

Unified Access Wireless LAN Controllers Guest Anchor with Converged Access Configuration Example



by [surbg](#) on 06-02-2014 11:34 AM



- edited on 06-18-2014 08:52 AM by [rarowell](#)

Table of Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Network Diagram](#)

[Configurations](#)

[Part 1 - Configuration on the 5508 Anchor WLC](#)

[Part 2 -Converged Access Mobility Configuration between the 5508/5760 Series WLC and the Catalyst](#)

38...

[Part 3: Configuration on the Foreign Catalyst 3850 Series Switch](#)

[Verify](#)

[Troubleshoot](#)

Introduction

This document describes how to configure the 5508/5760 Series Wireless LAN Controllers (WLCs) and the Catalyst 3850 Series Switch for the wireless client Guest Anchor in the new mobility deployment setup where the 5508 Series WLC acts as the Mobility Anchor and the Catalyst 3850 Series Switch acts as a Mobility Foreign Controller for the clients. Additionally, the Catalyst 3850 Series Switch acts as a Mobility Agent to a 5760 Series WLC that acts as a Mobility Controller from where the Catalyst 3850 Series Switch acquires the Access Point (AP) license.

Contributed by Surendra BG, Cisco TAC Engineer.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics before you attempt this configuration:

- Cisco IOS® GUI or CLI with the Converged Access 5760 and 3650 Series WLCs and the Catalyst 3850 Series Switch
- GUI and CLI access with the 5508 Series WLC
- Service Set Identifier (SSID) configuration
- Web authentication

Components Used

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

- Cisco 5760 Release 3.3.3 (Next Generation Wiring Closet [NGWC])
- Catalyst 3850 Series Switch

- Cisco 5508 Series WLC Release 7.6.120
- Cisco 3602 Series Lightweight APs
- Cisco Catalyst 3560 Series Switches

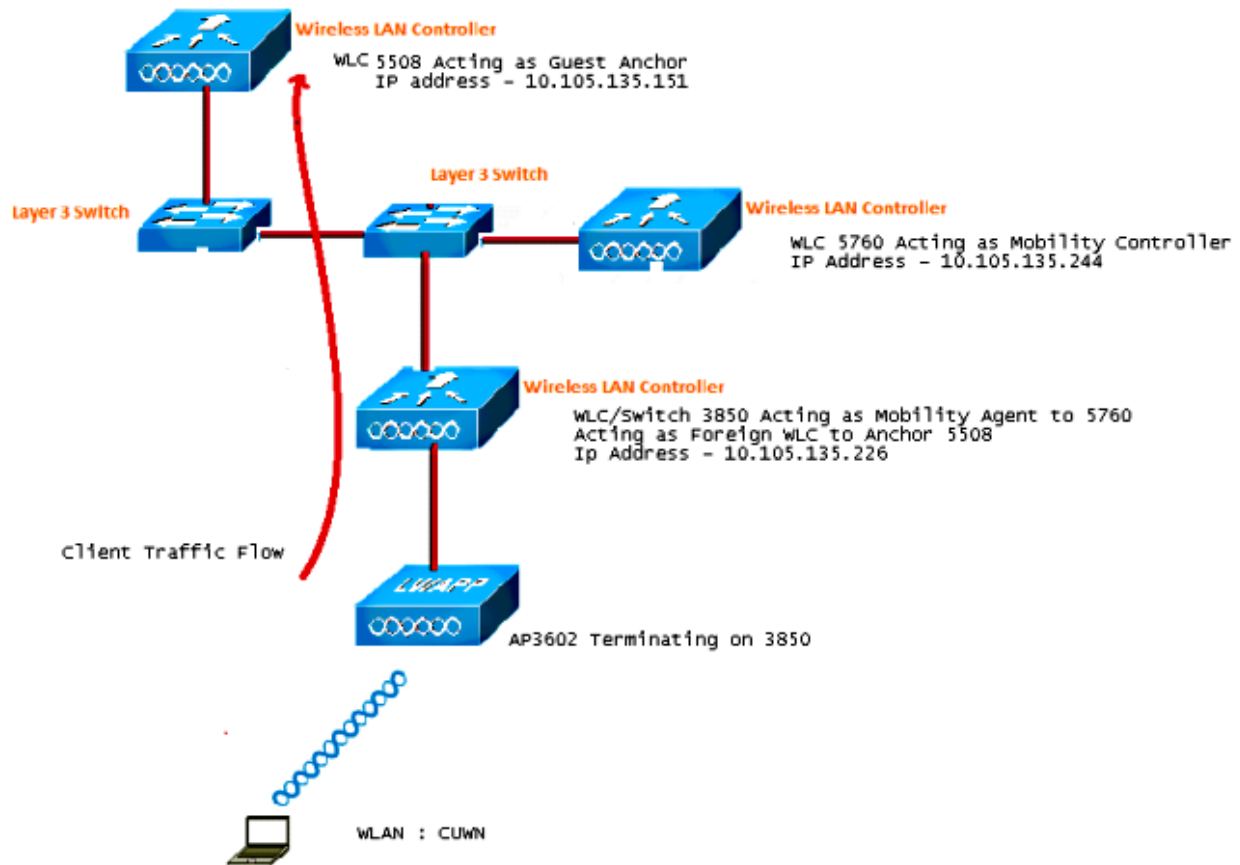
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configure

Note: Use the [Command Lookup Tool](#) (registered customers only) in order to obtain more information on the commands used in this section.

Network Diagram

The 5508 Series WLC acts as an Anchor Controller, and the Catalyst 3850 Series Switch acts as a Foreign Controller and the Mobility Agent that obtains the license from the Mobility Controller 5760.



Note: In the network diagram, the 5508 Series WLC acts as the Anchor Controller, the 5760 Series WLC acts as the Mobility Controller, and the Catalyst 3850 Series Switch acts as the Mobility Agent and Foreign WLC. At any point in time, the Anchor Controller for the Catalyst 3850 Series Switch is either the 5760 Series WLC or the 5508 Series WLC. Both cannot be Anchors at the same time, because the double anchor does not work.

Configurations

The configuration includes three parts:

[Part 1 - Configuration on the 5508 Anchor WLC](#)

[Part 2 - Converged Access Mobility Configuration between the 5508/5760 Series WLC and the Catalyst 3...](#)

[Part 3 - Configuration on the Foreign Catalyst 3850 Series Switch](#)

