und Profile > Richtlinie**. Erstellen Sie ein neues Policy-Tag, oder verwenden Sie das Standard-Policy-Tag. Ordnen Sie das WLAN dem Richtlinienprofil im Richtlinien-Tag zu.

Add Policy Tag ✕

Name*

Description

▼ WLAN-POLICY Maps: 1

WLAN Profile	Policy Profile
<input type="checkbox"/> 9800DNASpaces	DNASpaces-PP

◀ 1 ▶ 10 items per page 1 - 1 of 1 items

➤ RLAN-POLICY Maps: 0

Schritt 2: Wenden Sie die Richtlinien-Tag-Nummer auf den AP an, um die SSID zu übertragen. Navigieren Sie zu **Configuration > Wireless > Access Points**, wählen Sie den betreffenden Access Point aus, und fügen Sie die Policy Tag (Richtlinien-Tag) hinzu. Dadurch startet der AP seinen CAPWAP-Tunnel neu und stellt eine Verbindung zum 9800-Controller her:

General

AP Name*

Location*

Base Radio MAC

Ethernet MAC

Admin Status ENABLED

AP Mode

Operation Status

Fabric Status

LED State ENABLED

LED Brightness Level

CleanAir [NSI Key](#)

Version

Primary Software Version	16.12.2.132
Predownloaded Status	N/A
Predownloaded Version	N/A
Next Retry Time	N/A
Boot Version	1.1.2.4
IOS Version	16.12.2.132
Mini IOS Version	0.0.0.0

IP Config

CAPWAP Preferred Mode	IPv6
SLAAC IPv6 Address	2001:172:16:30:ed0:f8ff:fe94:118c
Static IP (IPv4/IPv6)	<input type="checkbox"/>

Tags

⚠ Changing Tags will cause the AP to momentarily lose association with the Controller.

Policy

Site

RF

Time Statistics

Up Time	11 days 22 hrs 49 mins 12 secs
Controller Association Latency	3 mins 44 secs

CLI-Konfiguration:

```
Andressi-9800L(config)#wlan
```

```
Andressi-9800L(config-wlan)#no security wpa
Andressi-9800L(config-wlan)#no security wpa akm dot1x
Andressi-9800L(config-wlan)#no security wpa wpa2 ciphers aes
Andressi-9800L(config-wlan)#security web-auth
Andressi-9800L(config-wlan)#security web-auth parameter-map
Andressi-9800L(config-wlan)#no shutdown
```

```
Andressi-9800L(config)#wireless profile policy
```

```
Andressi-9800L(config-wireless-policy)#vlan <id>  
Andressi-9800L(config-wireless-policy)#urlfilter list pre-auth-filter
```

```
Andressi-9800L(config-wireless-policy)#no shutdown
```

```
Andressi-9800L(config)#wireless tag policy
```

```
Andressi-9800L(config-policy-tag)#wlan
```

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 Web Auth-Parameterzuordnung auf dem 9800-Controller

Schritt 1: Erstellen einer Web-Authentifizierungsparameterzuordnung Navigieren Sie zu **Configuration > Security > Web Auth**, klicken Sie auf **+Add**, konfigurieren Sie den Namen der Parameterzuordnung, und wählen Sie **webauth** als Typ aus:

Create Web Auth Parameter ✕

Parameter-map name*	DNASpaces-PM
Maximum HTTP connections	1-200
Init-State Timeout(secs)	60-3932100
Type	webauth ▼

✕ Close ✓ Apply to Device

Schritt 2: Klicken Sie auf die in Schritt 1 konfigurierte Parameterzuordnung, klicken Sie auf **Erweitert**, und geben Sie die Umleitung für die Anmeldung, Anfügen für AP-MAC-Adresse, Anfügen für Client-MAC-Adresse, Anfügen für WLAN-SSID und Portal-IPv4-Adresse ein. Klicken Sie auf **Aktualisieren und anwenden**:

General

Advanced

Redirect to external server

Redirect for log-in

Redirect On-Success

Redirect On-Failure

Redirect Append for AP MAC Address


Redirect Append for Client MAC Address

Redirect Append for WLAN SSID

Portal IPV4 Address

Portal IPV6 Address

Customized page


Login Failed Page 

Login Page 

Logout Page 

Login Successful Page 

✕ Cancel

 Update & Apply

Hinweis: Um die URL der Splash-Seite und die IPv4-Umleitungsadresse abzurufen, klicken Sie auf die Option **Manuell konfigurieren** der SSID, die in Schritt 3 des Abschnitts **Erstellen der SSID auf DNA-Spaces** unter **Erstellen der SSIDs in WLC Direct Connect** Abschnitt Erstellen der **Konfiguration** der Zugriffskontrollliste Abschnitt erstellt wurde.

Hinweis: Das Cisco DNA Spaces-Portal kann in zwei IP-Adressen aufgelöst werden. Der Controller 9800 lässt jedoch nur die Konfiguration einer IP-Adresse zu. In einem Fall können Sie eine dieser IP-Adressen in der Parameterzuordnung als IPv4-Adresse des Portals konfigurieren.

Anmerkung: Stellen Sie sicher, dass sowohl virtuelle IPv4- als auch IPv6-Adressen in der globalen Parameterzuordnung für die Webauthentifizierung konfiguriert sind. Wenn das virtuelle IPv6 nicht konfiguriert ist, werden die Clients manchmal zum internen Portal umgeleitet, anstatt zum konfigurierten DNA Spaces-Portal. Aus diesem Grund muss immer eine virtuelle IP konfiguriert werden. "192.0.2.1" kann als virtuelles IPv4 und FE80:0:0:0:903A::11E4 als virtuelles IPV6 konfiguriert werden. Es gibt wenig bis gar keine Gründe, andere IPs als diese zu verwenden.

CLI-Konfiguration:

```
Andressi-9800L(config)#parameter-map type webauth
Andressi-9800L(config-params-parameter-map)#type webauth
Andressi-9800L(config-params-parameter-map)#timeout init-state sec 600
Andressi-9800L(config-params-parameter-map)#redirect for-login
```

```
Andressi-9800L(config-params-parameter-map)#redirect append ap-mac tag ap_mac
Andressi-9800L(config-params-parameter-map)#redirect append wlan-ssid tag wlan
Andressi-9800L(config-params-parameter-map)#redirect append client-mac tag client_mac
Andressi-9800L(config-params-parameter-map)#redirect portal ipv4
```

```
Andressi-9800L(config-params-parameter-map)#logout-window-disabled
Andressi-9800L(config-params-parameter-map)#success-window-disabled
```

Konfiguration der RADIUS-Server auf dem Controller 9800

Schritt 1: Konfigurieren der RADIUS-Server Cisco DNA Spaces fungiert als RADIUS-Server für die Benutzerauthentifizierung und kann auf zwei IP-Adressen antworten. Navigieren Sie zu **Configuration > Security > AAA**, klicken Sie auf **+Add**, und konfigurieren Sie beide RADIUS-Server:

