Enabling Central Web Authentication on ISE

The document describes the procedure to enable Central Web Authentication (CWA) on Identity Services Engine (ISE).

Enabling CWA on ISE through Global Configuration Commands

Use the following commands to enable CWA on ISE to work with Converged Access controllers:

Command or Action	Description/Purpose/Example
show run aaa	Displays the Authorization, Authentication, and Accounting (AAA) related configurations.
aaa authentication login *ext_ise group rad_ise*	Defines the 'exe ise' login method list which points to the ISE server 'rad_ise'.
aaa authorization network cwa_mac group *rad_ise*	The authorization method 'cwa_mac' is the mac filter list name which is called under the WLAN configuration. It points to the ISE server 'rad_ise' for authorization.
radius server *ise* **address ipv4** 192.0.2.1 **auth-port** 1812 **acct-port** 1813 **key** *Cisco123*	Displays the RADIUS server definition for the 'ise' server.
aaa group server radius *rad_ise* **server name** *ise*	The 'rad_ise' AAA group server points to the server 'ise'.

aaa server radius dynamic-author **client** 192.0.2.1 **server-key** *Cisco123* **auth-type** *any*	Required for Change of Authorization (CoA). For more information on CoA, refer to Dynamic Authorization Commands.

Enabling External Policy Server using Dynamic Authorization Commands

Use the following dynamic authorization commands to enable an external policy server to dynamically send updates to a device:

Command or Action	Description/Purpose/Example
radius-server attribute 31 send nas -port-detail mac-only Or, **radius-server attribute 31 send nas-port-detail**	Sends the calling station ID for MAC. Sends calling station ID for all operating systems other than MAC.
ip access-list extended ACL-REDIRECT	This is a url-redirect-acl. To redirect the guest portal, the Identity Services Engine (ISE) returns an AAA override and the redirect URL. The url-redirect-acl is a punt ACL which is a reverse ACL that is used for unified architecture. You need to block access to DHCP, DHCP Server, DNS, DNS server, and ISE server and allow www, 443 port, or the 8443 port as required. The ISE guest portal uses port 8443 and the redirection works with the following ACL: 10 deny udp any eq bootps any 20 deny udp any any eq bootpc 30 deny udp any eq bootpc any 40 deny ip any host 192.0.2.1 50 deny ip any host 192.0.2.2 60 permit tcp any any eq www
mac access-list extended **cwa_mac permit any** *any*	The access list is defined based on the MAC Authentication Bypass (MAB) rule.

Related Commands

The following table displays the commands that are associated with dynamic authorization:

Command or Action	Description/Purpose/Example
auth-type (ISO)	Specifies the server authorization type.
Client	Specifies a RADIUS client from which a device accepts CoA and disconnects requests.
Default	Sets the RADIUS application command to default domain and then specifies the username domain options.
Ignore	Overrides a behavior to ignore the parameters that are specified.
Port	Specifies a port on which local RADIUS server listens to.
server-key	Specifies the encryption key shared with the RADIUS clients.

Configuring WLAN Commands

The following example describes the WLAN configuration:

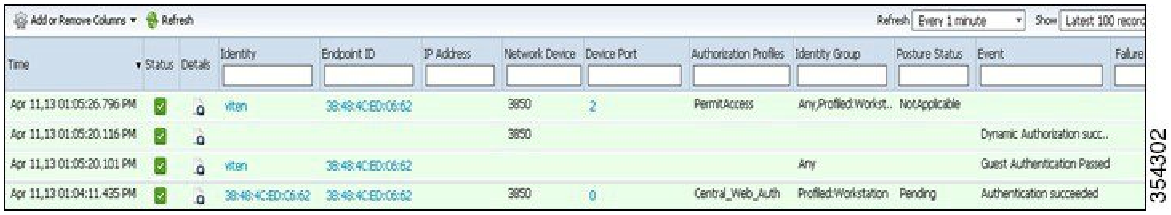
```
wlan cwa_guest 11 cwa_guest
aaa-override
client vlan 263
mac-filtering cwa_mac ----> mac filter pointing to authorization on ISE server
nac
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
no shutdown
```

