# Configure External web authentication with Converged Access (5760/3650/3850)

## Contents

## Introduction

This document defines how to configure external web auth with Converged Access controllers. The guest portal page and credentials authentication are both on Identity Services Engine (ISE) in this example.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

1. Cisco converged access controllers.

2. Web authentication

3. Cisco ISE

### Components Used

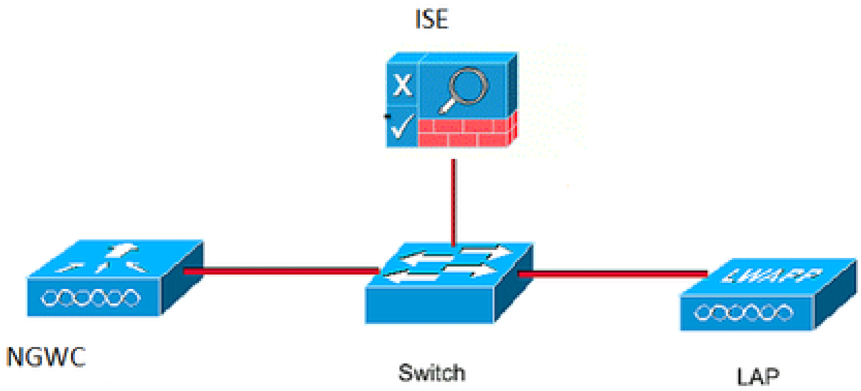
The information in this document is based on these software and hardware versions:

1. Cisco 5760 controller (NGWC on the below diagram), 03.06.05E

2. ISE 2.2

## Configure

### Network Diagram



## CLI Configuration

Radius configuration on controller

step 1 : Define external radius server

```
radius server ISE.161
address ipv4 10.48.39.161 auth-port 1812 acct-port 1813
timeout 10
retransmit 5
key Cisco123
```

step 2:. Define AAA radius group and specify the radius server to be used

```
aaa group server radius ISE-Group
server name ISE.161
deadtime 10
```

step 3. Define method list pointing to the radius group and map it under the WLAN.

```
aaa authentication login webauth group ISE-Group
```

Parameter Map configuration

step 4. Configure global parameter map with virtual ip address which is required for external and internal webauth. Logout button uses virtual ip. Its always a good practice to configure a non-routable virtual ip.

```
parameter-map type webauth global
type webauth
virtual-ip ipv4 1.1.1.1
```

step 5 : Configure a named parameter map.It will act like a type of webauth method. This will be called under the WLAN config.

```
parameter-map type webauth web
type webauth
redirect for-login https://10.48.39.161:8443/portal/PortalSetup.action?portal=0c712cd0-6d90-11e5-978e-005056bf2f0a
redirect portal ipv4 10.48.39.161
```

### Pre authentication ACL. This will also be called under the WLAN.

### step 6: Configure Preauth_ACL which allows access to ISE, DHCP and DNS before authentication is over

```
ip access-list extended Preauth_ACL
permit ip any host 10.48.39.161
permit ip host 10.48.39.161 any
permit udp any eq bootps any
permit udp any any eq bootpc
permit udp any eq bootpc any
permit udp any eq domain any
permit udp any any eq domain
```

### WLAN config

### step 7 : configure the WLAN

```
wlan ext-webauth 7 ext-webauth
client vlan vlan232
ip access-group web Preauth_ACL
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
security web-auth
security web-auth authentication-list webauth
security web-auth parameter-map web
session-timeout 1800
no shutdown
```

