

WEB REDIRECTION WITH CISCO ISE

CONTENTS

Web Redirection With Cisco ISE	1
Requirements.....	1
Overview.....	1
Aruba Switch Configuration.....	2
Adding VSA to The HP Dictionary.....	4
Creating a Network Device Profile.....	8
Adding A switch To ISE.....	11
Guest Portal Settings.....	13
Web Redirection Policy.....	18
Verification.....	22
TIPS.....	26

REQUIREMENTS

- ArubaOS-Switch (2930M/F, 3810M, 5400R) 16.08 and Above
- Cisco ISE (2.3 And Above)

OVERVIEW

This document will cover Web Redirection with Cisco ISE.

For this scenario, we will be creating a Mac Authentication Fallback policy within Cisco ISE to allow guest devices some network connectivity. This network connectivity will only allow users access to Cisco ISE to register their device . Once the Client is registered, we only want that client to have basic internet access so we will configure a second role to allow for this to work. This same concept can be used for BYOD and a Sponsor Portal with Cisco ISE.

ARUBA SWITCH CONFIGURATION

Switch Configuration

Pointing the switch to ISE Server

```
radius-server host <Radius-IP> dyn-authorization
radius-server host <Radius-IP> time-window 0
radius-server key < KEY-STR>
```

Configuring AAA on the switch for Mac Authentication as a fall back and Configuration for enabling AAA.

```
aaa port-access authenticator <Ports>
aaa port-access mac-based <Ports>
aaa port-access <Ports> auth-order authenticator mac-based
aaa port-access <Ports> auth-priority authenticator mac-based
aaa port-access authenticator active
aaa authentication port-access eap-radius
aaa authentication captive-portal enable
aaa authorization user-role enable
```

Web Redirection User Role Configuration

Redirection Policy and Class map Configuration

```
class ipv4 "DNS"
  10 match udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 53
  exit
class ipv4 "DHCP"
  10 match udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 67
  exit
class ipv4 "WEB-TRAFFIC"
  10 match tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 80
  20 match tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 443
  exit
class ipv4 "CLEARPASS-WEB"
  30 match tcp 0.0.0.0 255.255.255.255 10.6.3.15 0.0.0.0 eq 80
  40 match tcp 0.0.0.0 255.255.255.255 10.6.3.15 0.0.0.0 eq 443
  50 match tcp 0.0.0.0 255.255.255.255 10.6.3.15 0.0.0.0 eq 8443
policy user "ISE-REDIRECT"
  10 class ipv4 "DNS" action permit
  20 class ipv4 "DHCP" action permit
  30 class ipv4 "CLEARPASS-WEB" action permit
  40 class ipv4 "WEB-TRAFFIC" action redirect captive-portal
```

User Role Configuration for web redirection User-Role

```
aaa authorization user-role name "ISE-CAP-PORTAL"  
  captive-portal-profile "use-radius-vsa"  
  policy "ISE-REDIRECT"  
  vlan-id 505  
  Exit
```

Guest User Role Configuration

User Role Configuration for web redirection User-Role

```
class ipv4 "BLOCK_INTERNAL"  
  10 match ip 0.0.0.0 255.255.255.255 10.0.0.0 0.255.255.255  
  20 match ip 0.0.0.0 255.255.255.255 192.168.0.0 0.0.255.255  
  30 match ip 0.0.0.0 255.255.255.255 172.16.0.0 0.15.255.255  
  Exit  
class ipv4 "GUEST_ACCESS"  
  40 match ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255  
  Exit  
policy user "GUEST_ACCESS"  
  10 class ipv4 "BLOCK_INTERNAL" action deny  
  20 class ipv4 "GUEST_ACCESS" action permit  
  Exit
```

User Role Configuration for CoA to guest Access

```
aaa authorization user-role name "Guest_Access"  
  policy "GUEST_ACCESS"  
  vlan-id 100  
  Exit
```

ADDING VSA TO THE HP DICTIONARY

Description

Cisco ISE does not have all the VSA's that are needed by default so in order to use web redirection with Cisco ISE the VSA's need to be added.

1. Navigate to "Work Centers> Network Access> Dictionaries"

From this page go to

"System> Radius > HP"

The screenshot displays the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes "Identity Services Engine" and "Work Centers". The breadcrumb trail is "Network Access > Guest Access > TrustSec > BYOD > Profiler > Posture > Device Administration > PassiveID > Overview > Identities > Id Groups > Ext Id Sources > Network Resources > Policy Elements > Policy Sets > Troubleshoot > Reports > Settings > Dictionaries".

The left sidebar shows a tree view of "Dictionaries" under "RADIUS Vendors". The "HP" dictionary is selected. The main content area shows the configuration for the "HP" dictionary:

- * Dictionary Name: HP
- Description: Dictionary for Vendor HP
- * Vendor ID: 11
- Vendor Attribute Type Field Length: 1
- Vendor Attribute Size Field Length: 1

Buttons for "Save" and "Reset" are visible at the bottom of the configuration form.