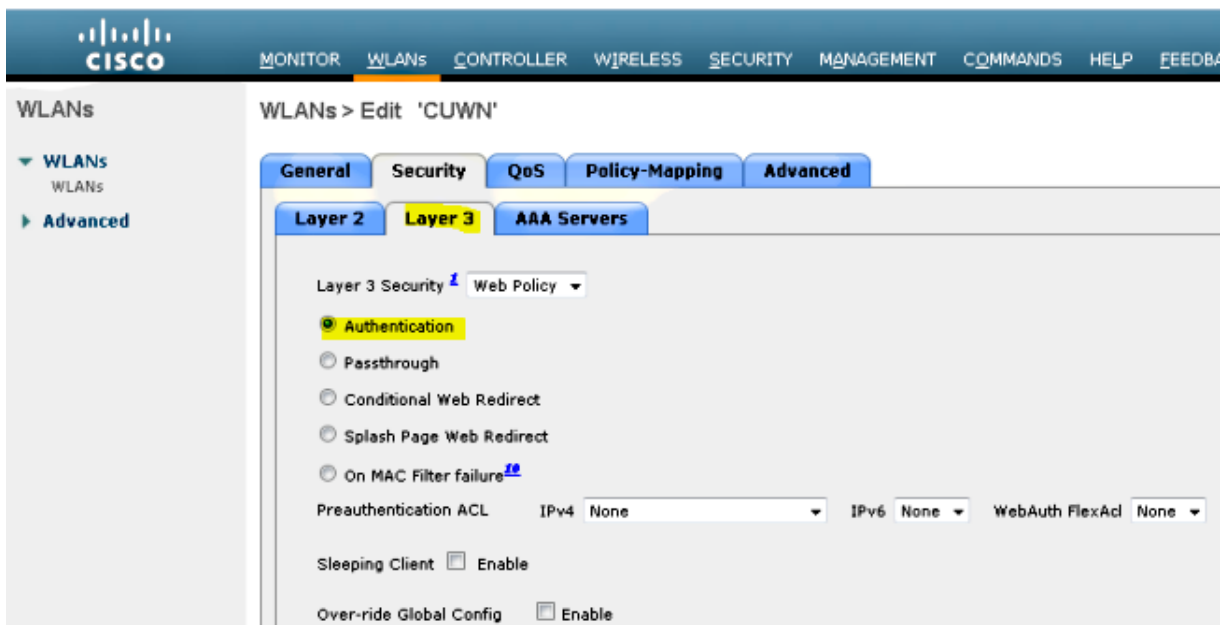
Part 1 - Configuration on the 5508 Anchor WLC

1. On the 5508 Series WLC, hover over **WLAN > New** in order to create a new Wireless LAN (WLAN).

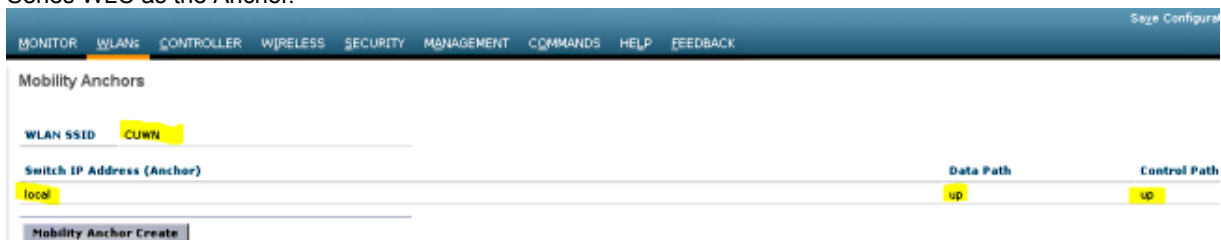
The screenshot shows the Cisco WLC configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', and 'HELP'. The 'WLANs' section is active, and the breadcrumb path is 'WLANs > Edit 'CUWN''. The configuration page is divided into tabs: 'General', 'Security', 'QoS', 'Policy-Mapping', and 'Advanced'. The 'General' tab is selected, showing the following configuration details:

| | |
|------------------------------|--|
| Profile Name | CUWN |
| Type | WLAN |
| SSID | CUWN |
| Status | <input checked="" type="checkbox"/> Enabled |
| Security Policies | WEB POLICY, Web-Auth (Modifications done under security tab will appear after applying the changes.) |
| Radio Policy | All |
| Interface/Interface Group(G) | vlan60 |
| Multicast Vlan Feature | <input type="checkbox"/> Enabled |
| Broadcast SSID | <input checked="" type="checkbox"/> Enabled |
| NAS-ID | 5508 |

2. Hover over **WLAN > WLAN Edit > Security > Layer 3 enabled Web-authentication** in order to configure Layer 3 Security.

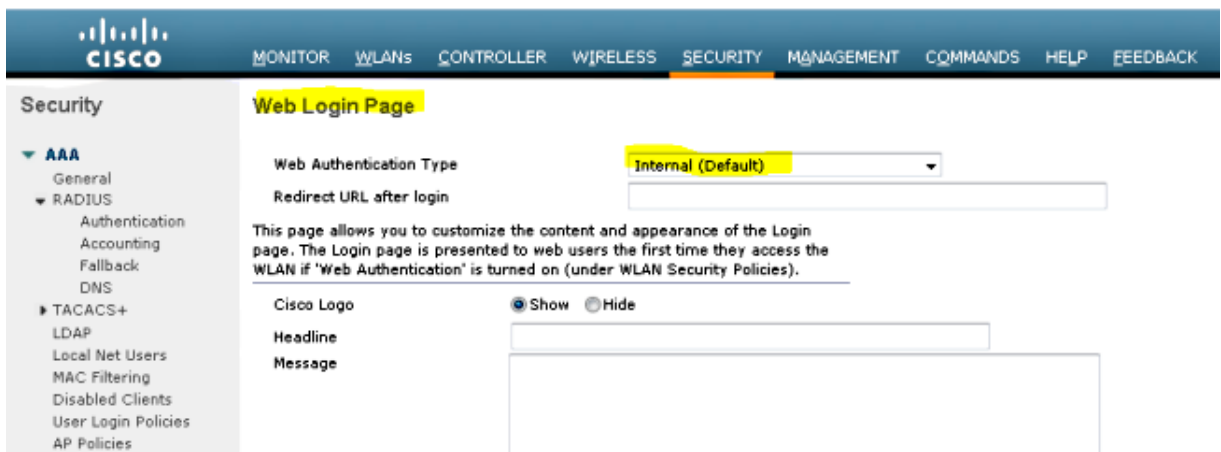


3. Make the Anchor address **local** under the WLAN mobility Anchor configuration window in order to add the 5508 Series WLC as the Anchor.

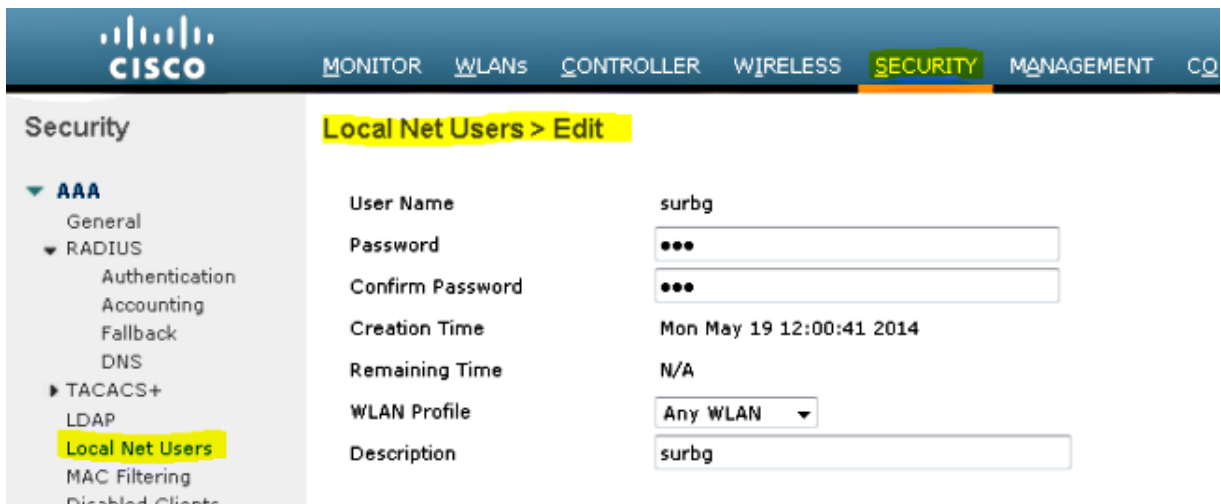


4. Hover over **Security > Webauth > Webauth page** in order to configure the Webauth page to be used for the client authentication.

