Configure Local Web Authentication with External Authentication

Contents

Introduction

This document describes how to configure Local Web Authentication with External Authentication on a 9800 WLC and ISE.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- 9800 Wireless LAN Controllers (WLC) configuration
- Lightweight Access Points (LAPs)
- How to set up and configure an external web server Identity Services Engine (ISE).
- How to set up and configure DHCP and DNS servers.

Components Used

The information in this document is based on these software and hardware versions:

- 9800-L WLC Cisco IOS® XE, Version 17.9.3
- Identity Services Engine (ISE), Version 2.6 Patch 10

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Web Authentication

Web authentication is a Layer 3 security feature that allows guest users to have access to the network.

This feature is designed to provide easy and secure guest access to open SSIDs, without the need to configure a user profile, and it can also work with Layer 2 security methods.

The purpose of web authentication is to allow untrusted devices (guests) to access the network with limited network access privileges, through a guest WLAN that can be configured with security mechanisms, and the security of the network not compromised. For the guest users to have access to the network, they need to authenticate successfully, that is, they need to provide the correct credentials or accept the Acceptable Use Policy (AUP) to gain access to the network.

Web authentication is a benefit for companies because it drives user loyalty, makes the company compliant to use a disclaimer that the guest user must accept, and allows the company to engage with visitors.

To deploy web authentication, it must be taken in consideration how the guest portal and authentication are handled. There are two common methods:

- Local web authentication (LWA): A method of redirection of guest users to a portal directly from the WLC. The redirection and pre-WebAuth ACL are locally configured on the WLC.
- Central web authentication (CWA): A method of redirection of guest users where the redirection URL and the redirect ACL are centrally configured on an external server (for example ISE) and communicated to the WLC via RADIUS. In central web authentication the redirect URL and redirect ACL are centrally located on an external server (such as RADIUS). The RADIUS server is the one that handles the authentication, it sends instructions to the WLC. In CWA, the WLC does not require a local web-auth certificate, only one certificate is needed on the central web portal, and requires a central authentication server, such as ISE. To read CWA in more detail navigate to Configure Central Web Authentication (CWA) on Catalyst 9800 WLC and ISE.

In Local Web Authentication, the web portal can be present on the WLC or on an external server. In LWA with External Authentication, the web portal is present on the WLC. In LWA with External Web Server, the web portal is present on an external server (such as DNA Spaces). An example of LWA with External Web Server is described in detail at: Configure DNA Spaces Captive Portal with Catalyst 9800 WLC.

Diagram of the different web authentication methods:

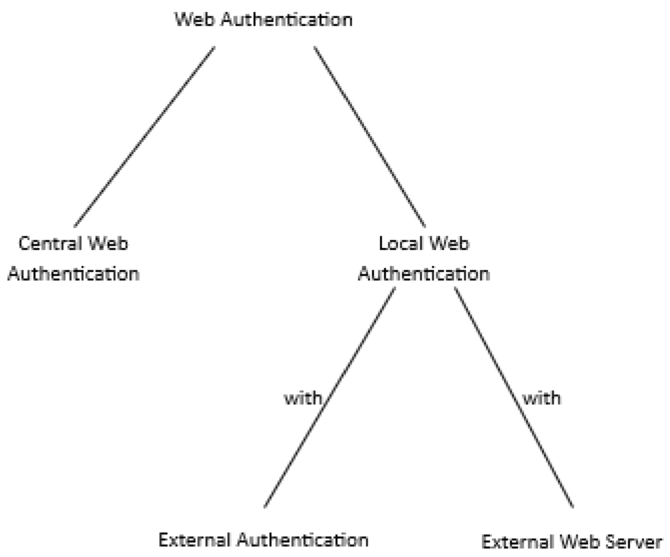
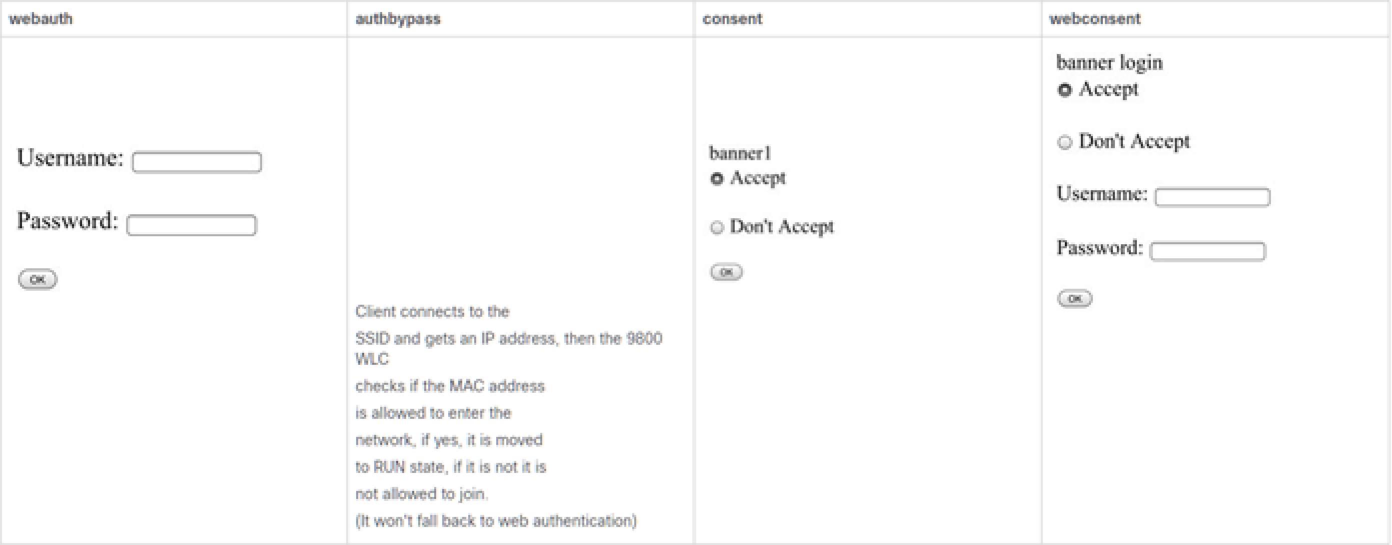


Diagram of the Different Web Authentication Methods

Types of authentication

There are four types of authentication to authenticate the guest user:

- Webauth: Enter username and password.
- Consent (web-passthrough): Accept AUP.
- Authbypass: Authentication based on the MAC address of the guest user device.
- Webconsent: A mix between username/password and accept AUP.



webauth	authbypass	consent	webconsent
Username: Password: OK	Client connects to the SSID and gets an IP address, then the 9800 WLC checks if the MAC address is allowed to enter the network, if yes, it is moved to RUN state, if it is not it is not allowed to join. (It won't fall back to web authentication)	banner1 ● Accept ○ Don't Accept OK	banner login ● Accept ○ Don't Accept Username: Password: OK

Four Types of Authentication to Authenticate the Guest User

Database for Authentication

The credentials for authentication can be store on an LDAP server, locally on the WLC or on the RADIUS server.

