Credocom

WHEN IT HAS TO BE SAFE

How to wired Cisco MAC Caching

Bo Nielsen, CCIE #53075 (Sec)

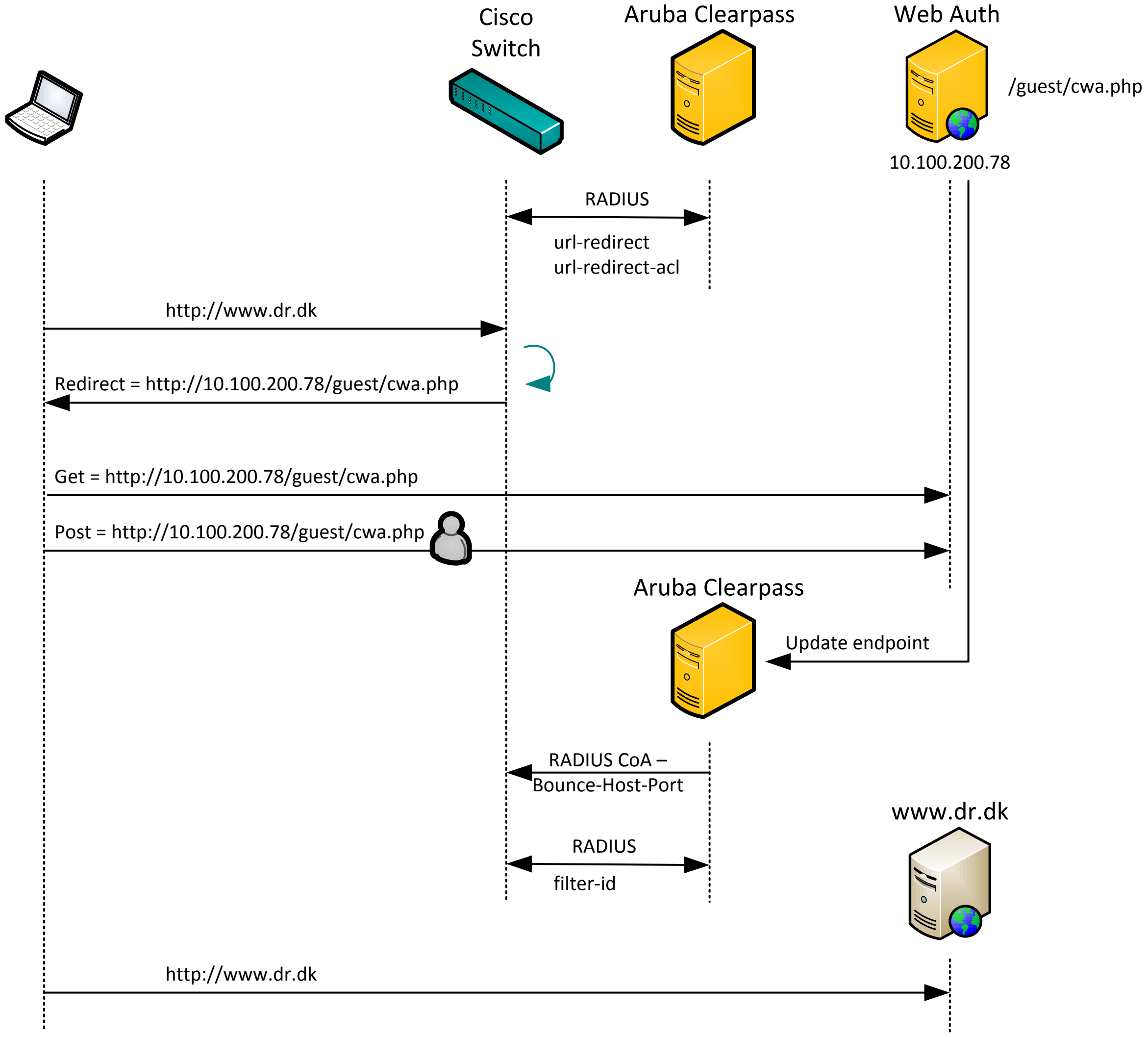
Oktober 2016, V1.00

Overview

The principle is that a guest user is created in advanced on Aruba ClearPass Guest and then the user connects his computer to the wired network. The first time the user tries to access a web page on port 80, the user is sent to a captive portal. The user enters his login on the captive portal, and the web application on Aruba ClearPass will add some parameters to the endpoints MAC address.

The next time the user's computer connects to the wired network, the MAC address is approved for guest access. The guest access can be given as an access list or a VLAN for guests on the switch. In this guide I will use the guest access based on an access list.

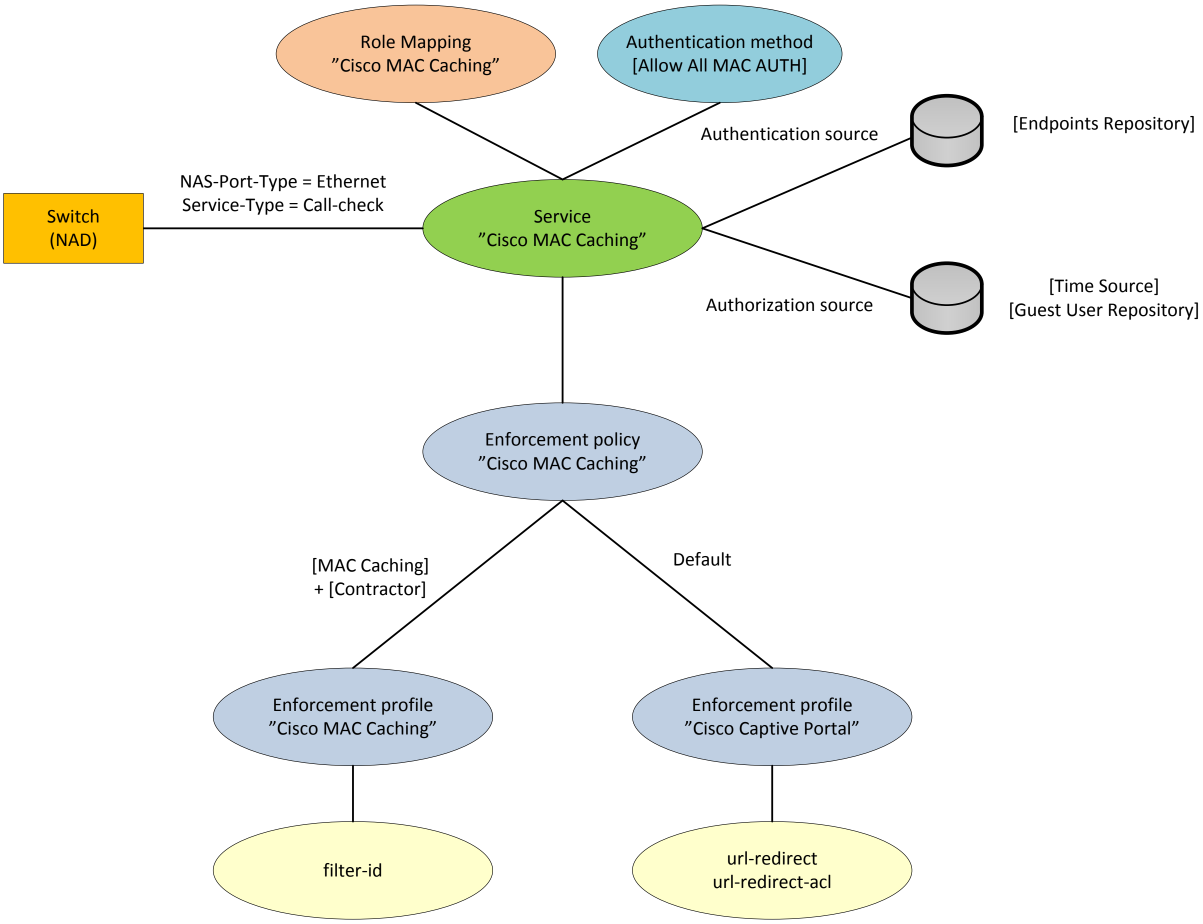
The provision flow for MAC address caching is illustrated here:



Captive portal in Aruba ClearPass will be set to *Server-Initiated*, and this web application on Aruba ClearPass will handle the provisioning of the user's endpoint along with a CoA to the switch.

Aruba Clearpass RADIUS

An overview of the service rules enforcement policy and profiles:



RADIUS attribute *Filter-Id* provides access to the network after provision.

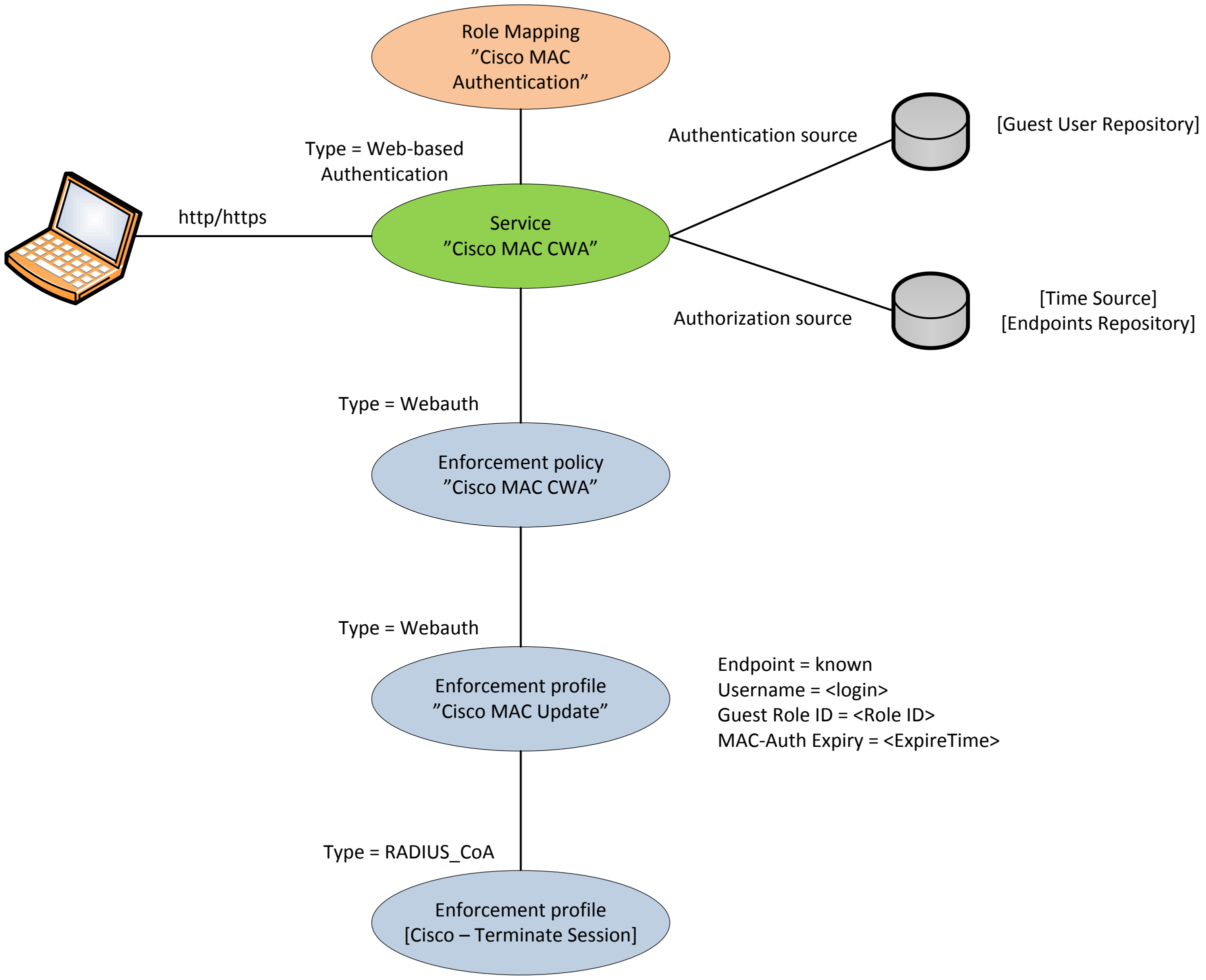
Before provision a static access list is used as *authentication open* to the interface.
URL redirection parameters are created as (case sensitive):

Cisco-AVPair	Værdi
url-redirect	http://10.100.200.78/guest/cwa.php?mac=%{Connection:Client-Mac-Address-NoDelim}
url-redirect-acl	ACL-redirect

The web application on Aruba ClearPass is set to the URL **/guest/cwa.php**.

