

[Register](#)[Login](#)[Cisco Support Community](#) / [Wireless - Mobility](#) / [Wireless - Mobility Documents](#) / [Central Web Authentication \(CWA\) for gu...](#)[Options](#)[All community](#)

Central Web Authentication (CWA) for guests with ISE

- [Introduction](#)
- [Setup Used](#)
- [WLC Configuration](#)

Introduction

There are multiple ways of doing Web Authentication on the WLC. The first one is Local Web Authentication. In this case, the WLC will redirect the HTTP Traffic to an internal or external server where the user will be prompted to authenticate. The WLC will then fetch this credentials (sent back via HTTP GET Request in case of external server), and make a radius authentication. In case of guest user, we need an external server (like ISE or NGS), as the portal can provide some feature like Device Registering, Self Provisioning, ...

The flow would be the following:

- User associate to the Web Auth SSID
- User starts its browser
- The WLC Redirect to the guest portal (ISE/NGS)
- The user authenticate on the portal
- The Guest Portal redirect back to the WLC with the credentials entered
- The WLC Authenticate the guest user via Radius
- The WLC Redirects back to the original URL.

That makes a lot of redirection. The new approach is to use Central Web Authentication. This works with ISE > 1.1 and WLC > 7.2.

The flow in this case would be:

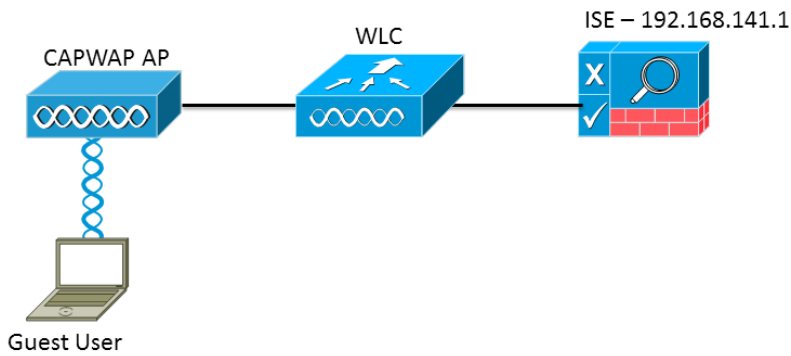
- User associate to the Web Auth SSID
- User starts its browser
- The WLC Redirect to the guest portal (ISE)

-The user authenticates on the portal

-The ISE sends a Radius Change Of Authorization (CoA - UDP Port 3799) to indicate to the controller that the user is valid, and eventually push radius attributes (ACL for example).

-The User is prompted to retry his original URL

Setup Used



The versions used are:

ISE: 1.1.1.268

WLC: 7.2.110.0

WLC Configuration

The WLC Configuration is pretty straight-forward. We use a "trick" (same as on Switches) to get the dynamic authentication URL from the ISE (as it is using CoA, a session needs to be created, and the session ID is part of the URL). We need to configure the SSID to use MAC Filtering. We will configure the ISE to return an access-accept even if the mac address is not found, so that it will send the redirection URL for all users.

In addition to this, we need to enable Radius NAC and AAA Override. The Radius NAC allows the ISE to send a CoA Request to indicate that the user is now authenticated and can access the network. It is also used for Posture Assessment, in which case the ISE would change the user profile based on posture result.

We need also to be sure that the radius server has RFC 3576 (CoA) enabled, which is by default.

CISCO MONITOR WLANs CONTROLLER WIRELESS **SECURITY** MANAGEMENT COMMANDS HELP FEEDBACK

Security

- AAA
 - General
 - RADIUS
 - Authentication**
 - Accounting
 - Fallback
 - TACACS+
 - LDAP
 - Local Net Users
 - MAC Filtering
 - Disabled Clients
 - User Login Policies
 - AP Policies
 - Password Policies
- Local EAP
- Priority Order
- Certificate
- Access Control Lists

RADIUS Authentication Servers > New

Server Index (Priority) 15

Server IP Address 192.168.141.1

Shared Secret Format ASCII

Shared Secret *****

Confirm Shared Secret *****

Key Wrap (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

Port Number 1812

Server Status Enabled

Support for RFC 3576 Enabled

Server Timeout 2 seconds

Network User Enable

Management Enable

IPSec Enable

WLANs > New

Type WLAN

Profile Name ISE_CWA

SSID ISE_CWA

ID 2

WLANs > Edit 'ISE_CWA'

General Security QoS Advanced

Layer 2 Layer 3 AAA Servers

Layer 2 Security None

MAC Filtering

Fast Transition

Fast Transition

WLANs > Edit 'ISE_CWA'

General Security QoS Advanced

Layer 2 Layer 3 AAA Servers

Layer 3 Security None

Web Policy

WLANs > Edit 'ISE_CWA'