2. Click Dictionary Attributes then click “+Add”

Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration PassiveID

Overview Identities Id Groups Ext Id Sources Network Resources Policy Elements Policy Sets Troubleshoot Reports Settings **Dictionary**

Dictionaries

Network Condition

NMAP

NMAPEExtension

Normalised Radius

PassiveID

Posture

PROFILER

Radius

IETF

RADIUS Vendors

Airespace

Alcatel-Lucent

Aruba

Aruba_Wired

Brocade

Cisco

Cisco-BBSSM

Cisco-VPN3000

H3C

HP

Juniper

Microsoft

Motorola-Symbol

Ruckus

WISPr

Session

SNMP

SXP

TACACS

TC-NAC

Threat

TrustSec

User

Dictionaries > ... > RADIUS Vendors > HP

Dictionary Dictionary Attributes

Dictionary Attributes

+ Add Edit Delete

Name	Number	Type	Direction	Description	Predefined
HP-Bandwidth-Max-Egr...	48	UINTEGER	BOTH	Attribute HP-Bandwidth-Max-Egr...	NO
HP-Bandwidth-Max-Ingr...	46	UINTEGER	BOTH	Attribute HP-Bandwidth-Max-Ingr...	NO
HP-Capability-Advert	255	OCTET_STRING	BOTH	Attribute HP-Capability-Advert	NO
HP-Command-Exception	3	UINTEGER	BOTH	Attribute HP-Command-Exception	NO
HP-Command-String	2	STRING	BOTH	Attribute HP-Command-String	NO
HP-Cos	40	STRING	BOTH	Attribute HP-Cos	NO
HP-Egress-VLAN-Name	65	STRING	BOTH	Attribute HP-Egress-VLAN-Name	NO
HP-Egress-VLANID	64	UINTEGER	BOTH	Attribute HP-Egress-VLANID	NO
HP-Management-Proto...	26	UINTEGER	BOTH	Attribute HP-Management-Protocol	NO
HP-Nas-Filter-Rule	61	STRING	BOTH	Attribute HP-Nas-Filter-Rule	NO
HP-Nas-Rules-IPv6	63	UINTEGER	BOTH	Attribute HP-Nas-Rules-IPv6	NO
HP-Port-Auth-Mode-Dot...	13	UINTEGER	BOTH	Attribute HP-Port-Auth-Mode-Dot1x	NO
HP-Port-Client-Limit-Do...	10	UINTEGER	BOTH	Attribute HP-Port-Client-Limit-Dot...	NO
HP-Port-Client-Limit-MA	11	UINTEGER	BOTH	Attribute HP-Port-Client-Limit-MA	NO
HP-Port-Client-Limit-WA	12	UINTEGER	BOTH	Attribute HP-Port-Client-Limit-WA	NO
HP-Privilege-Level	1	UINTEGER	BOTH	Attribute HP-Privilege-Level	NO
<input checked="" type="checkbox"/> HPE-Port-MA-Port-Mode	14	UINTEGER	BOTH	words	NO

3. A New Page will appear enter the Attribute information below

Attribute Name: "HP-User-Role"

Data type: "String"

Direction: "Both"

ID: "25"

Click Save

The screenshot displays the Cisco Identity Services Engine (ISE) Administration interface. The breadcrumb navigation path is "Dictionaries > ... > HP > HP-User-Role". The left-hand navigation pane shows a tree structure under "Dictionaries" with "RADIUS" expanded to show various vendors, including "HP". The main configuration area contains the following fields and options:

- * Attribute Name: HP-User-Role
- Description: (empty text box)
- * Data Type: STRING (dropdown menu)
- Enable MAC option:
- * Direction: BOTH (dropdown menu)
- * ID: 25 (0-255)
- Allow Tagging:
- Allow multiple instances of this attribute in a profile:

At the bottom of the configuration area are "Save" and "Reset" buttons.

The Captive Portal VSA has to be added Click “+Add”

Attribute Name: “HP-Captive-Portal-URL”

Data type: “String”

Direction: “Both”

ID: “24”

Click Save

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation is: Dictionaries > ... > HP > HP-Captive-Portal-URL. The configuration form includes the following fields:

- * Attribute Name: HP-Captive-Portal-URL
- Description: (empty text box)
- * Data Type: STRING (dropdown menu)
- Enable MAC option:
- * Direction: BOTH (dropdown menu)
- * ID: 24 (text box) (0-255)
- Allow Tagging:
- Allow multiple instances of this attribute in a profile:

At the bottom of the form are "Save" and "Reset" buttons. On the left, a "Dictionaries" sidebar shows a tree view with categories like Network Access, Network Condition, NMAP, NMAPExtension, Normalised Radius, PassivelD, Posture, PROFILER, RADIUS, and RADIUS Vendors (including Airespace, Alcatel-Lucent, and Aruba).

There should now be two New VSA's in Cisco ISE that can be used.

