

Cisco-SW redirect Web Authen and use MAC Caching

Switch	Ports	Model	SW Version	SW Image
-----	-----	-----	-----	-----
* 1	28	WS-C2960S-24TS-L	15.0(2)SE8	C2960S-UNIVERSALK9-M

CISCO-SW CLI

```
radius-server host 192.100.10.62 key 123456
aaa new-model
aaa authorization network default group radius
aaa accounting update periodic 1
```

```
aaa server radius dynamic-author
client 192.100.10.62 server-key 123456
port 3799
auth-type all
exit
```

```
ip device tracking
ip http server
radius-server vsa send authentication
```

```
ip access-list extended redir-acl
deny udp host 0.0.0.0 host 255.255.255.255 eq bootps
deny tcp any host 192.100.10.62
permit tcp any any
```

```
interface gi1/0/1
switchport access vlan 1
switchport mode access
mab
authentication port-control auto
```

Clearpass Setup

1)

2 Services

1. MAC Authentication
2. Web Login – Web Auth

MAC Authentication Service

→ RADIUS Accept with URL-Redirect Attribute
(http://(Clearpass-IP)/guest/(page-name).php)

Web Login – Web Auth Service

→ RADIUS CoA Terminate Session

MAC Authentication Service

→ RADIUS Accept. Full Access.

Create Service for MAC Authen

Monitoring Configuration

- Start Here
- Services**
- Authentication
 - Methods
 - Sources
- Identity
 - Posture
- Enforcement
 - Policies
 - Profiles
- Network
 - Policy Simulation
 - Profile Settings

Services - Mac Auth - Mac Caching

Summary Service **Authentication** Authorization Roles Enforcement

Name: Mac Auth - Mac Caching

Description: MAC Authentication Caching

Type: MAC Authentication

Status: Enabled

Monitor Mode: ☐ Enable to monitor network access without enforcement

More Options: ☒ Authorization ☐ Audit End-hosts ☐ Profile Endpoints ☐ Accounting Proxy

Service Rule

Matches ☐ ANY or ☒ ALL of the following conditions:

Type	Name	Operator	Value
1. Connection	Client-Mac-Address	EQUALS	%{Radius:IETF:User-Name}
2. Connection	NAD-IP-Address	EQUALS	172.18.1.192
3. Click to add...			

Services - Mac Auth - Mac Caching

Summary Service **Authentication** Authorization Roles Enforcement

Authentication Methods:

[Allow All MAC AUTH]

Move Up

Move Down

Remove

View Details

Modify

--Select to Add--

Authentication Sources:

[Endpoints Repository] [Local SQL DB]

[Local User Repository] [Local SQL DB]

AD-Zenith [Active Directory]

Move Up

Move Down

Remove

View Details

Modify

--Select to Add--

Strip Username Rules: ☐ Enable to specify a comma-separated list of rules to strip username prefixes or suffixes

- need [Allow All MAC Auth]
- Endpoints Repository needs for check MAC Caching [Endpoint know or unknow]

Services - Mac Auth - Mac Caching

Summary	Service	Authentication	Authorization	Roles	Enforcement								
<div>Authorization Details:</div> <div> <div>Authorization sources from which role mapping attributes are fetched (for each Authentication Source)</div> <table border="1"> <thead> <tr> <th>Authentication Source</th> <th>Attributes Fetched From</th> </tr> </thead> <tbody> <tr> <td>1. [Endpoints Repository] [Local SQL DB]</td> <td>[Endpoints Repository] [Local SQL DB]</td> </tr> <tr> <td>2. [Local User Repository] [Local SQL DB]</td> <td>[Local User Repository] [Local SQL DB]</td> </tr> <tr> <td>3. AD-Zenith [Active Directory]</td> <td>AD-Zenith [Active Directory]</td> </tr> </tbody> </table> </div> <div> <div>Additional authorization sources from which to fetch role-mapping attributes -</div> <div> <div> <div>[Time Source] [Local SQL DB]</div> <div>[Guest User Repository] [Local SQL DB]</div> <div>[Local User Repository] [Local SQL DB]</div> <div>AD-Zenith [Active Directory]</div> <div>--Select to Add--</div> </div> <div> <div>Remove</div> <div>View Details</div> <div>Modify</div> </div> </div> <div>Add new #</div> </div>						Authentication Source	Attributes Fetched From	1. [Endpoints Repository] [Local SQL DB]	[Endpoints Repository] [Local SQL DB]	2. [Local User Repository] [Local SQL DB]	[Local User Repository] [Local SQL DB]	3. AD-Zenith [Active Directory]	AD-Zenith [Active Directory]
Authentication Source	Attributes Fetched From												
1. [Endpoints Repository] [Local SQL DB]	[Endpoints Repository] [Local SQL DB]												
2. [Local User Repository] [Local SQL DB]	[Local User Repository] [Local SQL DB]												
3. AD-Zenith [Active Directory]	AD-Zenith [Active Directory]												