Aruba Clearpass Webapplikation

An overview of the service rules enforcement policy and profiles:

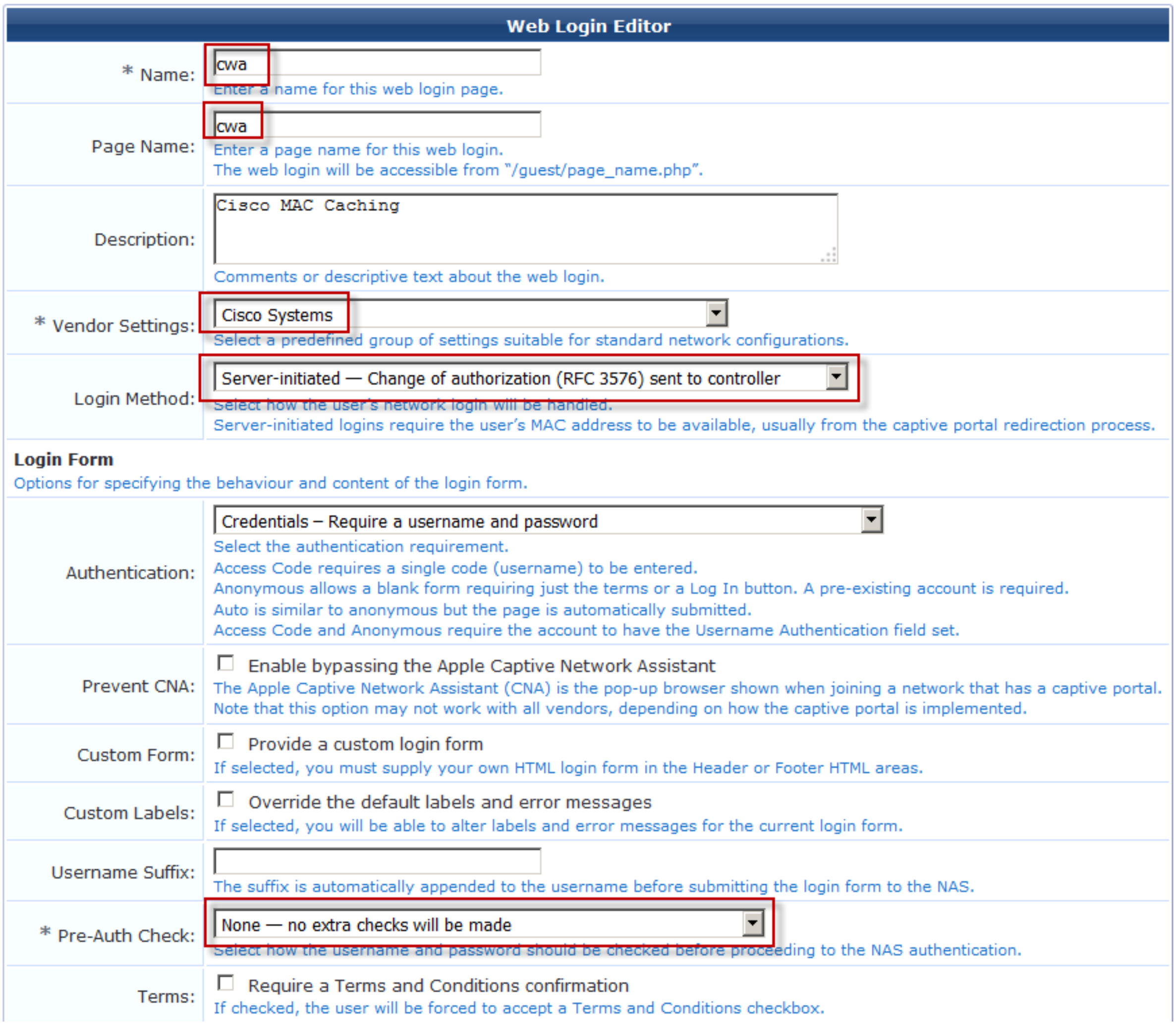


Before approval the status of Endpoint is *unknown*, and this status is used in the role mapping by RADIUS authentication to determine whether the user will be sent to the captive portal or not.

Note: There will be an alert in Access Tracker when role mapping is performed for a MAC address that is not provisioned. This is because the attributes of the endpoint is not available until after provision is completed.

Web page for the captive portal (server initiated)

Configuration -> Pages -> Web Logins



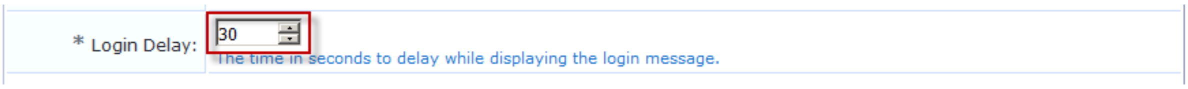
Web Login Editor

* Name:	cwa Enter a name for this web login page.
Page Name:	cwa Enter a page name for this web login. The web login will be accessible from "/guest/page_name.php".
Description:	Cisco MAC Caching Comments or descriptive text about the web login.
* Vendor Settings:	Cisco Systems Select a predefined group of settings suitable for standard network configurations.
Login Method:	Server-initiated — Change of authorization (RFC 3576) sent to controller Select how the user's network login will be handled. Server-initiated logins require the user's MAC address to be available, usually from the captive portal redirection process.

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.
Custom Form:	☐ Provide a custom login form If selected, you must supply your own HTML login form in the Header or Footer HTML areas.
Custom Labels:	☐ Override the default labels and error messages If selected, you will be able to alter labels and error messages for the current login form.
Username Suffix:	The suffix is automatically appended to the username before submitting the login form to the NAS.
* Pre-Auth Check:	None — no extra checks will be made Select how the username and password should be checked before proceeding to the NAS authentication.
Terms:	☐ Require a Terms and Conditions confirmation If checked, the user will be forced to accept a Terms and Conditions checkbox.

There is also added a delay, and the delay is necessary when the CoA is set to port bounce. The port bounce will cause some delay before the endpoint is re-authenticated after provisioning.



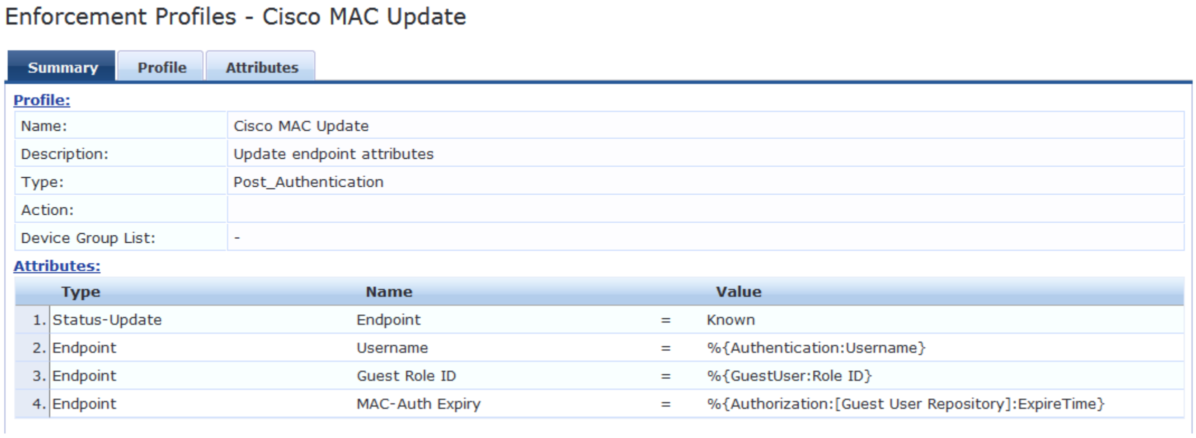
* Login Delay:	30 The time in seconds to delay while displaying the login message.