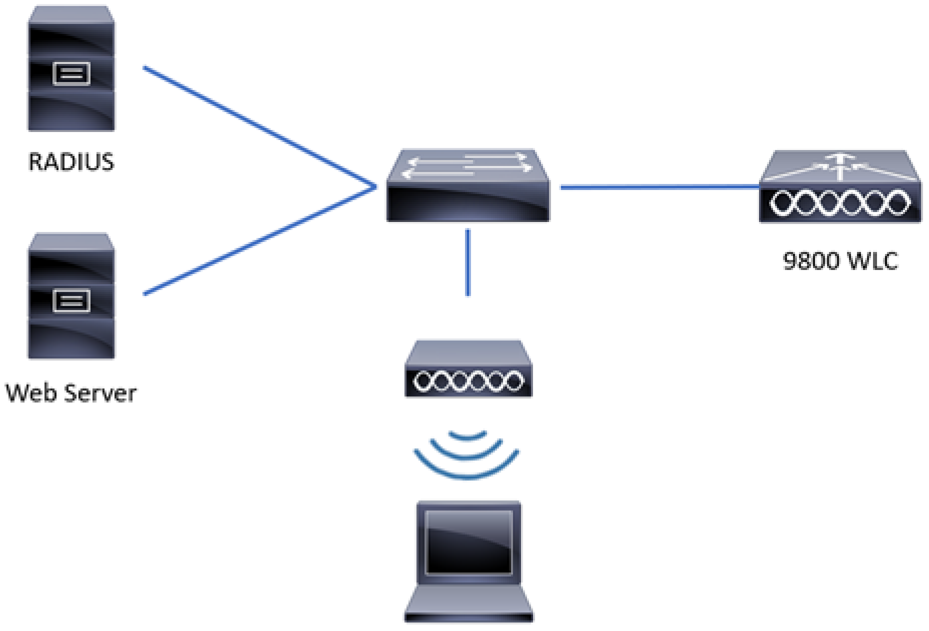
- Local database: The credentials (username and password) are stored locally on the WLC.
- LDAP database: The credentials are stored in the LDAP back-end database. The WLC queries the LDAP server for the credentials of a particular user in the database.
- RADIUS database: The credentials are stored at the RADIUS back-end database. The WLC queries the RADIUS server for credentials of a particular user in the database.

Local Web Authentication

In local web authentication the guest user is redirected to a web portal directly from the WLC.

The web portal can be in the WLC or in another server. What it makes local is the fact that the redirect URL and the ACL that matches traffic must be on the WLC (not the location of the web portal). In LWA, when a guest user connects to the guest WLAN, the WLC intercepts the connection from the guest user and redirects them to the web portal URL, where the guest user is asked to authenticate. When the guest user enters credentials (username and password), the WLC captures the credentials. The WLC authenticates the guest user with a LDAP server, RADIUS server or local database (database present locally on the WLC). In case of RADIUS server (an external server such as ISE), it can be used not also to store credentials, but also to provide options for device registration and self-provisioning. In case of an external web server, such as DNA Spaces, the web portal is present there. In LWA there is one certificate on the WLC and another on the web portal.

The image represents the generic topology of LWA:



Generic Topology of LWA

Devices in the network topology of LWA:

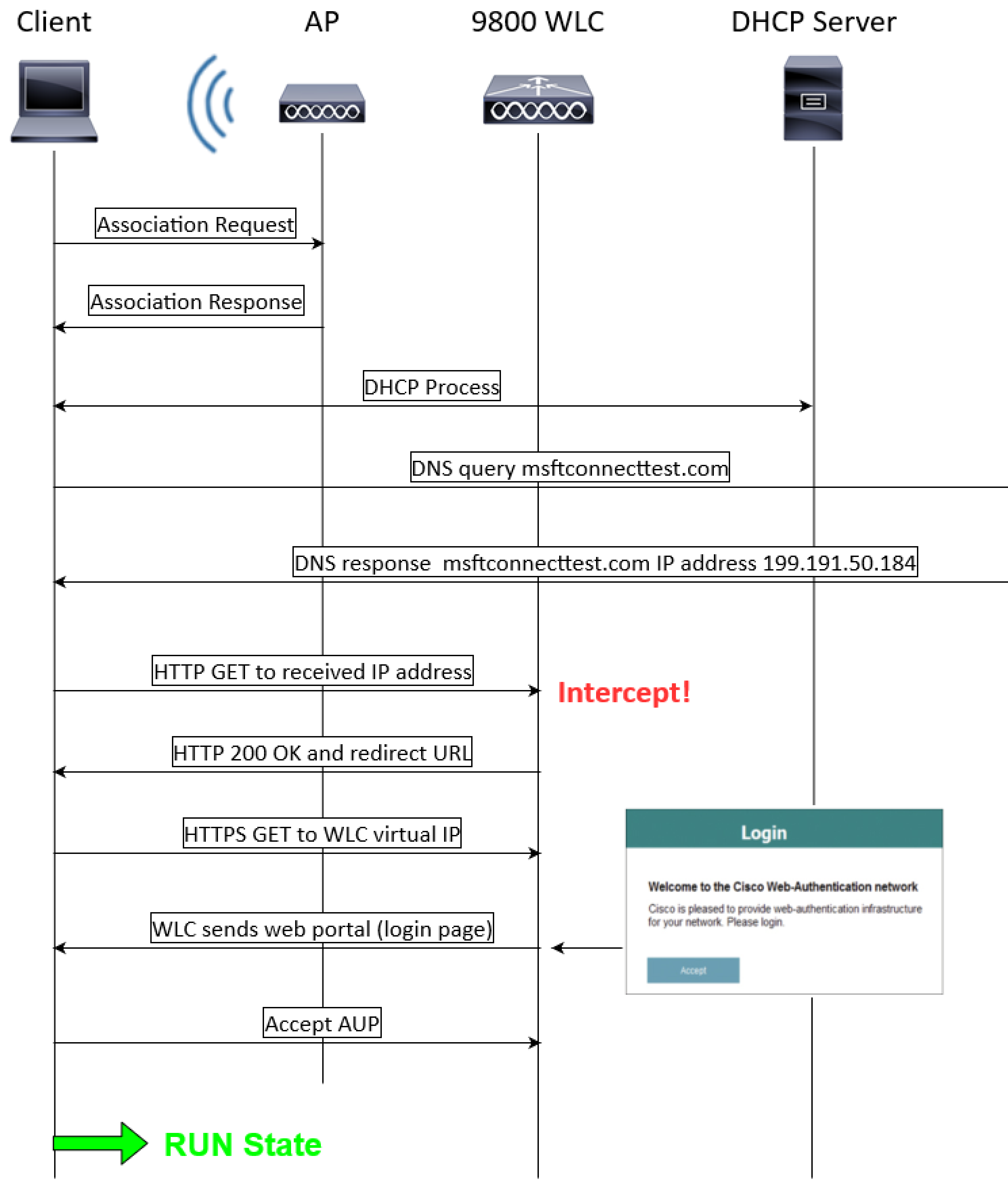
- Client: Sends requests to DHCP and DNS server, requests access to the guest WLAN, and responds to requests from the WLC.
- Access Point: Connected to a switch, broadcasts the guest WLAN, and provides wireless connection to guest users devices. It also allows DHCP and DNS packets before the guest user is authenticated (before enter valid credentials).
- WLC: Manages the APs and clients. The WLC hosts the redirect URL and the ACL that matches traffic. Intercepts HTTP requests from the guest users, redirects them to an web portal (log in page) where guest users have to authenticate. It captures the credentials and authenticates the guest users,