Configuration > Security > AAA

+ AAA Wizard

Servers / Groups AAA Method List AAA Advanced

+ Add - Delete

RADIUS

Servers Server Groups

TACACS+

Create AAA Radius Server

Name*	DNASpaces1
IPv4 / IPv6 Server Address*	34.197.146.105
PAC Key	<input type="checkbox"/>
Key Type	0
Key*	*****
Confirm Key*	*****
Auth Port	1812
Acct Port	1813
Server Timeout (seconds)	1-1000
Retry Count	0-100
Support for CoA	ENABLED <input checked="" type="checkbox"/>

Cancel Apply to Device

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 die RADIUS-Servergruppe, und fügen Sie beide RADIUS-Server hinzu. Navigieren Sie zu **Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups**, klicken Sie auf **+add**, konfigurieren Sie den Servergruppennamen, das MAC-Trennzeichen als **Bindestrich**, die MAC-Filterung als **MAC**, und weisen Sie die beiden RADIUS-Server zu:

+ AAA Wizard

Servers / Groups AAA Method List AAA Advanced

+ Add

Delete

RADIUS

TACACS+

LDAP

Servers Server Groups

Name Server 1 Server 2

0 10 items per page

Create AAA Radius Server Group

Name* DNASpaces

Group Type RADIUS

MAC-Delimiter hyphen

MAC-Filtering mac

Dead-Time (mins) 1-1440

Available Servers

> <

Assigned Servers

DNASpaces1
DNASpaces2

Cancel

Apply to Device

Schritt 3: Konfigurieren einer Liste von Authentifizierungsmethoden Navigieren Sie zu **Configuration > Security > AAA > AAA Method List > Authentication**, und klicken Sie auf **+add**. Konfigurieren Sie den Namen der Methodenliste, wählen Sie **login** als Typ aus, und weisen Sie die Servergruppe zu:

Configuration > Security > AAA

+ AAA Wizard

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

Authentication

Authorization

Accounting

+ Add - Delete

Name	Type	Group Type	Group1	Group2
<input type="checkbox"/> default	dot1x	local	N/A	N/A

10 items per page

Quick Setup: AAA Authentication

Method List Name* DNASpaces

Type* login

Group Type group

Fallback to local

Available Server Groups

- radius
- ldap
- tacacs+

Assigned Server Groups

- DNASpaces

Cancel Apply to Device

Schritt 4: Konfigurieren einer Liste von Autorisierungsmethoden Navigieren Sie zu **Configuration > Security > AAA > AAA Method List > Authorization**, und klicken Sie auf **+hinzufügen**. Konfigurieren Sie den Namen der Methodenliste, wählen Sie **Netzwerk** als Typ aus, und weisen Sie die Servergruppe zu:

Configuration > Security > AAA

+ AAA Wizard

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

Authentication

Authorization

Accounting

+ Add × Delete

Name	Type	Group Type	Group1	Group2
<input type="checkbox"/> MeshAP	credential-download	local	N/A	N/A

10 items per page

Quick Setup: AAA Authorization

Method List Name* DNASpaces

Type* network

Group Type group

Fallback to local

Authenticated

Available Server Groups

radius
ldap
tacacs+

Assigned Server Groups

DNASpaces

Cancel Apply to Device

Erstellen der SSID auf dem 9800-Controller

Schritt 1: Navigieren Sie zu **Konfiguration > Tags & Profile > WLANs**, und klicken Sie auf **+Hinzufügen**. Konfigurieren Sie den Profilnamen und die SSID, und aktivieren Sie das WLAN. Stellen Sie sicher, dass der SSID-Name mit dem in Schritt 3 des Abschnitts **Erstellen der SSID auf DNA-Spaces** konfigurierten Namen übereinstimmt.

Add WLAN ✕

General Security Advanced

Profile Name* Radio Policy

SSID* Broadcast SSID

WLAN ID*

Status

Schritt 2: Navigieren Sie zu **Sicherheit > Schicht 2**. Setzen Sie den Layer 2-Sicherheitsmodus auf **None**, aktivieren Sie die MAC-Filterung, und fügen Sie die Autorisierungsliste hinzu:

Add WLAN ✕

General **Security** Advanced

Layer2 Layer3 AAA

Layer 2 Security Mode Fast Transition

MAC Filtering Over the DS

Transition Mode WLAN ID Reassociation Timeout

Authorization List*

Schritt 3: Navigieren Sie zu **Sicherheit > Layer 3**. Aktivieren Sie die Webrichtlinie, konfigurieren Sie die Webauthentifizierungsparameterzuordnung und die Authentifizierungsliste. Aktivieren Sie On Mac Filter Failure (Bei Mac-Filterfehler), und fügen Sie die ACL für die Vorauthentifizierung hinzu. Klicken Sie auf **Auf Gerät anwenden**.

Add WLAN



General **Security** Advanced

Layer2 **Layer3** AAA

Web Policy	<input checked="" type="checkbox"/>
Web Auth Parameter Map	DNASpaces-PM
Authentication List	DNASpaces

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

<< Hide

On Mac Filter Failure	<input checked="" type="checkbox"/>
-----------------------	-------------------------------------

Splash Web Redirect	<input type="checkbox"/> DISABLED
---------------------	-----------------------------------

Preauthentication ACL

IPv4	DNASpaces-ACL
------	---------------

IPv6	None
------	------

Cancel

Apply to Device

Richtlinienprofil auf dem 9800-Controller konfigurieren

Schritt 1: Navigieren Sie zu **Configuration > Tags & Profiles > Policy**, und erstellen Sie ein neues Richtlinienprofil, oder verwenden Sie das standardmäßige Richtlinienprofil. Konfigurieren Sie auf der Registerkarte Access Policies (Zugriffsrichtlinien) das Client-VLAN, und fügen Sie den URL-Filter hinzu.

Edit Policy Profile



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

RADIUS Profiling	<input type="checkbox"/>
Local Subscriber Policy Name	Search or Select

WLAN Local Profiling

Global State of Device Classification **Disabled** ⓘ

HTTP TLV Caching	<input type="checkbox"/>
------------------	--------------------------

DHCP TLV Caching	<input type="checkbox"/>
------------------	--------------------------

VLAN

VLAN/VLAN Group	VLAN2672
-----------------	----------

Multicast VLAN	Enter Multicast VLAN
----------------	----------------------

WLAN ACL

IPv4 ACL	Search or Select
----------	------------------

IPv6 ACL	Search or Select
----------	------------------

URL Filters

Pre Auth	DNASpaces
----------	-----------

Post Auth	Search or Select
-----------	------------------

Schritt 2: Aktivieren Sie auf der Registerkarte Advanced die Option AAA Override, und konfigurieren Sie optional die Abrechnungsmethodenliste:

Edit Policy Profile



General

Access Policies

QOS and AVC

Mobility

Advanced

WLAN Timeout

Session Timeout (sec)	<input type="text" value="1800"/>
Idle Timeout (sec)	<input type="text" value="300"/>
Idle Threshold (bytes)	<input type="text" value="0"/>
Client Exclusion Timeout (sec)	<input checked="" type="checkbox"/> <input type="text" value="60"/>

DHCP

IPv4 DHCP Required	<input type="checkbox"/>
DHCP Server IP Address	<input type="text"/>

[Show more >>>](#)