Enforcement profiles for the web application

Captive Portal, where logon is approved, creates the following attributes to the user's endpoint:

- Status = known
- Username = <guest login name>
- Guest Role ID = <guest role ID>
- MAC-Auth expiry = <guest expire date>

Configuration -> Enforcement -> Profiles



Enforcement Profiles - Cisco MAC Update

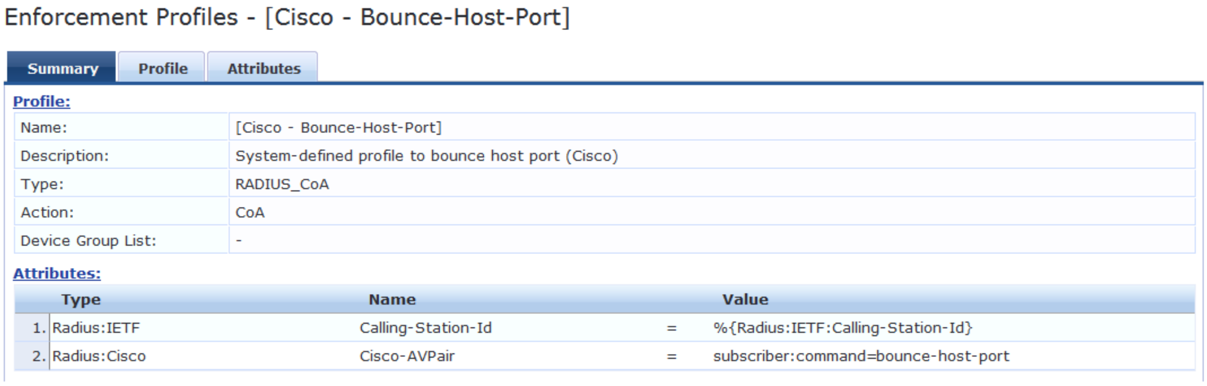
Profile:

Name:	Cisco MAC Update
Description:	Update endpoint attributes
Type:	Post_Authentication
Action:	
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Status-Update	Endpoint	=	Known
2.	Endpoint	Username	=	%{Authentication:Username}
3.	Endpoint	Guest Role ID	=	%{GuestUser:Role ID}
4.	Endpoint	MAC-Auth Expiry	=	%{Authorization:[Guest User Repository]:ExpireTime}

RADIUS CoA is already created by the system:



Enforcement Profiles - [Cisco - Bounce-Host-Port]

Profile:

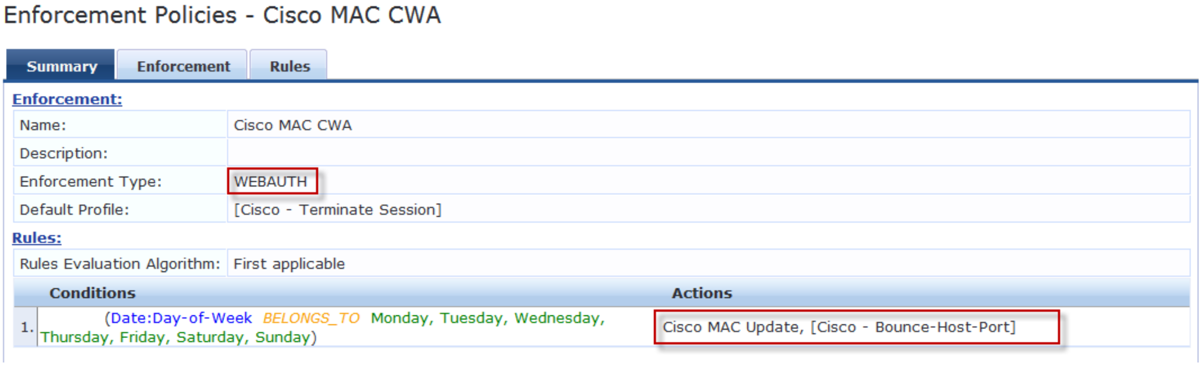
Name:	[Cisco - Bounce-Host-Port]
Description:	System-defined profile to bounce host port (Cisco)
Type:	RADIUS_CoA
Action:	CoA
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:IETF	Calling-Station-Id	=	%{Radius:IETF:Calling-Station-Id}
2.	Radius:Cisco	Cisco-AVPair	=	subscriber:command=bounce-host-port

Enforcement policy for the web application

Configuration -> Enforcement -> Policies



Enforcement Policies - Cisco MAC CWA

Enforcement:

Name:	Cisco MAC CWA
Description:	
Enforcement Type:	WEBAUTH
Default Profile:	[Cisco - Terminate Session]

Rules:

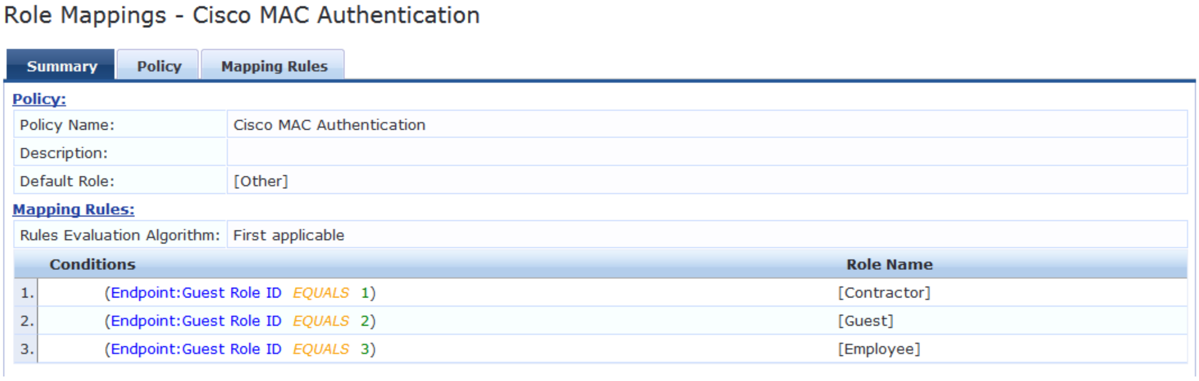
Rules Evaluation Algorithm:	First applicable

	Conditions	Actions
1.	(Date:Day-of-Week BELONGS_TO Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday)	Cisco MAC Update, [Cisco - Bounce-Host-Port]

Role mapping for the web application

The role mapping is used to update the attribute *Endpoint: Guest Role ID* and the update is done from the Post_authentication method.