CREATING A NETWORK DEVICE PROFILE

Description

Since Cisco ISE does not have the Captive portal VSA, we have to allow it to be used by the network profile. Cisco ISE does not let you edit existing profiles so we must create a copy of the existing “HP Wired” Profile so that it can be edited to use the captive portal VSA that was just created.

1. Navigate to “Administration>Network Resources> Network Device Profiles

The screenshot shows the Cisco ISE Administration console. The breadcrumb navigation is: Administration > Network Resources > Network Device Profiles. The page title is "Network Device Profiles". Below the title are several action buttons: Edit, Add, Duplicate, Import, Cisco Communities Import, Export Selected, and Delete Selected. The main content is a table with the following data:

Name	Description	Vendor	Source
AlcatelWired	Profile for Alcatel switches	Alcatel	Cisco Provided
ArubaWireless	Profile for Aruba wireless network access devices	Aruba	Cisco Provided
BrocadeWired	Profile for Brocade switches	Brocade	Cisco Provided
Cisco	Generic profile for Cisco network access devices	Cisco	Cisco Provided
HPWired	Profile for HP switches	HP	Cisco Provided
HPWired_SNMP_CoA	Profile for HP switches with no RADIUS CoA	HP	Cisco Provided
HPWireless	Profile for HP wireless network access devices	HP	Cisco Provided
MotorolaWireless	Profile for Motorola wireless network access devices	Motorola	Cisco Provided
RuckusWireless	Profile for Ruckus wireless network access devices	Ruckus	Cisco Provided

2. Select the “HP Wired” Profile then click Duplicate, it will automatically pull up the configuration of the New Profile.

The screenshot shows the 'New Network Device Profile' configuration page in the Aruba Identity Services Engine. The breadcrumb trail is: Network Device Profile List > New Network Device Profile. The page title is 'Network Device Profile'. There are 'Submit' and 'Cancel' buttons at the top right.

Network Device Profile

Name: HPWired_copy

Description: Profile for HP switches

Icon: Change icon... Set To Default

Vendor: HP

Supported Protocols

- RADIUS:
- TACACS+:
- TrustSec:

RADIUS Dictionaries: HP H3C

Templates

Expand All / Collapse All

- ▶ Authentication/Authorization
- ▶ Permissions
- ▶ Change of Authorization (CoA)
- ▶ Redirect
- ▶ Advanced

Submit Cancel

3. Click the Redirect Dropdown, Select “Dynamic URL” in the drop down box select the “HP-Captive-Portal-URL” VSA that we created earlier in this document

Next check the “Client MAC Address” and Enter the following information below

Client IP Address: ip
Client MAC Address: mac
Originating URL: url

[Expand All / Collapse All](#)

▶ Authentication/Authorization

▶ Permissions

▶ Change of Authorization (CoA)

▼ Redirect

Type

=

Dynamic URL Parameter

- Session ID
- Client MAC Address
- None

Redirect URL Parameter Names

Client IP Address

Client MAC Address

Originating URL

Session ID

SSID

Click Save

ADDING A SWITCH TO ISE

Description

This section will go over adding a device into Cisco ISE.

1. Navigate to Administration > Network Devices. Click Add.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation menu at the top includes Home, Context Visibility, Operations, Policy, Administration, and Work Centers. The left sidebar contains Network Devices, Default Device, and Device Security Settings. The main content area is titled 'Network Devices' and features a toolbar with options: Edit, Add, Duplicate, Import, Export, Generate PAC, and Delete. Below the toolbar is a table with the following data:

Name	IP/Mask	Profile Name	Location	Type
<input type="checkbox"/> 2930M-ISE	10.128.1.10/32	HPWired_copy	All Locations	All Device Types

- Enter the IP address, RADIUS shared secret, and model of the switch and select the “HPWired_copy” switch profile. If the switch is already added to ISE then just edit the device and select the “HPWired_copy” Profile

Network Devices List > 2930M-ISE

Network Devices

* Name

Description

IP Address /

i IPv6 is supported only for TACACS. At least one IPv4 must be defined when RADIUS is selected

* Device Profile

Model Name

Software Version

* Network Device Group

Location

IPSEC

Device Type

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

* Shared Secret

CoA Port

RADIUS DTLS Settings *i*

DTLS Required *i*

Shared Secret *i*

CoA Port

Issuer CA of ISE Certificates for CoA *i*

DNS Name

General Settings

Enable KeyWrap *i*

* Key Encryption Key

* Message Authenticator Code Key

Key Input Format ASCII HEXADECIMAL

GUEST PORTAL SETTINGS

Description

Before editing the Guest portal there needs to be an Identity group for the self-registered users so that devices that register don't have to re-register every single time the move offices or sites.

