

在Catalyst 9800 WLC和ISE上配置FlexConnect EWA

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[网络图](#)

[配置](#)

[验证](#)

[RA跟踪成功尝试的示例](#)

[相关信息](#)

简介

本文档介绍如何在Catalyst 9800 WLC和ISE上配置FlexConnect EWA。

先决条件

要求

Cisco建议您了解9800无线局域网控制器(WLC)的配置。

使用的组件

本文档中的信息基于以下软件和硬件版本：

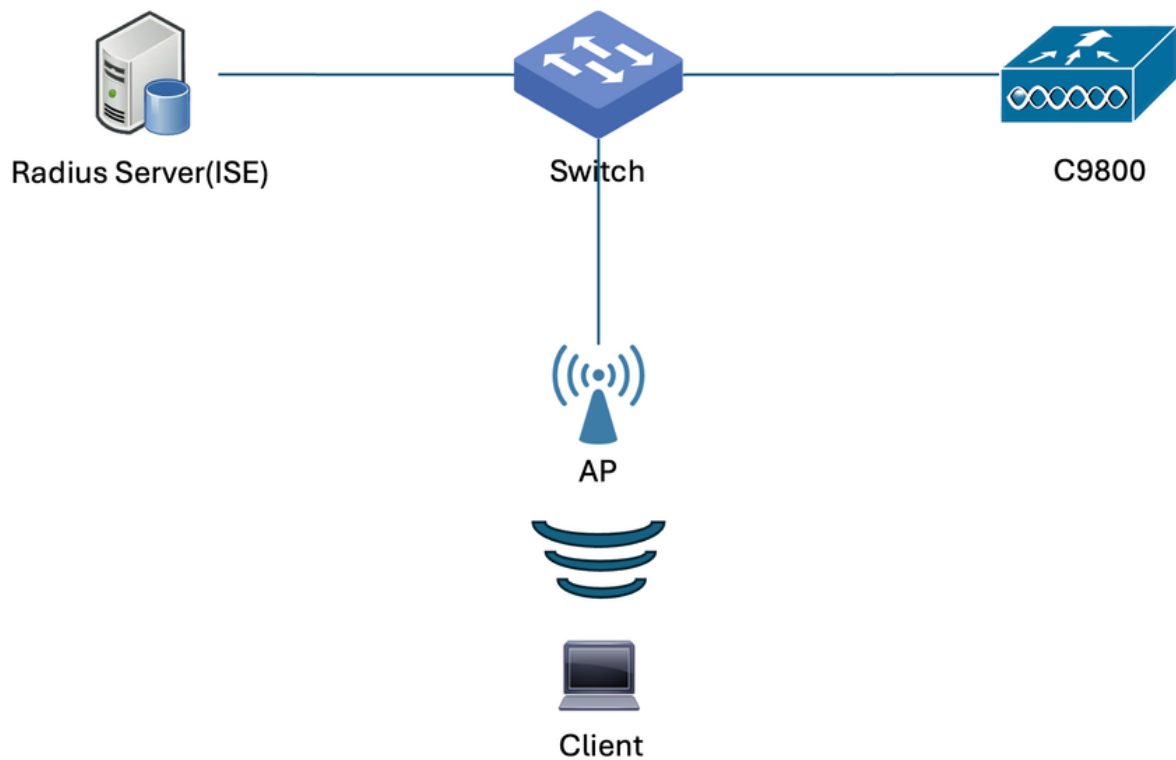
- Cisco Catalyst 9800 WLC Cisco IOS®XE版本17.15.3
- 身份服务引擎(ISE)v3.4.0.608