In this example, the WLC Internal Webauth page is selected:

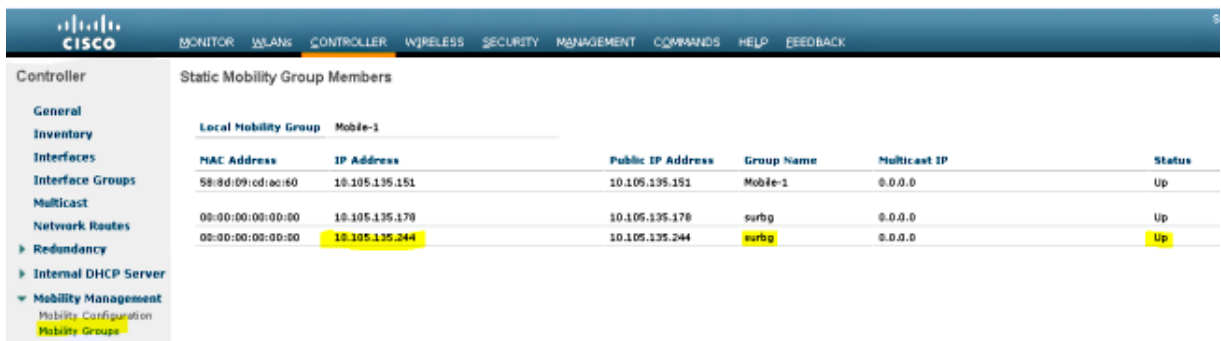


5. Create a local net user. This username/password pair is used by the user when prompted on the Webauth page.

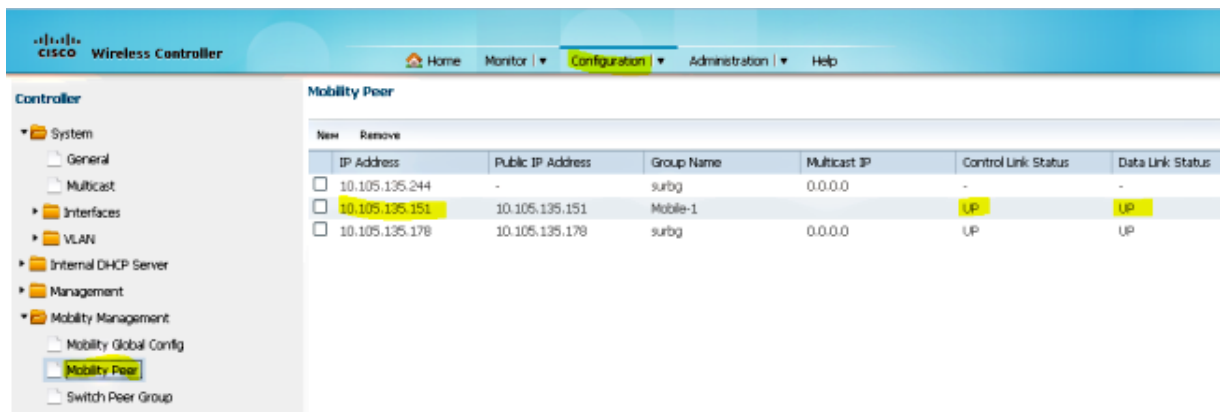


Part 2 -Converged Access Mobility Configuration between the 5508/5760 Series WLC and the Catalyst 3850 Series Switch

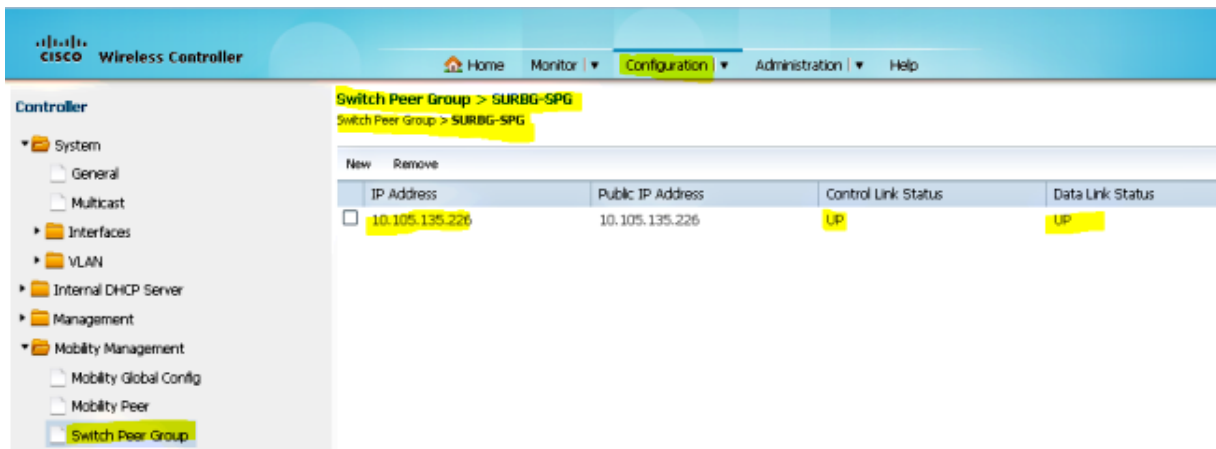
1. On the 5508 Series WLC, add the 5760 Series WLC as the Mobility Peer.



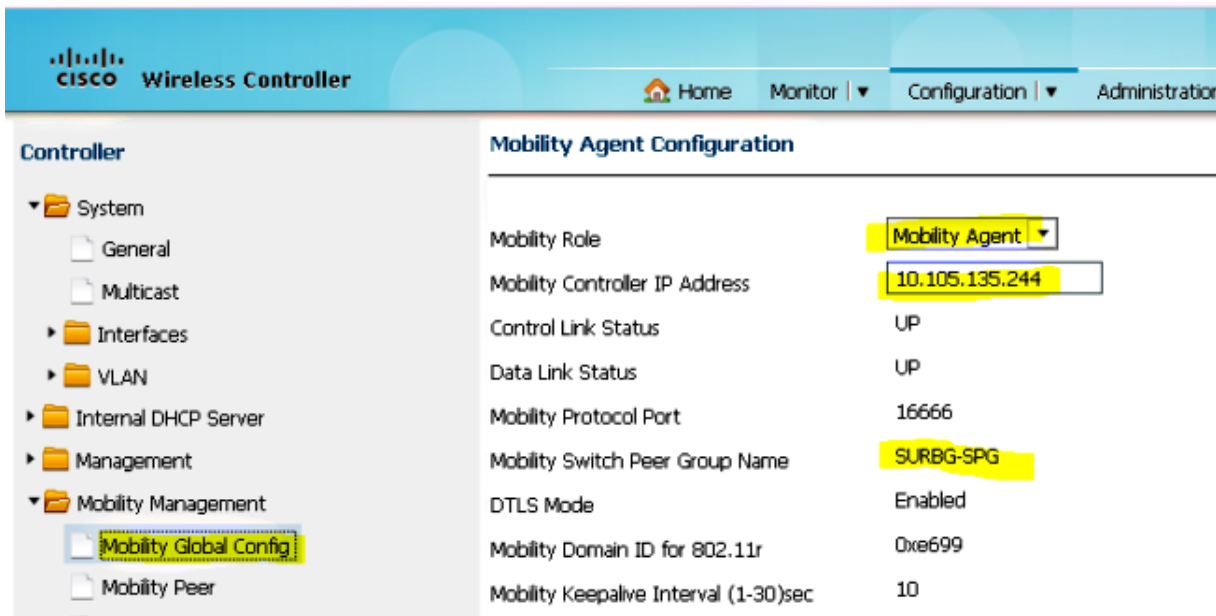
2. On the 5760 Series WLC, acting as a Mobility Controller, add the 5508 Series WLC as the Mobility Peer.