and it sends access requests to an external server, LDAP server or local database to confirm if the credentials are valid.

- Authentication server: Responds to access requests from the WLC with access accept/reject. The authentication server validate the credentials from the guest user and notifies the WLC if the credentials are valid or not valid. If credentials are valid, the guest user is authorized to access the network (the authentication server provides options for device registration and self-provisioning). If credentials are not valid, the guest user is denied access to the network.

LWA flow:

- The guest user associates with an AP that broadcasts the guest WLAN.
- The guest user goes through the DHCP process in order to get an IP address.
- The guest user wants to make an internet connectivity check to the captive portal. If it is an Apple device, it tries the Apple captive portal; if it is an Android device it tries the Android captive portal; if it is a Windows device it tries the Windows connect test portal.
- The guest user sends a DNS query to ask for the captive portal IP address. The DNS server responds to the query with the correspondent IP address.
- The guest user sends an HTTP GET message to the IP address of the captive portal.
- The WLC intercepts that message and replies to the guest user with HTTP 200 OK and the redirect URL.
- The guest user sends a HTTPS GET message to the WLC virtual IP and the WLC responds with the web portal.
- The guest user is asked to enter authentication credentials on the web portal.
- The web portal redirects the user back to the WLC with the provided credentials (if an external web portal is used).
- The WLC authenticates the guest user through a local database, or it sends a query to the RADIUS or LDAP server, to confirm if the credentials are correct (if the authentication type is webconsent or webauth).
- If the credentials are correct, the WLC authenticates the guest user and it goes to RUN state. If credentials are wrong, the WLC deletes the guest user.
- The WLC redirects the client back to the original URL that was entered in the web browser.

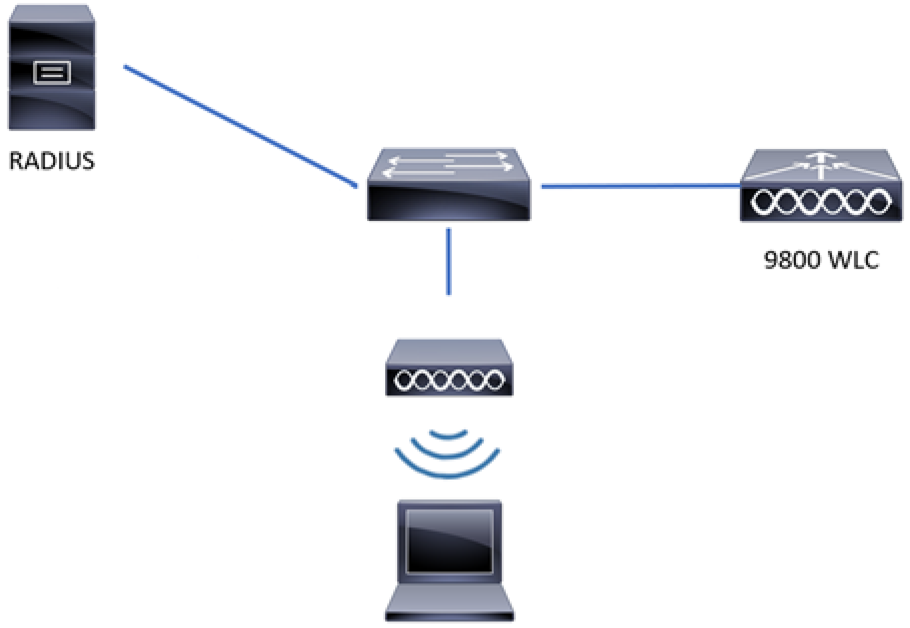

Client
AP
9800 WLC
DHCP Server
Association Request
Association Response
DHCP Process
DNS query msftconnecttest.com
DNS response msftconnecttest.com IP address 199.191.50.184
HTTP GET to received IP address
Intercept!
HTTP 200 OK and redirect URL
HTTPS GET to WLC virtual IP
WLC sends web portal (login page)
Accept AUP
RUN State
Login
Accept

Welcome to the Cisco Web-Authentication network

Cisco is pleased to provide web-authentication infrastructure for your network. Please login.