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

网络图

本文档基于以下拓扑：

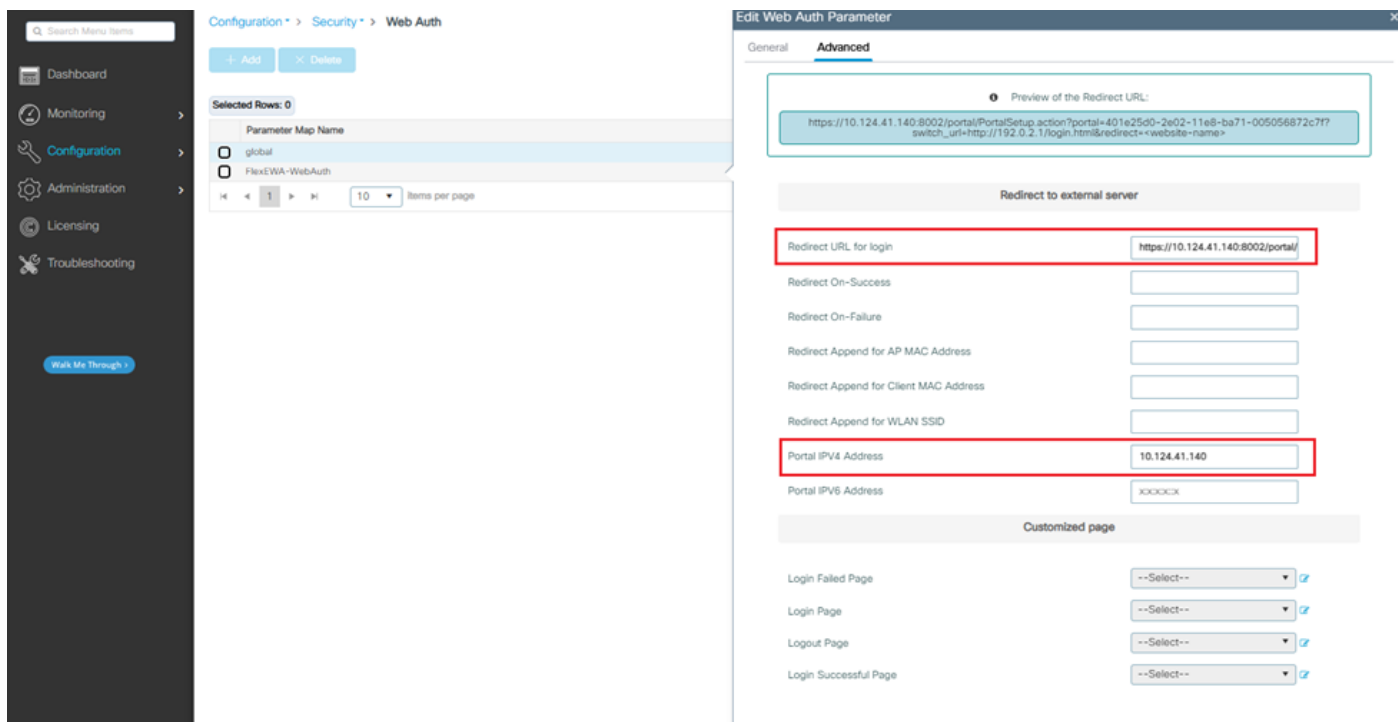


配置

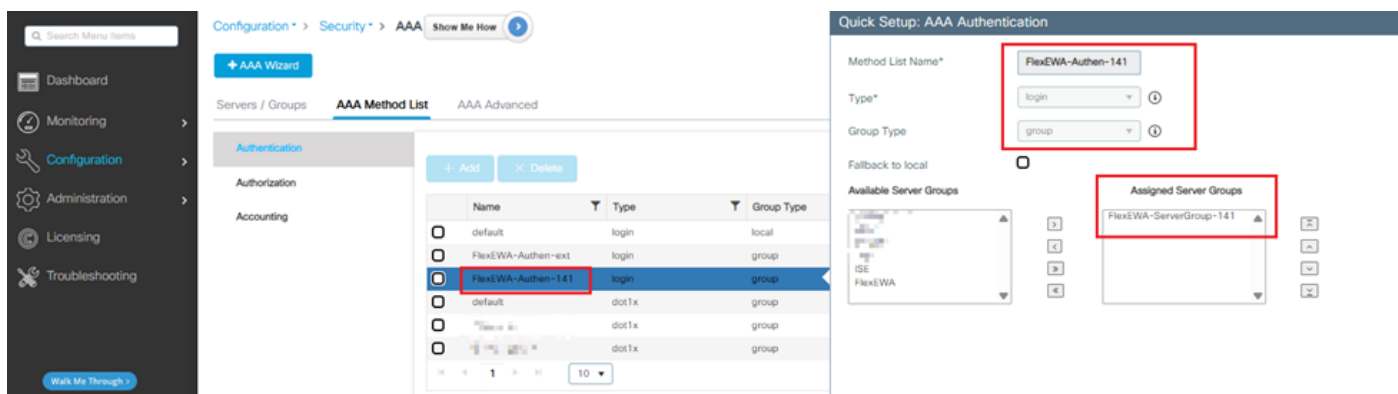
步骤1.导航到配置>安全> Web身份验证> +添加Web身份验证参数映射。

The screenshot shows the Cisco ISE configuration interface. On the left is a navigation menu with options like Dashboard, Monitoring, Configuration, Administration, Licensing, and Troubleshooting. The main area displays the 'Configuration > Security > Web Auth' path. A table lists parameter maps, including 'FlexEWA-WebAuth' and 'FlexEWA-WebAuth-141'. The 'Edit Web Auth Parameter' dialog is open, showing the 'General' tab. The 'Parameter-map Name' is set to 'FlexEWA-WebAuth-1'. The 'Type' is set to 'webauth'. Other settings include 'Maximum HTTP connections' (100), 'Init-State Timeout(secs)' (120), and 'Sleeping Client Timeout (minutes)' (720). The 'Banner Configuration' section shows 'Banner Title' and 'Banner Type' (set to 'None').

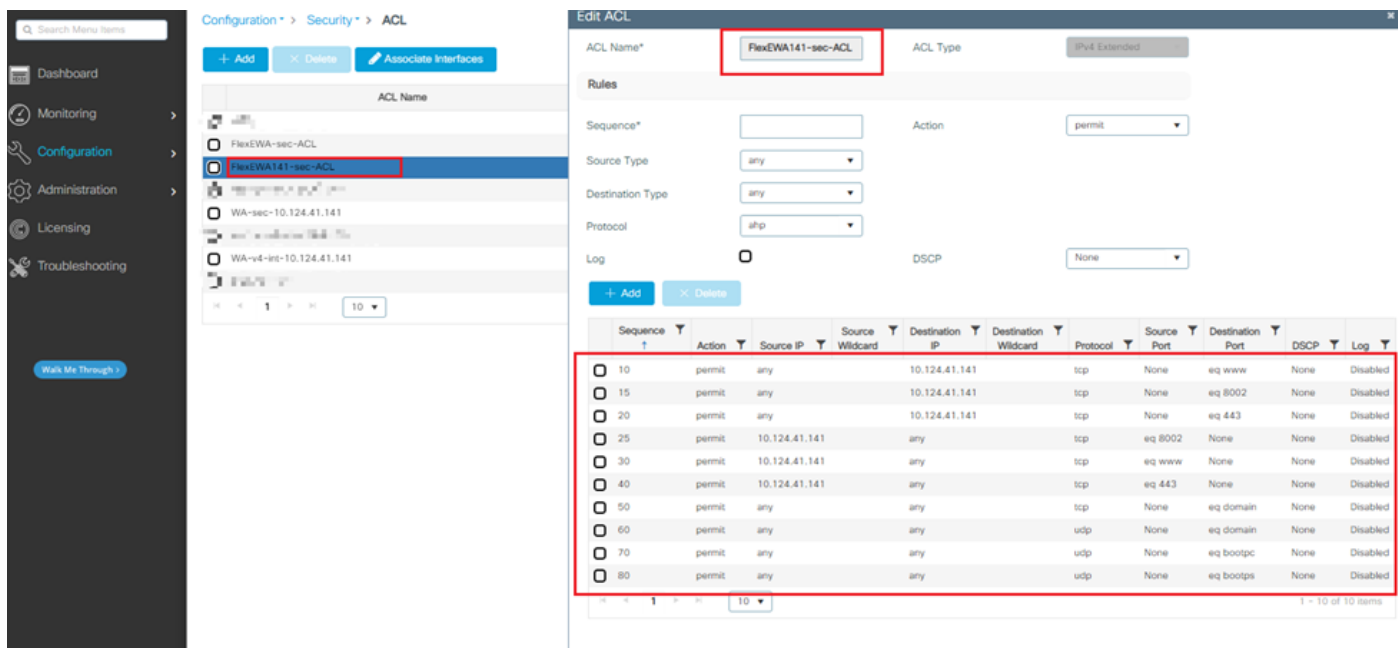
门户URL从ISE生成 (第7步)。



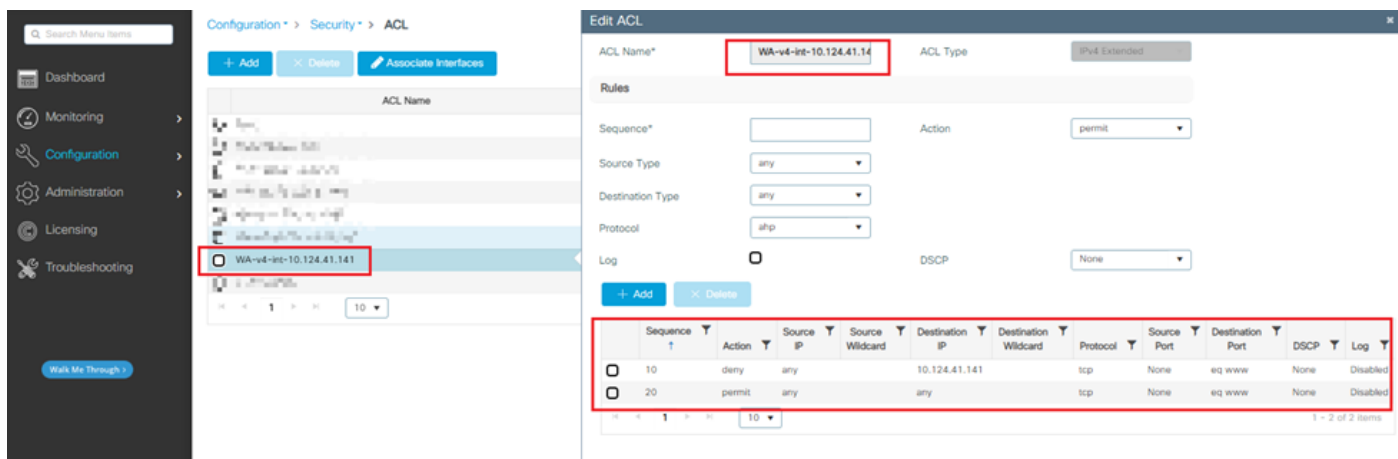
步骤2.导航到配置>安全> AAA > AAA方法列表>身份验证> +添加身份验证列表。