### step 8 : Turn on http server.

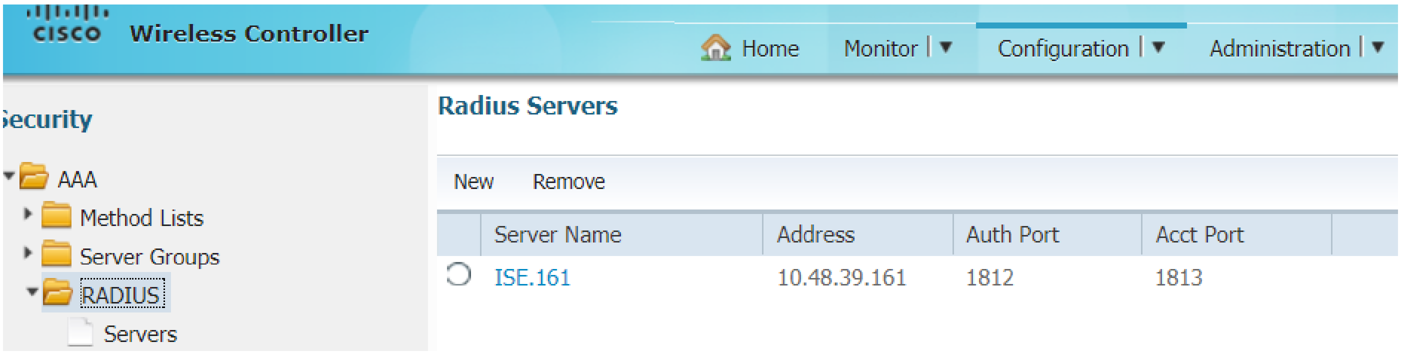
```
ip http server

ip http secure-server (for secure web-auth, use 'no' to disable secure web)
```

**GUI configuration**

We are following here the same steps as above. The screenshots are just provided for cross-reference.

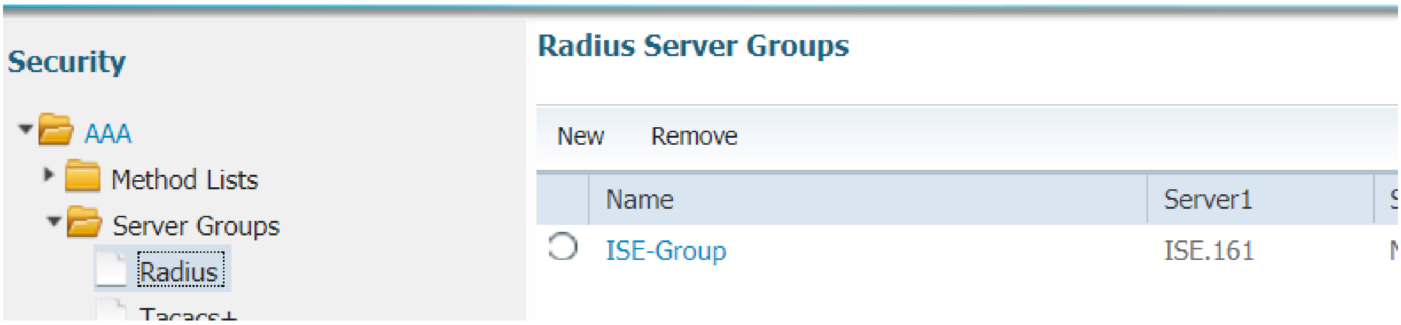
### step 1 : Define an external radius server



Radius Servers

| Server Name | Address | Auth Port | Acct Port |
|---|---|---|---|
| ISE.161 | 10.48.39.161 | 1812 | 1813 |

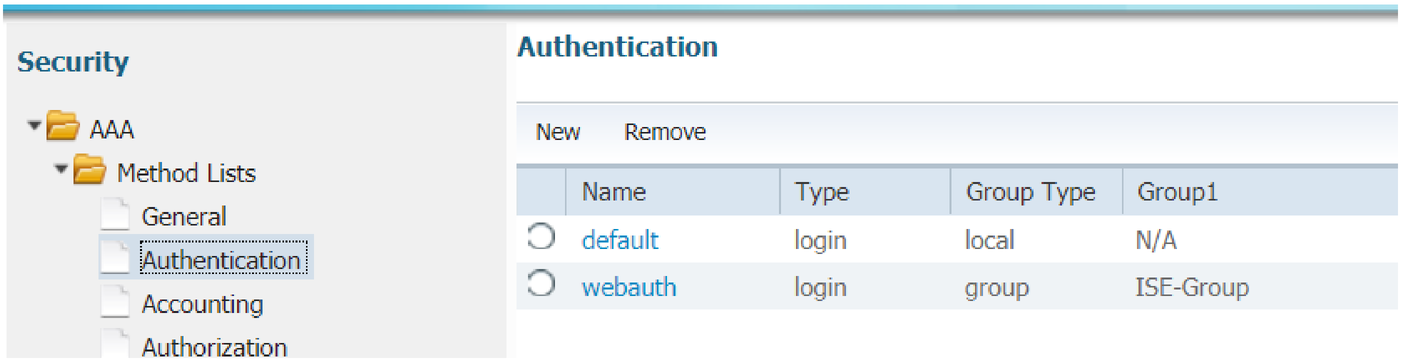
### step 2:. Define AAA radius group and specify the radius server to be used