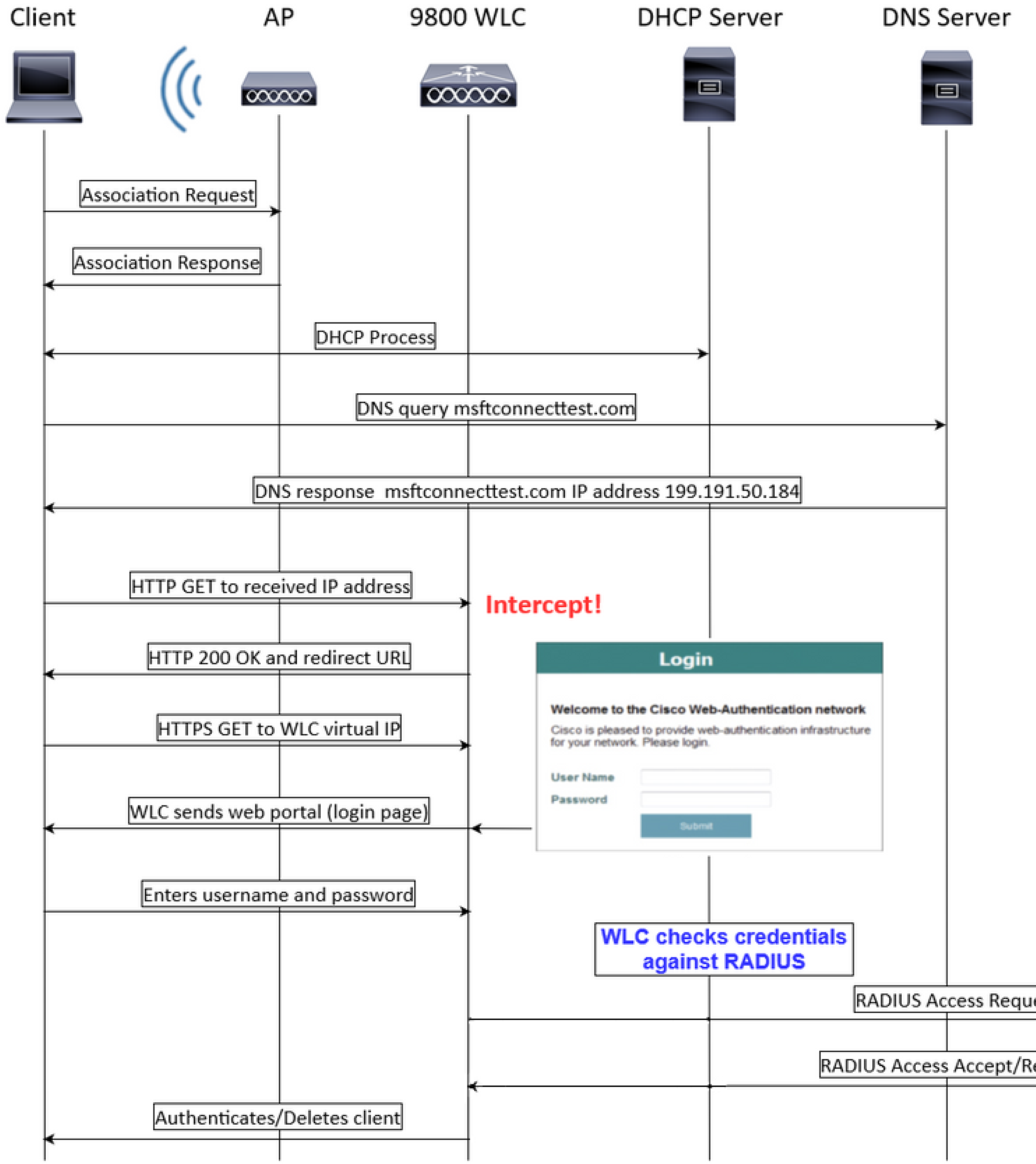
LWA Flow

Local Web Authentication with External Authentication



Generic Topology of LWA-EA

LWA-EA is a method of LWA where the web portal and redirection URL are located on the WLC and the credentials are stored on an external server, such as ISE. The WLC captures the credentials and authenticates the client through an external RADIUS server. When guest user enters credentials, the WLC checks the credentials against RADIUS, it sends a RADIUS Access Request and receives a RADIUS Access Accept/Reject from the RADIUS server. Then, if the credentials are correct, the guest user goes to RUN state. If the credentials are incorrect, the guest user is deleted by the WLC.


Client
AP
9800 WLC
DHCP Server
DNS Server
Association Request
Association Response
DHCP Process
DNS query msftconnecttest.com
DNS response msftconnecttest.com IP address 199.191.50.184
HTTP GET to received IP address
Intercept!
HTTP 200 OK and redirect URL
Login
Welcome to the Cisco Web-Authentication network
Cisco is pleased to provide web-authentication infrastructure for your network. Please login.
User Name
Password
Submit
HTTPS GET to WLC virtual IP
WLC sends web portal (login page)
Enters username and password
WLC checks credentials against RADIUS
RADIUS Access Requ
RADIUS Access Accept/Re
Authenticates/Deletes client

LWA-EA Flow

Configure

Network Diagram

: This configuration example only covers central switching/authentication. The flex local switching configuration have slight different requirements for to configure web authentication.

Configure Local Web Authentication with External Authentication on the CLI

Configure AAA Server and Server Group

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#radius server RADIUS
9800WLC(config-radius-server)#address ipv4 <ip address> auth-port 1812 acct-port 1813
9800WLC(config-radius-server)#key cisco
9800WLC(config-radius-server)#exit
9800WLC(config)#aaa group server radius RADIUSGROUP
9800WLC(config-sg-radius)#server name RADIUS
9800WLC(config-sg-radius)#end
```

Configure Local Authentication and Authorization

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#aaa new-model
9800WLC(config)#aaa authentication login LWA_AUTHENTICATION group RADIUSGROUP
9800WLC(config)#aaa authorization network LWA_AUTHORIZATION group RADIUSGROUP
9800WLC(config)#end
```

Configure Parameter Maps

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)# parameter-map type webauth global
9800WLC(config-params-parameter-map)#virtual-ip ipv4 192.0.2.1
9800WLC(config-params-parameter-map)#trustpoint <trustpoint name>
9800WLC(config-params-parameter-map)#webauth-http-enable
9800WLC(config-params-parameter-map)#end
```

Configure WLAN Security Parameters

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#wlan LWA_EA 1 LWA_EA
```

```
9800WLC(config-wlan)#no security wpa
9800WLC(config-wlan)#no security wpa wpa2
9800WLC(config-wlan)#no security wpa wpa2 ciphers aes
9800WLC(config-wlan)#no security wpa akm dot1x
9800WLC(config-wlan)#security web-auth
9800WLC(config-wlan)#security web-auth authentication-list LWA_AUTHENTICATION
9800WLC(config-wlan)#security web-auth parameter-map global
9800WLC(config-wlan)#no shutdown
9800WLC(config-wlan)#end
```

Create Wireless Policy Profile

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#wireless profile policy POLICY_PROFILE
9800WLC(config-wireless-policy)#vlan <vlan name>
9800WLC(config-wireless-policy)#no shutdown
9800WLC(config-wireless-policy)#end
```

Create a Policy Tag

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#wireless tag policy POLICY_TAG
9800WLC(config-policy-tag)#wlan LWA_EA policy POLICY_PROFILE
9800WLC(config-policy-tag)# end
```

Assign a Policy Tag to an AP

```
9800WLC> enable
9800WLC# configure terminal
9800WLC(config)#ap <MAC address>
9800WLC(config-ap-tag)#policy-tag POLICY_TAG
9800WLC(config-ap-tag)#end
```