General Security QoS Advanced

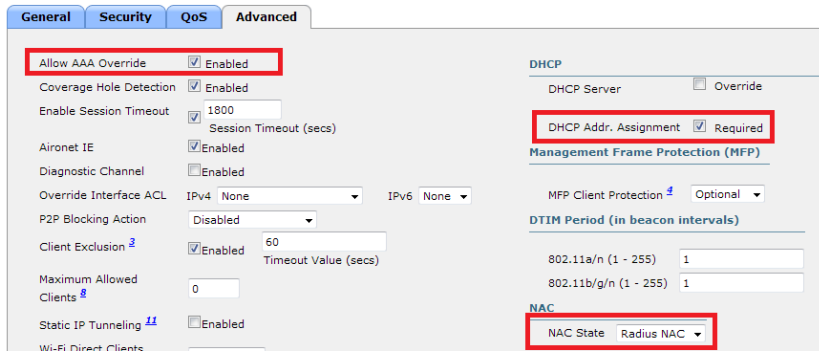
Layer 2 Layer 3 AAA Servers

Select AAA servers below to override use of default servers on this WLAN

Radius Servers

Radius Server Overwrite interface Enabled

	Authentication Servers	Accounting Servers
Server 1	<input checked="" type="checkbox"/> Enabled IP:192.168.141.1, Port:1812	<input checked="" type="checkbox"/> Enabled IP:192.168.141.1, Port:1813
Server 2	None	None
Server 3	None	None



The final step is to create a Redirect-ACL. This ACL will be referenced in the access-accept of the ISE and will define what traffic should be redirected (denied by ACL), and what traffic shouldn't (permitted by the ACL). Basically, we need to permit DNS and traffic to/from ISE.

General

Access List Name: cwa_redirect
Deny Counters: 3

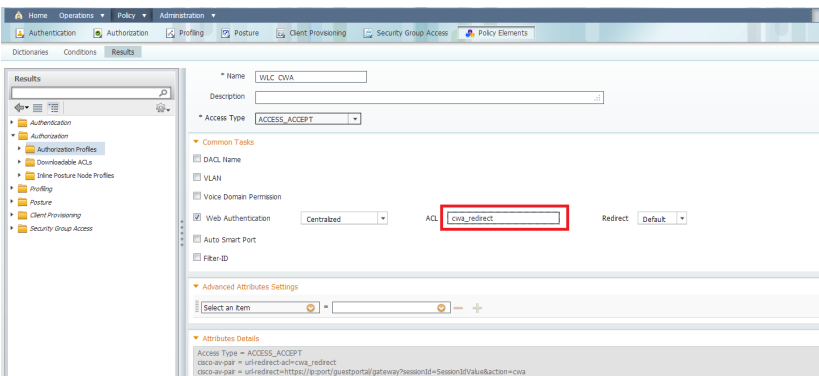
Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	192.168.141.1 / 255.255.255.255	Any	Any	Any	Any	Any	45
2	Permit	192.168.141.1 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	44
3	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Any	2
4	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Any	0

Everything is now complete on the WLC. Let's configure the ISE

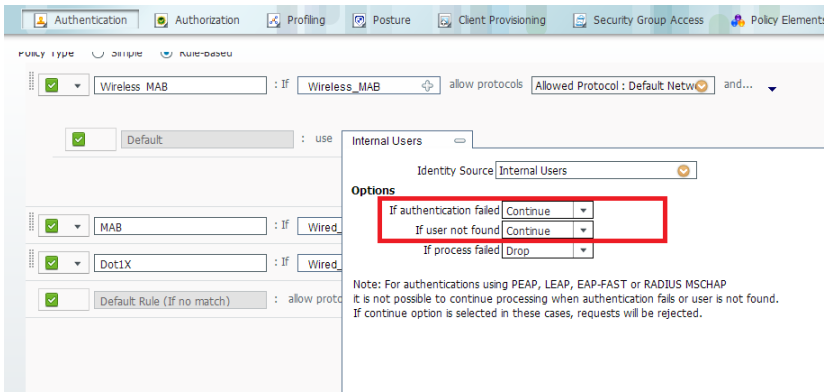
ISE Configuration

On the ISE, we need to make authorization profile, and then we can configure authentication and authorization. The WLC should already be configured as a network device.