Radius Server Groups

| | Name | Server1 | S |
|---|---|---|---|
| ○ | ISE-Group | ISE.161 | N |

step 3. Define method list pointing to the radius group and map it under the WLAN.



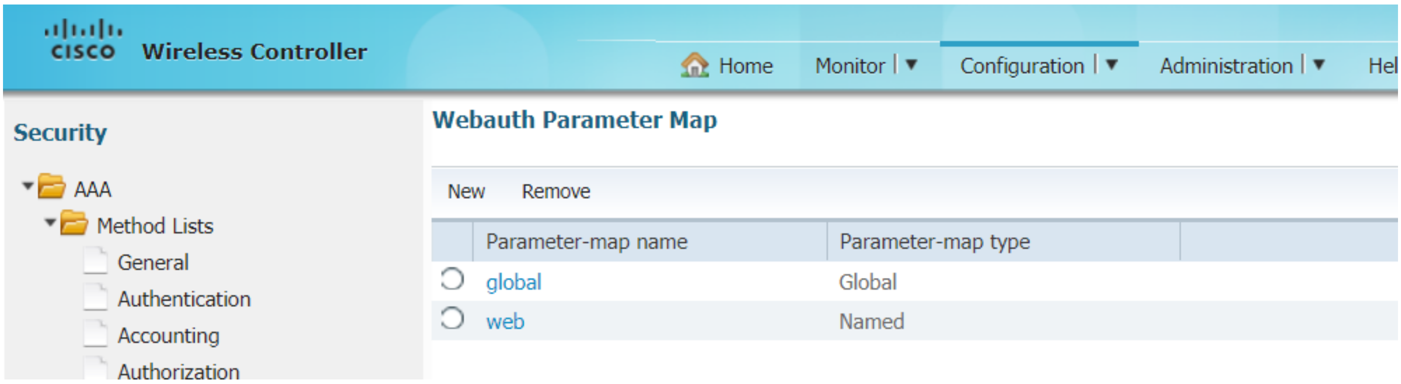
Authentication

| | Name | Type | Group Type | Group1 |
|---|---|---|---|---|
| ○ | default | login | local | N/A |
| ○ | webauth | login | group | ISE-Group |

Parameter Map configuration

step 4. Configure global parameter map with virtual ip address which is required for external and internal webauth. Logout button uses virtual ip. Its always a good practice to configure a non-routable virtual ip.

step 5 : Configure a named parameter map.It will act like a type of webauth method. This will be called under the WLAN config.