1. To do this navigate to

“Administration> Groups>Endpoint Identity Groups”

Click “+ Add” and name the group and Click Save

The screenshot displays the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Administration' menu is expanded to show 'System', 'Identity Management', 'Network Resources', 'Device Portal Management', 'pxGrid Services', 'Feed Service', and 'Threat Centric NAC'. The 'Identity Management' menu is further expanded to show 'Identities', 'Groups', 'External Identity Sources', 'Identity Source Sequences', and 'Settings'. The 'Groups' menu item is selected, and the 'Endpoint Identity Group List > New Endpoint Group' page is displayed. The page title is 'Endpoint Identity Group'. The form contains the following fields: '* Name' (text input with value 'Self_Register_Guest'), 'Description' (text input), and 'Parent Group' (dropdown menu). At the bottom of the form are 'Submit' and 'Cancel' buttons. On the left side, there is a sidebar titled 'Identity Groups' with a search bar and a tree view showing 'Endpoint Identity Groups' and 'User Identity Groups'.

2. Edit the Guest Portal Settings

Navigate to

“Work Centers>Guest Access>Portals & Components.

Select Guest Types Duplicate the “Daily (Default)”

The screenshot displays the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes the Cisco logo and the text "Identity Services Engine". Below this, a secondary navigation bar contains links for "Home", "Context Visibility", "Operations", "Policy", "Administration", and "Work Centers". A third navigation bar lists various modules: "Network Access", "Guest Access", "TrustSec", "BYOD", "Profiler", "Posture", "Device Administration", and "PassiveID". The "Guest Access" module is expanded, showing sub-links for "Overview", "Identities", "Identity Groups", "Ext Id Sources", "Administration", "Network Devices", "Portals & Components", "Manage Accounts", "Policy Elements", "Policy Sets", and "Reports".

The left sidebar contains a tree view with the following items: "Guest Portals", "Guest Types", "Sponsor Groups", and "Sponsor Portals". The "Guest Types" item is selected and highlighted.

The main content area is titled "Guest Types" and includes the following text: "You can edit and customize the default guest types and create additional ones." Below this text is a toolbar with four buttons: "Create", "Edit", "Duplicate", and "Delete".

The main content area displays a list of guest types, each in a light blue box:

- Contractor (default)**: Default settings allow network access for up to a year.
- Daily (default)**: Default settings allow network access for just 1-5 days.
- Daily (default)_copy1**: Default settings allow network access for just 1-5 days.

3. Select the “Daily (Default) Copy1” Guest type and Edit the Guest type.

Change the Guest type name and change the endpoint Identity group to the Self_Register_Guest group that was created before. Edit any other settings that are needed

Guest Type

Guest type name: *

Description:

▾

Collect Additional Data

Maximum Access Time

Account duration starts

From first login

From sponsor-specified date (or date of self-registration, if applicable)

Maximum account duration

Default (1-999)

Allow access only on these days and times:

From To Sun Mon Tue Wed Thu Fri Sat

Configure guest Account Purge Policy at:
[Work Centers > Guest Access > Settings > Guest Account Purge Policy](#)

Login Options

Maximum simultaneous logins (1-999)

When guest exceeds limit:

Disconnect the oldest connection

Disconnect the newest connection

Redirect user to a portal page showing an error message ⓘ
This requires the creation of an authorization policy rule

Maximum devices guests can register: (1-999)

Endpoint identity group for guest device registration: ⓘ

Configure endpoint identity groups at: [Work Centers > Guest Access > Identity Groups](#)
The endpoints in this group will be purged according to the policies defined in: [Administration > Identity Management > Settings > Endpoint purge](#)

Allow guest to bypass the Guest portal

4. Edit the Guest portal Edit the “Self-Registered Guest Portal (default)” or Duplicate this portal.

In the portal settings change the “employees using this portal as guest inherit login options” to the Self_Register_Guest. This will allow internal user to just gain internet access quickly.

ps Ext Id Sources Administration Network Devices Portals & Components Manage Accounts Policy Elements Policy Sets Reports Custom Portal Files Settings

Portals Settings and Customization Save Close

Portal Name: * Self-Registered Guest Portal (default) Description: Guests may create their own accounts and be assigned a username and pa: Portal test URL Language File

Portal Behavior and Flow Settings
Use these settings to specify the guest experience for this portal.

Portal Page Customization
Customize portal pages by applying a theme and specifying field names and messages displayed to users.

Portal & Page Settings

Portal Settings

HTTPS port: * 8443 (8000 - 8999)

Allowed interfaces: * Make selections in one or both columns based on your PSN configurations.