- Time Source needs for check expire of endpoint (MAC Caching)

Services - Mac Auth - Mac Caching

Summary	Service	Authentication	Authorization	Roles	Enforcement				
<div>Use Cached Results: <input type="checkbox"/> Use cached Roles and Posture attributes from previous sessions</div> <div> <div>Enforcement Policy:</div> <div>MAC Caching Enforcement</div> <div>Modify</div> </div>									
<div>Enforcement Policy Details</div> <div> <div>Description:</div> <div>Default Profile: Cisco Web Auth</div> <div>Rules Evaluation Algorithm: first-applicable</div> </div>									
<table border="1"> <thead> <tr> <th>Conditions</th> <th>Enforcement Profiles</th> </tr> </thead> <tbody> <tr> <td>1. (Authorization:[Endpoints Repository]:Status EQUALS Known)</td> <td>[Allow Access Profile]</td> </tr> </tbody> </table>						Conditions	Enforcement Profiles	1. (Authorization:[Endpoints Repository]:Status EQUALS Known)	[Allow Access Profile]
Conditions	Enforcement Profiles								
1. (Authorization:[Endpoints Repository]:Status EQUALS Known)	[Allow Access Profile]								

- Endpoint status = Known means this endpoint (MAC) already success to login with Web Authen
- Cisco Web Auth for whole client not yet login with Web Authen , see figure as below

Enforcement Profiles - Cisco Web Auth

Summary	Profile	Attributes
Profile:		
Name:	Cisco Web Auth	
Description:		
Type:	RADIUS	
Action:	Accept	
Device Group List:	-	
Attributes:		
Type	Name	Value
1. Radius: Cisco	Cisco-AVPair	= url-redirect-acl=redir-acl
2. Radius: Cisco	Cisco-AVPair	= url-redirect=http://192.100.10.62/guest/login.php?mac=%{Connection:Client-Mac-Address-Colon}

url-redirect-acl=redir-acl (follow ACL of SW)

url-redirect=http://192.100.10.62/guest/login.php?mac=%{Connection:Client-Mac-Address-Colon}

2) Create Service for Web Authen to Enforce Endpoint to known

Services - Web Auth - User login

Summary	Service	Authentication	Roles	Enforcement
Name:	Web Auth - User login			
Description:				
Type:	Web-based Authentication			
Status:	Enabled			
Monitor Mode:	<input type="checkbox"/> Enable to monitor network access without enforcement			
More Options:	<input type="checkbox"/> Authorization <input type="checkbox"/> Posture Compliance			
Service Rule				
Matches <input checked="" type="radio"/> ANY or <input type="radio"/> ALL of the following conditions:				
Type	Name	Operator	Value	
1.	Click to add...			

- Select Type = Web-based Authentication

Because this service for client login Captive-portal direct with Clearpass (not login with SW)

Services - Web Auth - User login

Summary	Service	Authentication	Roles	Enforcement
Authentication Sources:				
		AD-Zenith [Active Directory] [Guest User Repository] [Local SQL DB] [Local User Repository] [Local SQL DB]	Move Up Move Down Remove View Details Modify	
		--Select to Add--		
Strip Username Rules:				
		<input type="checkbox"/> Enable to specify a comma-separated list of rules to strip use		

Services - Web Auth - User login

Summary	Service	Authentication	Roles	Enforcement
Use Cached Results:	<input type="checkbox"/> Use cached Roles and Posture attributes from previous sessions			
Enforcement Policy:	web succ		Modify	Add new Enforc
Enforcement Policy Details				
Description:				
Default Profile:	[Cisco - Terminate Session]			
Rules Evaluation Algorithm:	first-applicable			
Conditions	Enforcement Profiles			
1. (Authentication:Username EXISTS)	[Update Endpoint Known], [Cisco - Terminate Session]			

- [Update Endpoint Known] = Enforce CPPM keep MAC to Endpoint Known
- [Cisco - Terminate session] = terminate client to re-authen with MAC again

You must create Web_login page to appropriate with your url-redirect and Select Vendor Setting = "Captive portal with Clearpass Web Auth"

Guest

Onboard

Configuration

Start Here

Advertising

Authentication

Content Manager

Guest Manager

Hotspot Manager

Transaction Processors

Pages

Web Logins

Receipts

SMS Services

Translations

Home » Configuration » Pages » Web Logins

Web Login (login-cisco)

Use this form to make changes to the Web Login **login-cisco**.