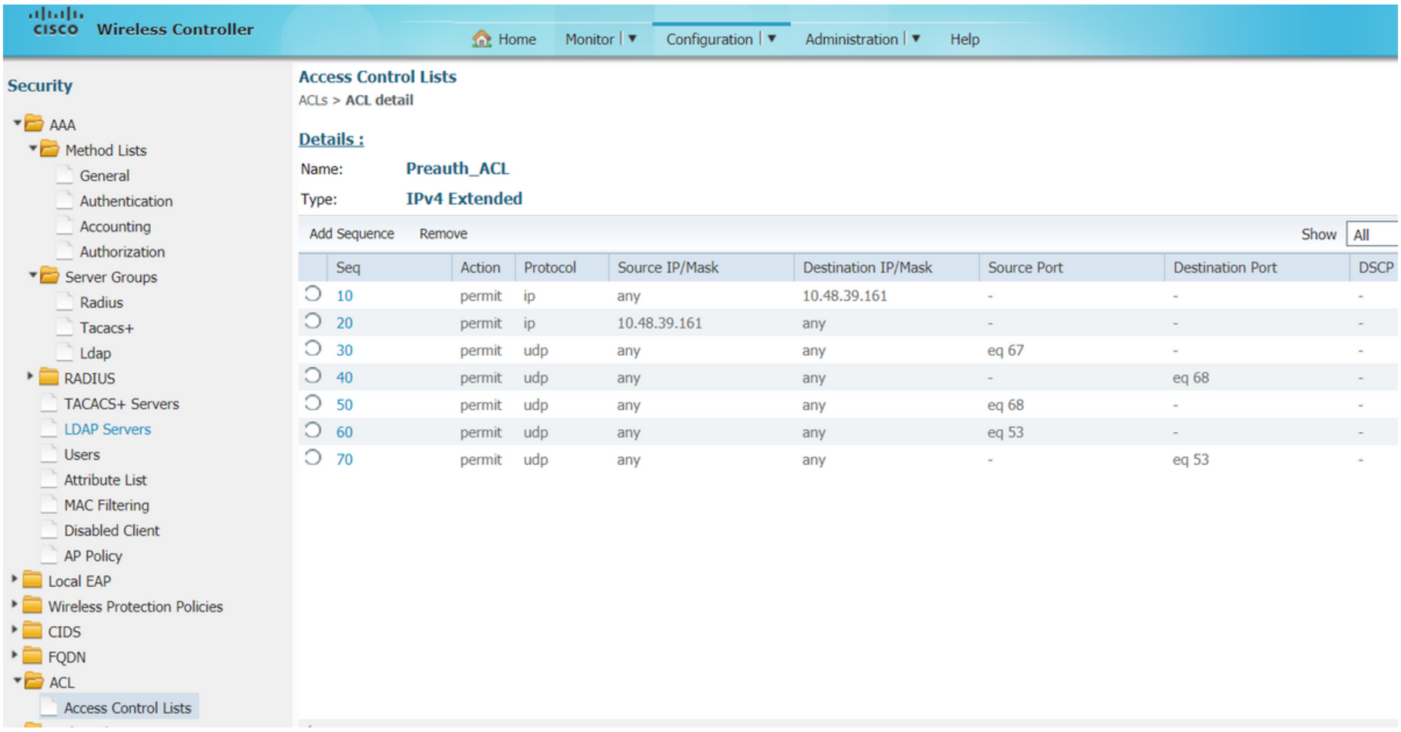


Webauth Parameter Map

| | Parameter-map name | Parameter-map type |
|---|---|---|
| ○ | global | Global |
| ○ | web | Named |

Pre authentication ACL. This will also be called under the WLAN.

step 6: Configure Preauth_ACL which allows access to ISE, DHCP and DNS before authentication is over



Access Control Lists

ACLs > ACL detail

Details :