<p>If bonding is not configured (i) on a PSN, use:</p> <p><input checked="" type="checkbox"/> Gigabit Ethernet 0</p> <p><input type="checkbox"/> Gigabit Ethernet 1</p> <p><input type="checkbox"/> Gigabit Ethernet 2</p> <p><input type="checkbox"/> Gigabit Ethernet 3</p> <p><input type="checkbox"/> Gigabit Ethernet 4</p> <p><input type="checkbox"/> Gigabit Ethernet 5</p>	<p>If bonding is configured (i) on a PSN, use:</p> <p><input checked="" type="checkbox"/> Bond 0 <i>Uses Gigabit Ethernet 0 as primary, 1 as backup.</i></p> <p><input type="checkbox"/> Bond 1 <i>Uses Gigabit Ethernet 2 as primary, 3 as backup.</i></p> <p><input type="checkbox"/> Bond 2 <i>Uses Gigabit Ethernet 4 as primary, 5 as backup.</i></p>
---	--

Certificate group tag: * Default Portal Certificate Group

Configure certificates at:
Work Centers > Guest Access > Administration > System Certificates

Authentication method: * Guest_Portal_Sequence (i)

Configure authentication methods at:
Work Centers > Guest Access > Identities > Identity Source Sequences
Work Centers > Guest Access > Ext Id Sources > SAML Identity Providers

Employees using this portal as guests inherit login options from: * Self_Register_Guest

Display language: Use browser locale
Fallback language: English - English

Always use: English - English

5. Enable Vlan DHCP Release this will make CoA work more smoothly.

VLAN DHCP Release Page Settings

Enable VLAN DHCP release

Delay to release: 1 seconds (1 - 200)
Enter the amount of time to wait before releasing the IP address after the applet downloads.

Delay to CoA: 8 seconds (1 - 200)
Enter a time longer than the "Delay to release" value to allow enough time for the applet to download and the IP address to be released.

Delay to renew: 12 seconds (1 - 200)
Enter a time longer than the "Delay to CoA" value to allow enough time for the change of authorization to occur.

6. In the registration from edit it to fit the needs of your deployment. Click Save

▼ Registration Form Settings

Assign to guest type **Self_Register_Guest** ▼

Configure guest types at:
[Work Centers > Guest Access > Configure > Guest Types](#)

Account valid for: Days ▼ Maximum: 30 DAYS

Require a registration code

Fields to include	Required
<input type="checkbox"/> User name	<input type="checkbox"/>
<input checked="" type="checkbox"/> First name	<input type="checkbox"/>
<input checked="" type="checkbox"/> Last name	<input type="checkbox"/>
<input checked="" type="checkbox"/> Email address	<input checked="" type="checkbox"/>
<input type="checkbox"/> Phone number	<input type="checkbox"/>
<input type="checkbox"/> Company	<input type="checkbox"/>
<input checked="" type="checkbox"/> Location	<input checked="" type="checkbox"/>

Guests can choose from these locations to set their time zone:

Guests see the locations list only if multiple locations are specified.
Configure guest locations at:
[Work Centers > Guest Access > Settings > Guest Locations and SSIDs](#)

SMS Service Provider

Guests can choose from these SMS providers:

- Global Default
- T-Mobile
- ATT
- Verizon

Guest see providers list only if multiple are selected
Configure SMS providers at:
[Work Centers > Guest Access > Administration > SMS Gateway Providers](#)

Person being visited

Reason for visit

Configure custom fields at:
[Work Centers > Guest Access > Settings > Custom Fields](#)

Include an AUP ▼

WEB REDIRECTION POLICY

Description

This section will go over how to use the VSA in a Policy Set in ISE, however this will not cover how to create a policy set in ISE.

1. There needs to be two authorization profiles created so configure more than one authorization profile

Navigate to “Policy>Policy Elements>Results

And Select Authorization > Authorization profiles

The screenshot shows the Aruba Identity Services Engine (ISE) web interface. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Policy' menu is expanded to show 'Policy Sets', 'Profiling', 'Posture', 'Client Provisioning', and 'Policy Elements'. The 'Policy Elements' menu is further expanded to show 'Dictionaries', 'Conditions', and 'Results'. The 'Results' menu is selected, and the 'Authorization' sub-menu is expanded to show 'Authorization Profiles', 'Downloadable ACLs', 'Profiling', 'Posture', and 'Client Provisioning'. The main content area displays the 'Standard Authorization Profiles' page, which includes a table of profiles and a list of actions (Edit, Add, Duplicate, Delete).

Name	Profile
ACL	ArubaWireless
Blackhole_Wireless_Access	Cisco
Cisco_IP_Phones	Cisco
Cisco_Temporal_Onboard	Cisco
Cisco_WebAuth	Cisco
Main_Portal_Profile	Cisco
NSP_Onboard	Cisco
Non_Cisco_IP_Phones	Cisco
VLAN1027	Cisco
VLAN1030	Cisco
Vlan 10	Cisco
Vlan 1022 Camera	Cisco
Vlan 2 Cisco	Cisco
Vlan 4	Cisco
Vlan1021	Cisco

2. Click Add , Check the “Web Redirection box”

Select “Centralized Web Auth” from the Drop down then Select the Guest Portal that was configured with the settings configured before.

Then Click Advanced attributes and select the HP-User-Role and enter in the captive portal user-role that was configured on the switch before in this case it will be “ISE-CAP-PORTAL”.