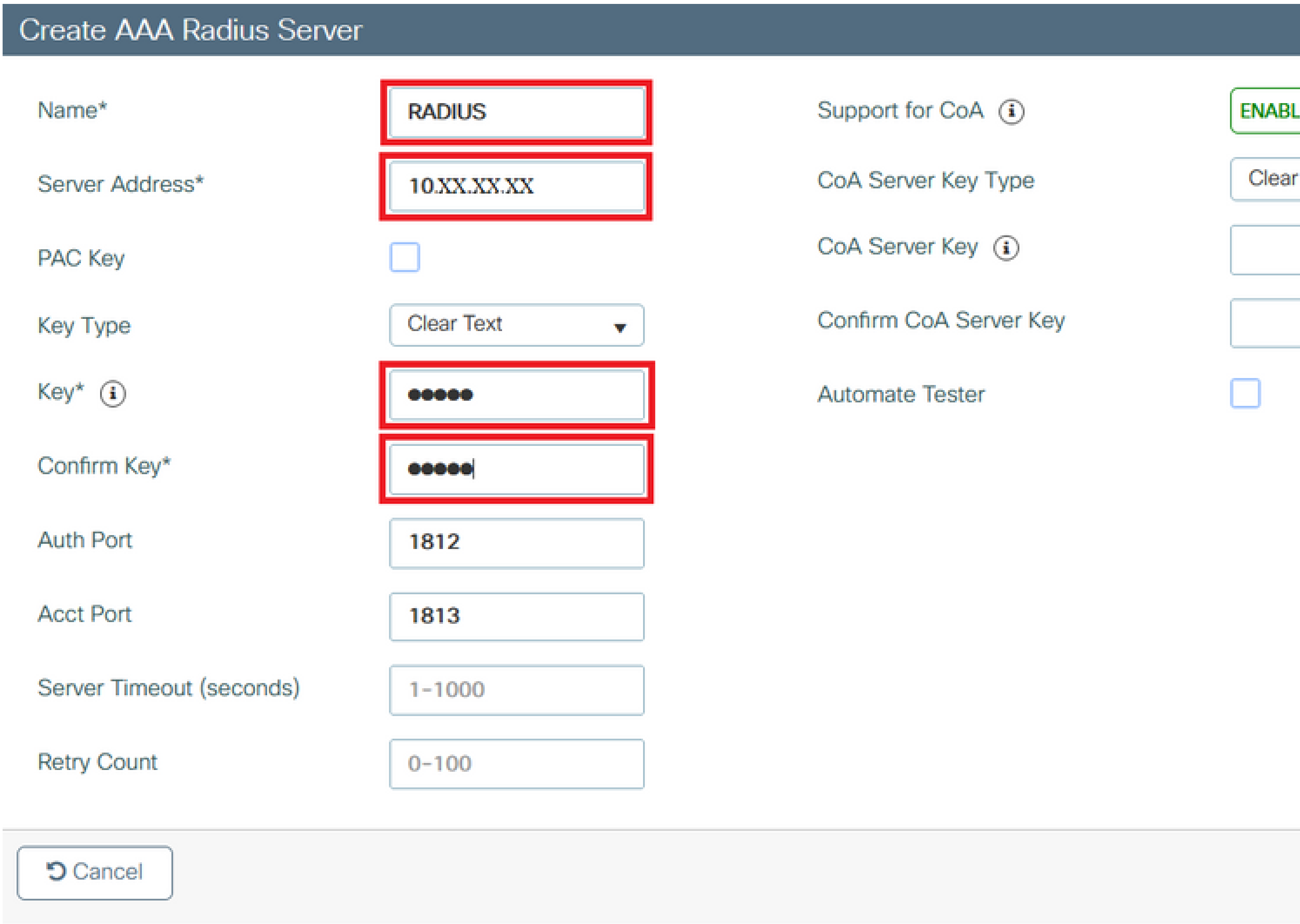
To finish the configuration on the ISE side, please jump to the section ISE Configuration.

Configure Local Web Authentication with External Authentication on the WebUI

AAA Configuration on 9800 WLC

Step 1. Add the ISE server to the 9800 WLC configuration.

Navigate to **Configuration > Security > AAA > Servers/Groups > RADIUS > Servers > + Add** and enter the RADIUS server information as shown in the image:



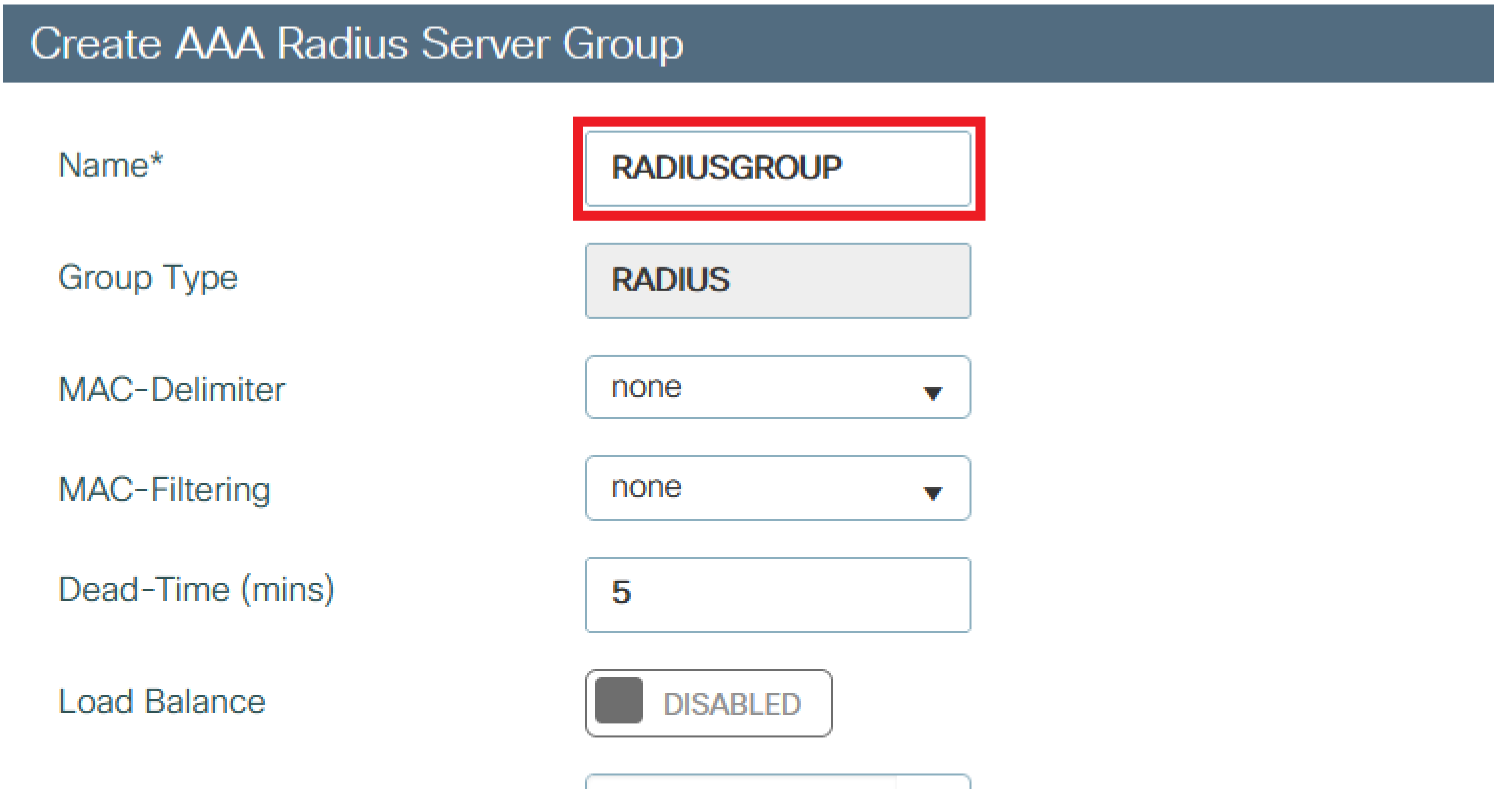
Create AAA Radius Server

Name*	RADIUS	Support for CoA	ENABL
Server Address*	10.XX.XX.XX	CoA Server Key Type	Clear
PAC Key	□	CoA Server Key	
Key Type	Clear Text	Confirm CoA Server Key	
Key*	●●●●●	Automate Tester	□
Confirm Key*	●●●●●		
Auth Port	1812		
Acct Port	1813		
Server Timeout (seconds)	1-1000		
Retry Count	0-100		

AAA Configuration on 9800 WLC

Step 2. Add the RADIUS server group.

Navigate to **Configuration** > **Security** > **AAA** > **Servers/Groups** > **RADIUS** > **Servers Group** > + **Add** and enter the RADIUS server group information:

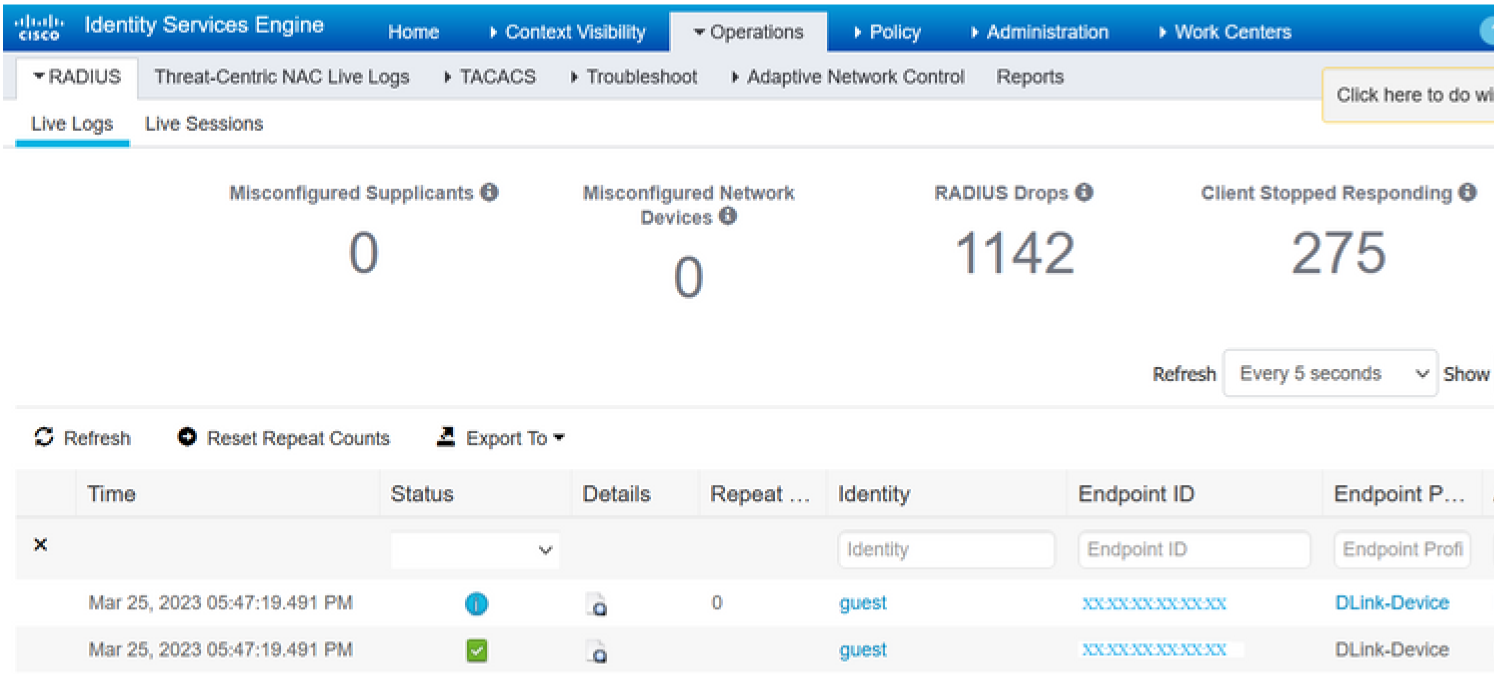


Create AAA Radius Server Group

Name*	RADIUSGROUP
Group Type	RADIUS
MAC-Delimiter	none
MAC-Filtering	none
Dead-Time (mins)	5
Load Balance	DISABLED

: The URL presented was provided by the WLC. It contains the WLC Virtual IP and the redirect for the Windows connect test URL.

Step 3. Navigate to **Operations > RADIUS > Live Logs**. You can see the client device authenticated.



Misconfigured Supplicants 0

Misconfigured Network Devices 0

RADIUS Drops 1142

Client Stopped Responding 275

Refresh Every 5 seconds Show

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...
×				Identity	Endpoint ID	Endpoint Profi
Mar 25, 2023 05:47:19.491 PM	●		0	guest	XX:XX:XX:XX:XX:XX	DLink-Device
Mar 25, 2023 05:47:19.491 PM	✓			guest	XX:XX:XX:XX:XX:XX	DLink-Device

Radius Live Logs

Verify

Use this section in order to confirm that your configuration works properly.

Show WLAN Summary

```
<#root>

9800WLC#show wlan summary

Number of WLANs: 3
ID Profile Name SSID Status Security
-------------------------------------------------
1 WLAN1 WLAN1 DOWN [WPA2][802.1x][AES]
2 WLAN2 WLAN2 UP [WPA2][PSK][AES],MAC Filtering

34 LWA_EA LWA_EA UP [open],[Web Auth]


9800WLC#

show wlan name LWA_EA


WLAN Profile Name : LWA_EA
================================================
Identifier : 34
Description :
Network Name (SSID) : LWA_EA
Status : Enabled
Broadcast SSID : Enabled
Advertise-Apname : Disabled
Universal AP Admin : Disabled
(...)
Accounting list name :
802.1x authentication list name : Disabled
802.1x authorization list name : Disabled
```

```
Security
802.11 Authentication : Open System

Static WEP Keys : Disabled
Wi-Fi Protected Access (WPA/WPA2/WPA3) : Disabled

OWE Transition Mode : Disabled
OSEN : Disabled
FT Support : Adaptive
FT Reassociation Timeout (secs) : 20
FT Over-The-DS mode : Disabled
PMF Support : Disabled
PMF Association Comeback Timeout (secs): 1
PMF SA Query Time (msecs) : 200
Web Based Authentication : Enabled

IPv4 ACL : Unconfigured
IPv6 ACL : Unconfigured
Conditional Web Redirect : Disabled
Splash-Page Web Redirect : Disabled
Webauth On-mac-filter Failure : Disabled
Webauth Authentication List Name : LWA_AUTHENTICATION


Webauth Authorization List Name : Disabled


Webauth Parameter Map : global

Band Select : Disabled
Load Balancing : Disabled
(...)
```