* Name:

login-cisco

Enter a name for this web login page.

Page Name:

login

Enter a page name for this web login.
The web login will be accessible from "/guest/page_name.php".

Description:

Comments or descriptive text about the web login.

* Vendor Settings:

Captive portal with ClearPass Web Auth

Select a predefined group of settings suitable for standard network configurations.

Login Form

Options for specifying the behaviour and content of the login form.

Authentication:

Credentials – Require a username and password

Select the authentication requirement.
Access Code requires a single code (username) to be entered.
Anonymous allows a blank form requiring just the terms or a Log In button. A pre-existing account is required.
Auto is similar to anonymous but the page is automatically submitted.
Access Code and Anonymous require the account to have the Username Authentication field set.

Prevent CNA:

☒ Enable bypassing the Apple Captive Network Assistant

The Apple Captive Network Assistant (CNA) is the pop-up browser shown when joining a network that has a captive portal.
Note that this option may not work with all vendors, depending on how the captive portal is implemented.

☐ Provide a custom login form

3) How to Track

Switch#show authentication session

Interface	MAC Address	Method	Domain	Status	Session ID
Gi1/0/1	f0de.f1f8.ce20	mab	DATA	Authz Success	AC1201C0000000200082E3C2

Monitoring » Live Monitoring » **Access Tracker**

Access Tracker Nov 19, 2015 16:16:21 ICT

Request Details

Summary Input **Output** Accounting Alerts

Enforcement Profiles: Cisco Web Auth

System Posture Status: UNKNOWN (100)

Audit Posture Status: UNKNOWN (100)

RADIUS Response

Radius:Cisco:Cisco-AVPair url-redirect-acl=redir-acl

Radius:Cisco:Cisco-AVPair url-redirect=http://192.100.10.62/guest/login.php?mac=f0:de:f1:f8:ce:20

- Client should be redirect to Captive portal from CPPM

192.100.10.62/guest/login.php?mac=f0:de:f1:f8:ce:20&_browser=1

Please login to the network using your username and password.

Nothing to lose

Username:

Password:

Contact a staff member if you are experiencing difficulty logging in.

- After user post credential for this Captive portal
If you see like exam below , it work ...

#	Server	Source	Username	Service	Login Status
1.	192.100.10.62	RADIUS	f0def1f8ce20	Mac Auth - Mac Caching	ACCEPT
2.	192.100.10.62	WEBAUTH	openall	Web Auth - User login	ACCEPT

Request Details

Summary Input **Output**

Enforcement Profiles: [Update Endpoint Known], [Cisco - Terminate Session]

System Posture Status: UNKNOWN (100)

Audit Posture Status: UNKNOWN (100)

RADIUS Response

Radius:IETF:Calling-Station-Id F0-DE-F1-F8-CE-20

Radius:IETF:Service-Type 1

Status-Update:Endpoint Known

#	Server	Source	Username	Service	Login St
1.	192.100.10.62	RADIUS	f0def1f8ce20	Mac Auth - Mac Caching	ACCEPT
2.	192.100.10.62	WEBAUTH	openall	Web Auth - User login	ACCEPT

Request Details

Summary	Input	Output	Accounting	Alerts
---------	-------	--------	------------	--------

Username:	f0def1f8ce20
End-Host Identifier:	F0-DE-F1-F8-CE-20 (Computer / Windows / Windows)
Access Device IP/Port:	172.18.1.192:50101 (cisco-sw / Cisco)

RADIUS Request

Authorization Attributes

Authorization:[Endpoints Repository]:IsProfiled	true
Authorization:[Endpoints Repository]:MAC Vendor	Wistron InfoComm (Kunshan)Co
Authorization:[Endpoints Repository]:Status	Known
Authorization:[Endpoints Repository]:Unique-Device-Count	1
Authorization:[Time Source]:Now DT	2015-11-19 16:00:00
Authorization:[Time Source]:One Day DT	2015-11-20 16:00:00
Authorization:[Time Source]:One Month DT	2015-12-19 16:00:00
Authorization:[Time Source]:One Week DT	2015-11-26 16:00:00
Authorization:[Time Source]:Six Months DT	2016-05-19 16:00:00

- Option : Time Source need for limit expire for MAC Caching

Configuration » Identity » Endpoints
Endpoints

Filter: MAC Address contains ce20 Go Clear Filter

#	MAC Address	Hostname	Device Category	Device OS Family	Status
1.	f0def1f8ce20		Computer	Windows	Known

Showing 1-1 of 1

Authentication Records Trigger Server Action Update F