3. This step is very important! Add the Catalyst 3850 Series Switch as the Mobility Agent on the 5760 Series WLC under the Switch Peer Group tab under Mobility Management.



4. On the Catalyst 3850 Series Switch, add the 5760 Series WLC as the Mobility Controller. Once you do this, the Catalyst 3850 Series Switch grabs the AP count license from the Mobility Controller 5760.

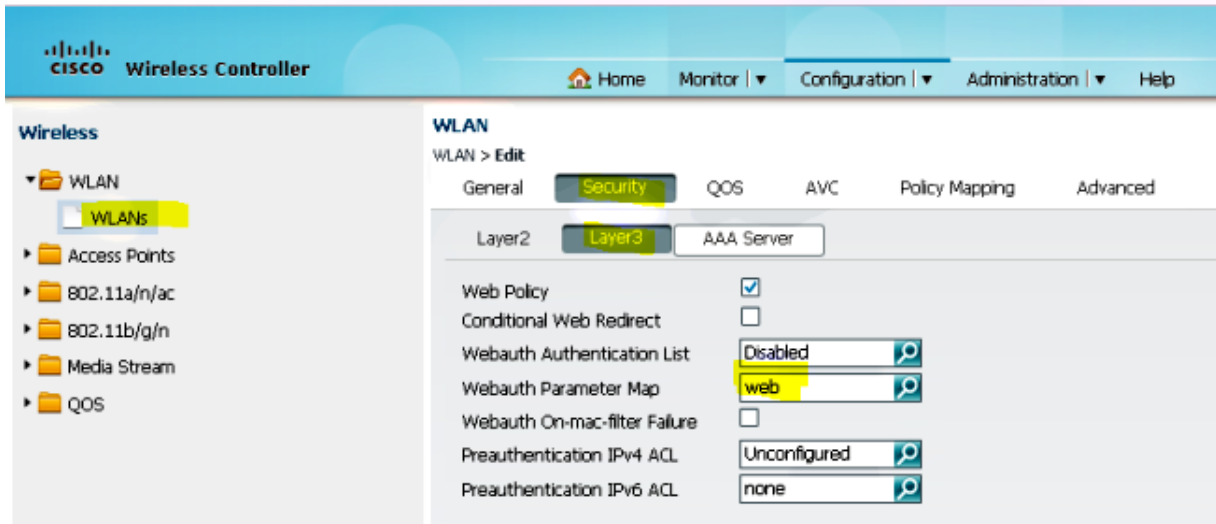


Part 3: Configuration on the Foreign Catalyst 3850 Series Switch

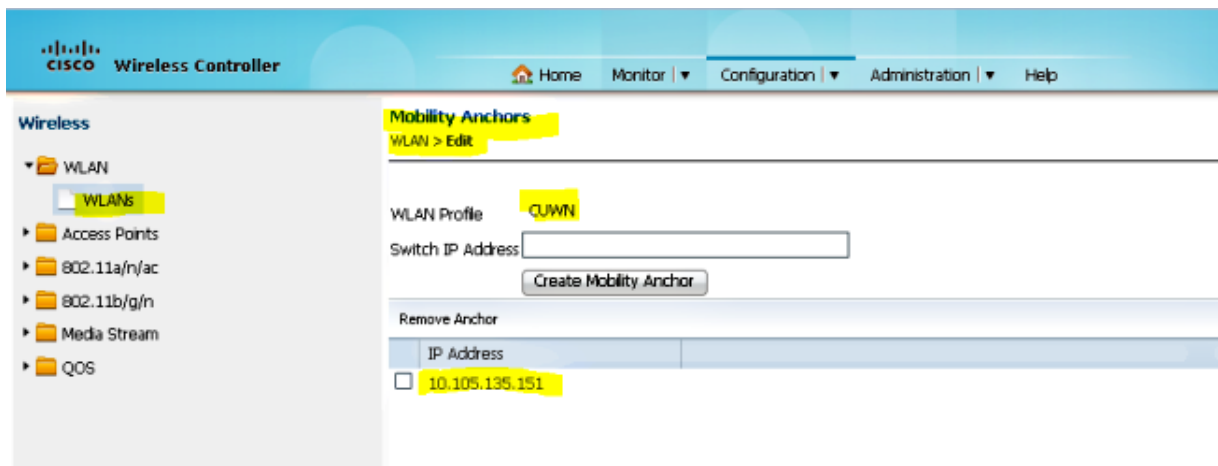
1. Hover over **GUI > Configuration > Wireless > WLAN > New** in order to configure the Exact SSID/WLAN on the Catalyst 3850 Series Switch.



2. Hover over **WLAN > WLAN Edit > Security > Layer 3 enabled Web-authentication** in order to configure Layer 3 Security.