AAA Policy

Allow AAA Override	<input checked="" type="checkbox"/>
NAC State	<input type="checkbox"/>
Policy Name	<input type="text" value="default-aaa-policy x"/>
Accounting List	<input type="text" value="DNASpaces x"/>

Fabric Profile	<input type="checkbox"/> <input type="text" value="Search or Select"/>
Umbrella Parameter Map	<input type="text" value="Not Configured"/>
mDNS Service Policy	<input type="text" value="default-mdns-service"/> Clear

WLAN Flex Policy

VLAN Central Switching	<input type="checkbox"/>
Split MAC ACL	<input type="text" value="Search or Select"/>

Air Time Fairness Policies

2.4 GHz Policy	<input type="text" value="Search or Select"/>
5 GHz Policy	<input type="text" value="Search or Select"/>

Konfigurieren der Richtlinien-Tag-Nummer auf dem 9800-Controller

Schritt 1: Navigieren Sie zu **Konfiguration > Tags und Profile > Richtlinie**. Erstellen Sie ein neues Policy-Tag, oder verwenden Sie das Standard-Policy-Tag. Ordnen Sie das WLAN dem Richtlinienprofil im Richtlinien-Tag zu.

Add Policy Tag ✕

Name*

Description

▼ WLAN-POLICY Maps: 1

WLAN Profile	Policy Profile
<input type="checkbox"/> 9800DNASpaces	DNASpaces-PP

◀ 1 ▶ 10 items per page 1 - 1 of 1 items

➤ RLAN-POLICY Maps: 0

Schritt 2: Wenden Sie die Richtlinien-Tag-Nummer auf den AP an, um die SSID zu übertragen. Navigieren Sie zu **Configuration > Wireless > Access Points**, wählen Sie den betreffenden Access Point aus, und fügen Sie die Policy Tag (Richtlinien-Tag) hinzu. Dadurch startet der AP seinen CAPWAP-Tunnel neu und stellt eine Verbindung zum 9800-Controller her:

General

AP Name*

Location*

Base Radio MAC

Ethernet MAC

Admin Status ENABLED

AP Mode

Operation Status

Fabric Status

LED State ENABLED

LED Brightness Level

CleanAir [NSI Key](#)

Version

Primary Software Version	16.12.2.132
Predownloaded Status	N/A
Predownloaded Version	N/A
Next Retry Time	N/A
Boot Version	1.1.2.4
IOS Version	16.12.2.132
Mini IOS Version	0.0.0.0

IP Config

CAPWAP Preferred Mode	IPv6
SLAAC IPv6 Address	2001:172:16:30:ed0:f8ff:fe94:118c
Static IP (IPv4/IPv6)	<input type="checkbox"/>

Tags

⚠ Changing Tags will cause the AP to momentarily lose association with the Controller.

Policy

Site

RF

Time Statistics

Up Time	11 days 22 hrs 49 mins 12 secs
Controller Association Latency	3 mins 44 secs

CLI-Konfiguration:

```
Andressi-9800L(config)#wlan
```

```
Andressi-9800L(config-wlan)#ip access-group web
```

```
Andressi-9800L(config-wlan)#no security wpa
Andressi-9800L(config-wlan)#no security wpa akm dot1x
```

```
Andressi-9800L(config-wlan)#no security wpa wpa2 ciphers aes
Andressi-9800L(config-wlan)#mac-filtering
```

```
Andressi-9800L(config-wlan)#security web-auth
Andressi-9800L(config-wlan)#security web-auth authentication-list
```

```
Andressi-9800L(config-wlan)#security web-auth on-macfilter-failure
Andressi-9800L(config-wlan)#security web-auth parameter-map
Andressi-9800L(config-wlan)#no shutdown
```

```
Andressi-9800L(config)#wireless profile policy
```

```
Andressi-9800L(config-wireless-policy)#aaa-override
Andressi-9800L(config-wireless-policy)#accounting-list
```

```
Andressi-9800L(config-wireless-policy)#vlan <id>
Andressi-9800L(config-wireless-policy)#urlfilter list pre-auth-filter
```

```
Andressi-9800L(config-wireless-policy)#no shutdown
```

```
Andressi-9800L(config)#wireless tag policy
```

```
Andressi-9800L(config-policy-tag)#wlan
```

Globale Parameterzuordnung konfigurieren

Unempfehlenswerter Schritt: Führen Sie diese Befehle aus, um die HTTPS-Umleitung zu ermöglichen. Beachten Sie jedoch, dass die Umleitung im HTTPS-Datenverkehr des Clients nicht erforderlich ist, wenn das Client-Betriebssystem Captive Portal erkennt, eine intensivere CPU-Auslastung verursacht und immer eine Zertifikatwarnung ausgibt. Es wird daher empfohlen, die Konfiguration zu vermeiden, wenn sie nicht für einen bestimmten Anwendungsfall erforderlich ist.

```
Andressi-9800L(config)#parameter-map type webauth global
Andressi-9800L(config-params-parameter-map)#intercept-https-enable
```

Hinweis: Sie müssen über ein gültiges SSL-Zertifikat für die virtuelle IP verfügen, das auf dem Cisco Catalyst Wireless Controller der Serie 9800 installiert ist.

Schritt 1: Kopieren Sie die signierte zertifizierte Datei mit der Erweiterung .p12 auf einen TFTP-Server, und führen Sie diesen Befehl aus, um das Zertifikat zu übertragen und auf dem 9800-Controller zu installieren:

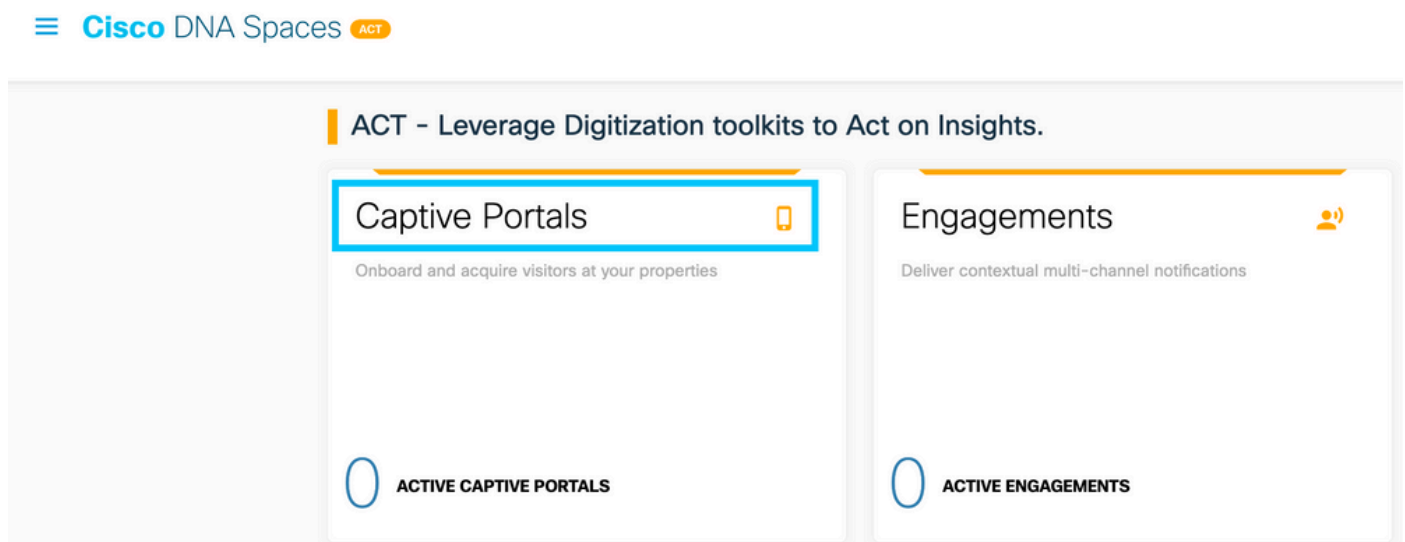
```
Andressi-9800L(config)#crypto pki import
```