The screenshot shows the configuration page for an Authorization Profile named "Web_Auth" in the Aruba Identity Services Engine. The page is divided into several sections:

- Header:** Identity Services Engine, with navigation tabs for Home, Context Visibility, Operations, Policy (selected), Administration, and Work Centers.
- Sub-headers:** Policy Sets, Profiling, Posture, Client Provisioning, and Policy Elements (selected).
- Left Sidebar:** A navigation menu with categories: Authentication, Authorization (selected), Profiling, Posture, and Client Provisioning. Under Authorization, there are sub-items: Authorization Profiles, Downloadable ACLs, and Results.
- Main Content Area:**
 - Authorization Profile:**
 - * Name: Web_Auth
 - Description: (empty text box)
 - * Access Type: ACCESS_ACCEPT
 - Network Device Profile: HPWired_copy
 - Common Tasks:**
 - Web Redirection (CWA, MDM, NSP, CPP)
 - Centralized Web Auth (dropdown)
 - Value: Self-Registered Guest Custom (dropdown)
 - Advanced Attributes Settings:**
 - HP:HP-User-Role = ISE-CAP-PORTAL
 - Attributes Details:**
 - Access Type = ACCESS_ACCEPT
 - HP-Captive-Portal-URL = https://ip:port/portal/gateway?mac=ClientMacValue&portal=b31a9550-4125-11e9-9082-000c29217326&daysToExpiry=value&action=cwa
 - HP-User-Role = ISE-CAP-PORTAL
- Buttons:** Submit and Cancel.

- The guest user role authorization profile has to be created. Click add again Name the Authorization profile then Click Advanced Attributes to add the “HP-User-Role” VSA and Enter the “Guest_Access” user role that was configured on the switch. Then Click “Save”

The screenshot shows the Aruba Identity Services Engine (ISE) configuration interface. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The main menu includes Policy Sets, Profiling, Posture, Client Provisioning, and Policy Elements. The left sidebar shows a tree view with Authentication, Authorization (selected), Downloadable ACLs, Profiling, Posture, and Client Provisioning. The main content area is titled 'Authorization Profiles > Guest Vlan 100' and 'Authorization Profile'. The configuration fields are:

- * Name: Guest Vlan 100
- Description: (empty)
- * Access Type: ACCESS_ACCEPT
- Network Device Profile: HPWired_copy

 Below these fields is a 'Common Tasks' section with an 'ACL' checkbox. The 'Advanced Attributes Settings' section shows a configuration: HP:HP-User-Role = Guest_Access. The 'Attributes Details' section displays:

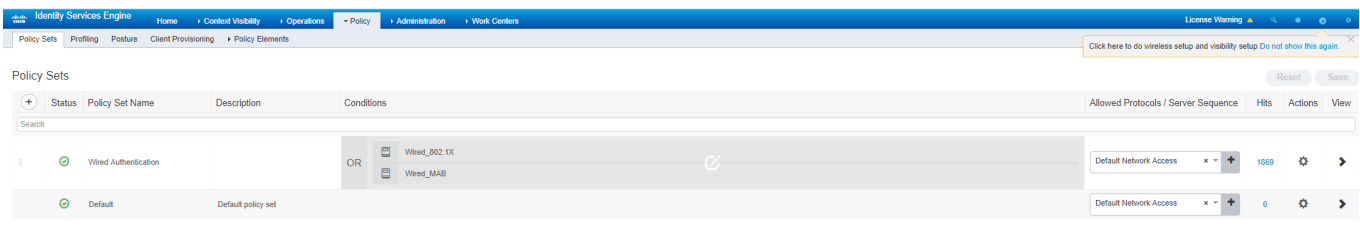
- Access Type = ACCESS_ACCEPT
- HP-User-Role = Guest_Access

 At the bottom, there are 'Save' and 'Reset' buttons.