3. Add the 5508 Series WLC IP address as the Anchor under the WLAN Mobility Anchor configuration

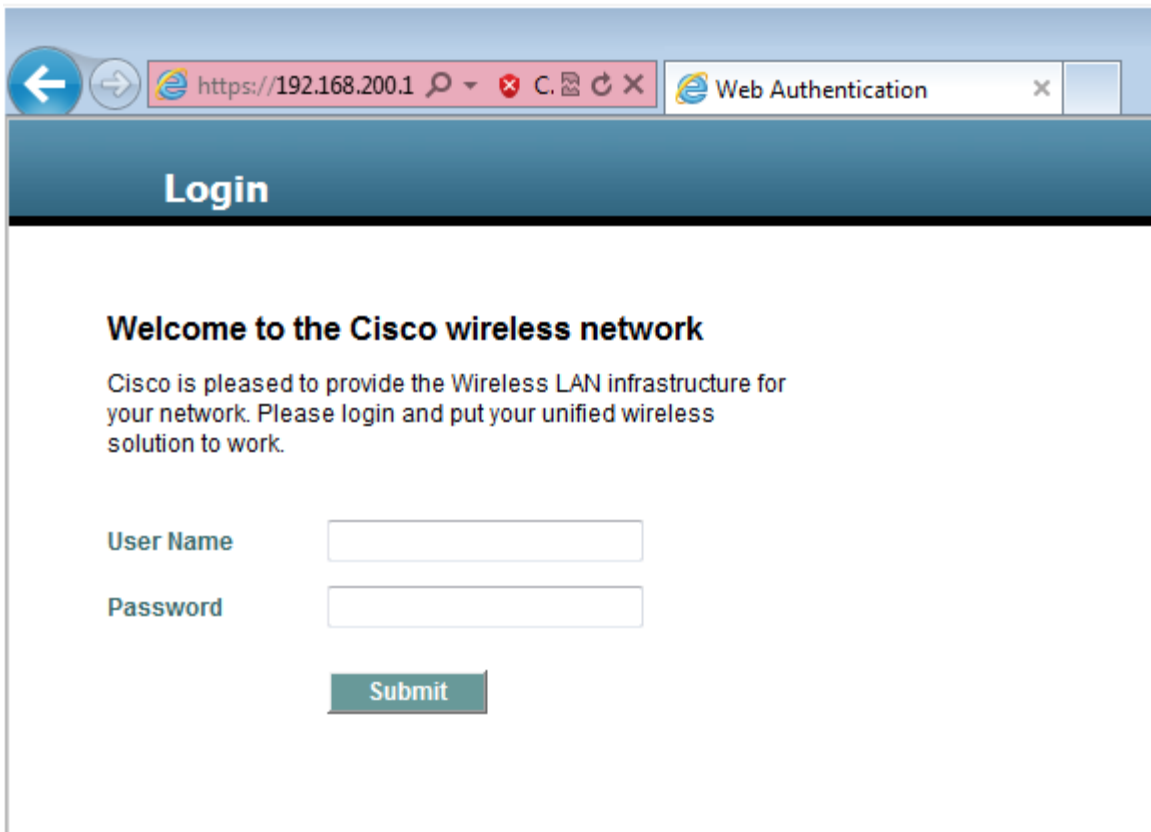


Verify

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

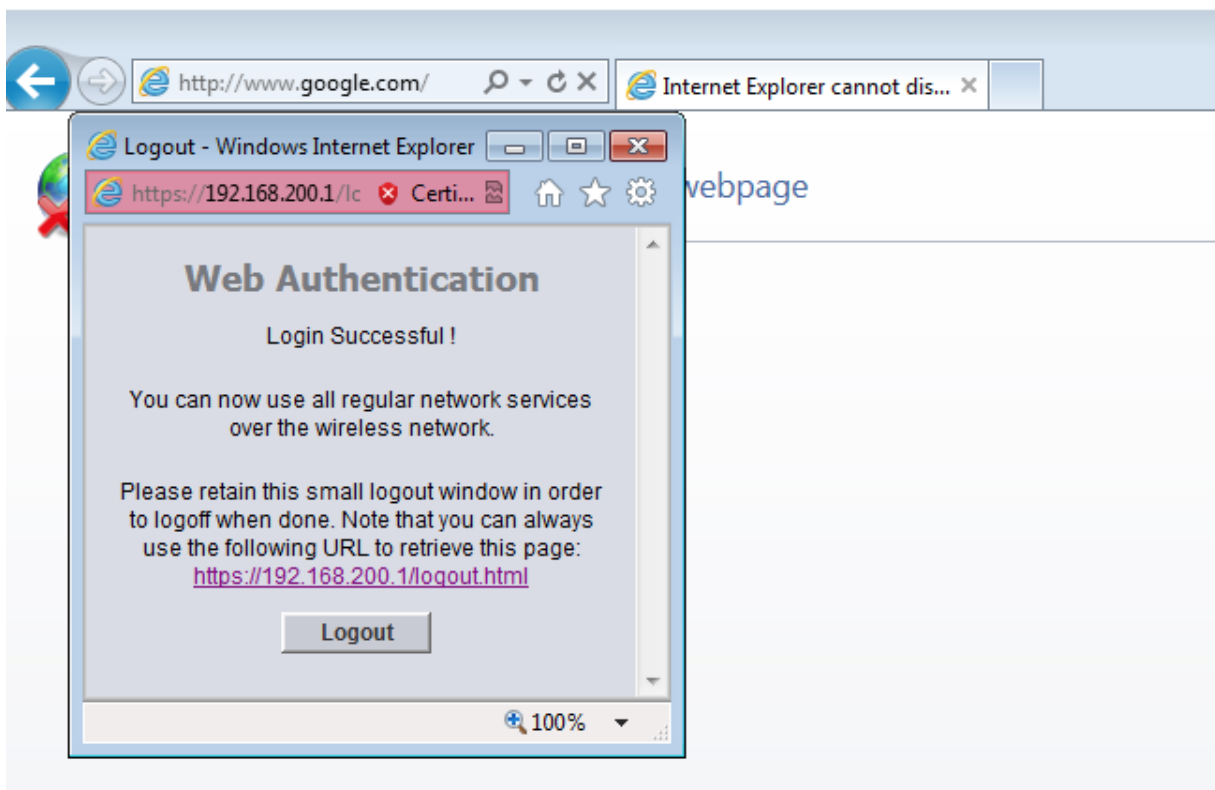
Connect the client to the WLAN Cisco Unified Wireless Network (CUWN). Here is the work flow:

1. The client receives an IP address.
2. The client opens a browser and accesses any website.
3. The first TCP packet sent by the client is hijacked by the WLC, and the WLC intercepts and sends the Webauth page.
4. If the DNS is properly configured, the client gets the Webauth page.
5. The client must provide the username/password in order to get authenticated.
6. After successful authentication, the client is redirected to the original access page.



The screenshot shows a web browser window with the address bar containing `https://192.168.200.1`. The page title is "Web Authentication". The main heading is "Login". Below the heading, there is a message: "Welcome to the Cisco wireless network. Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your unified wireless solution to work." There are two input fields: "User Name" and "Password". Below these fields is a "Submit" button.

7. After the client provides the right credentials, the client passes the auth.



Troubleshoot

In order to troubleshoot your configuration, enter these debugs on the 5508 Series WLC, which acts as a Guest Anchor:

```
Debug Client <client mac addr>
Debug web-auth redirect enable mac <client mac addr>
```

Here is an example:

```
Debug Client 00:17:7C:2F:B6:9A
Debug web-auth redirect enable mac 00:17:7C:2F:B6:9A

show debug

MAC Addr 1..... 00:17:7C:2F:B6:9A

Debug Flags Enabled:
  dhcp packet enabled.
  dot11 mobile enabled.
  dot11 state enabled
  dot1x events enabled.
  dot1x states enabled.
  FlexConnect ft enabled.
  pem events enabled.
  pem state enabled.
  CCKM client debug enabled.
  webauth redirect enabled.

*mmMaListen: May 19 13:36:34.276: 00:17:7c:2f:b6:9a Adding mobile on Remote AP
00:00:00:00:00:00(0)
*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a override for default ap group,
marking intgrp NULL
*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a Applying Interface policy on
Mobile, role Unassociated. Ms NAC State 2 Quarantine Vlan 0 Access Vlan 0

*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a Re-applying interface policy
for client

*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a 0.0.0.0 START (0) Changing
IPv4
ACL 'none' (ACL ID 255) ==> 'none' (ACL ID 255) --- (caller apf_policy.c:2219)
*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a 0.0.0.0 START (0) Changing
IPv6
ACL 'none' (ACL ID 255) ==> 'none' (ACL ID 255) --- (caller apf_policy.c:2240)
*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a apfApplyWlanPolicy: Apply WLAN
Policy over PMIPv6 Client Mobility Type
*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a override from intf group to an
intf for roamed client - removing intf group from msch

*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a 0.0.0.0 AUTHCHECK (2) Change
state to L2AUTHCOMPLETE (4) last state AUTHCHECK (2)

*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a 0.0.0.0 L2AUTHCOMPLETE (4)
```