Configuration -> Identity -> Role Mappings



Role Mappings - Cisco MAC Authentication

Policy:

Policy Name:	Cisco MAC Authentication
Description:	
Default Role:	[Other]

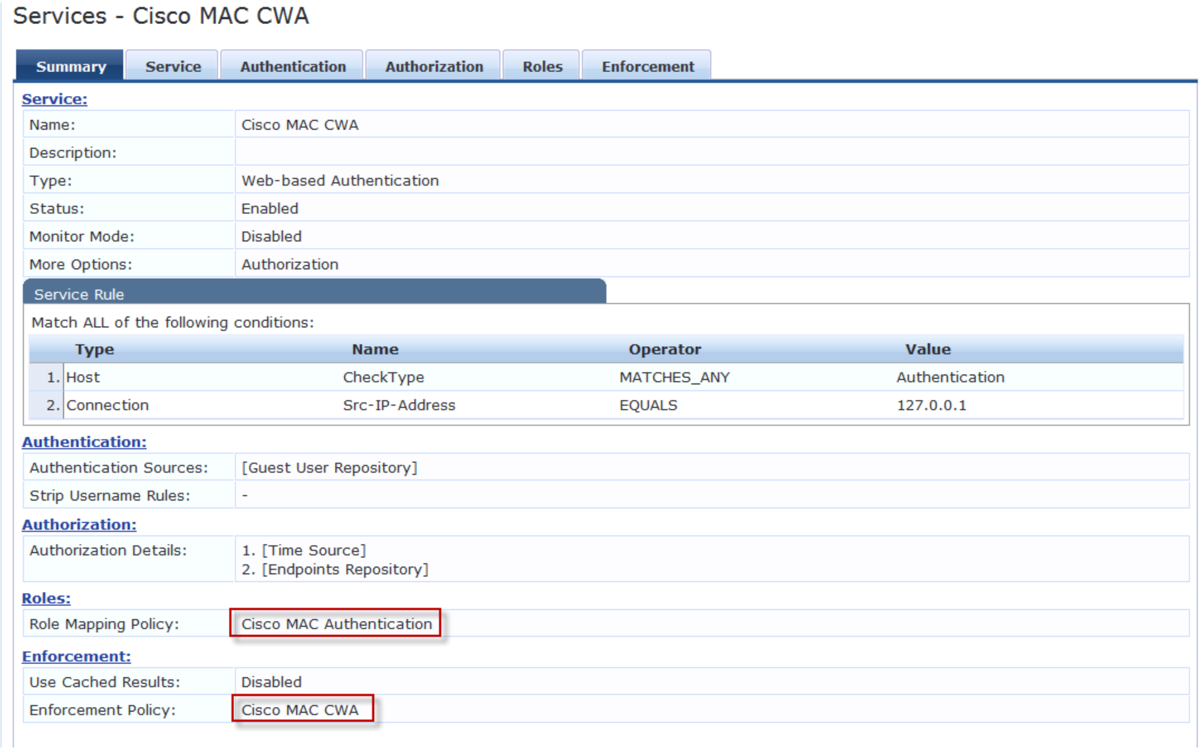
Mapping Rules:

Rules Evaluation Algorithm:	First applicable

	Conditions	Role Name
1.	(Endpoint:Guest Role ID EQUALS 1)	[Contractor]
2.	(Endpoint:Guest Role ID EQUALS 2)	[Guest]
3.	(Endpoint:Guest Role ID EQUALS 3)	[Employee]

Service rule for the web application

Configuration -> Services



Services - Cisco MAC CWA

Service:

Name:	Cisco MAC CWA
Description:	
Type:	Web-based Authentication
Status:	Enabled
Monitor Mode:	Disabled
More Options:	Authorization

Service Rule

Match ALL of the following conditions:

	Type	Name	Operator	Value
1.	Host	CheckType	MATCHES_ANY	Authentication
2.	Connection	Src-IP-Address	EQUALS	127.0.0.1

Authentication:

Authentication Sources:	[Guest User Repository]
Strip Username Rules:	-

Authorization:

Authorization Details:	1. [Time Source] 2. [Endpoints Repository]

Roles:

Role Mapping Policy:	Cisco MAC Authentication

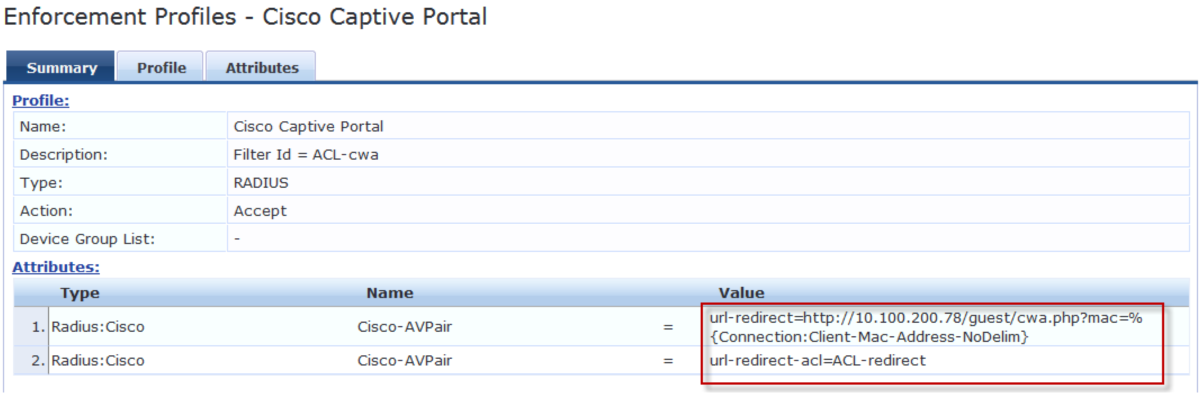
Enforcement:

Use Cached Results:	Disabled
Enforcement Policy:	Cisco MAC CWA

Enforcement profiles for RADIUS

Configuration -> Enforcement -> Profiles

Before MAC Caching



Enforcement Profiles - Cisco Captive Portal

Profile:

Name:	Cisco Captive Portal
Description:	Filter Id = ACL-cwa
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:Cisco	Cisco-AVPair	=	url-redirect=http://10.100.200.78/guest/cwa.php?mac=%{Connection:Client-Mac-Address-NoDelim}
2.	Radius:Cisco	Cisco-AVPair	=	url-redirect-acl=ACL-redirect