In the authorization profile, we need to put the name of the ACL that has been created earlier on the WLC:



Now, we need to make sure the ISE is accepting all the MAC Authentication from the WLC and return the profile:



We can use the Built-In Wireless MAB condition, which match :

- Radius:Service-Type : Call Check (Mac Authorization use Call Check on WLC and Switches).
- Radius:NAS-Port-Type: Wireless - IEEE 802.11

Now, we need to configure the authorization. One important thing to understand is that there will be 2 authentication / authorization:

- One when the user associate to the SSID, and when we need to return the cwa profile
- Another when the user authenticate on the web portal. This one will match the default rule (internal users), in my situation (you can configure it as you want). What is important is that the authorization part doesn't match the CWA Profile again, otherwise we would have a redirection loop. We can use the attribute "Network Access:UseCase Equals Guest Flow" to match this second authentication.

The result looks like this:

Authorization Policy
Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

First Matched Rule Applies

Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	Guest Portal Auth	if Network Access:UseCase EQUALS Guest Flow	then PermitAccess
<input checked="" type="checkbox"/>	Guest Redirection	if Wireless_MAB	then WLC_CWA

Test

Once we associate to the SSID, we can see the auth in the ISE page:

Live Authentications

Add or Remove Columns Refresh Refresh Every 1 minute Show Latest 10

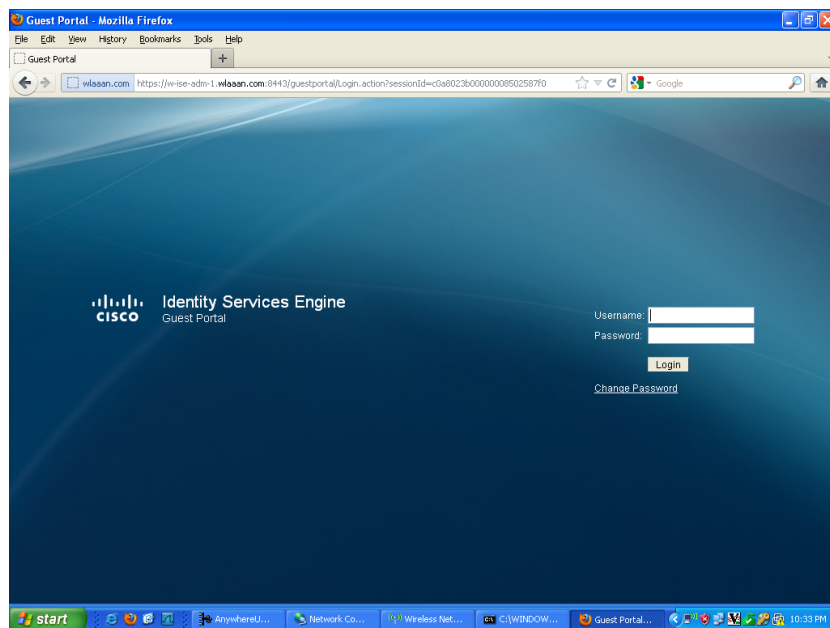
Time	Status	Details	Identity	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles	Identity Group	Posture Status	Event
Aug 11, 12 11:33:57.237 AM	<input checked="" type="checkbox"/>		ED-46-9A:18:2A:08	ED-46-9A:18:2A:08		WLC5505-3		WLC_CWA	Profiled	Pending	Authentication...

And if we check the client details in the WLC, we can see the Redirection URL and ACL are applied:

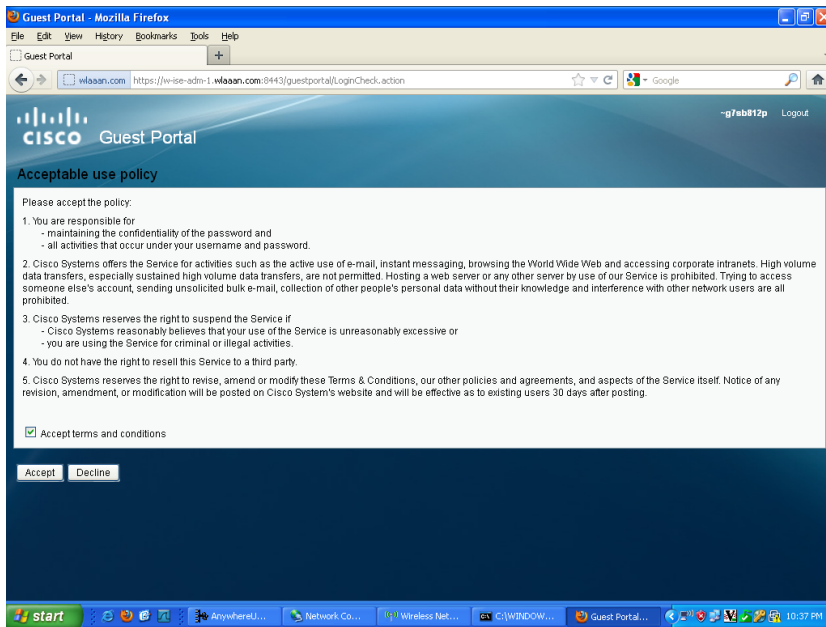
Security Information

Security Policy Completed	No
Policy Type	N/A
Encryption Cipher	None
EAP Type	N/A
SNMP NAC State	Access
Radius NAC State	POSTURE_REQD
CTS Security Group Tag	Not Applicable
<hr/>	
AAA Override ACL Name	cwa_redirect
AAA Override ACL Applied Status	Yes
Redirect URL	https://w-ise-adm-1.wlaaan.com:8443/guestportal/gate
IPv4 ACL Name	none
IPv4 ACL Applied Status	Unavailable
IPv6 ACL Name	none
IPv6 ACL Applied Status	Unavailable