Change state to DHCP_REQD (7) last state L2AUTHCOMPLETE (4)

```
*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a Resetting web IPv4 acl from
255 to 255

*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a Resetting web IPv4 Flex acl
from 65535 to 65535

*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a Stopping deletion of Mobile
Station: (callerId: 53)
*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7) Adding
Fast Path rule   type = Airespace AP - Learn IP address
  on AP 00:00:00:00:00:00, slot 0, interface = 1, QOS = 0
  IPv4 ACL ID = 255, IPv
*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7) Fast
Path
rule (contd...) 802.1P = 0, DSCP = 0, TokenID = 15206  Local Bridging Vlan = 60,
Local Bridging intf id = 13
*mmMaListen: May 19 13:36:34.277: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7)
Successfully plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)
*mmMaListen: May 19 13:36:34.278: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7) State
Update from Mobility-Incomplete to Mobility-Complete, mobility role=ExpAnchor,
client state=APF_MS_STATE_ASSOCIATED
*mmMaListen: May 19 13:36:34.278: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7)
Change state to DHCP_REQD (7) last state DHCP_REQD (7)

*mmMaListen: May 19 13:36:34.278: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7)
pemAdvanceState2 5807, Adding TMP rule
*mmMaListen: May 19 13:36:34.278: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7)
Replacing Fast Path rule
  type = Airespace AP - Learn IP address
  on AP 00:00:00:00:00:00, slot 0, interface = 1, QOS = 0
  IPv4 ACL ID = 255,
*mmMaListen: May 19 13:36:34.278: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7)
Fast Path rule (contd...) 802.1P = 0, DSCP = 0, TokenID = 15206  Local
Bridging Vlan = 60, Local Bridging intf id = 13
*mmMaListen: May 19 13:36:34.278: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7)
Successfully plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)
*pemReceiveTask: May 19 13:36:34.278: 00:17:7c:2f:b6:9a Set bi-dir guest tunnel
for 00:17:7c:2f:b6:9a as in Export Anchor role
*pemReceiveTask: May 19 13:36:34.278: 00:17:7c:2f:b6:9a 0.0.0.0 Added NPU entry
of type 9, dtlFlags 0x4
*pemReceiveTask: May 19 13:36:34.278: 00:17:7c:2f:b6:9a Sent an XID frame
*pemReceiveTask: May 19 13:36:34.278: 00:17:7c:2f:b6:9a Set bi-dir guest tunnel
for 00:17:7c:2f:b6:9a as in Export Anchor role
*pemReceiveTask: May 19 13:36:34.278: 00:17:7c:2f:b6:9a 0.0.0.0 Added NPU entry
of type 9, dtlFlags 0x4
*IPv6_Msg_Task: May 19 13:36:34.281: 00:17:7c:2f:b6:9a Pushing IPv6 Vlan Intf
ID 13: fe80:0000:0000:0000:6c1a:b253:d711:0c7f , and MAC: 00:17:7C:2F:B6:9A ,
Binding to Data Plane. SUCCESS !! dhcpv6bitmap 0
*IPv6_Msg_Task: May 19 13:36:34.281: 00:17:7c:2f:b6:9a Calling
mmSendIpv6AddrUpdate
for addition of IPv6: fe80:0000:0000:0000:6c1a:b253:d711:0c7f , for MAC:
00:17:7C:2F:B6:9A
*IPv6_Msg_Task: May 19 13:36:34.281: 00:17:7c:2f:b6:9a mmSendIpv6AddrUpdate:4800
Assigning an IPv6 Addr fe80:0000:0000:0000:6c1a:b253:d711:0c7f  to the client in
Anchor state update the foreign switch 10.105.135.226
*IPv6_Msg_Task: May 19 13:36:34.281: 00:17:7c:2f:b6:9a Link Local address fe80::
```

```
6c1a:b253:d711:c7f updated to mscb. Not Advancing pem state.Current state: mscb
in apfMsMmInitial mobility state and client state APF_MS_STATE_AS
*mmMaListen: May 19 13:36:34.298: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7)
Replacing Fast Path rule
  type = Airespace AP - Learn IP address
  on AP 00:00:00:00:00:00, slot 0, interface = 1, QOS = 0
  IPv4 ACL ID = 255,
*mmMaListen: May 19 13:36:34.298: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7)
Fast Path rule (contd...) 802.1P = 0, DSCP = 0, TokenID = 15206 Local Bridging
Vlan = 60, Local Bridging intf id = 13
*mmMaListen: May 19 13:36:34.298: 00:17:7c:2f:b6:9a 0.0.0.0 DHCP_REQD (7)
Successfully plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)
*pemReceiveTask: May 19 13:36:34.298: 00:17:7c:2f:b6:9a Set bi-dir guest tunnel
for
00:17:7c:2f:b6:9a as in Export Anchor role
*pemReceiveTask: May 19 13:36:34.298: 00:17:7c:2f:b6:9a 0.0.0.0 Added NPU entry of
type 9, dtlFlags 0x4
*dtlArpTask: May 19 13:36:34.564: 00:17:7c:2f:b6:9a Static IP client associated to
interface vlan60 which can support client subnet.
*dtlArpTask: May 19 13:36:34.564: 00:17:7c:2f:b6:9a 60.60.60.11 DHCP_REQD (7)
Change state to WEBAUTH_REQD (8) last state DHCP_REQD (7)

*dtlArpTask: May 19 13:36:34.564: 00:17:7c:2f:b6:9a 60.60.60.11 WEBAUTH_REQD (8)
pemAdvanceState2 6717, Adding TMP rule
*dtlArpTask: May 19 13:36:34.564: 00:17:7c:2f:b6:9a 60.60.60.11 WEBAUTH_REQD (8)
Replacing Fast Path rule
  type = Airespace AP Client - ACL passthru
  on AP 00:00:00:00:00:00, slot 0, interface = 1, QOS = 0
  IPv4 ACL
*dtlArpTask: May 19 13:36:34.564: 00:17:7c:2f:b6:9a 60.60.60.11 WEBAUTH_REQD (8)
Fast Path rule (contd...) 802.1P = 0, DSCP = 0, TokenID = 15206 Local Bridging
Vlan = 60, Local Bridging intf id = 13
*dtlArpTask: May 19 13:36:34.564: 00:17:7c:2f:b6:9a 60.60.60.11 WEBAUTH_REQD (8)
Successfully plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)
*dtlArpTask: May 19 13:36:34.564: 00:17:7c:2f:b6:9a Plumbing web-auth redirect
rule
due to user logout
*dtlArpTask: May 19 13:36:34.564: 00:17:7c:2f:b6:9a apfAssignMscbIpAddr:1148
Assigning an Ip Addr 60.60.60.11 to the client in Anchor state update the foreign
switch 10.105.135.226
*dtlArpTask: May 19 13:36:34.565: 00:17:7c:2f:b6:9a Assigning Address 60.60.60.11
to mobile
*pemReceiveTask: May 19 13:36:34.565: 00:17:7c:2f:b6:9a Set bi-dir guest tunnel
for
00:17:7c:2f:b6:9a as in Export Anchor role
*pemReceiveTask: May 19 13:36:34.565: 00:17:7c:2f:b6:9a 60.60.60.11 Added NPU
entry
of type 2, dtlFlags 0x4
*pemReceiveTask: May 19 13:36:34.565: 00:17:7c:2f:b6:9a Pushing IPv6:
fe80:0000:0000:0000:6c1a:b253:d711:0c7f , and MAC: 00:17:7C:2F:B6:9A , Binding to
Data Plane. SUCCESS !!
*pemReceiveTask: May 19 13:36:34.565: 00:17:7c:2f:b6:9a Sent an XID frame

(5508-MC) >
(5508-MC) >
(5508-MC) >*DHCP Socket Task: May 19 13:36:44.259: 00:17:7c:2f:b6:9a DHCP received
op BOOTREQUEST (1) (len 314,vlan 0, port 1, encap 0xec07)
*DHCPSocket Task: May 19 13:36:44.259: 00:17:7c:2f:b6:9a DHCP (encap type 0xec07)
```

```
mstype 3ff:ff:ff:ff:ff:ff
*DHCPSocketTask: May 19 13:36:44.259: 00:17:7c:2f:b6:9a DHCP selecting relay 1 -
control block settings:
    dhcpServer: 0.0.0.0, dhcpNetmask: 0.0.0.0,
    dhcpGateway: 0.0.0.0, dhcpRelay: 0.0.0.0 VLAN: 0
*DHCPSocketTask: May 19 13:36:44.259: 00:17:7c:2f:b6:9a DHCP selected relay 1 -
60.60.60.251 (local address 60.60.60.2, gateway 60.60.60.251, VLAN 60, port 1)
*DHCPSocketTask: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP transmitting DHCP
REQUEST (3)
*DHCPSocketTask: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP op: BOOTREQUEST,
htype: Ethernet, hlen: 6, hops: 1
*DHCPSocketTask: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP xid: 0xad00ada3
(2902502819), secs: 3072, flags: 0
*DHCPSocketTask: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP chaddr:
00:17:7c:2f:b6:9a
*DHCPSocketTask: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP ciaddr: 0.0.0.0,
yiaddr: 0.0.0.0
*DHCPSocketTask: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP siaddr: 0.0.0.0,
giaddr: 60.60.60.2