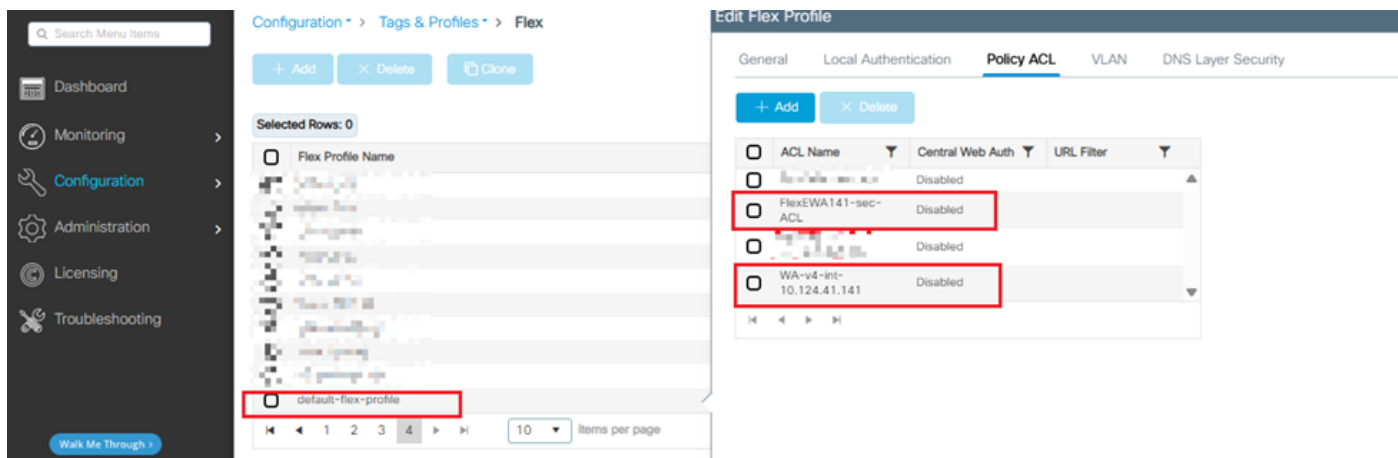
步骤3.假设HTTPS端口为8002，请参阅自动生成的ACL WA-sec-10.124.41.140以添加新的预身份验证ACL。



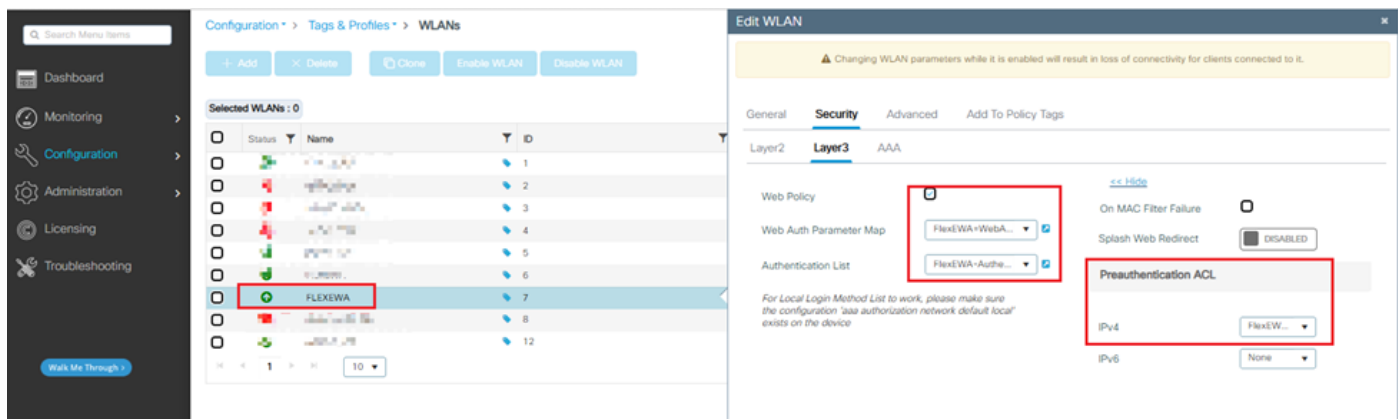
步骤4.检查自动生成的ACL WA-v4-int 10.124.41.141。



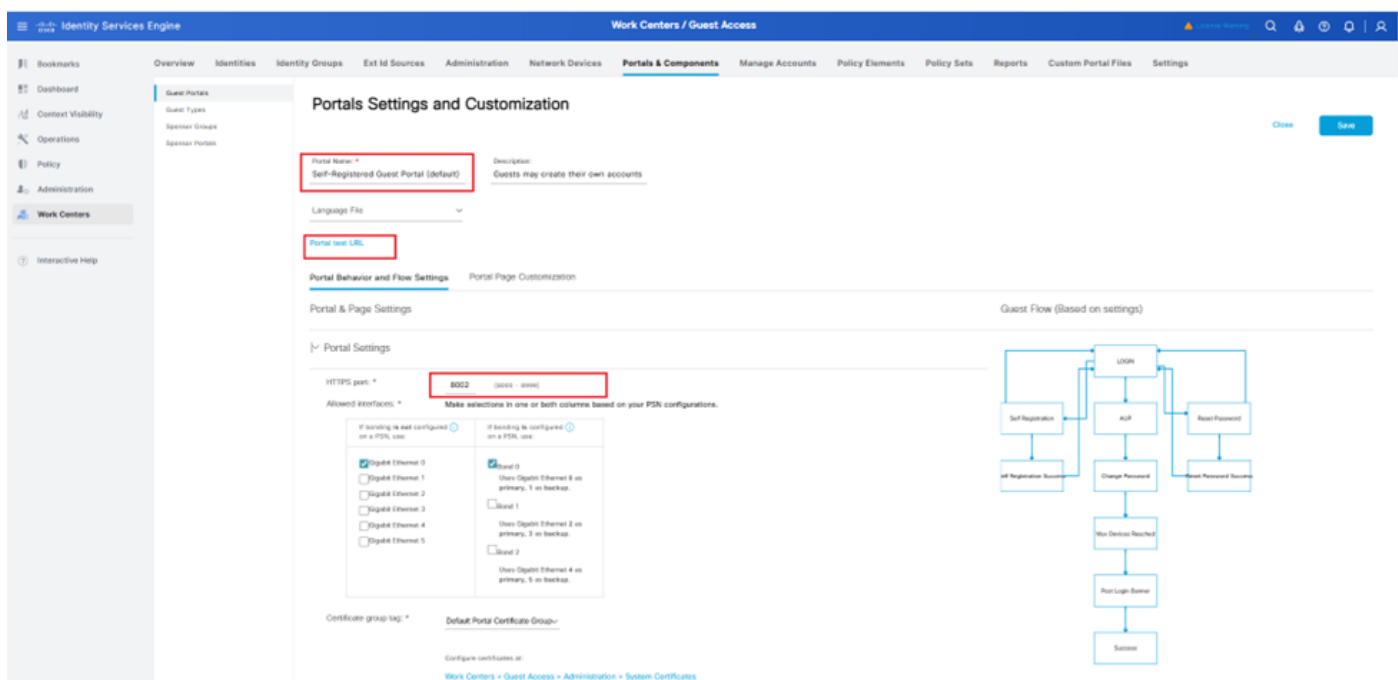
步骤5.将两个ACL应用于Configuration > Tags&Profiles > Flex > Flex Profile > Policy ACL。