Now, when we open any address on the client, we are redirected to our ISE (be careful to have DNS setup correctly).



Then the user needs to accept the policies, and then it will be granted access to the network.




If we look back at my ISE, we can now see the authentication, the change of authorization, and that the profile applied is permitAccess:

Live Authentications

Time	Status	Details	Identity	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profile	Identity Group	Posture Status	Event
Aug 11, 12 12:16:01.970 PM	Success		--g74812p	E0469A:1B2A:0B		WLC585-3		PermitAccess	Guest_Profile:Wor...	NotApplicable	Dynamic Authorization succeeded
Aug 11, 12 12:16:01.964 PM	Success					WLC585-3					Dynamic Authorization succeeded
Aug 11, 12 12:16:01.959 PM	Success		--g74812p	E0469A:1B2A:0B		WLC585-3			Guest		Guest Authentication Passed
Aug 11, 12 12:16:01.982 PM	Success		E0469A:1B2A:0B	E0469A:1B2A:0B		WLC585-3		WLC_OWA	Profiled	Pending	Authentication succeeded

On the controller, the Policy Manager State and Radius NAC State should change from "POSTURE_REQD" to "RUN"

Version history

Revision #: 2 of 2
Last update: 08-28-2017 01:38 AM
Updated by: Bastien Migette 

[View article history](#)

Labels (1)

Security and Network Ma...

Contributors

 Bastien Migette

Everyone's tags (8)

 0 Helpful

Share

COMMENTS



Tarik Admani  Green

08-11-2012 10:24

Bastien,

I have configured ISE many times and was curious as to how you were able to validate the following statement:

"The WLC Redirects back to the original URL."

My experiences when using CWA that you always get redirected to the page that shows the exit button and to retry the original url request.

Thanks,

Tarik Admani



Bastien Migette  Cisco Employee

08-12-2012 01:10

Hello Tarik, You are right, with CWA, the ISE shows a message indicating the user he can retry his original URL. This is a current limitation, as the ISE doesn't know the original URL.

What you can do is to create a custom portal with HTML Files and modify the success page to redirect to an arbitrary web page.



Peter Nugent  Cisco Employee

08-20-2012 03:35

Just getting started with ISE.

This looks ok but could use a little more detail if I could ask around creating the Authorization policy Guest redirect.

However its only valid for code 7.2. It seems a lot more complicated in 7.0.

Any chance you could do this for 802.1x PEAP? Also with code 7.0. as I am really struggling getting my head around the interface and policy creations.



Bastien Migette Cisco Employee

08-20-2012 03:45

Hello Peter,

Welcome to the ISE world... It can be hard to do what we want at first glance due to numerous features, but after some time you'll get used to it.

Concerning the guest redirect, here's basically how it works:

-The Guest user associate to the WLC

-The WLC send a MAB Request to ISE

-the ISE match the first authorization rules, and send the redirect parameters (acl and URL)

-The WLC will redirect the GUEST to the ISE

-Once the guest is authenticated, the ISE will make a second authorization (that we call Radius Change of Authorization - CoA, which require 7.2 Code). In this second authorization, we need to return a profile so the guest is permitted access to the network. We can use usecase: guestflow to easily match this second authorization.

For PEAP, you may have a look at this doc, there's an example of 802.1x:

http://www.cisco.com/en/US/products/ps10315/products_tech_note09186a0080bba10d.shtml

I hope this is clear.



Peter Nugent Cisco Employee

08-20-2012 05:02

It is becoming clear! Just the ability to run 7.2 is an issue for me at the present time. Also there are alot of features as you say.



Bastien Migette Cisco Employee

08-20-2012 05:04

Good,

You can still use Local Web Auth (LWA) with WLC 7.0. There's an example in the BYOD Guide (link above) as well.



edondurguti New Member

08-23-2012 01:18

I have a default deny rule in the authorization and if users come in first time they are always denied, they have to re-connect manually and once that's done they are okay forever.

CoA is globally enabled for ReAuth.