*DHCPSocketTask: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP requested ip:
60.60.60.11
*DHCPSocketTask: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP sending REQUEST to
60.60.60.251 (len 358, port 1, vlan 60)
*DHCPSocketTask: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP selecting relay 2 -
control block settings:
    dhcpServer: 0.0.0.0, dhcpNetmask: 0.0.0.0,
    dhcpGateway: 0.0.0.0, dhcpRelay: 60.60.60.2 VLAN: 60
*DHCPSocketTask: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP selected relay 2 -
NONE (server address 0.0.0.0, local address 0.0.0.0, gateway 60.60.60.251, VLAN 60,
port 1)
*DHCPSocketTask: May 19 13:36:44.260: 00:17:7c:2f:b6:9a DHCP received op
BOOTREPLY
(2) (len 308, vlan 60, port 1, encap 0xec00)
*DHCPSocketTask: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP setting server
from ACK
(server 60.60.60.251, yiaddr 60.60.60.11)
*DHCPSocketTask: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP transmitting DHCP
ACK (5)
*DHCPSocketTask: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP op: BOOTREPLY,
htype:
Ethernet, hlen: 6, hops: 0
*DHCPSocketTask: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP xid: 0xad00ada3
(2902502819), secs: 0, flags: 0
*DHCPSocketTask: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP chaddr:
00:17:7c:2f:b6:9a
*DHCPSocketTask: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP ciaddr: 0.0.0.0,
yiaddr: 60.60.60.11
*DHCPSocketTask: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP siaddr: 0.0.0.0,
giaddr: 0.0.0.0
*DHCPSocketTask: May 19 13:36:44.261: 00:17:7c:2f:b6:9a DHCP server id:
192.168.200.1 rcvd server id: 60.60.60.251
*webauthRedirect: May 19 13:36:47.678: 0:17:7c:2f:b6:9a- received connection

*webauthRedirect: May 19 13:36:47.680: captive-bypass detection disabled, Not
checking for wispr in HTTP GET, client mac=0:17:7c:2f:b6:9a
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- Preparing redirect
URL according to configured Web-Auth type
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- Checking custom-web
```

```
config for WLAN ID:4
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- unable to get the
hostName
for virtual IP, using virtual IP =192.168.200.1
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- Global status is enabled,
checking on web-auth type
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- Web-auth type Internal,
no further redirection needed. Presenting default login page to user
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- http_response_msg_body1
is <HTML><HEAD><TITLE> Web Authentication Redirect</TITLE><META http-equiv=
"Cache-control" content="no-cache"><META http-equiv="Pragma" content="n
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- http_response_msg_body2
is "></HEAD></HTML>

*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- parser host is
www.facebook.com
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- parser path is /
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- added redirect=,
URL is now https://192.168.200.1/login.html?
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- str1 is now
https://192.168.200.1/login.html?redirect=www.facebook.com/
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- clen string is
Content-Length: 312

*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- Message to be sent is
HTTP/1.1 200 OK
Location: https://192.168.200.1/login.html?redirect=www.facebook.com/
Content-Type: text/html
Content-Length: 312

<HTML><HEAD
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- send data length=448
*webauthRedirect: May 19 13:36:47.680: 0:17:7c:2f:b6:9a- Web-auth type External,
but unable to get URL
*webauthRedirect: May 19 13:36:47.681: 0:17:7c:2f:b6:9a- received connection

*emWeb: May 19 13:36:48.731: SSL Connection created for MAC:0:17:7c:2f:b6:9a

*webauthRedirect: May 19 13:36:51.795: 0:17:7c:2f:b6:9a- received connection

*webauthRedirect: May 19 13:36:51.795: captive-bypass detection disabled, Not
checking for wispr in HTTP GET, client mac=0:17:7c:2f:b6:9a
*webauthRedirect: May 19 13:36:51.795: 0:17:7c:2f:b6:9a- Preparing redirect URL
according to configured Web-Auth type
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- Checking custom-web
config for WLAN ID:4
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- unable to get the
hostName
for virtual IP, using virtual IP =192.168.200.1
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- Global status is enabled,
checking on web-auth type
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- Web-auth type Internal,
no further redirection needed. Presenting default login page to user
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- http_response_msg_body1
is <HTML><HEAD><TITLE> Web Authentication Redirect</TITLE><META http-equiv=
"Cache-control" content="no-cache"><META http-equiv="Pragma" content="n
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- http_response_msg_body2
```

```
is "></HEAD></HTML>

*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- parser host is
www.facebook.com
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- parser path is
/favicon.ico
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- added redirect=, URL is
now https://192.168.200.1/login.html?
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- str1 is now
https://192.168.200.1/login.html?redirect=www.facebook.com/favicon.ico
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- clen string is
Content-Length: 323

*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- Message to be sent is
HTTP/1.1 200 OK
Location: https://192.168.200.1/login.html?redirect=www.facebook.com/favicon.ico
Content-Type: text/html
Content-Length: 323

*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- send data length=470
*webauthRedirect: May 19 13:36:51.796: 0:17:7c:2f:b6:9a- Web-auth type External,
but unable to get URL
*DHCP Socket Task: May 19 13:37:03.905: 00:17:7c:2f:b6:9a DHCP received op
BOOTREQUEST (1) (len 308,vlan 0, port 1, encap 0xec07)
*DHCP Socket Task: May 19 13:37:03.905: 00:17:7c:2f:b6:9a DHCP (encap type 0xec07)
mstype 3ff:ff:ff:ff:ff:ff
*DHCP Socket Task: May 19 13:37:03.905: 00:17:7c:2f:b6:9a DHCP selecting relay 1 -
control block settings:
    dhcpServer: 60.60.60.251, dhcpNetmask: 255.255.255.0,
    dhcpGateway: 60.60.60.251, dhcpRelay: 60.60.60.2 VLAN: 60

*emWeb: May 19 13:38:35.187:
ewaURLHook: Entering:url=/login.html, virtIp = 192.168.200.1, ssl_connection=1,
secureweb=1

*emWeb: May 19 13:38:35.199: WLC received client 0:17:7c:2f:b6:9a request for
Web-Auth page /login.html
*emWeb: May 19 13:38:35.199: WLC received client 0:17:7c:2f:b6:9a request for
Web-Auth page /login.html
*emWeb: May 19 13:38:47.215:
ewaURLHook: Entering:url=/login.html, virtIp = 192.168.200.1, ssl_connection=1,
secureweb=1

*ewmwebWebauth1: May 19 13:38:47.216: 00:17:7c:2f:b6:9a Username entry (surbg)
created for mobile, length = 5
*ewmwebWebauth1: May 19 13:38:47.216: 00:17:7c:2f:b6:9a Username entry (surbg)
created in mscb for mobile, length = 5
*ewmwebWebauth1: May 19 13:38:47.216: 00:17:7c:2f:b6:9a 60.60.60.11 WEBAUTH_REQD
(8) Change state to WEBAUTH_NOL3SEC (14) last state WEBAUTH_REQD (8)

*ewmwebWebauth1: May 19 13:38:47.216: 00:17:7c:2f:b6:9a apfMsRunStateInc
*ewmwebWebauth1: May 19 13:38:47.216: 00:17:7c:2f:b6:9a 60.60.60.11
WEBAUTH_NOL3SEC
```