Schritt 2: Führen Sie die folgenden Befehle aus, um das installierte Zertifikat der Webauthentifizierungsparameterzuordnung zuzuordnen:

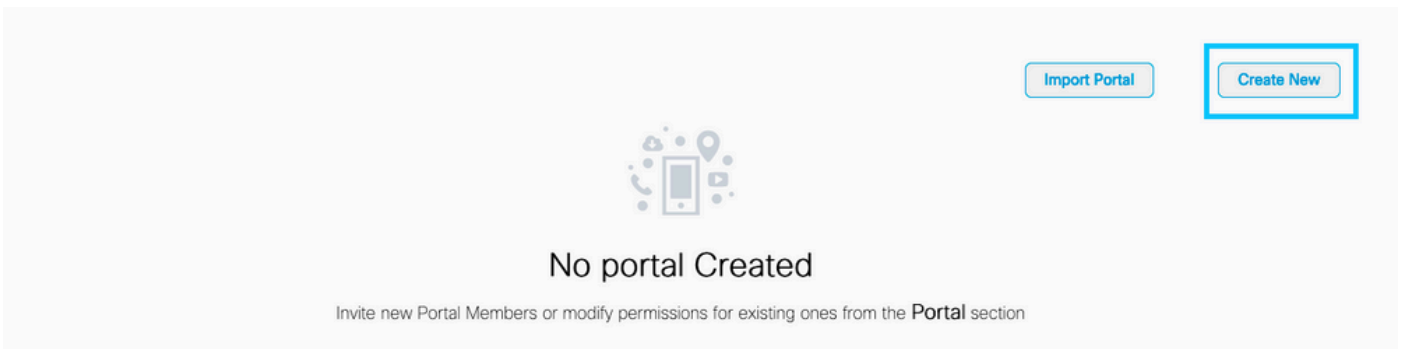
```
Andressi-9800L(config)#parameter-map type webauth global
Andressi-9800L(config-params-parameter-map)#trustpoint
```

Portal zu DNA Spaces erstellen

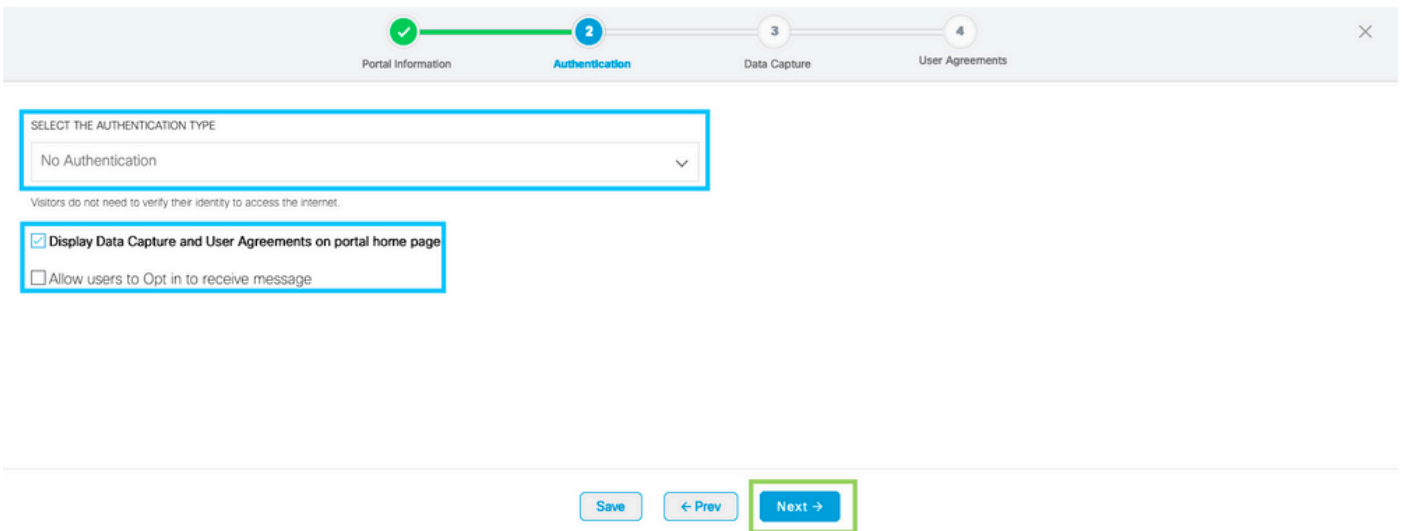
Schritt 1: Klicken Sie auf **Captive Portals** im Armaturenbrett von DNA Spaces:



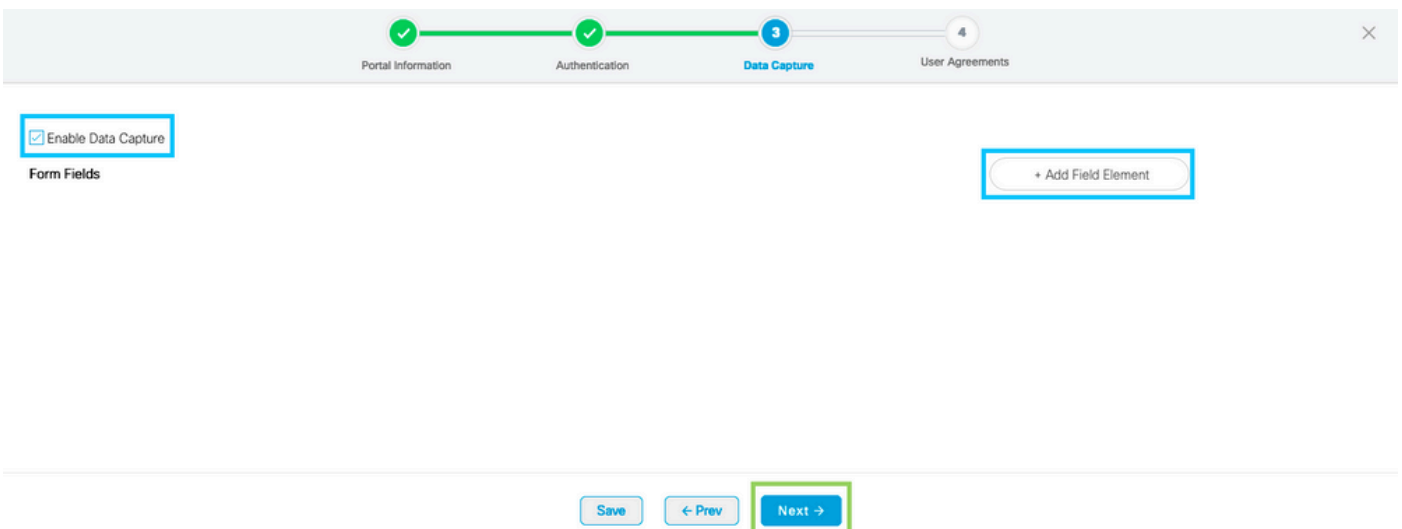
Schritt 2: Klicken Sie auf **Neu erstellen**, geben Sie den Portalnamen ein, und wählen Sie die Standorte aus, die das Portal nutzen können:



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**:

✓ Portal Information
✓ Authentication
✓ Data Capture
4 User Agreements

This section allows you to enable and configure Terms & Conditions and Privacy policy Statements.