I've tried many things but never got it working and kinda found a workaround with isolated vlan with ip helpers :s



Bastien Migette Cisco Employee

08-23-2012 01:24

Hello Edondurguti,

It's hard to give you an answer without knowing the details of your setup. Maybe you should try to open a separate post on this forum, or open a TAC Case if you have a support contract.

Regards,
Bastien



Dominic Stalder New Member

08-31-2012 03:17

Hi Bastien

thanks a lot for this great post!

I have a question about CWA design in association with an anchor / foreigner installation. We would like to use CWA in this scenario:

- The ISE is located in the internal server subnet
- The foreign WLC is located in the same server subnet
- The anchor WLC ist located in the DMZ subnet

Between the server subnet and the DMZ, the traffic is blocked (except for guest mobility and so on --> no ISE traffic allowed).

No our problem:

1. The client connects to the guest SSID and does need to do a MAB (Layer 2), this works fine because the foreign WLC has connection to the ISE
2. The client gets an IP address via DHCP from the anchor WLC (Layer 3), so the client is now located in a quarantine VLAN behind the firewall and does not have any connection to the ISE, BUT the client should be redirected to the guest portal of the ISE

Now my question, is CWA the right way or should we better use LWA for anchor / foreign scenarios. And if CWA is good, what is a good design to implement it in these scenarios?

Thanks a lot in advance and best regards

Dominic



Bastien Migette Cisco Employee

09-03-2012 01:53

Hello Dominic,

When you have anchor/foreign, the web auth traffic always go to the anchor, so with CWA, the traffic from the anchor to the ISE will need to be permitted.

Now, both LWA and CWA works fine, but CWA is the new way to do things, and I personally think it's a bit more cleaner, regarding the process flow than LWA...

If this is not an option to open connectivity to the ISE from behind the firewall, then I guess you will have to go for LWA.

Regards,

Bastien



Dominic Stalder New Member

09-03-2012 01:58

Hi Bastien

thanks a lot for your feedback, I think it would be nice to have CWA, but if the communication should not be possible, then LWA is the way to go.

Thanks and best regards

Dominic



Dominic Stalder New Member

09-19-2012 11:29

Hi Bastien

one more question about the design above. You use the "Mac Filtering" to have a redirect to the guest portal of the ISE, this makes it necessary, that Layer 2 authentication traffic flows from the foreign controller to the ISE. In the "Cisco Bring Your Own Device (BYOD) Smart Solution Design Guide" I can see, that this is solved via the "External Web Auth URL" under Security > Web Auth > Web Login Page:

The screenshot shows the Cisco ISE configuration interface for the 'Web Login Page'. The configuration is as follows:

- Web Authentication Type: External (Redirect to external server)
- Redirect URL after login: http://me-v6serv-1
- External Webauth URL: https://10.17.1.88:8443/guestportal/portals/SponsoredGuests/portal.jsp

A red box highlights the External Webauth URL field, with a callout text stating: "Web Auth Login Redirected to the URL of the Guest Portal which has been Configured within the Cisco ISE Server".

So we don't have any traffic from the foreign controller to the ISE. Is that correct?

Best regards

Dominic



Bastien Migette Cisco Employee

09-21-2012 12:11

Hello Dominic,

When you have Anchor/Foreign, basically all L2 Authentication is made on the foreign, but all L3 Traffic (including webauth) is going through the anchor, so whether you use CWA or External Server, the traffic will need to be allowed from anchor to ISE. If you don't want this, then you can use Local Web Auth, and use the ISE as radius server, but still the foreign will need to be allowed to contact the ISE via Radius.

Hope this is clear.



Dominic Stalder New Member

09-21-2012 01:08

Hi Bastien

thanks, that's clear and that is what I want: ONLY allow traffic from the anchor to the ISE, but NOT from the foreign as it would go with L2 MAC authentication bypass.

Short summary:

- CWA with MAB as you mentioned above --> L2 from foreign AND L3 from anchor
- CWA with external server -> ONLY L3 from anchor

Best regards and have a nice weekend

Dominic



guillerm New Member

02-19-2013 10:37

Hello,

I have set up a Guest Portal with WLC 5508 7.4 and ISE 1.1.1 ;

everything is OK, except one thing :

the Guest VLAN, associated to the Guest SSID is, actually, a DMZ behind my customer firewall and the DHCP parameters provided to the wireless Guest equipment connected on this VLAN include the public ISP DNS servers addresses, not the customer internal DNS servers addresses;

this seems OK since the idea of this Guest SSID is to give a pure Internet access to the Guests, and no connection at all towards the customer internal servers;

the problem is that, when the wireless guest receives the redirect URL from ISE (URL to access the ISE Guest Portal), this URL is based on the ISE DNS name, not on its IP address; so, the PC can't resolve this internal DNS name by using the ISP DNS servers addresses provided by the DHCP server, and, so, it can't access the Guest Portal at all ;

Apart from changing those DNS values in the DHCP server (the customer does not accept this solution), how could we solve this problem ?