Authentication Flow on ISE

The ISE logs shown in the following figure displays the authentication flow on the ISE:

The following figure displays the authentication Flow based on the ISE logs:

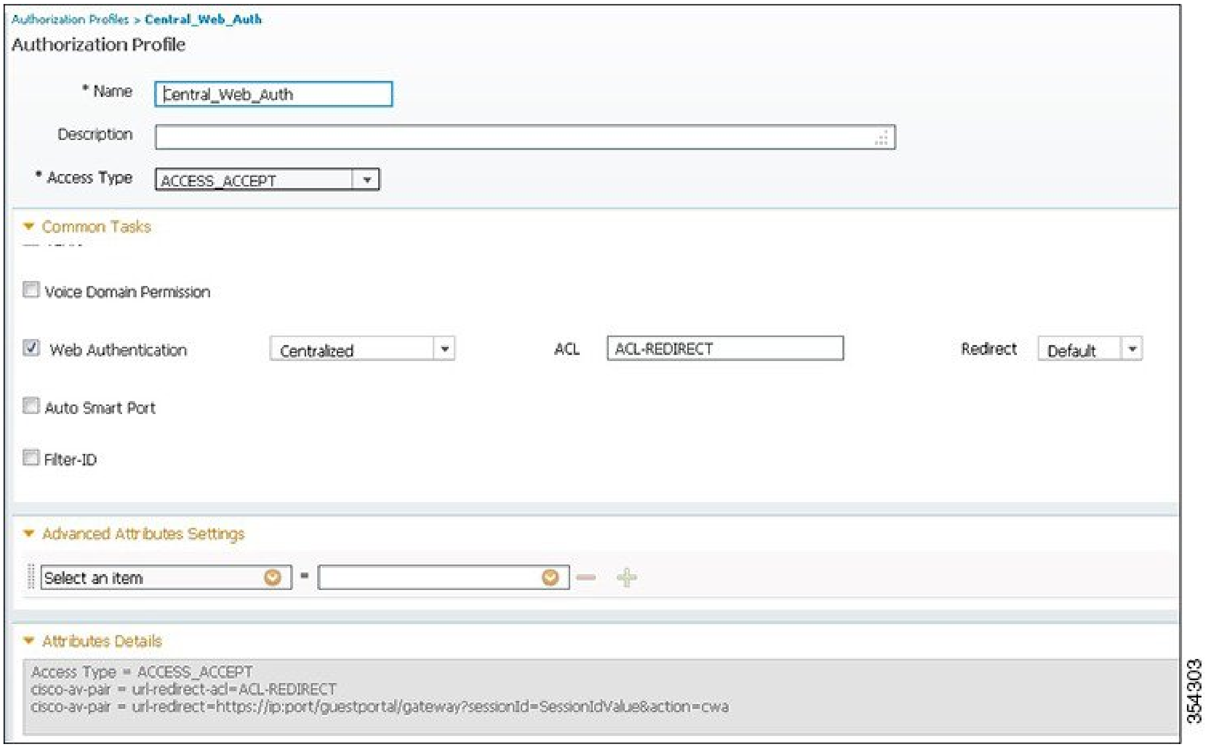
Figure 1: Authentication Flow



Time	Status	Details	Identity	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles	Identity Group	Posture Status	Event	Failure
Apr 11,13 01:05:26.796 PM	✓		viten	38:48:4C:ED:C6:62		3850	2	PermitAccess	Any,Profiled:Workst...	NotApplicable		
Apr 11,13 01:05:20.116 PM	✓					3850					Dynamic Authorization succ...	
Apr 11,13 01:05:20.101 PM	✓		viten	38:48:4C:ED:C6:62					Any		Guest Authentication Passed	
Apr 11,13 01:04:11.435 PM	✓		38:48:4C:ED:C6:62	38:48:4C:ED:C6:62		3850	0	Central_Web_Auth	Profiled:Workstation	Pending	Authentication succeeded	

The following figure displays the authorization profile details for CWA:

Figure 2: Authorization Profile



Authorization Profiles > Central_Web_Auth

Authorization Profile

* Name	Central_Web_Auth
Description	
* Access Type	ACCESS_ACCEPT

▾ Common Tasks

- □ Voice Domain Permission
- ☑ Web Authentication — Centralized — ACL: ACL-REDIRECT — Redirect: Default
- □ Auto Smart Port
- □ Filter-ID

▾ Advanced Attributes Settings

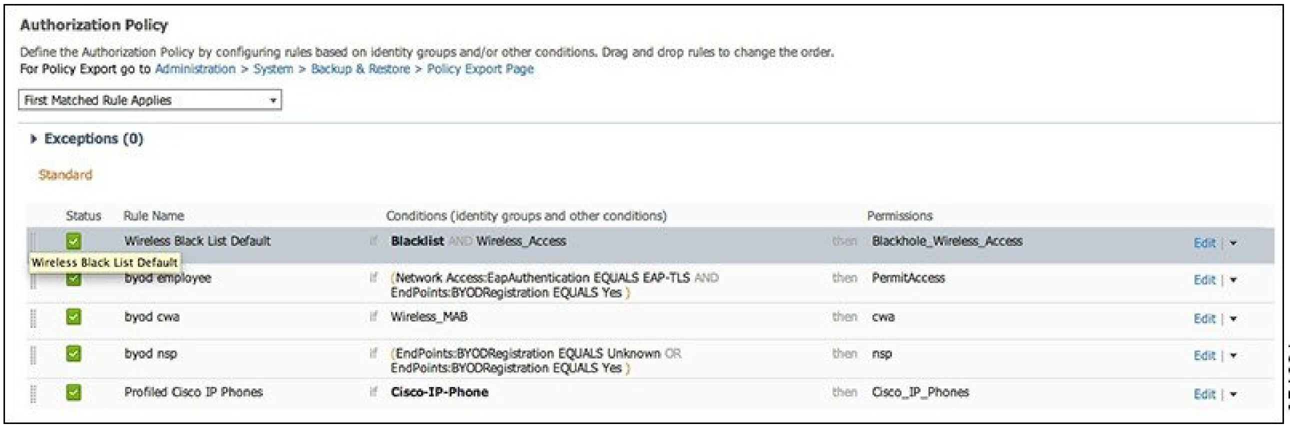
Select an item =

▾ Attributes Details

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = url-redirect-acl=ACL-REDIRECT
cisco-av-pair = url-redirect=https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=cwa
```

The following illustration displays the authorization policy on ISE to redirect Mobile Devices to CWA:

Figure 3: Authorization Policy



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.
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

First Matched Rule Applies

▸ Exceptions (0)

Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
✓	Wireless Black List Default	if	**Blacklist** AND Wireless_Access	then	Blackhole_Wireless_Access	Edit | ▾
✓	byod employee	if	(Network Access:EapAuthentication EQUALS EAP-TLS AND EndPoints:BYODRegistration EQUALS Yes)	then	PermitAccess	Edit | ▾
✓	byod cwa	if	Wireless_MAB	then	cwa	Edit | ▾
✓	byod nsp	if	(EndPoints:BYODRegistration EQUALS Unknown OR EndPoints:BYODRegistration EQUALS Yes)	then	nsp	Edit | ▾
✓	Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	then	Cisco_IP_Phones	Edit | ▾

Note

- To integrate ISE into the design, the foreign controller is the only Network Access Device (NAD) that interacts with the ISE.

  The foreign controller that is configured for Layer 2 MAC filtering, where the guests access the Wireless MAB, continue the authentication rule on ISE.

- In a static anchor setup that uses controllers and Access Control Server (ACS), if AAA override is enabled to dynamically assign VLAN and QoS, the foreign controller updates the anchor controller with the right VLAN after a Layer 2 authentication (802.1x).

  For Layer 3 RADIUS authentication, the RADIUS requests for authentication are sent by the anchor controller.

For more information, refer to the 'Information About Mobility' chapter in the Cisco Wireless LAN Controller Configuration Guide, Release 7.4.