Show Parameter Map Configuration

```
9800WLC#show running-config | section parameter-map type webauth global

parameter-map type webauth global
type webauth
virtual-ip ipv4 192.0.2.1
trustpoint 9800-17-3-3_WLC_TP
webauth-http-enable
```

Show AAA Information

<#root>

```
9800WLC#show aaa method-lists authentication

authen queue=AAA_ML_AUTHEN_LOGIN
name=default valid=TRUE id=0 :state=ALIVE : LOCAL

name=LWA_AUTHENTICATION valid=TRUE id=E0000007 :state=ALIVE : SERVER_GROUP RADIUSGROUP


authen queue=AAA_ML_AUTHEN_ENABLE
authen queue=AAA_ML_AUTHEN_PPP
authen queue=AAA_ML_AUTHEN_SGBP
(...)

9800WLC#show aaa method-lists authorization

author queue=AAA_ML_AUTHOR_SHELL
name=default valid=TRUE id=0 :state=ALIVE : LOCAL
author queue=AAA_ML_AUTHOR_NET
name=default valid=TRUE id=0 :state=ALIVE : LOCAL
name=rq-authoAAA valid=TRUE id=83000009 :state=ALIVE : SERVER_GROUP RADIUSGROUP

name=LWA_AUTHORIZATION valid=TRUE id=DB00000A :state=ALIVE : SERVER_GROUP RADIUSGROU

P
author queue=AAA_ML_AUTHOR_CONN
author queue=AAA_ML_AUTHOR_IPMOBILE
author queue=AAA_ML_AUTHOR_RM
(...)

9800WLC#show aaa servers


RADIUS: id 3, priority 1, host 10.48.39.247,
auth-port 1812, acct-port 1813, hostname RADIUS


State: current UP, duration 171753s, previous duration 0s
Dead: total time 0s, count 0
Platform State from SMD: current UP, duration 171753s, previous duration 0s
SMD Platform Dead: total time 0s, count 0
Platform State from WNCD (1) : current UP
(...)
```

Troubleshoot

Common Issues

These are several guides on how to troubleshoot Web Authentication issues, such as:

- Users cannot authenticate.
- Certificate problems.
- Redirection URL does not work.
- Guest users cannot connect to the guest WLAN.
- Users do not obtain an IP address.
- Redirection to the Web Authentication Log in Page fails.
- After successful Authentication, guest users fail to get access to the Internet.

These guides describe troubleshoot steps in detail:

- Troubleshoot Common Issues for Web Authentication
- Other Situations to Troubleshoot

Conditional Debug and Radio Active Trace and Embedded Packet Capture

You can enable conditional debug and capture Radio Active (RA) trace, which provides debug level traces for all processes that interact with the specified condition (client mac address in this case). In order to enable conditional debug, use the steps in the guide, Conditional Debug and RadioActive trace.

You can also collect Embedded Packet capture (EPC). EPC is a packet capture facility that allows a view into packets destined to, sourced from, and passes through the Catalyst 9800 WLCs, namely DHCP, DNS, HTTP GET packets in LWA. These captures can be exported for offline analysis with Wireshark. For detailed steps on how to do this, refer to Embedded Packet Capture.

Example of a Successful Attempt

This is the output from the RA_traces for a successful attempt to identify each of the phases upon the association/authentication process, while in connection to a guest SSID with RADIUS server.

802.11 association/authentication:

```
[client-orch-sm] [17062]: (note): MAC: 0c0e.766c.0e97 Association received. BSSID cc70.edcf.552f, WLAN LWA_EA, Slot 1 AP cc70.edcf.5520, DO_NOT_MOVE.Static_AP1
[client-orch-sm] [17062]: (debug): MAC: 0c0e.766c.0e97 Received Dot11 association request. Processing started,SSID: LWA_EA, Policy profile: POLICY_PROFILE, AP Name: DO_NOT_MOVE.Static_AP1, Ap Mac Address: cc70.edcf.5520BSSID MAC0000.0000.0000wlan ID: 1RSSI: -49, SNR: 46
[client-orch-state] [17062]: (note): MAC: 0c0e.766c.0e97 Client state transition: S_CO_INIT -> S_CO_ASSOCIATING
[dot11-validate] [17062]: (info): MAC: 0c0e.766c.0e97 Dot11 ie validate ext/supp rates. Validation Passed for Supported rates radio_type 2
[dot11-validate] [17062]: (info): MAC: 0c0e.766c.0e97 WiFi direct: Dot11 validate P2P IE. P2P IE not present.
[dot11] [17062]: (debug): MAC: 0c0e.766c.0e97 dot11 send association response. Framing association response with resp_status_code: 0
[dot11] [17062]: (debug): MAC: 0c0e.766c.0e97 Dot11 Capability info byte1 1, byte2: 11
[dot11-frame] [17062]: (info): MAC: 0c0e.766c.0e97 WiFi direct: skip build Assoc Resp with P2P IE: Wifi direct policy disabled
[dot11] [17062]: (info): MAC: 0c0e.766c.0e97 dot11 send association response. Sending assoc response of length: 130 with resp_status_code: 0, DOT11_STATUS: DOT11_STATUS_SUCCESS
[dot11] [17062]: (note): MAC: 0c0e.766c.0e97 Association success. AID 1, Roaming = False, WGB = False, 11r = False, 11w = False Fast roam = False
[dot11] [17062]: (info): MAC: 0c0e.766c.0e97 DOT11 state transition: S_DOT11_INIT -> S_DOT11_ASSOCIATED
[client-orch-sm] [17062]: (debug): MAC: 0c0e.766c.0e97 Station Dot11 association is successful.
```