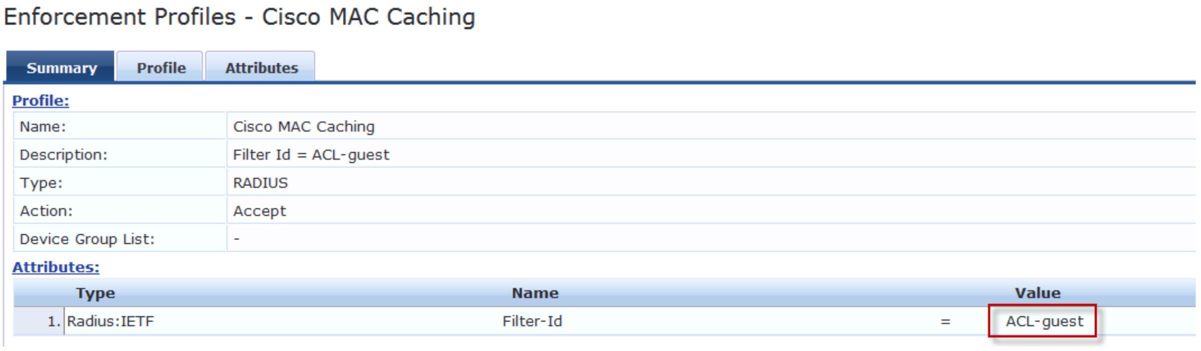
The access list to the url-redirect is reversed. It should be understood in the sense that the permit statement is the traffic that should be redirected. Deny statement in this usage will not reject traffic, but a Deny statement will not allow redirection. The access list for redirect looks like this:

```
ip access-list extended ACL-redirect
 deny   tcp any host 10.100.200.78 eq www
 deny   tcp any host 10.100.200.78 eq 443
 permit tcp any any eq www
 permit tcp any any eq 443
 deny   ip any any
```

The first two Deny rules prevents that access to captive portal will not be redirected. Please note, that the http(s) server has to run on the switch in order to do the URL-redirection:

```
ip http server
ip http secure-server
```

After MAC Caching



Enforcement Profiles - Cisco MAC Caching

Profile:

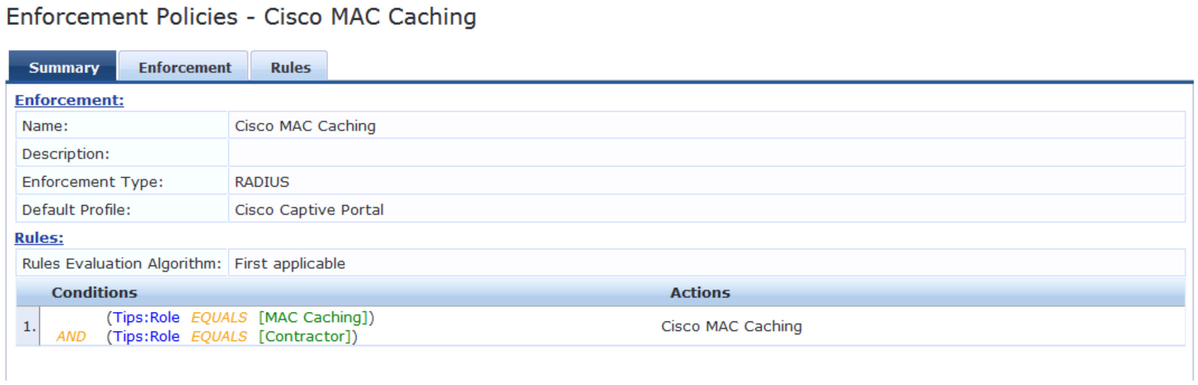
Name:	Cisco MAC Caching
Description:	Filter Id = ACL-guest
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:IETF	Filter-Id	=	ACL-guest

Enforcement policy for RADIUS

Configuration -> Enforcement -> Policies



Enforcement Policies - Cisco MAC Caching

Enforcement:

Name:	Cisco MAC Caching
Description:	
Enforcement Type:	RADIUS
Default Profile:	Cisco Captive Portal

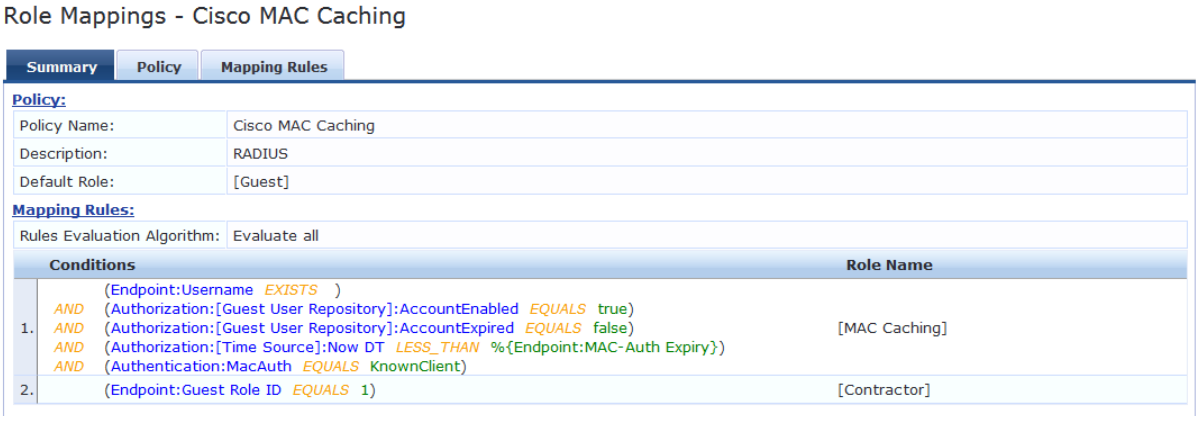
Rules:

Rules Evaluation Algorithm:	First applicable

	Conditions	Actions
1.	(Tips:Role EQUALS [MAC Caching]) AND (Tips:Role EQUALS [Contractor])	Cisco MAC Caching

Role mapping for RADIUS

Configuration -> Identity -> Role Mappings



Role Mappings - Cisco MAC Caching

Policy:

Policy Name:	Cisco MAC Caching
Description:	RADIUS
Default Role:	[Guest]

Mapping Rules:

Rules Evaluation Algorithm:	Evaluate all

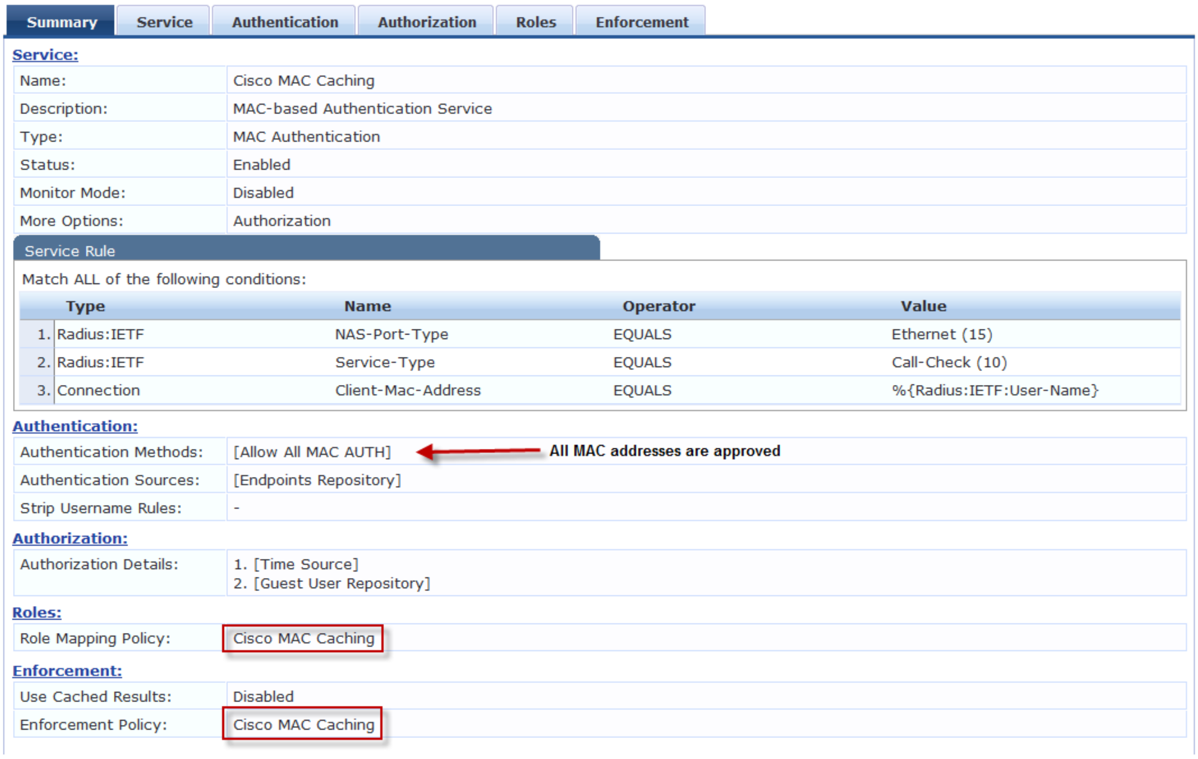
	Conditions	Role Name
1.	(Endpoint:Username EXISTS) AND (Authorization:[Guest User Repository]:AccountEnabled EQUALS true) AND (Authorization:[Guest User Repository]:AccountExpired EQUALS false) AND (Authorization:[Time Source]:Now DT LESS_THAN %{Endpoint:MAC-Auth Expiry}) AND (Authentication:MacAuth EQUALS KnownClient)	[MAC Caching]
2.	(Endpoint:Guest Role ID EQUALS 1)	[Contractor]

Please note that the role [Contractor] is derived from the Endpoint attribute *Role ID*.

Service rule for RADIUS

Configuration -> Services

Services - Cisco MAC Caching



Service:

Name:	Cisco MAC Caching
Description:	MAC-based Authentication Service
Type:	MAC Authentication
Status:	Enabled
Monitor Mode:	Disabled
More Options:	Authorization

Service Rule

Match ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	EQUALS	Ethernet (15)
2.	Radius:IETF	Service-Type	EQUALS	Call-Check (10)
3.	Connection	Client-Mac-Address	EQUALS	%{Radius:IETF:User-Name}

Authentication:

Authentication Methods:	[Allow All MAC AUTH]
Authentication Sources:	[Endpoints Repository]
Strip Username Rules:	-

All MAC addresses are approved

Authorization:

Authorization Details:	1. [Time Source] 2. [Guest User Repository]

Roles:

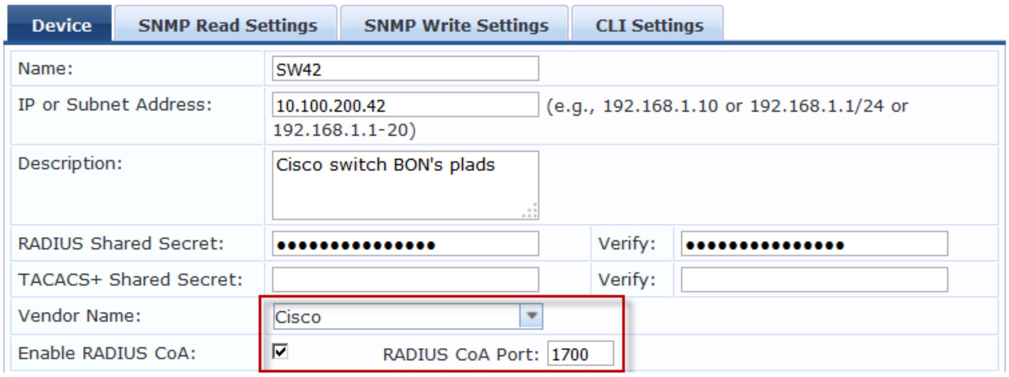
Role Mapping Policy:	Cisco MAC Caching

Enforcement:

Use Cached Results:	Disabled
Enforcement Policy:	Cisco MAC Caching

Device

Configuration -> Network -> Devices



Name:	SW42		
IP or Subnet Address:	10.100.200.42 (e.g., 192.168.1.10 or 192.168.1.1/24 or 192.168.1.1-20)		
Description:	Cisco switch BON's plads		
RADIUS Shared Secret:	●●●●●●●●●●●●●●●	Verify:	●●●●●●●●●●●●●●●
TACACS+ Shared Secret:		Verify:	
Vendor Name:	Cisco		
Enable RADIUS CoA:	☑ RADIUS CoA Port: 1700		