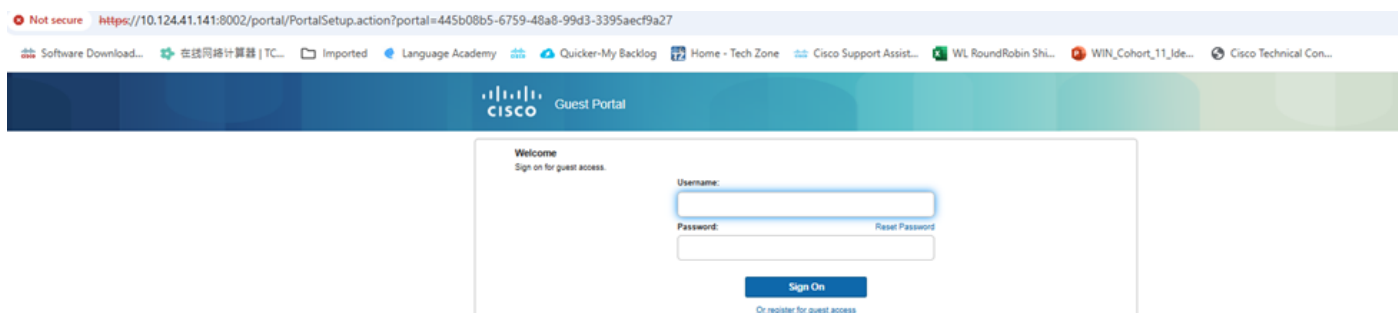
步骤6.将新创建的Web Auth Parameter Map、Authentication List和Preauthentication ACL应用到WLAN。



第7步：导航到工作中心(Work Centers)>门户和组件(Portals & Components)>访客门户(Guest Portals)>门户设置和自定义(Portals Settings and Customization)>门户名称(Portal Name)>自注册访客门户(Self-Registered Guest Portal) (默认)，从ISE生成门户URL。