I have tried to code, in the CWA Authorization profile, the equivalent URL redirect via the CISCO av-pair as follows :

```
cisco-av-pair=url-redirect=https://192.168.1.10:8443/guestportal/gateway?sessionId=sessionIdValue&action=cwa,
```

but, it does not work, since the sessionIdValue is not replaced by its real value when sent to the wireless client

any comment welcomed



jwhiteak Cisco Employee

04-02-2013 07:05

Do we have a sample setup for the IOS controllers running IOS-XE 3.2.0SE release with ISE ?



aporcario01 New Member

04-18-2013 06:21

Hi,

I'm trying to configure a certificate in order to gain access to the Internet for a guest wlan, the problem is that an error message says that the certificate isn't trusted and click next to continue... i'm using a certificate from the www.digicert.com.

Could you give me a tip or document explain how to configure a certificate on Ise.

I have a WLC that redirect to a web page login on Cisco ISE.

Tks for the help

Adriano Porcaro



Bastien Migette  Cisco Employee

04-24-2013 01:49

Hello Adriano,

You can find help to install the certificates on ISE here:

http://www.cisco.com/en/US/docs/security/ise/1.1.1/user_guide/ise_man_cert.html

Basically, you need to have the digicert in the Server Certificates session, and enabled for HTTP.

Regards,

Bastien.



Christos Stefanekou  Bronze

06-07-2013 07:48

Hello,

Has anyone tested web authentication for wireless guest access using WS 3850?

Regards,

Chris



Bastien Migette  Cisco Employee

06-07-2013 08:26

Hello Christos,

From my head I believe the current NGWC image have no support or no full support for CoA, therefore you should be able get redirected to the ISE, but the CoA wouldn't work. This will be fixed in the next release.



Christos Stefanekou  Bronze

06-07-2013 08:37

Hi Bastien,

Thanks for your response.

I don't need CoA for wireless guest access. I managed to setup ISE + WLC 2504 for web authentication but the same scenario using ISE + SW 3850 failed.

I used as reference the following guide:

http://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/security/configuration_guide/b_sec_1501_3850_cg_chapter_010010.html

It's not very clear how web authentication works on 3850 wlan.

Best regards,

Chris



jerry.larson New Member

07-31-2013 12:07

If I do not see Wireless_Mab under conditions for the Authorization Policy, how do I add it?

thanks,



Bastien Migette Cisco Employee

07-31-2013 11:08

Hi Jerry,

It should be by default in later ISE version (starting 1.1.2 I think).

Otherwise you can match service-type = call-check (10) and nas-port-type=802.11



Tiago Andrade de Paula New Member

08-27-2013 05:25

Guys,

I have some problems with this design.

First: My WLC is 7.0.240 IOS version. **obs:** I can't search 7.2 WLC IOS to download int cisco website.

My ISE version is 1.2.

Wired authentication is ok for 802.1x with Digital certificate and Guest wired too, with redirect page + acl on switch port.

The problem is WIFI:

802.1x wifi ok

BUT Guest redirect isn't Working.

In the Client logs i can't see Url Redirect - none and I see just the ACL.

In the SSID Guest - Radius Nac State I cant put to enable cuz the WLC show the message : "

radius nac is available only for wlan with 802.1x/WPA/WPA2 Layer 2 security"

My WebAuth Athorization profile is correct. My access-list in WLC permit DNS and all ip to ISE.
Somebody have some Idea why can't redirect to the guest portal????

I need this Help for a important implementation.



gnijis ★ Bronze

10-07-2013 03:06

I have the same problem. I think it is because i am still running 7.0.230.0, i think i have to go to > 7.2



grabonlee ★ Bronze

10-07-2013 03:55

Hi,

Mac Authentication Bypass is only supported from 7.2 and above. Hence it's only supported on WLC 5508 and higher controllers.



Cristian Popescu New Member

11-06-2013 02:18

Hi,

When using MAC Filtering on the Controller, as in the example above, the guest sessions were not visible anymore in Operations->Catalog->Session Directory.

After reverting back to WLC L3 web redirect with external authentication, the sessions were once again available.

Is there anything else that could be done to have the Session feature available? We really need it for controlling the guests...

The current design with L3 web auth on the WLC and the link statically configured on WLC has some problems with redirection after successful login - some browser don't accept the WLC page with the virtual ip framed in a page from the ISE server.



Bastien Migette Cisco Employee

11-06-2013 02:30

Hello Cristian,

As far as I know, the guest sessions should be visible once the guest users logs in. You may open a TAC case to sort this if you can reproduce this behaviour.