Name: Preauth_ACL

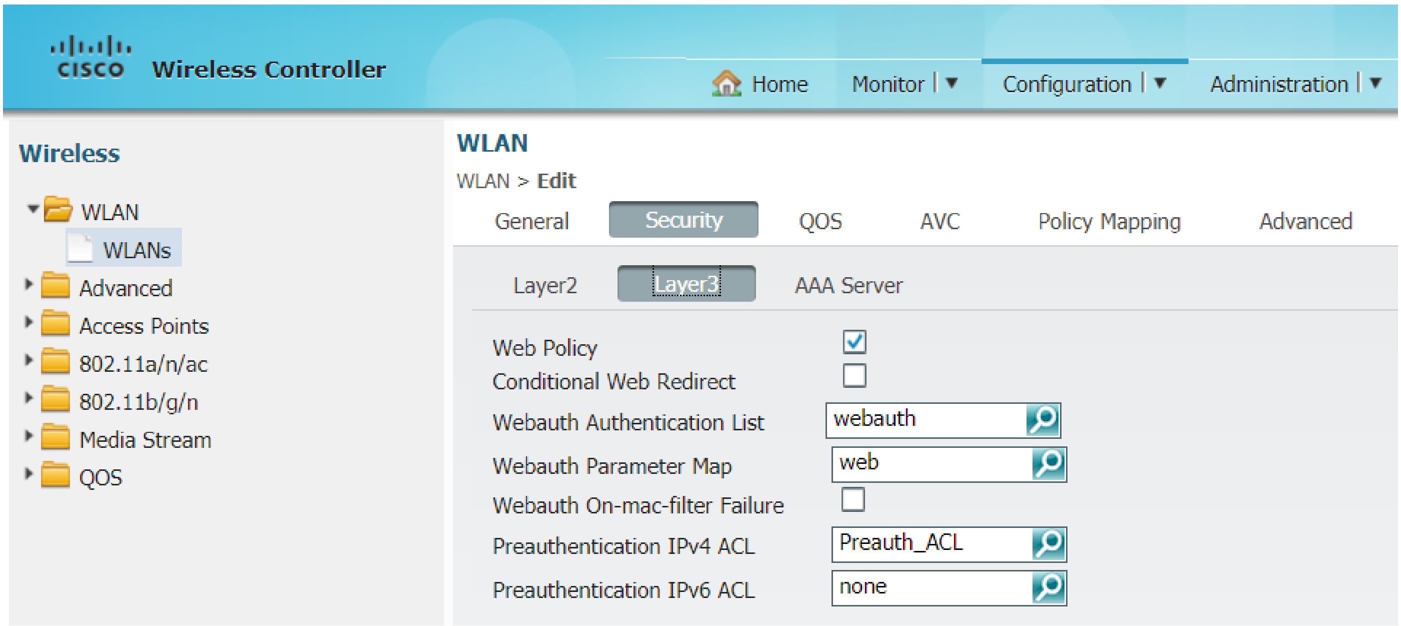
Type: IPv4 Extended

| Seq | Action | Protocol | Source IP/Mask | Destination IP/Mask | Source Port | Destination Port | DSCP |
|---|---|---|---|---|---|---|---|
| 10 | permit | ip | any | 10.48.39.161 | - | - | - |
| 20 | permit | ip | 10.48.39.161 | any | - | - | - |
| 30 | permit | udp | any | any | eq 67 | - | - |
| 40 | permit | udp | any | any | - | eq 68 | - |
| 50 | permit | udp | any | any | eq 68 | - | - |
| 60 | permit | udp | any | any | eq 53 | - | - |
| 70 | permit | udp | any | any | - | eq 53 | - |

| | | | | | |
|---|---|---|---|---|---|
| ○ ext-webauth | 7 | ext-webauth | 232 | Enabled | Web-Auth |

WLAN config

step 7 : configure the WLAN



WLAN

WLAN > Edit

Web Policy ☑

Conditional Web Redirect □

Webauth Authentication List: webauth

Webauth Parameter Map: web

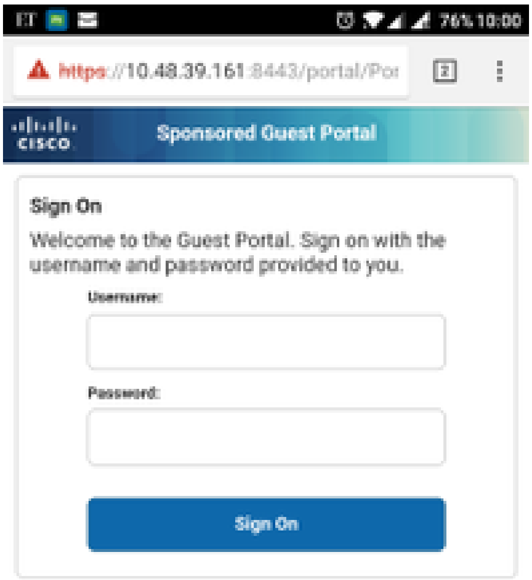
Webauth On-mac-filter Failure □

Preauthentication IPv4 ACL: Preauth_ACL

Preauthentication IPv6 ACL: none

# Verify

Connect a client and make sure that if you open a browser, the client will be redirected to your login portal page. The below screenshot illustrates the ISE guest portal page.