IP Learn process:

```
[client-orch-state] [17062]: (note): MAC: 0c0e.766c.0e97 Client state transition: S_CO_DPATH_PLUMB_IN_PROGRESS -> S_CO_IP_LEARN_IN_PROGRESS
[client-iplearn] [17062]: (info): MAC: 0c0e.766c.0e97 IP-learn state transition: S_IPLEARN_INIT -> S_IPLEARN_IN_PROGRESS
[client-auth] [17062]: (info): MAC: 0c0e.766c.0e97 Client auth-interface state transition: S_AUTHIF_L2_WEBAUTH_DONE -> S_AUTHIF_L2_WEBAUTH_DONE
[client-iplearn] [17062]: (note): MAC: 0c0e.766c.0e97 Client IP learn successful. Method: DHCP IP: 10.48.39.243
[client-iplearn] [17062]: (info): MAC: 0c0e.766c.0e97 IP-learn state transition: S_IPLEARN_IN_PROGRESS -> S_IPLEARN_COMPLETE
```

```
[client-orch-sm] [17062]: (debug): MAC: 0c0e.766c.0e97 Received ip learn response. method: IPLEARN_METHOD_DHCP
```

Layer 3 authentication:

```
[client-orch-sm] [17062]: (debug): MAC: 0c0e.766c.0e97 Triggered L3 authentication. status = 0x0, Success
[client-orch-state] [17062]: (note): MAC: 0c0e.766c.0e97 Client state transition: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_L3_AUTH_IN_PROGRESS
[client-auth] [17062]: (note): MAC: 0c0e.766c.0e97 L3 Authentication initiated. LWA
[client-auth] [17062]: (info): MAC: 0c0e.766c.0e97 Client auth-interface state transition: S_AUTHIF_L2_WEBAUTH_DONE -> S_AUTHIF_WEBAUTH_PENDING
```

```
[webauth-httpd] [17062]: (info): capwap_90000004[0c0e.766c.0e97][ 10.48.39.243]GET rcvd when in LOGIN state
[webauth-httpd] [17062]: (info): capwap_90000004[0c0e.766c.0e97][ 10.48.39.243]HTTP GET request
[webauth-httpd] [17062]: (info): capwap_90000004[0c0e.766c.0e97][ 10.48.39.243]Parse GET, src [10.48.39.243] dst [10.107.221.82] url [http://firefox detect portal/]
[webauth-httpd] [17062]: (info): capwap_90000004[0c0e.766c.0e97][ 10.48.39.243]Read complete: parse_request return 8
[webauth-io] [17062]: (info): capwap_90000004[0c0e.766c.0e97][ 10.48.39.243]56538/219 IO state READING -> WRITING
[webauth-io] [17062]: (info): capwap_90000004[0c0e.766c.0e97][ 10.48.39.243]56538/219 IO state WRITING -> READING
[webauth-io] [17062]: (info): capwap_90000004[0c0e.766c.0e97][ 10.48.39.243]56539/218 IO state NEW -> READING
[webauth-io] [17062]: (info): capwap_90000004[0c0e.766c.0e97][ 10.48.39.243]56539/218 Read event, Message ready
[webauth-httpd] [17062]: (info): capwap_90000004[0c0e.766c.0e97][ 10.48.39.243]POST rcvd when in LOGIN state
```

Layer 3 authentication successful, move the client to the RUN state:

```
[auth-mgr] [17062]: (info): [0c0e.766c.0e97:capwap_90000004] Received User-Name guest for client 0c0e.766c.0e97
[auth-mgr] [17062]: (info): [0c0e.766c.0e97:capwap_90000004] auth mgr attr add/change notification is received for attr auth-domain(954)
[auth-mgr] [17062]: (info): [0c0e.766c.0e97:capwap_90000004] Method webauth changing state from 'Running' to 'Authc Success'
[auth-mgr] [17062]: (info): [0c0e.766c.0e97:capwap_90000004] Context changing state from 'Running' to 'Authc Success'
[auth-mgr] [17062]: (info): [0c0e.766c.0e97:capwap_90000004] auth mgr attr add/change notification is received for attr method(757)
[auth-mgr] [17062]: (info): [0c0e.766c.0e97:capwap_90000004] Raised event AUTHZ_SUCCESS (11)
[auth-mgr] [17062]: (info): [0c0e.766c.0e97:capwap_90000004] Context changing state from 'Authc Success' to 'Authz Success'
[webauth-acl] [17062]: (info): capwap_90000004[0c0e.766c.0e97][ 10.48.39.243]Applying IPv4 logout ACL via SVM, name: IP-Adm-V4-LOGOUT-ACL, priority: 51, IIF-ID: 0
[webauth-sess] [17062]: (info): capwap_90000004[0c0e.766c.0e97][ 10.48.39.243]Param-map used: global
[webauth-state] [17062]: (info): capwap_90000004[0c0e.766c.0e97][ 10.48.39.243]Param-map used: global
[webauth-state] [17062]: (info): capwap_90000004[0c0e.766c.0e97][ 10.48.39.243]State AUTHC_SUCCESS -> AUTHZ
[webauth-page] [17062]: (info): capwap_90000004[0c0e.766c.0e97][ 10.48.39.243]Sending Webauth success page
[webauth-io] [17062]: (info): capwap_90000004[0c0e.766c.0e97][ 10.48.39.243]56539/218 IO state AUTHENTICATING -> WRITING
[webauth-io] [17062]: (info): capwap_90000004[0c0e.766c.0e97][ 10.48.39.243]56539/218 IO state WRITING -> END
[webauth-httpd] [17062]: (info): capwap_90000004[0c0e.766c.0e97][ 10.48.39.243]56539/218 Remove IO ctx and close socket, id [99000029]
[client-auth] [17062]: (note): MAC: 0c0e.766c.0e97 L3 Authentication Successful. ACL:[]
[client-auth] [17062]: (info): MAC: 0c0e.766c.0e97 Client auth-interface state transition: S_AUTHIF_WEBAUTH_PENDING -> S_AUTHIF_WEBAUTH_DONE
[webauth-httpd] [17062]: (info): capwap_90000004[0c0e.766c.0e97][ 10.48.39.243]56538/219 Remove IO ctx and close socket, id [D7000028]
[errmsg] [17062]: (info): %CLIENT_ORCH_LOG-6-CLIENT_ADDED_TO_RUN_STATE: R0/0: wncd: Username entry (guest) joined with ssid (LWA_EA) for device with MAC: 0c0e.766c.0e97
```

```
[aaa-attr-inf] [17062]: (info): [ Applied attribute :bsn-vlan-interface-name 0 "VLAN0039" ]
[aaa-attr-inf] [17062]: (info): [ Applied attribute : timeout 0 1800 (0x708) ]
[aaa-attr-inf] [17062]: (info): [ Applied attribute : url-redirect-acl 0 "IP-Adm-V4-LOGOUT-ACL" ]
[ewlc-qos-client] [17062]: (info): MAC: 0c0e.766c.0e97 Client QoS run state handler
[rog-proxy-capwap] [17062]: (debug): Managed client RUN state notification: 0c0e.766c.0e97
[client-orch-state] [17062]: (note): MAC: 0c0e.766c.0e97 Client state transition: S_CO_L3_AUTH_IN_PROGRESS -> S_CO_RUN
```

Related Information

- **Cisco Technical Support & Downloads**