(14) Change state to RUN (20) last state WEBAUTH_NOL3SEC (14)

```
*ewmwebWebauth1: May 19 13:38:47.216: 00:17:7c:2f:b6:9a Session Timeout is 0 -
not starting session timer for the mobile
*ewmwebWebauth1: May 19 13:38:47.216: 00:17:7c:2f:b6:9a 60.60.60.11 RUN (20)
Reached PLUMBFASPATH: from line 6605
*ewmwebWebauth1: May 19 13:38:47.216: 00:17:7c:2f:b6:9a 60.60.60.11 RUN (20)
Replacing Fast Path rule
  type = Airespace AP Client
  on AP 00:00:00:00:00:00, slot 0, interface = 1, QOS = 0
  IPv4 ACL ID = 255, IPv6 ACL ID =
```

Here is the client-side packet capture.

The client gets the IP address.

| | | | |
|-------------------|-----------------|------|--|
| Smart11n_2f:b6:9a | Broadcast | ARP | 42 who has 60.60.60.11? Tell 0.0.0.0 |
| Smart11n_2f:b6:9a | Broadcast | ARP | 42 who has 60.60.60.251? Tell 60.60.60.11 |
| Smart11n_2f:b6:9a | Broadcast | ARP | 42 Gratuitous ARP for 60.60.60.11 (Request) |
| 0.0.0.0 | 255.255.255.255 | DHCP | 348 DHCP Request - Transaction ID 0xd73b645b |
| 192.168.200.1 | 60.60.60.11 | DHCP | 346 DHCP ACK - Transaction ID 0xd73b645b |

The client opens a browser and types **www.facebook.com**.

| | | | |
|--------------|--------------|-----|---|
| 60.60.60.11 | 50.50.50.251 | DNS | 76 standard query 0x18bc A www.facebook.com |
| 50.50.50.251 | 60.60.60.11 | DNS | 92 Standard query response 0x18bc A 56.56.56.56 |
| 60.60.60.11 | 50.50.50.251 | DNS | 76 Standard query 0xab1b AAAA www.facebook.com |
| 60.60.60.11 | 50.50.50.251 | DNS | 76 Standard query 0xab1b AAAA www.facebook.com |
| 60.60.60.11 | 50.50.50.251 | DNS | 76 Standard query 0xab1b AAAA www.facebook.com |


```
Frame 508: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface 0
Ethernet II, Src: Smart11n_2f:b6:9a (00:17:7c:2f:b6:9a), Dst: Cisco_Fc:96:a8 (f0:f7:55:fc:96:a8)
Internet Protocol Version 4, Src: 60.60.60.11 (60.60.60.11), Dst: 50.50.50.251 (50.50.50.251)
User Datagram Protocol, Src Port: 62672 (62672), Dst Port: domain (53)
Domain Name System (query)
  Transaction ID: 0xab1b
  Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  Queries
    www.facebook.com: type AAAA, class IN
```

The WLC intercepts the client's first TCP packet and pushes its virtual IP address and the internal Webauth page.

| | | | |
|-------------|-------------|------|--|
| 56.56.56.56 | 60.60.60.11 | TCP | 54 http > 49720 [ACK] Seq=1 Ack=207 Win=6656 Len=0 |
| 56.56.56.56 | 60.60.60.11 | HTTP | 524 HTTP/1.1 200 OK (text/html) |
| 56.56.56.56 | 60.60.60.11 | TCP | 54 http > 49720 [ACK] Seq=1 Ack=207 Win=6656 Len=0 |


```
Frame 550: 524 bytes on wire (4192 bits), 524 bytes captured (4192 bits) on interface 0
Ethernet II, Src: Cisco_fc:96:a8 (f0:f7:55:fc:96:a8), Dst: Smart11n_2f:b6:9a (00:17:7c:2f:b6:9a)
Internet Protocol Version 4, Src: 56.56.56.56 (56.56.56.56), Dst: 60.60.60.11 (60.60.60.11)
Transmission Control Protocol, Src Port: http (80), Dst Port: 49720 (49720), Seq: 1, Ack: 207, Len: 470
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Location: https://192.168.200.1/login.html?redirect=www.facebook.com/favicon.ico\r\n
  Content-Type: text/html\r\n
  Content-Length: 323\r\n
  \r\n
  [HTTP response 1/1]
```

After successful web authentication, the rest of the work flow completes.

| | | | |
|---------------|---------------|-------|---|
| 60.60.60.11 | 50.50.50.251 | DNS | 86 Standard query 0x64dd A fe9cv11st.1e.microsoft.com |
| 60.60.60.11 | 192.168.200.1 | TCP | 66 49724 > https [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1 |
| 192.168.200.1 | 60.60.60.11 | TCP | 66 https > 49724 [SYN, ACK] Seq=0 Ack=1 win=5560 Len=0 MSS=1390 SACK_PERM=1 WS=64 |
| 60.60.60.11 | 192.168.200.1 | TCP | 54 49724 > https [ACK] Seq=1 Ack=1 win=16680 Len=0 |
| 60.60.60.11 | 192.168.200.1 | TLSv1 | 190 Client Hello |
| 192.168.200.1 | 60.60.60.11 | TCP | 54 https > 49724 [ACK] Seq=1 Ack=137 win=6656 Len=0 |
| 192.168.200.1 | 60.60.60.11 | TLSv1 | 192 Server Hello, Change Cipher Spec, Encrypted Handshake Message |
| 60.60.60.11 | 192.168.200.1 | TLSv1 | 113 Change cipher spec, encrypted Handshake Message |
| 60.60.60.11 | 50.50.50.251 | DNS | 83 Standard query 0xb814 A ctld1.windowsupdate.com |
| 192.168.200.1 | 60.60.60.11 | TCP | 54 https > 49724 [ACK] Seq=139 Ack=196 win=6656 Len=0 |



powered by **Lithium**