Enable Terms & Conditions

TERMS & CONDITION MESSAGE English

Wi-Fi Terms of Use, Last updated: September 27, 2013.

These Wi-Fi Terms & Conditions Of Use (the Wi-Fi Terms) together with the TERMS OF USE govern your use of the Wi-Fi service.

Description of the Service

The Service provides you with wireless access to the Internet within the premises. We do not, as an ordinary practice, proactively monitor the activities of those who use the Service or exercise any editorial control over any material transmitted, hosted or posted using the Service to ensure that users comply with these Wi-Fi Terms and/or the law, although it reserves the right to do so.

Save
← Prev
Save & Configure Portal

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

LOCATIONS: 1 Location ✓ | AUTH TYPE: No Authentication ✓ | USER AGREEMENTS: Enabled ✓ | DATA CAPTURE: Email, Mobile Number ✓

PORTAL EDITOR - Select a section to configure. Drag the items to reorder modules.

- Brand Name
- Welcome Message
- Notice
- Data Capture
- Venue Map
- Videos
- Feedback
- Help
- Get Apps
- Get Internet
- Promos & Offers

+ Add Module

WELCOME MESSAGE

First time visitor welcome text

Welcome to Cisco Mexico

Add a custom message for Repeat visitors

Hi \${firstName} \${lastName}, Welcome to \$location x

Note
If any variables used in the message above are not available. We will default to the message shown for first time visitors.