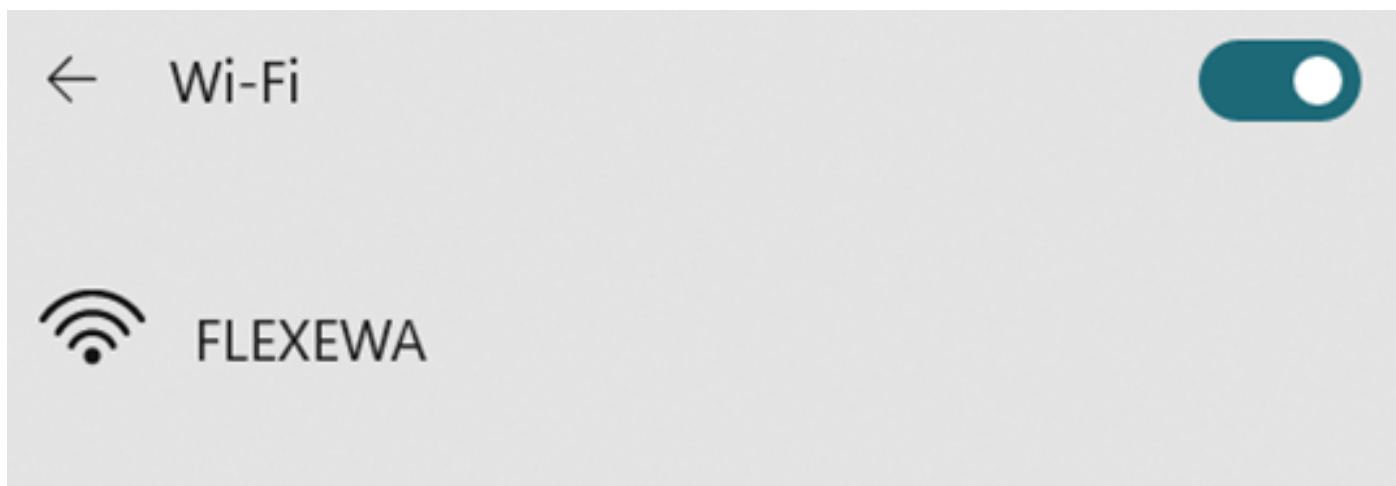


点击Portal test URL后会弹出列出的此Web门户。

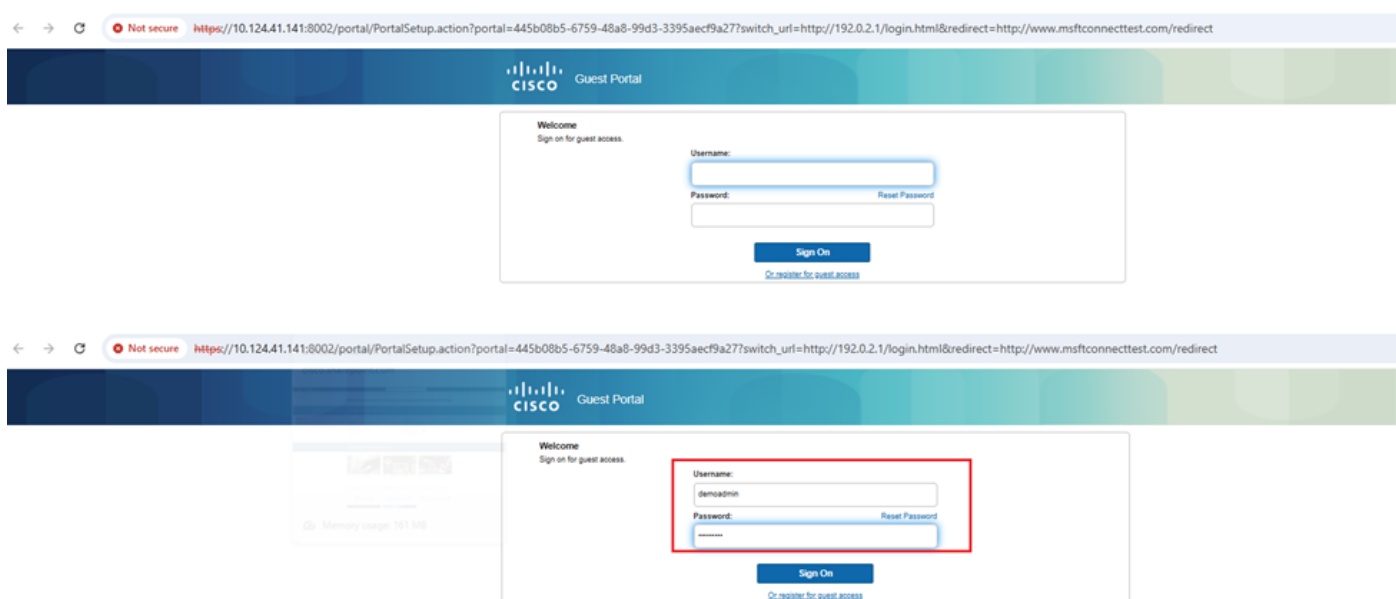


验证

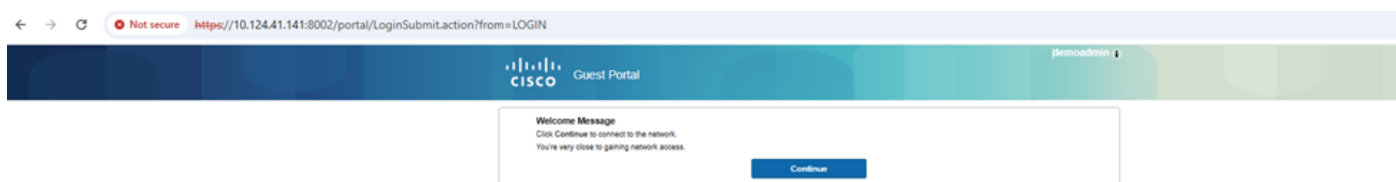
步骤1.连接FLEXEWA SSID。



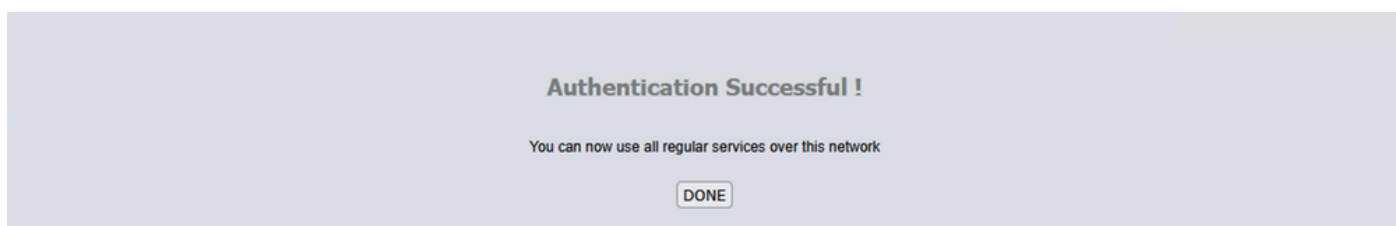
步骤2.重定向到门户并输入用户名和密码。



步骤3.系统随即会弹出访客门户：



步骤4.单击Continue后，身份验证成功：



RA跟踪成功尝试的示例

这是从Radio Active trace角度成功尝试连接的输出。使用此参考来确定连接到第3层Web身份验证SSID的客户端的客户端会话阶段。

已成功关联客户端：

```
2025/09/09 15:21:48.617769958 {wncd_x_R0-0}{1}: [client-orch-sm] [17842]: ( 注 ) : MAC :收到
f0b6.1e39.9ce8关联。BSSID c418.fc82.bb0b、WLAN FLEXEWA、插槽1 AP c418.fc82.bb00、
9178_1、站点标记HK、策略标记default-policy-tag、策略配置文件default-policy-profile、交换中心
、套接字延迟0ms、AP BSSID MAC c418.fc82.bb0b
2025/09/09 15:21:48.617813534 {wncd_x_R0-0}{1}: [client-orch-sm] [17842]: ( 调试 ) : MAC
:f0b6.1e39.9ce8已收到Dot11关联请求。处理已启动，SSID:FLEXEWA，策略配置文件：default-
policy-profile，AP名称：9178_1,Ap Mac地址：c418.fc82.bb00BSSID MAC0000.0000.0000wlan
ID:7RSSI:-30,SNR:67
2025/09/09 15:21:48.618002570 {wncd_x_R0-0}{1}: [客户端工作状态] [17842]: ( 注 ) : MAC
:f0b6.1e39.9ce8客户端状态转换：S_CO_INIT -> S_CO_ASSOCIATING
2025/09/09 15:21:48.618017149 {wncd_x_R0-0}{1}: [client-orch-sm] [17842]: ( 错误 ) : MAC
:f0b6.1e39.9ce8无法获取dot11记录
2025/09/09 15:21:48.618301251 {wncd_x_R0-0}{1}: [dot11-validate] [17842]: ( 信息 ) MAC
:f0b6.1e39.9ce8 Dot11 ie验证扩展/支持速率。支持费率验证通过radio_type 2
2025/09/09 15:21:48.618320304 {wncd_x_R0-0}{1}: [dot11-validate] [17842]: ( 调试 ) : MAC
:f0b6.1e39.9ce8 Dot11 ie validate rsnx, client not using sae, skip check
2025/09/09 15:21:48.618339230 {wncd_x_R0-0}{1}: [dot11-validate] [17842]: ( 信息 ) MAC
:f0b6.1e39.9ce8 WiFi直接：Dot11验证P2P IE。P2P IE不存在。
2025/09/09 15:21:48.618598747 {wncd_x_R0-0}{1}: [dot11] [17842]: ( 调试 ) : MAC
:f0b6.1e39.9ce8 dot11发送关联响应。使用resp_status_code建立关联响应：0
2025/09/09 15:21:48.618604733 {wncd_x_R0-0}{1}: [dot11] [17842]: ( 调试 ) : MAC
:f0b6.1e39.9ce8 Dot11功能信息byte1 1,byte2:11
2025/09/09 15:21:48.618696034 {wncd_x_R0-0}{1}: [dot11-frame] [17842]: ( 信息 ) MAC
:f0b6.1e39.9ce8 WiFi直接：使用P2P IE跳过构建关联响应：Wifi直接策略已禁用
2025/09/09 15:21:48.618785409 {wncd_x_R0-0}{1}: [dot11] [17842]: ( 信息 ) MAC :f0b6.1e39.9ce8
dot11发送关联响应。正在发送相关响应，响应长度为：177，带
resp_status_code:0,DOT11_STATUS:DOT11_STATUS_SUCCESS
2025/09/09 15:21:48.618791096 {wncd_x_R0-0}{1}: [dot11] [17842]: ( 注 ) : MAC
:f0b6.1e39.9ce8关联成功。AID 33，漫游=假，WGB =假，11r =假，11w =假快速漫游=假
2025/09/09 15:21:48.618806595 {wncd_x_R0-0}{1}: [dot11] [17842]: ( 信息 ) MAC :f0b6.1e39.9ce8
DOT11状态转换：S_DOT11_INIT -> S_DOT11_ASSOCIATED
2025/09/09 15:21:48.618855282 {wncd_x_R0-0}{1}: [client-orch-sm] [17842]: ( 调试 ) : MAC
:f0b6.1e39.9ce8 Station Dot11关联成功。
```