https://10.48.39.161:8443/portal/Por

Sponsored Guest Portal

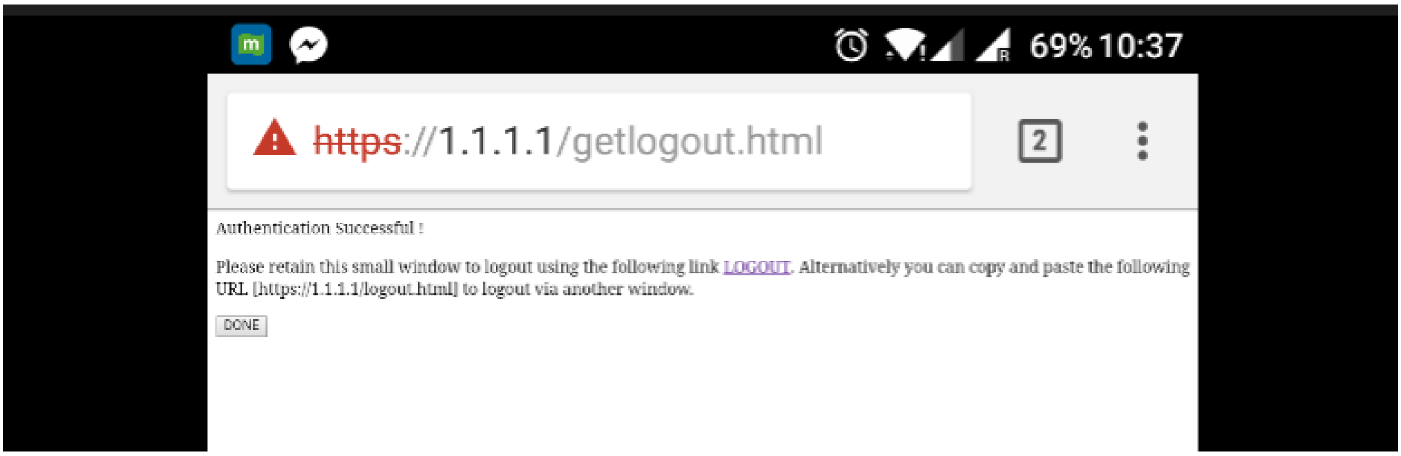
Sign On

Welcome to the Guest Portal. Sign on with the username and password provided to you.

Username:

Password:

Once proper credentials are submitted, the success page will be shown :

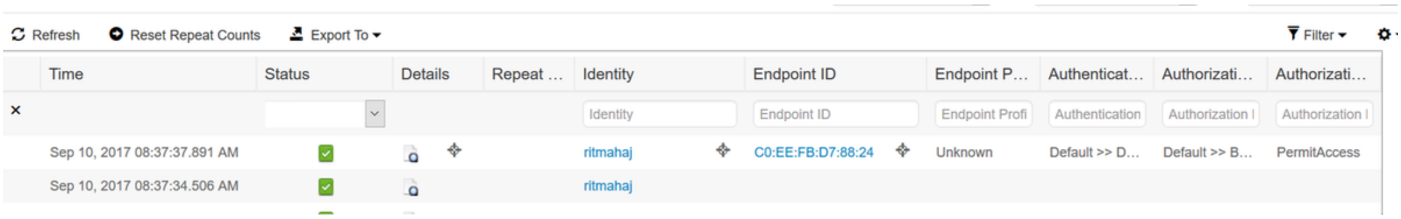


https://1.1.1.1/getlogout.html

Authentication Successful !

Please retain this small window to logout using the following link LOGOUT. Alternatively you can copy and paste the following URL [https://1.1.1.1/logout.html] to logout via another window.

The ISE server will report two authentication : one on the guest page itself (the bottom line with only the username) and a second authentication once the WLC provides the same username/password through radius authentication (only this authentication will make the client move to the success phase). If the radius authentication (with mac address and WLC details as NAS) does not occur, the radius configuration is to be verified.



| | Time | Status | Details | Repeat ... | Identity | Endpoint ID | Endpoint P... | Authenticat... | Authorizati... | Authorizati... |
|---|---|---|---|---|---|---|---|---|---|---|
| × | | | | | Identity | Endpoint ID | Endpoint Profi | Authentication | Authorization I | Authorization I |
| | Sep 10, 2017 08:37:37.891 AM | ✓ | | | ritmahaj | C0:EE:FB:D7:88:24 | Unknown | Default >> D... | Default >> B... | PermitAccess |
| | Sep 10, 2017 08:37:34.506 AM | ✓ | | | ritmahaj | | | | | |