PORTAL PREVIEW

Home Screen

ACME Company

Welcome to Cisco Mexico

SIGN-UP FOR WIFI

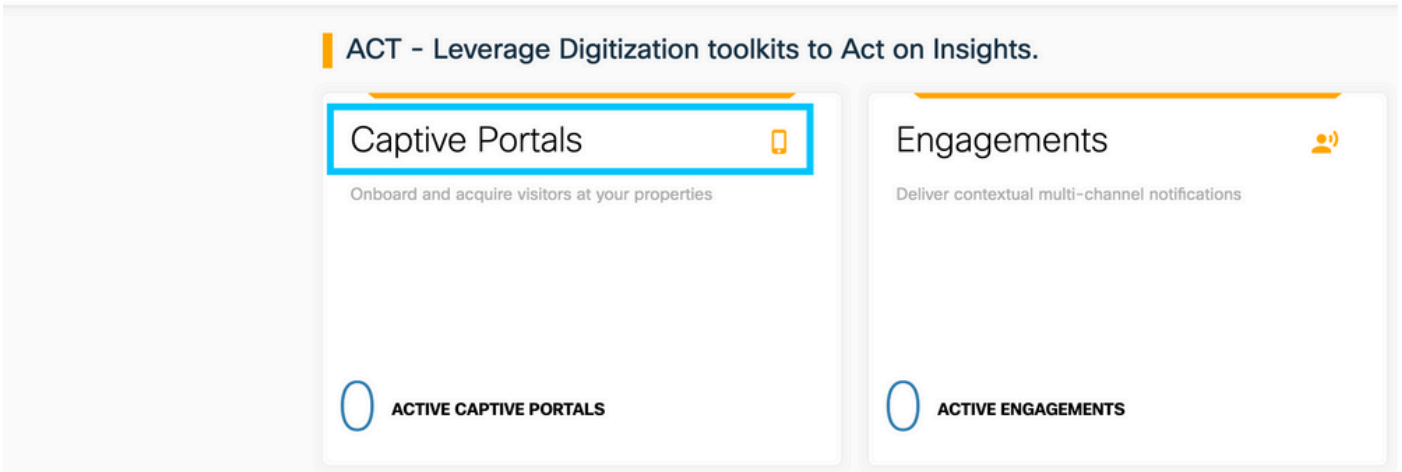
Email Address

Mobile Number

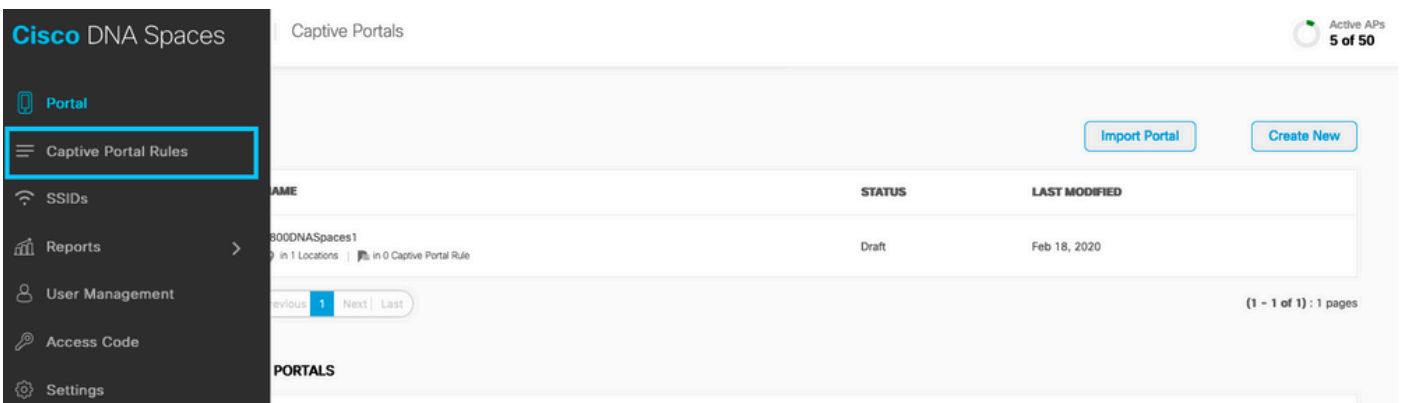
Save
Cancel

Konfigurieren der Captive Portal-Regeln für DNA-Bereiche

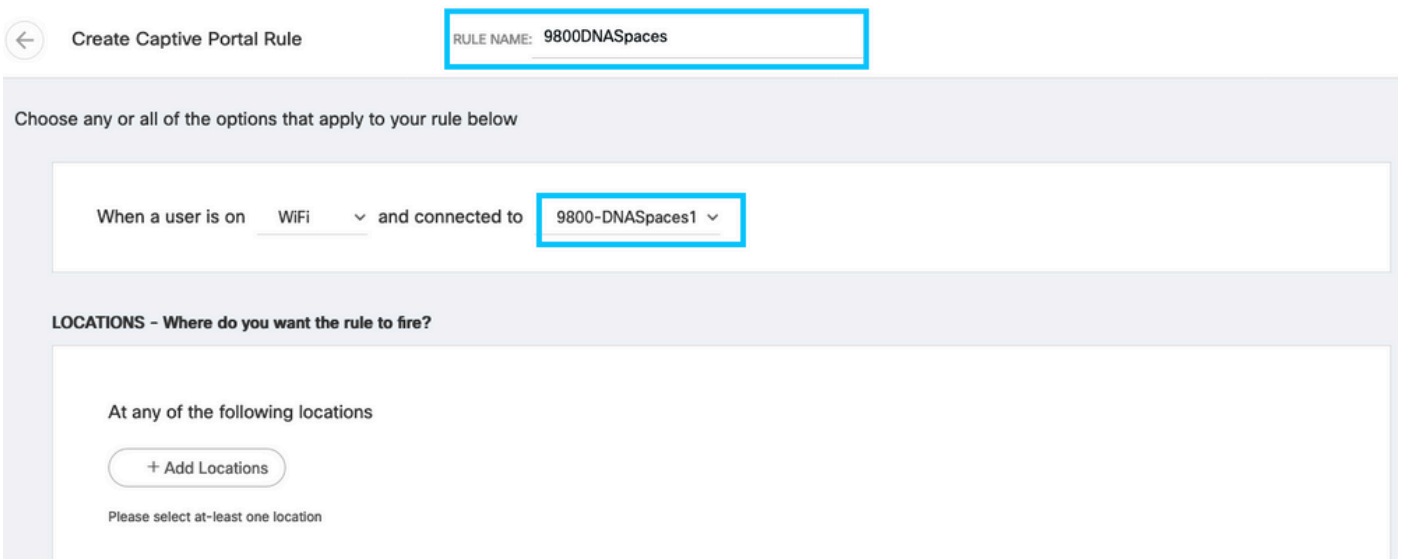
Schritt 1: Klicken Sie auf **Captive Portals** im Armaturenbrett von DNA Spaces:



Schritt 2: Öffnen Sie das Captive Portal-Menü, und klicken Sie auf **Captive Portal Rules**:



Schritt 3: Klicken Sie auf **+ Neue Regel erstellen**. Geben Sie den Regelnamen ein, und wählen Sie die zuvor konfigurierte SSID aus.



Schritt 4: Wählen Sie die Standorte aus, an denen das Portal verfügbar ist. Klicken Sie im Abschnitt **STANDORTE** auf **Standort hinzufügen**. Wählen Sie die gewünschte Option aus der Standorthierarchie aus.

Choose Locations

Location Hierarchy

MEX-EAST-1	<input type="checkbox"/>
+ 5508-1-CMX	<input type="checkbox"/>
+ 5508-2-Connector	<input type="checkbox"/>
+ 5520-1-DirectConnect	<input type="checkbox"/>
9800L-DirectConnect	<input checked="" type="checkbox"/>

Selected Locations

9800L-DirectConnect X

Schritt 5: 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**.

ACTIONS

Show Captive Portal
Choose a Portal to be displayed to Users when they connect to the wifi.

9800DNASpaces1

Session Duration

Bandwidth Limit

Seamlessly Provision Internet
Directly provision internet without showing any authentication

Deny Internet
Stop users from accessing the internet

Tags these users as
Choose - Associate/Disassociate users to chosen tags.

+ Add Tags

Trigger API

Save & Publish Save

SCHEDULE

ACTION

Show Captive Portal
Portal : 9800DNASpaces1

Spezifische Informationen von DNA Spaces abrufen

Welche IP-Adressen verwenden DNA Spaces?

Um zu überprüfen, welche IP-Adressen DNA-Spaces für das Portal in Ihrer Region verwenden, gehen Sie zur Seite des Captivals auf der Homepage von DNA Space. Klicken Sie im linken Menü auf **SSID** und anschließend unter Ihrer SSID auf **Manuell konfigurieren**. Die IP-Adressen werden im ACL-Beispiel angegeben. Dies sind die IP-Adressen des Portals zur Verwendung in ACLs und in der Webauthentifizierungsparameterzuordnung. DNA Spaces verwenden andere IP-Adressen für die gesamte NMSP-/Cloud-Anbindung der Kontrollebene.

Import/Configure SSID

Cisco Meraki SSIDs

SSID Configuration
You haven't added any Cisco Meraki SSIDs yet.
Select below to get started.

Cisco Aironet SSIDs

Guest LAB-DNAS

Delete Configure Manually Delete **Configure Manually**

Im ersten Abschnitt des Popup-Fensters werden in Schritt 7 die in der ACL-Definition genannten IP-Adressen angezeigt. Sie müssen diese Anweisungen nicht ausführen und keine ACL erstellen. Notieren Sie sich nur die IP-Adressen. Dies sind die IPs, die vom Portal in Ihrer Region verwendet werden

Configure



Creating the Access Control List

To create the access control list, perform the following steps:

- 1 Log in to the WLC Direct Connect with your WLC Direct Connect credentials.
- 2 Choose **Security > Access Control Lists > Access Control Lists**.
For FlexConnect local mode, choose **Security > Access Control Lists > FlexConnect ACLs**.
- 3 To add an ACL, click **New**.
- 4 In the **New** page that appears, enter the following:
 - a. In the **Access Control List Name** field, enter a name for the new ACL.

Note:
You can enter up to 32 alphanumeric characters.

- b. Choose the ACL type as **IPv4**.

Note:
This option is not available for FlexConnect ACLs.

- c. Click **Apply**.

- 5 When the **Access Control Lists** page reappears, click the name of the new ACL.
- 6 In the **Edit** page that appears, click **Add New Rule**. The **Rules > New** page appears.
- 7 Configure a rule for this ACL with the following wall garden ranges.

No	Dir	Source IP Address/Netmask	Destination IP Address/Netmask	Protocol	Source Port Range	Dest Port Range	DSCP	Action
1.	Any	0.0.0.0/0.0.0.0	54.77.207.183/255.255.255.255	TCP	Any	HTTPS	Any	Permit
2.	Any	54.77.207.183/255.255.255.255	0.0.0.0/0.0.0.0	TCP	HTTPS	Any	Any	Permit
3.	Any	0.0.0.0/0.0.0.0	34.252.175.120/255.255.255.255	TCP	Any	HTTPS	Any	Permit
4.	Any	34.252.175.120/255.255.255.255	0.0.0.0/0.0.0.0	TCP	HTTPS	Any	Any	Permit

Welche URL verwendet das DNA Spaces-Anmeldeportal?

Um zu überprüfen, welche Login-Portal-URL DNA-Spaces für das Portal in Ihrer Region verwenden, gehen Sie zur Seite des Captivals auf der Homepage von DNA Space. Klicken Sie im linken Menü auf **SSID** und anschließend unter Ihrer SSID auf **Manuell konfigurieren**.



Blättern Sie im Pop-Up nach unten, das erscheint, und im zweiten Abschnitt zeigt Schritt 7 die URL an, die Sie in Ihrer Parameterzuordnung auf dem 9800 konfigurieren müssen.