已跳过第2层身份验证：

```
2025/09/09 15:21:48.618992721 {wncd_x_R0-0}{1}: [client-orch-sm] [17842]: ( 调试 ) : MAC
:f0b6.1e39.9ce8开始L2身份验证。状态机中的Bssid:c418.fc82.bb0b请求中的Bssid为
：c418.fc82.bb0b
2025/09/09 15:21:48.619006036 {wncd_x_R0-0}{1}: [客户端工作状态] [17842]: ( 注 ) : MAC
:f0b6.1e39.9ce8客户端状态转换：S_CO_ASSOCIATING -> S_CO_L2_AUTH_IN_PROGRESS
2025/09/09 15:21:48.619093387 {wncd_x_R0-0}{1}: [client-auth] [17842]: ( 注 ) : MAC
```

:f0b6.1e39.9ce8 L2身份验证已启动。方法WEBAUTH，策略VLAN 0,AAA覆盖= 0

[...]

2025/09/09 15:21:48.623839337 {wncd_x_R0-0}{1}:client-auth [17842]: (信息) MAC :f0b6.1e39.9ce8客户端身份验证接口状态转换：S_AUTHIF_L2_WEBAUTH_PENDING -> S_AUTHIF_L2_WEBAUTH_DONE

2025/09/09 15:21:48.623863687 {wncd_x_R0-0}{1}:auth-mgr [17842]: (信息) [f0b6.1e39.9ce8:capwap_90000008]会话的设备类型被检测为英特尔设备，会话的旧英特尔设备和设备名称被检测为英特尔公司和旧英特尔公司协议映射1，新版本为1

2025/09/09 15:21:48.623873529 {wncd_x_R0-0}{1}:auth-mgr [17842]: (信息) [f0b6.1e39.9ce8:capwap_90000008] auth mgr attr add/change notification is received for attr dc-profile-name(1130)

2025/09/09 15:21:48.623911035 {wncd_x_R0-0}{1}:client-orch-sm [17842]: (调试) : MAC :f0b6.1e39.9ce8 L2站点身份验证成功。 ,L3身份验证：1

ACL plumb:

2025/09/09 15:21:48.620896754 {wncd_x_R0-0}{1}:webauth-sm [17842]: (信息) [0.0.0.0]开始 Webauth，mac [f0:b6:1e:39:9c:e8],IIF 0,audit-ID D1257C0A000000CA2D54F867

2025/09/09 15:21:48.620927053 {wncd_x_R0-0}{1}:webauth-state [17842]: (信息) [f0b6.1e39.9ce8][0.0.0.0]使用的参数映射：全局

2025/09/09 15:21:48.620935005 {wncd_x_R0-0}{1}:webauth-state [17842]: (信息) [f0b6.1e39.9ce8][0.0.0.0]状态无效状态 —> INIT

2025/09/09 15:21:48.620942683 {wncd_x_R0-0}{1}:webauth-sess [17842]: (信息) capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]创建会话，添加地址0.0.0.0

2025/09/09 15:21:48.620946808 {wncd_x_R0-0}{1}:auth-mgr-feat_wireless [17842]: (信息) [0000.0000.0000:unknown]已检索bssid为0的区域ID 0x12364632846638254486

2025/09/09 15:21:48.620958619 {wncd_x_R0-0}{1}:webauth-state [17842]: (信息) capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]使用的参数映射：FlexEWA=WebAuth-141

2025/09/09 15:21:48.620962048 {wncd_x_R0-0}{1}:webauth-state [17842]: (信息) capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]状态INIT -> INIT

2025/09/09 15:21:48.620978097 {wncd_x_R0-0}{1}:webauth-sm [17842]: (信息) capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]发起会话，转发状态到0 IF 0x90000008 mac [f0b6.1e39.9ce8]

2025/09/09 15:21:48.620981018 {wncd_x_R0-0}{1}:webauth-sm [17842]: (信息) capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]发起会话，SM初始会话5

2025/09/09 15:21:48.620988217 {wncd_x_R0-0}{1}:webauth-state [17842]: (信息) capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]使用的参数映射：FlexEWA=WebAuth-141

2025/09/09 15:21:48.620991618 {wncd_x_R0-0}{1}:webauth-state [17842]: (信息) capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]状态INIT -> INIT

2025/09/09 15:21:48.621023019 {wncd_x_R0-0}{1}:webauth-acl [17842]: (信息) capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]通过SVM应用IPv4拦截ACL，名称：WA-v4-int-10.124.41.141-7，优先级：50,IIF-ID:0

2025/09/09 15:21:48.621032776 {wncd_x_R0-0}{1}:svm [17842]: (信息) SVM_INFO:应用服务模板WA-v4-int-10.124.41.141-7 (ML：无)

2025/09/09 15:21:48.621786262 {wncd_x_R0-0}{1}:epm [17842]: (信息) [f0b6.1e39.9ce8:capwap_90000008]功能 (EPM URL插件) 已启动 (状态成功)