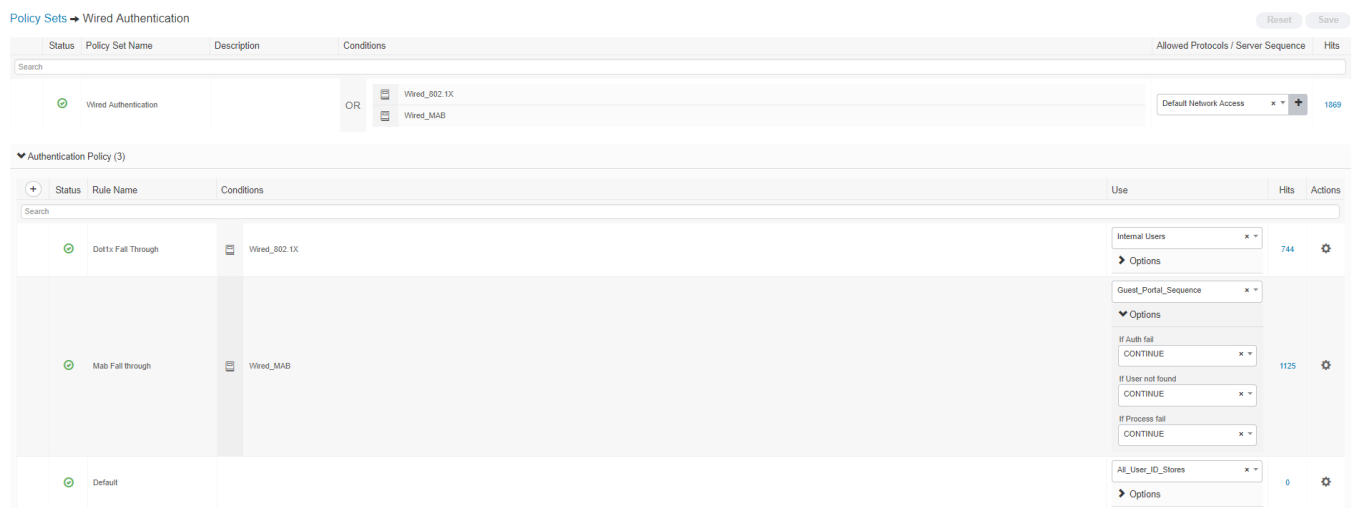
4. To create the Policy Navigate to

“Policy>Policy Sets”

In this case there is a Wired Authentication Rule to Catch all Dot1x and Mac Auth



5. Then create an authentication rule for Mac Auth Bypass so if the mac of the device cannot authenticate it will continue on to an authorization profile



6. Create two Authorization rules one rule for devices that have registered, this rule will match authenticated devices that have already registered and have been placed into the endpoint Identity Group that was created earlier in this document. Then select the authorization profile which will be the Guest Vlan 100 profile that was configured as the result to pass devices that match this condition.



- The second rule to create will be the last authorization rule which will match any devices doing Mac Auth and pass them the Web_Auth Profile that was configured before which will redirect the client to ISE

▼ Authorization Policy - Local Exceptions (3)

+	Status	Rule Name	Conditions	Results		Hits	Actions
				Profiles	Security Groups		
✎	✔	Registered Guest	IdentityGroup Name EQUALS Endpoint Identity Groups Self_Register_Guest	Guest_Vlan 100	Select from list	2	⚙
✔	✔	Local Exceptions Rule 1	Sponsor Guest identity Group	Guest_Vlan 100	Select from list	0	⚙
✎	✔	Guest Registration	Wired_MAB	Web_Auth	Select from list	1124	⚙

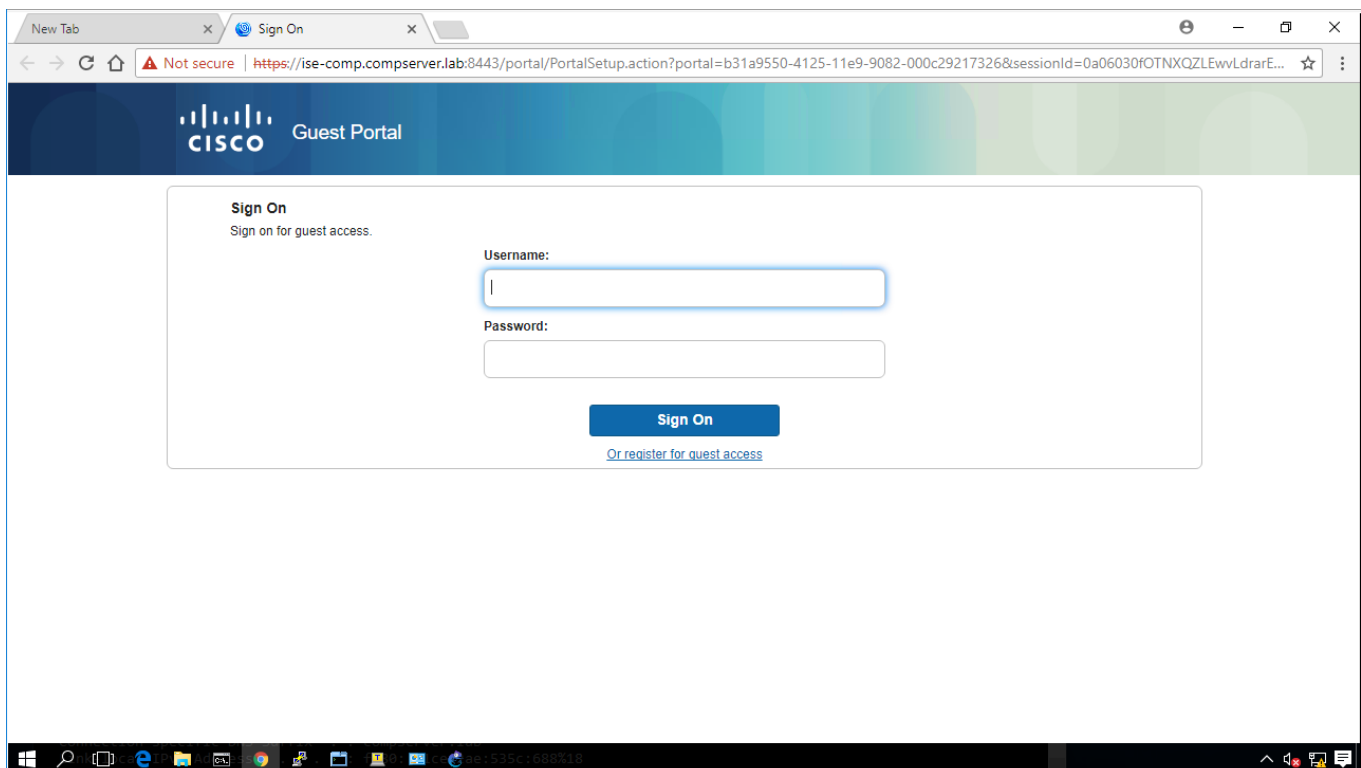
▶ Authorization Policy - Global Exceptions