Creating the SSIDs in WLC Direct Connect

To create the SSIDs in the WLC Direct Connect, perform the following steps:

- 1 In the WLC Direct Connect main window, click the **WLANS** tab.
- 2 To create a WLAN, choose **Create New** from the drop-down list at the right side of the page, and click **Go**.
- 3 In the New page that appears, enter the WLAN details like Type, Profile Name, SSID, and so on.
- 4 Click **Apply**.
The WLAN added appears in the WLANS page.
- 5 Click the WLAN you have newly created.
- 6 Choose **Security > Layer 2** , and configure the Layer 2 Security as **None** .
- 7 In the **Layer 3 tab** , do the following configurations:
 - a.From the Layer 3 security drop-down list, choose **Web Policy** .
 - b.Choose the **Passthrough** radio button.
 - c.In the Preauthentication ACL area, from the IPv4 drop-down list, choose the ACL created earlier.
 - d.Select the Enable check box for the Sleeping Client.
 - e.Select the Enable check box for the Override Global Config.
 - f.From the Web Auth Type drop-down list, choose **External** .
 - g.In the URL field that appears, enter the Cisco DNA Spaces splash URL.

<https://splash.dnaspaces.eu/p2/emeabru2>

Was sind die RADIUS-Serverdetails für DNA Spaces?

Um herauszufinden, welche RADIUS-Server-IP-Adressen Sie verwenden müssen, sowie das gemeinsame Geheimnis, gehen Sie auf die Seite des Captivals Portal auf der DNA-Space-Homepage. Klicken Sie im linken Menü auf **SSID** und anschließend unter Ihrer SSID auf **Manuell konfigurieren**.



Scrollen Sie im Popup-Fenster im dritten Abschnitt (RADIUS) nach unten, und in Schritt 7 erhalten Sie die IP-Adresse/den Port und den gemeinsamen geheimen Schlüssel für die RADIUS-Authentifizierung. Die Abrechnung ist optional und wird in Schritt 12 behandelt.

- 7 In the New page that appears, enter the details of the radius server for authentication, such as server IP address, port number, and secret key, select the Server Status as **Enabled** , and click **Apply**.

Host: 52.51.31.103,34.241.1.84
Port: 1812
Secret Key: emeab1299E2PqvJK

- 8 Choose **Radius > Accounting**.

The Radius Accounting Servers page appears.

- 9 From the Acct Called Station ID Type, choose **AP MAC Address:SSID**.

- 10 From the MAC Delimiter drop-down list, choose **Hyphen**.

- 11 Click **New**.

- 12 In the New page that appears, enter the details of the radius server for accounting, such as server IP address, port number, and secret key, select the Server Status as **Enabled** , and click **Apply**.

Host: 52.51.31.103,34.241.1.84
Port: 1813
Secret Key: emeab1299E2PqvJK

Überprüfung

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

Client	
360 View General QOS Statistics ATF Statistics Mobility History Call Statistics	
Client Properties AP Properties Security Information Client Statistics QOS Properties	
Wireless LAN Id	1
WLAN Profile Name	9800-DNASpaces1
Wireless LAN Network Name (SSID)	9800-DNASpaces1
BSSID	10b3.d694.00ef
Uptime(sec)	64 seconds
Session Timeout	1800 sec (Remaining time: 1762 sec)
Session Warning Time	Timer not running
Client Active State	Active
Power Save mode	OFF
Current TxRateSet	m2 ss1
Supported Rates	9.0,18.0,36.0,48.0,54.0
Join Time Of Client	03/11/2020 17:47:25 Central
Policy Manager State	Run

Fehlerbehebung

Häufige Probleme

1. Wenn für die virtuelle Schnittstelle auf dem Controller keine IP-Adresse konfiguriert wurde, werden die Clients zum internen Portal umgeleitet, anstatt zum Umleitungsportal, das in der Parameterzuordnung konfiguriert wurde.
2. Wenn Clients einen *503-Fehler* erhalten, während sie zum Portal auf DNA-Spaces umgeleitet werden, stellen Sie sicher, dass der Controller in der **Standorthierarchie** auf DNA-Spaces konfiguriert ist.

Stets verfügbare Ablaufverfolgung

WLC 9800 bietet ALWAYS-ON-Tracing-Funktionen (immer aktiv). So wird sichergestellt, dass alle verbindungsbezogenen Fehler, Warnungen und Meldungen auf Benachrichtigungsebene ständig protokolliert werden und Sie Protokolle zu einem Vorfall oder einem Fehler anzeigen können, nachdem dieser aufgetreten ist.

Hinweis: Je nach Umfang der generierten Protokolle können Sie einige Stunden bis mehrere Tage zurückgehen.

Um die Traces anzuzeigen, die 9800 WLC standardmäßig gesammelt hat, können Sie sich über SSH/Telnet mit dem 9800 WLC verbinden und diese Schritte ausführen (Stellen Sie sicher, dass Sie die Sitzung in einer Textdatei protokollieren).

Schritt 1: Überprüfen Sie die aktuelle Uhrzeit des Controllers, damit Sie die Protokolle bis zum Auftreten des Problems nachverfolgen können.

```
# show clock
```

Schritt 2: Erfassen Sie die Syslogs aus dem Controller-Puffer oder dem externen Syslog gemäß der Systemkonfiguration. Dadurch erhalten Sie eine Kurzübersicht über den Systemstatus und etwaige Fehler.

```
# show logging
```

Schritt 3: Überprüfen Sie, ob Debug-Bedingungen aktiviert sind.

```
# show debugging
Cisco IOS-XE Conditional Debug Configs:
```

```
Conditional Debug Global State: Stop
```

```
Cisco IOS-XE Packet Tracing Configs:
```

```
Packet Infra debugs:
```

```
Ip Address                               Port
-----|-----
```

Hinweis: Wenn eine Bedingung aufgelistet wird, bedeutet dies, dass die Traces für alle Prozesse, bei denen die aktivierten Bedingungen auftreten (MAC-Adresse, IP-Adresse usw.) auf Debugging-Ebene protokolliert werden. Dies würde das Protokollvolumen erhöhen. Daher wird empfohlen, alle Bedingungen zu löschen, wenn gerade kein Debugging aktiv ist

Schritt 4: Wenn die zu testende MAC-Adresse in Schritt 3 nicht als Bedingung aufgeführt wurde, sammeln Sie die stets verfügbaren Traces für die jeweilige MAC-Adresse.

```
# show logging profile wireless filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file
always-on-<FILENAME.txt>
```

Sie können entweder den Inhalt der Sitzung anzeigen oder die Datei auf einen externen TFTP-Server kopieren.

```
# more bootflash:always-on-<FILENAME.txt>
or
# copy bootflash:always-on-<FILENAME.txt> tftp://a.b.c.d/path/always-on-<FILENAME.txt>
```

Bedingtes Debugging und Radio Active Tracing

Wenn die stets verfügbaren Ablaufverfolgungen nicht genügend Informationen liefern, um den Auslöser für das zu untersuchende Problem zu bestimmen, können Sie bedingtes Debuggen aktivieren und die Radio Active (RA)-Ablaufverfolgung erfassen, die Ablaufverfolgungen auf Debugebene für alle Prozesse bereitstellt, die mit der angegebenen Bedingung interagieren (in diesem Fall Client-MAC-Adresse). Führen Sie diese Schritte aus, um das bedingte Debuggen zu aktivieren.