Otherwise, ISE 1.2 has greatly improved the redirection process for external Web Auth on WLC, as it pushes back credentials over POST, and no longer via iFrames as depending on certificate trust and browser configuration, this used to have some issues.

Note: I have also tested this in ISE 1.2, I could see my guest users in the active sessions with CWA:

Current Active Sessions									
Generated at 2013-11-06 11:29:36.840									
From 11/06/2013 12:00:00.000 AM to 11/06/2013 11:29:36.840 AM									
Page << 1 >> Records 1 to 3									
Initiated	Updated	Session Time	Identity	Endpoint ID	CTS Security Group	Framed IP Address	Auth Method	Auth Protocol	
Wed Nov 06 11:29:31 CET 2013	Wed Nov 06 11:29:31 CET 2013	21m22s	bastien	F8:1A:67:18:08:D6		192.168.91.24	webauth		



John Capobianco New Member

11-21-2013 08:37

"

Hello Tarik, You are right, with CWA, the ISE shows a message indicating the user he can retry his original URL. This is a current limitation, as the ISE doesn't know the original URL.

What you can do is to create a custom portal with HTML Files and modify the success page to redirect to an arbitrary web page."

When is this limitation being overcome? It seems very clunky to have users not directly go to their homepage or the URL they specified initially or to have to force a user to go to a landing page.

Thanks

John



moises.rodriguez New Member

09-24-2014 01:52

Hi Guillem

I now you posted this long time ago, but I'm having the same issue, I'm just wondering if you got it resolved and how.

Thanks



Bastien Migette Cisco Employee

09-24-2014 11:36

Hello Moises,

Starting ISE 1.2, you have the ability to select "Static ip/hostname" in the authorization profile, under the WebAuth part. That way you can put ISE's Policy Node IP address if you don't have correct DNS Entry.



Abraham Camacho ★ Bronze

01-20-2015 03:23

Hi Bastien,

We are moving from LWA to CWA so I was wondering what you mean by USECASE:GUESTFLOW. I am assuming that GUESTFLOW has something to do with having the Authorization Profile --- > CWA redirect pointing to DEFAULT. So what happens if I the redirect points to a MANUAL Login Page that I loaded into the ISE instead of Default? Is the USECASE:VALUE still the same as before?

BTW, from the basic CWA configuration example from Cisco link next, that additional AUTHZ Policy with the USECASE:GUESTFLOW is required in order to avoid loops in the AUTHZ part (double authorization is performed).

Thanks for any orientation regarding this question.



Bastien Migette Cisco Employee

01-21-2015 12:31

Hello Abraham,

In CWA, there is 2 authentication sharing the same session. The first one redirects to the portal via MAB, the second one is the actual authentication on the guest portal.

When authenticating on guest portal, ISE sets the flag GuestFlow so we can identify it and apply the correct authorization policy.

I hope this is clear.



Abraham Camacho ★ Bronze

01-21-2015 07:51

Hi Bastien,

Thanks a lot for your note. Now I understand what means GUESTFLOW and how this Flag is used in the cisco example of the following link in order to avoid the Authorization LOOP mentioned as well on this link.

<http://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/115732-central-web-auth-00.html>

I will give a try in the lab and let you know but I was wondering if the FLAG is set with the same value = GuestFlow when I use a customized login page (Manual option selected in the redirect part of the CWA configuration for the AuthZ profile - see attached image)

On the other hand, I have been doing research for a while and I could not find a link or document that explain in details the meaning for all the NETWORKACCESS: USECASE equals to:

- Eap chaining
- Guest Flow
- Host Lookup
- Proxy

Please let me know if you have any link so I can take a look on it.

 cwa.png



Bastien Migette  Cisco Employee

01-21-2015 07:57

Hello Abraham,

Yes, all CWA auth will have the guest flow flag, whether you use a custom portal or not.


For host-lookup, this identifies MAB request (it basically checks service-type=6)

For EAP Chaining, this is when you have eap-chaining: http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/howto_80_eapchaining_deployment.pdf

Proxy I am not sure, I never had to use it.

I am not aware of any document that summarize all use-case, this is rather integrated on specific configuration example such as the one you pointed.



Abraham Camacho  Bronze

01-27-2015 08:11

Hi Bastien,

CWA works straightforward based on the Cisco configuration example. The only thing that I found weird is that when I am using Chrome on my Win7 laptop or a Chromebook device and connect to the SSID configured for CWA, 2 browsers are opened simultaneously. Do you have any idea about this?. Maybe this is something to do with the settings on the Chrome Browser but I was wondering if you have seen this before.

Thanks

Abraham



Bastien Migette  Cisco Employee

01-27-2015 08:33

Hello Abraham,

Glad you made this work. Concerning the issue with 2 browser being opened, I don't recall having seen anything similar, sorry.