2025/09/09 15:21:48.621804034 {wncd_x_R0-0}{1}:[epm-acl] [17842]: (信息) [f0b6.1e39.9ce8:capwap_90000008]过滤器Id:已收到FlexEWA141-sec-ACL
2025/09/09 15:21:48.622151544 {wncd_x_R0-0}{1}:[epm] [17842]: (信息) [f0b6.1e39.9ce8:capwap_90000008]功能 (EPM ACL插件) 已启动 (状态成功)
2025/09/09 15:21:48.622187815 {wncd_x_R0-0}{1}:[svm] [17842]: (信息) SVM_INFO:epm的响应为SYNC , 返回代码为Success
2025/09/09 15:21:48.622226011 {wncd_x_R0-0}{1}:[auth-mgr] [17842]: (信息) [f0b6.1e39.9ce8:capwap_90000008]正在提升此会话上激活的扩展事件模板(9) , 客户端 (未知) (0)
2025/09/09 15:21:48.622265240 {wncd_x_R0-0}{1}:[webauth-acl] [17842]: (信息) capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]通过SVM应用IPv6拦截ACL , 名称 : IP-Adm-V6-Int-ACL-global-7 , 优先级 : 52,IIF-ID:0
2025/09/09 15:21:48.622270327 {wncd_x_R0-0}{1}:[svm] [17842]: (信息) SVM_INFO:应用服务模板IP-Adm-V6-Int-ACL-global-7(ML:NONE)
2025/09/09 15:21:48.622898831 {wncd_x_R0-0}{1}:[epm] [17842]: (信息) [f0b6.1e39.9ce8:capwap_90000008]功能 (EPM URL插件) 已启动 (状态成功)
2025/09/09 15:21:48.622932973 {wncd_x_R0-0}{1}:[svm] [17842]: (信息) SVM_INFO:epm的响应为SYNC , 返回代码为Success
2025/09/09 15:21:48.622957784 {wncd_x_R0-0}{1}:[auth-mgr] [17842]: (信息) [f0b6.1e39.9ce8:capwap_90000008]正在提升此会话上激活的扩展事件模板(9) , 客户端 (未知) (0)
2025/09/09 15:21:48.623119047 {wncd_x_R0-0}{1}:[dot11] [17842]: (调试) : MAC :f0b6.1e39.9ce8 Dot11 SAE发现ipsk progress为0 , 未处于挂起状态
2025/09/09 15:21:48.623126095 {wncd_x_R0-0}{1}:[llbridge-main] [17842]: (调试) : MAC :f0b6.1e39.9ce8未为此客户端启用本地链路桥接 , 未检查VLAN有效性
2025/09/09 15:21:48.623205421 {wncd_x_R0-0}{1}:[auth-mgr] [17842]: (信息) [f0b6.1e39.9ce8:capwap_90000008]环境状态从“空闲”更改为“正在运行”
2025/09/09 15:21:48.623209350 {wncd_x_R0-0}{1}:[auth-mgr] [17842]: (信息) [f0b6.1e39.9ce8:capwap_90000008]方法webauth将状态从“Not run”更改为“Running”
2025/09/09 15:21:48.623572855 {wncd_x_R0-0}{1}:[auth-mgr] [17842]: (信息) [f0b6.1e39.9ce8:capwap_90000008] SM cannot send event Template Activated to PRE for 0x8D000C0
2025/09/09 15:21:48.623680228 {wncd_x_R0-0}{1}:[client-auth] [17842]: (信息) MAC :f0b6.1e39.9ce8客户端身份验证接口状态转换 : S_AUTHIF_AWAIT_L2_WEBAUTH_START_RESP -> S_AUTHIF_L2_WEBAUTH_PENDING

IP学习过程 :

2025/09/09 15:21:51.628124695 {wncd_x_R0-0}{1}:[客户端工作状态] [17842]: (注) : MAC :f0b6.1e39.9ce8客户端状态转换 : S_CO_DPATH_PLUMB_IN_PROGRESS -> S_CO_IP_LEARN_IN_PROGRESS
2025/09/09 15:21:51.628463813 {wncd_x_R0-0}{1}:[client-iplearn] [17842]: (信息) MAC :f0b6.1e39.9ce8 IP-learn状态转换 : S_IPLEARN_INIT -> S_IPLEARN_IN_PROGRESS
2025/09/09 15:21:51.632284534 {wncd_x_R0-0}{1}:[client-auth] [17842]: (信息) MAC :f0b6.1e39.9ce8客户端身份验证接口状态转换 : S_AUTHIF_L2_WEBAUTH_DONE -> S_AUTHIF_L2_WEBAUTH_DONE

2025/09/09 15:21:51.676501288 {wncd_x_R0-0}{1}:sisf-packet] [17842]: (信息) RX:IPv6 DHCP from intf capwap_90000008 on vlan 174 Src MAC:f0b6.1e39.9ce8目标MAC:3333.0001.0002
Ipv6源 : fe80::3f83:2848:d30:7aea , Ipv6 DST:ff02::1:2 , 类型 : 消息类型
: DHCPV6_MSG_SOLICIT xid:14443573

2025/09/09 15:21:51.676541447 {wncd_x_R0-0}{1}:sisf-packet] [17842]: (信息) 发射机 : IPv6 DHCP from intf capwap_90000008 on vlan 174 Src MAC:f0b6.1e39.9ce8目标
MAC:3333.0001.0002 Ipv6源 : fe80::3f83:2848:d30:7aea , Ipv6 DST:ff02::1:2 , 类型 : 消息类型
: DHCPV6_MSG_SOLICIT xid:14443573

2025/09/09 15:21:51.706187097 {wncd_x_R0-0}{1}:sisf-packet] [17842]: (信息) RX:来自vlan
174上的接口capwap_90000008的ARP源MAC:f0b6.1e39.9ce8目的MAC:ffff.ffff.ffff ARP请求
, ARP发送方MAC:f0b6.1e39.9ce8 ARP目标MAC:0000.0000.0000 ARP发送方
IP:169.254.137.222,ARP目标IP:169.254.137.222,
[...]

2025/09/09 15:21:52.686190945 {wncd_x_R0-0}{1}:client-iplern] [17842]: (注) : MAC
:f0b6.1e39.9ce8客户端IP学习成功。方法 : DHCP IP:10.124.37.251

2025/09/09 15:21:52.686244192 {wncd_x_R0-0}{1}:auth-mgr] [17842]: (信息
) [f0b6.1e39.9ce8:capwap_90000008] auth mgr attr add/change notification is received for attr
addr(8)

2025/09/09 15:21:52.686285422 {wncd_x_R0-0}{1}:webauth-sess] [17842]: (信息
) capwap_90000008[f0b6.1e39.9ce8][0.0.0.0]更改通知CB , 添加地址10.124.37.251
[f0b6.1e39.9ce8]

2025/09/09 15:21:52.686289265 {wncd_x_R0-0}{1}:auth-mgr-feat_wireless] [17842]: (信息
) [0000.0000.0000:unknown]已检索bssid为0的区域ID 0x12364632846638254486

2025/09/09 15:21:52.686291647 {wncd_x_R0-0}{1}:webauth-sess] [17842]: (信息) 为vrf id 0、
ipv4 vrf表id 0向ipv4哈希表添加webauth会话

2025/09/09 15:21:52.686430038 {wncd_x_R0-0}{1}:auth-mgr-feat_acct] [17842]: (信息
) [f0b6.1e39.9ce8:capwap_90000008] SM Notified attribute Add/Update addr 10.124.37.251

2025/09/09 15:21:52.686456653 {wncd_x_R0-0}{1}:epm] [17842]: (信息
) [0000.0000.0000:unknown] HDL = 0x0 vlan 174 fail count 0 dirty_counter 0 is_dirty 0

2025/09/09 15:21:52.686710209 {wncd_x_R0-0}{1}:client-iplern] [17842]: (信息) MAC
:f0b6.1e39.9ce8 IP-learn状态转换 : S_IPLEARN_IN_PROGRESS -> S_IPLEARN_COMPLETE

第3层身份验证和重定向过程 :

2025/09/09 15:21:52.687395906 {wncd_x_R0-0}{1}:client-auth] [17842]: (注) : MAC
:f0b6.1e39.9ce8 L3身份验证已启动。LWA

2025/09/09 15:21:52.687472722 {wncd_x_R0-0}{1}:client-auth] [17842]: (信息) MAC
:f0b6.1e39.9ce8客户端身份验证接口状态转换 : S_AUTHIF_L2_WEBAUTH_DONE ->
S_AUTHIF_WEBAUTH_PENDING