Schritt 1: Stellen Sie sicher, dass keine Debug-Bedingungen aktiviert sind.

```
# clear platform condition all
```

Schritt 2: Aktivieren Sie die Debug-Bedingung für die MAC-Adresse des Wireless-Clients, die Sie überwachen möchten.

Mit diesen Befehlen wird die angegebene MAC-Adresse 30 Minuten (1800 Sekunden) lang überwacht. Sie können diese Zeit optional auf bis zu 2085978494 Sekunden erhöhen.

```
# debug wireless mac <aaaa.bbbb.cccc> {monitor-time <seconds>}
```

Hinweis: Um mehr als einen Client gleichzeitig zu überwachen, führen Sie den Befehl „debug wireless mac <aaaa.bbbb.cccc>“ für jede MAC-Adresse aus.

Hinweis: Die Ausgabe der Client-Aktivität wird in der Terminal-Sitzung nicht angezeigt, da alles intern gepuffert wird, um später angezeigt zu werden.

Schritt 3: Reproduzieren Sie das Problem oder Verhalten, das Sie überwachen möchten.

Schritt 4: Stoppen Sie die Debugs, wenn das Problem reproduziert wird, bevor die standardmäßige oder konfigurierte Monitoring-Zeit abgelaufen ist.

```
# no debug wireless mac <aaaa.bbbb.cccc>
```

Sobald die Monitoring-Zeit abgelaufen ist oder das Wireless-Debugging beendet wurde, generiert der 9800 WLC eine lokale Datei mit dem Namen:

```
ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Schritt 5: Rufen Sie die Datei mit der MAC-Adressaktivität ab. Sie können entweder die Datei „ra trace.log“ auf einen externen Server kopieren oder die Ausgabe direkt auf dem Bildschirm anzeigen.

Überprüfen Sie den Namen der RA-Tracing-Datei

```
# dir bootflash: | inc ra_trace
```

Datei auf externen Server kopieren:

```
# copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log  
tftp://a.b.c.d/ra-FILENAME.txt
```

Inhalt anzeigen:

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

Schritt 6: Wenn die Ursache immer noch nicht offensichtlich ist, rufen Sie die internen Protokolle ab, die eine ausführlichere Ansicht der Protokolle auf Debug-Ebene darstellen. Sie müssen den Client nicht noch einmal debuggen, da wir uns nur noch ausführlicher mit Debug-Protokollen befassen, die bereits gesammelt und intern gespeichert wurden.

```
# show logging profile wireless internal filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> }
to-file ra-internal-<FILENAME>.txt
```

Hinweis: Diese Befehlsausgabe gibt Traces für alle Protokollierungsebenen für alle Prozesse zurück und ist sehr umfangreich. Wenden Sie sich an das Cisco TAC, um diese Nachverfolgungen zu analysieren.

Sie können entweder die Datei „ra-internal-FILENAME.txt“ auf einen externen Server kopieren oder die Ausgabe direkt auf dem Bildschirm anzeigen.

Datei auf externen Server kopieren:

```
# copy bootflash:ra-internal-<FILENAME>.txt tftp://a.b.c.d/ra-internal-<FILENAME>.txt
```

Inhalt anzeigen:

```
# more bootflash:ra-internal-<FILENAME>.txt
```

Schritt 7. Entfernen Sie die Debug-Bedingungen.

```
# clear platform condition all
```

Hinweis: Stellen Sie sicher, dass Sie die Debug-Bedingungen immer nach einer Fehlerbehebungssitzung entfernen.

Beispiel eines erfolgreichen Versuchs

Dies ist die Ausgabe von RA_traces für einen erfolgreichen Versuch, jede der Phasen während des Assoziierungs-/Authentifizierungsprozesses zu identifizieren, während eine Verbindung zu einer SSID ohne RADIUS-Server hergestellt wird.

802.11-Zuordnung/Authentifizierung:

```
Association received. BSSID 10b3.d694.00ee, WLAN 9800DNASpaces, Slot 1 AP 10b3.d694.00e0,
2802AP-9800L
Received Dot11 association request. Processing started,SSID: 9800DNASpaces1, Policy profile:
DNASpaces-PP, AP Name: 2802AP-9800L, Ap Mac Address: 10b3.d694.00e0 BSSID MAC0000.0000.0000 wlan
ID: 1RSSI: 0, SNR: 32
Client state transition: S_CO_INIT -> S_CO_ASSOCIATING
dot11 send association response. Sending association response with resp_status_code: 0
dot11 send association response. Sending assoc response of length: 144 with resp_status_code: 0,
DOT11_STATUS: DOT11_STATUS_SUCCESS
Association success. AID 1, Roaming = False, WGB = False, 11r = False, 11w = False
DOT11 state transition: S_DOT11_INIT -> S_DOT11_ASSOCIATED
Station Dot11 association is successful
```

IP-Lernprozess:

```
IP-learn state transition: S_IPLEARN_INIT -> S_IPLEARN_IN_PROGRESS
Client IP learn successful. Method: ARP IP: 10.10.30.42
IP-learn state transition: S_IPLEARN_IN_PROGRESS -> S_IPLEARN_COMPLETE
Received ip learn response. method: IPLEARN_METHOD_AR
```

Layer-3-Authentifizierung:

```
Triggered L3 authentication. status = 0x0, Success
Client state transition: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_L3_AUTH_IN_PROGRESS
L3 Authentication initiated. LWA
Client auth-interface state transition: S_AUTHIF_L2_WEBAUTH_DONE -> S_AUTHIF_WEBAUTH_PENDING
```

```
Client auth-interface state transition: S_AUTHIF_L2_WEBAUTH_DONE -> S_AUTHIF_WEBAUTH_PENDING
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]GET rcvd when in
INIT state
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]HTTP GET request
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]Parse GET, src
[10.10.30.42] dst [13.107.4.52] url [http://www.msftconnecttest.com/connecttest.txt]
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]Retrieved user-
agent = Microsoft NCSI
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]GET rcvd when in
LOGIN state
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]HTTP GET request
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]Parse GET, src
[10.10.30.42] dst [151.101.24.81] url [http://www.bbc.com/]
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]Retrieved user-
agent = Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
[webauth-httpd] [17798]: (info): capwap_90000005[34e1.2d23.a668][10.10.30.42]POST rcvd when in
LOGIN state
```

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

```
[34e1.2d23.a668:capwap_90000005] Received User-Name 34E1.2D23.A668 for client 34e1.2d23.a668
L3 Authentication Successful. ACL:[]
Client auth-interface state transition: S_AUTHIF_WEBAUTH_PENDING -> S_AUTHIF_WEBAUTH_DONE
%CLIENT_ORCH_LOG-6-CLIENT_ADDED_TO_RUN_STATE: Username entry (34E1.2D23.A668) joined with ssid
(9800DNASpaces) for device with MAC: 34e1.2d23.a668
Managed client RUN state notification: 34e1.2d23.a668
Client state transition: S_CO_L3_AUTH_IN_PROGRESS -> S_CO_RU
```


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.