CB90021204 New Member

02-08-2015 10:34

Hi Bastien,

I'm implementing the same scenario as Dominic above using a foreign/anchor controller.

Do you know what firewall ports are required to allow communication between the wireless controller and ISE?

Do the ports below look correct?

UDP:1645, 1812 (RADIUS Authentication)

UDP:1646, 1813 (RADIUS Accounting)

UDP: 1700 (RADIUS change of authorization Send)

UDP: 1700, 3799 (RADIUS change of authorization Listen/Relay)

http://www.cisco.com/c/en/us/td/docs/security/ise/1-2/installation_guide/ise_ig/ise_app_c-ports.html



Bastien Migette  Cisco Employee

02-09-2015 05:43

Hello,

That should be enough, but keep in mind Radius packets (MAB Requests) and CoA will be handled at Foreign WLC.

Accounting will go out from where it is configured, but it is recommended to enable it only at foreign as it can cause issue otherwise.

Lastly, Client traffic to ISE will use port 8443 or 8905/6/9 if you have Posture, and will go out of anchor.

I hope this helps.



CB90021204 New Member

02-09-2015 02:58

Thank you Bastien, yes thats very helpful.



acontes New Member

02-10-2015 05:00

Any hints how to configure this with a second ISE as backup? How does the redirect acl look like?



1s.bancha New Member

07-31-2015 06:56

Do you know if WLC CWA with ISE supports to intercept https traffic and redirect to guest portal?

If not, any roadmap?

Thank you,

Bancha



gohussai Cisco Employee

08-18-2015 09:55

That link is really useful

<http://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/115732-central-web-auth-00.html>



Abraham Camacho ★ Bronze

09-14-2015 09:45

Hi Bastien,

I am currently testing 1.4 patch3 - latest version on ISE because I am planning to use PEAP + AUP on HotSpot Option. However, my question on this case is the following:

Based on the link, we have a note that says the next:

<http://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-software/118741-configure-ise-00.html>

Note: The CoA Admin-Reset is specific for Hotspot functionality and described in Cisco bug ID [CSCus46754](#). The behavior for ISE Version 1.2 with a guest portal was different; a CoA Re-authenticate or Terminate was sent.

So my question is:

On CWA, are we using CoA Re-authenticate, right?. On what cases are we using Terminate?

thanks



Bastien Migette  Cisco Employee

09-14-2015 11:15

Hello Abraham, In most of the case you will have reauth action, because the purpose is to refresh the profile after some events, being profiling, auth, ...

The hotspot feature in 1.3 is a bit different and do not require authentication. In this scenario, the flow will be different, and the bug you mentioned is a documentation bug, meaning the product works as expected but this is not properly documented.

For regular Guest CWA portals, there should not be a difference.



Carlos Valderrama New Member

10-01-2015 06:21

Hello, i would like to know if it's possible to make https redirection in a WLC with CWA and ISE?



Bastien Migette  Cisco Employee

10-01-2015 11:18

Hello,

Yes that is possible with WLC 8.0 and later. You need to configure

```
config network web-auth https-redirect enable
```

And that the Redirect ACL is adjusted.

More Info here:

<https://supportforums.cisco.com/document/12398536/understanding-https-redirect-over-web-auth>

And

<http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/115951-web-auth-wlc-guide-00.html#anc7>



Carlos Valderrama New Member

10-04-2015 09:47

Hello Bastien.

Thanks for your soon reply, i tested the command, but our client complains about the certificate error with the https redirection.

On the link you provide says that it's unavoidable, but just to confirm, is there any possible way to fix the certificate error? otherwise we gonna have to unmount the ise guest solution because of that.



Bastien Migette  Cisco Employee

10-04-2015 11:38

Hello Carlos,

This is not technically possible. When a device intercept SSL Connection, it has to use its own certificate which is self signed, and event it would be a CA Signed one, would not match destination website, so you will always get a SSL Warning when you want to intercept SSL connection.



Philip Gerundt New Member

10-07-2015 07:32

So there is just a Radius communication between foreign and ISE ?

I thought with CWA the Anchor WLC handles the Radius Authentication ?

If no is there any communication between ISE and Anchor WLCs ?

Greetings

Philip

< Previous **1** 2 Next >

Top Tags

[VIEW ALL](#)

1200_ap 1100_ap configuration 1240_ap 1230_ap 1130_ap troubleshoot 1140_ap 1250_ap wireless ap
4400_wlc error_message wlc 5500_wlc 1400_bridge 1300_bridge 2100_wlc air_cb21ag 3750_wlc 2000_wlc
wireless_lan_controller wism wlcm wgb radius wcs eap 350_ap wlan_client