2025/09/09 15:21:52.687723489 {wncd_x_R0-0}{1}:sisf-packet] [17842]: (信息) RX:来自VLAN
174源MAC上接口Po1的DHCPv4:4006.d589.4e78目的MAC:ffff.ffff.ffff
src_ip:10.124.37.242,dst_ip:255.255.255.255、BOOTPREPLY、SISF_DHCPACK、
giaddr:0.0.0.0,yiaddr:10.124.37.251,CMAC:f0b6.1e39.9ce8

2025/09/09 15:21:52.687992316 {wncd_x_R0-0}{1}:sisf-packet] [17842]: (信息) 发射机 : 来自
VLAN 174源MAC上接口Po1的DHCPv4:4006.d589.4e78目的MAC:f0b6.1e39.9ce8
src_ip:10.124.37.242,dst_ip:255.255.255.255、BOOTPREPLY、SISF_DHCPACK、

giaddr:0.0.0.0,yiaddr:10.124.37.251,CMAC:f0b6.1e39.9ce8
2025/09/09 15:21:52.688020475 {wncd_x_R0-0}{1}:[ewlc-infra-evq] [17842]: (详细) : 类型
: EWLC_CAPWAP_HDR_AP , Id:23277

[...]

2025/09/09 15:21:55.663715832 {wncd_x_R0-0}{1}:[webauth-io] [17842]: (信息
) capwap_90000008[f0b6.1e39.9ce8][10.124.37.251]54129/197 IO状态新 — >读取
2025/09/09 15:21:55.664060604 {wncd_x_R0-0}{1}:[webauth-io] [17842]: (信息
) capwap_90000008[f0b6.1e39.9ce8][10.124.37.251]54129/197读取事件，消息就绪
2025/09/09 15:21:55.664071121 {wncd_x_R0-0}{1}:[webauth-httpd] [17842]: (信息
) capwap_90000008[f0b6.1e39.9ce8][10.124.37.251]处于INIT状态时GET rcvd
2025/09/09 15:21:55.664077798 {wncd_x_R0-0}{1}:[webauth-httpd] [17842]: (信息
) capwap_90000008[f0b6.1e39.9ce8][10.124.37.251]HTTP GET请求
2025/09/09 15:21:55.664094019 {wncd_x_R0-0}{1}:[webauth-httpd] [17842]: (信息
) capwap_90000008[f0b6.1e39.9ce8][10.124.37.251]解析GET , src [10.124.37.251] dst
[23.5.165.82] url [<http://www.msftconnecttest.com/connecttest.txt>]

[...]

2025/09/09 15:22:16.420792303 {wncd_x_R0-0}{1}:[webauth-httpd] [17842]: (信息
) capwap_90000008[f0b6.1e39.9ce8][10.124.37.251]处于LOGIN状态时的POST rcvd

2025/09/09 15:22:32.375197748 {wncd_x_R0-0}{1}:[webauth-acl] [17842]: (信息
) capwap_90000008[f0b6.1e39.9ce8][10.124.37.251]通过SVM取消应用IPv4概念ACL , 名称“WA-
v4-int-10.124.41.141-7” , pri 50,IIF 0
2025/09/09 15:22:32.376230716 {wncd_x_R0-0}{1}:[auth-mgr] [17842]: (信息
) [f0b6.1e39.9ce8:capwap_90000008]引发此会话上已停用扩展事件模板(11) , 客户端 (未知) (0)
2025/09/09 15:22:32.376262689 {wncd_x_R0-0}{1}:[webauth-acl] [17842]: (信息
) capwap_90000008[f0b6.1e39.9ce8][10.124.37.251]通过SVM取消应用IPv6概念ACL , 名称“IP-
Adm-V6-Int-ACL-global” , pri 52,IIF 0
2025/09/09 15:22:32.376734374 {wncd_x_R0-0}{1}:[auth-mgr] [17842]: (信息
) [f0b6.1e39.9ce8:capwap_90000008]引发此会话上已停用扩展事件模板(11) , 客户端 (未知) (0)
2025/09/09 15:22:32.376865998 {wncd_x_R0-0}{1}:[dot11] [17842]: (调试) : MAC
:f0b6.1e39.9ce8 Dot11 SAE发现ipsk progress为0 , 未处于挂起状态
2025/09/09 15:22:32.376870611 {wncd_x_R0-0}{1}:[llbridge-main] [17842]: (调试) : MAC
:f0b6.1e39.9ce8未为此客户端启用本地链路桥接 , 未检查VLAN有效性
2025/09/09 15:22:32.376949875 {wncd_x_R0-0}{1}:[auth-mgr] [17842]: (信息
) [f0b6.1e39.9ce8:capwap_90000008]从WebAuth成功身份验证 , 身份验证事件成功

转换到运行状态 :

2025/09/09 15:22:32.379351256 {wncd_x_R0-0}{1}:[client-auth] [17842]: (注) : MAC
:f0b6.1e39.9ce8 ADD MOBILE已发送。客户端状态标志 : 0x38 BSSID:MAC :c418.fc82.bb0b
capwap IFID:0x90000008 , 添加已发送的移动 : 1
2025/09/09 15:22:32.379583842 {wncd_x_R0-0}{1}:[errmsg] [17842]: (信息
) %CLIENT_ORCH_LOG-6-CLIENT_ADDED_TO_RUN_STATE:R0/0:wncd:带有MAC的设备用户
名条目(demoadmin)与ssid(FLEXEWA)加入 : 信道(100)上的f0b6.1e39.9ce8
2025/09/09 15:22:32.379671775 {wncd_x_R0-0}{1}:[aaa-attr-inf] [17842]: (信息) [Applied

attribute :bsn-vlan-interface-name 0 "wlc-management"]

2025/09/09 15:22:32.379673695 {wncd_x_R0-0}{1}:[aaa-attr-inf] [17842]: (信息) [应用的属性 : timeout 0 28800(0x7080)]

2025/09/09 15:22:32.379683417 {wncd_x_R0-0}{1}:[aaa-attr-inf] [17842]: (信息) [应用的属性 : url-redirect-acl 0 "IP-Adm-V4-LOGOUT-ACL"]

2025/09/09 15:22:32.379727993 {wncd_x_R0-0}{1}:[ewlc-qos-client] [17842]: (信息) MAC :f0b6.1e39.9ce8客户端QoS运行状态处理程序

2025/09/09 15:22:32.379756610 {wncd_x_R0-0}{1}:[rog-proxy-capwap] [17842]: (调试) : 托管客户端运行状态通知 : f0b6.1e39.9ce8

2025/09/09 15:22:32.379810670 {wncd_x_R0-0}{1}:[客户端工作状态] [17842]: (注) : MAC :f0b6.1e39.9ce8客户端状态转换 : S_CO_L3_AUTH_IN_PROGRESS -> S_CO_RUN

相关信息

- [在9800 WLC上配置外部Web身份验证并排除故障](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。