▶ Authorization Policy (1)

Reset Save

VERIFICATION

The Client will get redirected to the proper web portal



The Switch will apply the proper User Role

```

172.16.8.5 - PuTTYNG
505
 1/13 00-50-B6-7... 0050b6-79bdac n/a ISE-CAP-PORTAL MAC
505

2930M-ISE (eth-1/13) #
2930M-ISE (eth-1/13) #
2930M-ISE (eth-1/13) # show port-access clients

Port Access Client Status

  Port  Client Name  MAC Address  IP Address  User Role  Type
-----
VLAN
-----
 1/11  user01      a0cec8-02a948  n/a      denyall    8021X
 1
 1/13                0050b6-79bdac  n/a      8021X
505
 1/13  00-50-B6-7... 0050b6-79bdac  n/a      ISE-CAP-PORTAL  MAC
505

2930M-ISE (eth-1/13) #
  
```

ISE will show the proper Log

→ RADIUS | Threat-Centric NAC Live Logs | TACACS | Troubleshoot | Adaptive Network Control | Reports Click here to do wireless setup at

Live Logs | Live Sessions

Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	0	0	4

Refresh Every 5 seconds Show Latest 50 re

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authentication Policy	Authorization Policy	Authorization Profiles	IP Address	Network Device	Device
Mar 15, 2019 10:57:14.813 PM	●		4	00:50:B6:79:BD:AC	00:50:B6:79:BD:AC	Windows10...	Wired Authentication >> Mab ...	Wired Authentication >> Guest Re...	Web_Auth		2930M-ISE	1/13
Mar 15, 2019 10:29:40.818 PM	●			00:50:B6:79:BD:AC	00:50:B6:79:BD:AC	Windows10...	Wired Authentication >> Mab ...	Wired Authentication >> Guest Re...	Web_Auth		2930M-ISE	1/13

Now that the client can get to the web portal create an account and make sure the client can will get CoA properly

Registration

Please complete this registration form:

First name

Clarence

Last name

Hillard

Email address*

clarence.hillard@hpe.com

Person being visited(email)

John.Smith@hpe.com

Reason for visit

Stuff

Please accept the policy: You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password. Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited. Cisco Systems reserves the right to suspend the Service if Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party. Cisco Systems reserves the right to revise, amend

Account Created

Use the following information to sign on to the network.

Username: clarence.hillard@hpe.com
Password: 7495
First name: Clarence
Last name: Hillard
Email: clarence.hillard@hpe.com
Location: San Jose

Print

Sign On

Check the Switch

172.16.8.5 - PuTTYNG

```

1
1/13          0050b6-79bdac    n/a          8021X
100
1/13 00-50-B6-7... 0050b6-79bdac    n/a          Guest_Access  MAC
100

2930M-ISE(eth-1/13)# show port-access clients

Port Access Client Status

  Port  Client Name  MAC Address      IP Address      User Role      Type
-----
VLAN
-----
1/11  user01      a0cec8-02a948    n/a             denyall        8021X
1
1/13          0050b6-79bdac    n/a             8021X
100
1/13 00-50-B6-7... 0050b6-79bdac    n/a             Guest_Access   MAC
100

2930M-ISE(eth-1/13)#

```

Check Cisco ISE

0 0 0 0 0

Refresh Every 5 seconds Show Latest 50 records Within Last 24 hours

Time	Status	Details	Repeat	Identity	Endpoint ID	Endpoint P...	Authentication Policy	Authorization Policy	Authorization Profiles	IP Address	Network Device	Device Port	Identity Group	Posture S
Mar 15, 2018 11:09:45.812 PM	✓			00:50:B6:79:BD:AC	00:50:B6:79:BD:AC	Windows10...	Wired Authentication >> Mab ...	Wired Authentication >> Register...	Guest Vlan 100		2930M-ISE	1/13	Self_Register_Guest	Posture S

TIPS

If the Client Is not getting sent to the guest VLAN after registering, a port bounce VSA can be used as well to force the client back through the authentication process.

Make sure DNS is configured for the ISE server it will use its domain name to pass to the client.