Cisco konfiguration

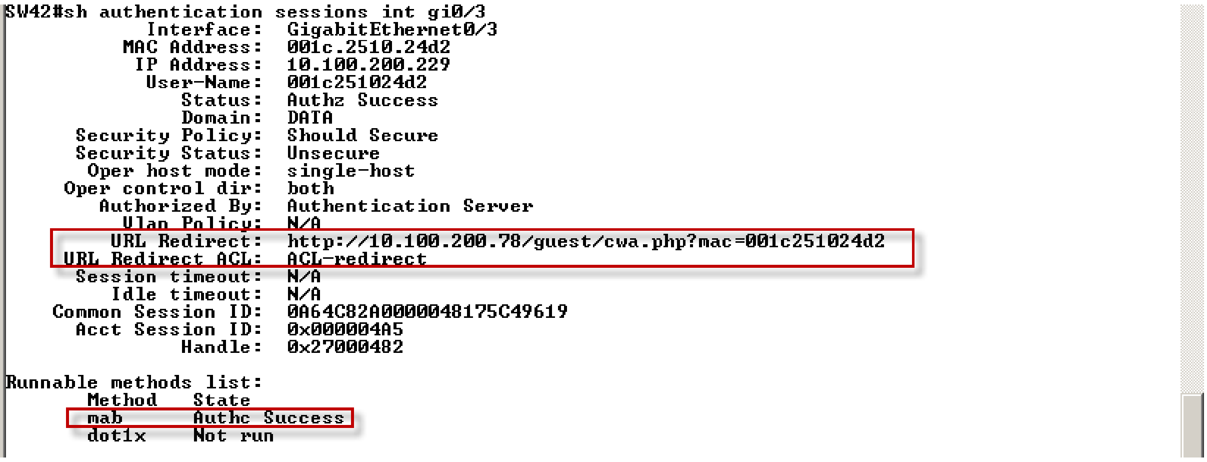
IP address of Aruba ClearPass is 10,100,200.78, and RADIUS key is set to "Aruba123".

```
aaa new-model

radius server CP01
 address ipv4 10.100.200.78 auth-port 1812 acct-port 1813
 key Aruba123

aaa group server radius CP
 server name CP01
aaa server radius dynamic-author
 client 10.100.200.78 server-key Aruba123

aaa authentication dot1x default group CP
aaa authorization network default group CP
aaa accounting dot1x default start-stop group CP

ip device tracking
dot1x system-auth-control

ip http server
ip http secure-server

radius-server attribute 11 default direction in
radius-server vsa send accounting
radius-server vsa send authentication

ip access-list extended ACL-cwa
 permit udp any any eq domain
 permit udp any any eq bootps
 permit tcp any any eq www
 permit tcp any any eq 443

ip access-list extended ACL-guest
 permit udp any any eq domain
 deny   ip any 10.0.0.0 0.255.255.255
 deny   ip any 192.168.0.0 0.0.255.255
 deny   ip any 172.16.0.0 0.15.255.255
 permit ip any any

ip access-list extended ACL-redirect
 deny   tcp any host 10.100.200.78 eq www
 deny   tcp any host 10.100.200.78 eq 443
 permit tcp any any eq www
 permit tcp any any eq 443
 deny   ip any any

interface GigabitEthernet <interface-id>
 switchport mode access
 ip access-group ACL-cwa in
 authentication open
 authentication order mab dot1x
 authentication priority dot1x mab
 authentication port-control auto
 authentication violation restrict
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 3
 spanning-tree portfast
```

Verification

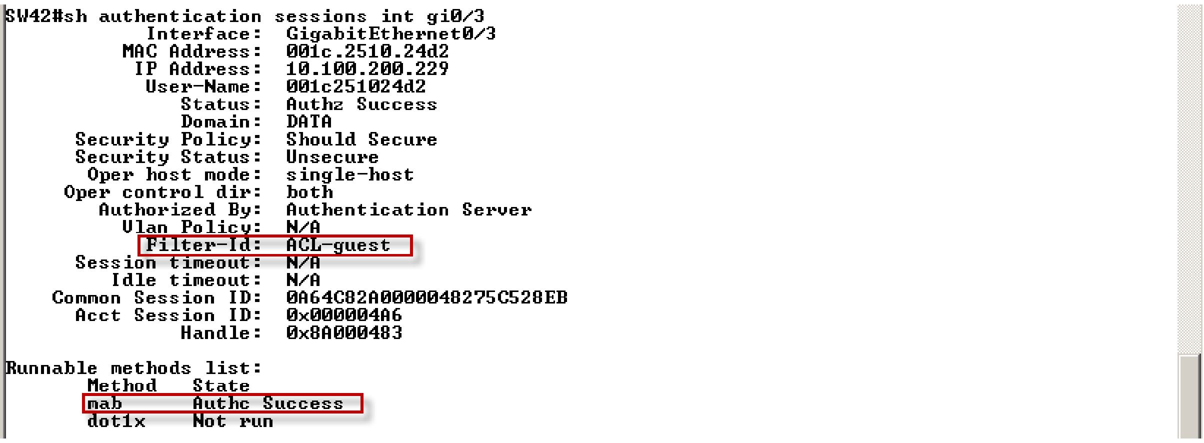
Cisco switch

Before provision



```
SW42#sh authentication sessions int gi0/3
            Interface:  GigabitEthernet0/3
          MAC Address:  001c.2510.24d2
           IP Address:  10.100.200.229
            User-Name:  001c251024d2
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  single-host
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  N/A
         URL Redirect:  http://10.100.200.78/guest/cwa.php?mac=001c251024d2
     URL Redirect ACL:  ACL-redirect
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A64C82A0000048175C49619
      Acct Session ID:  0x000004A5
               Handle:  0x27000482

Runnable methods list:
       Method   State
       mab      Authc Success
       dot1x    Not run
```

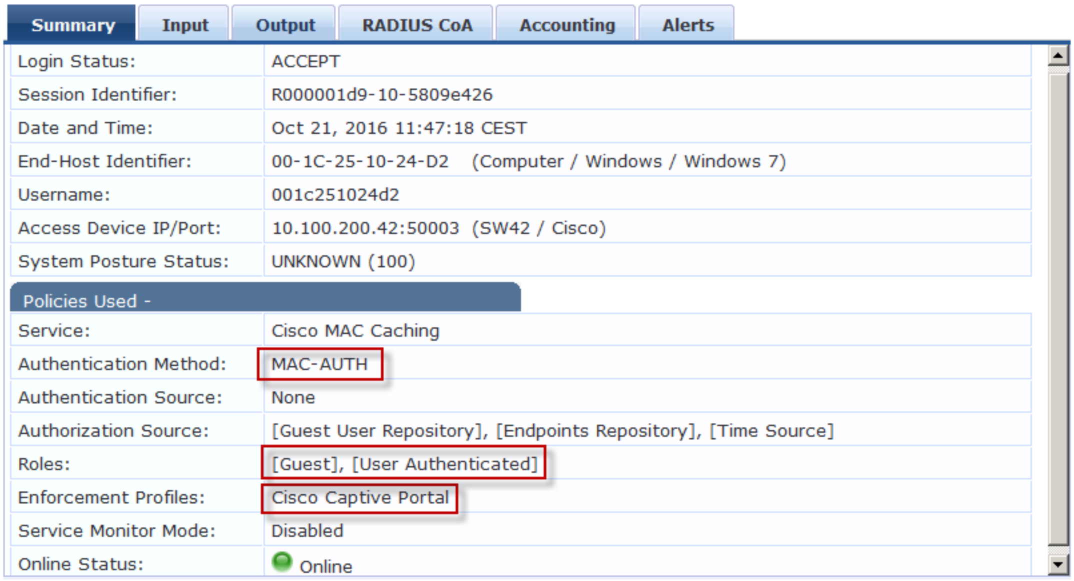
After provision



```
SW42#sh authentication sessions int gi0/3
            Interface:  GigabitEthernet0/3
          MAC Address:  001c.2510.24d2
           IP Address:  10.100.200.229
            User-Name:  001c251024d2
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  single-host
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  N/A
            Filter-Id:  ACL-guest
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A64C82A0000048275C528EB
      Acct Session ID:  0x000004A6
               Handle:  0x8A000483

Runnable methods list:
       Method   State
       mab      Authc Success
       dot1x    Not run
```

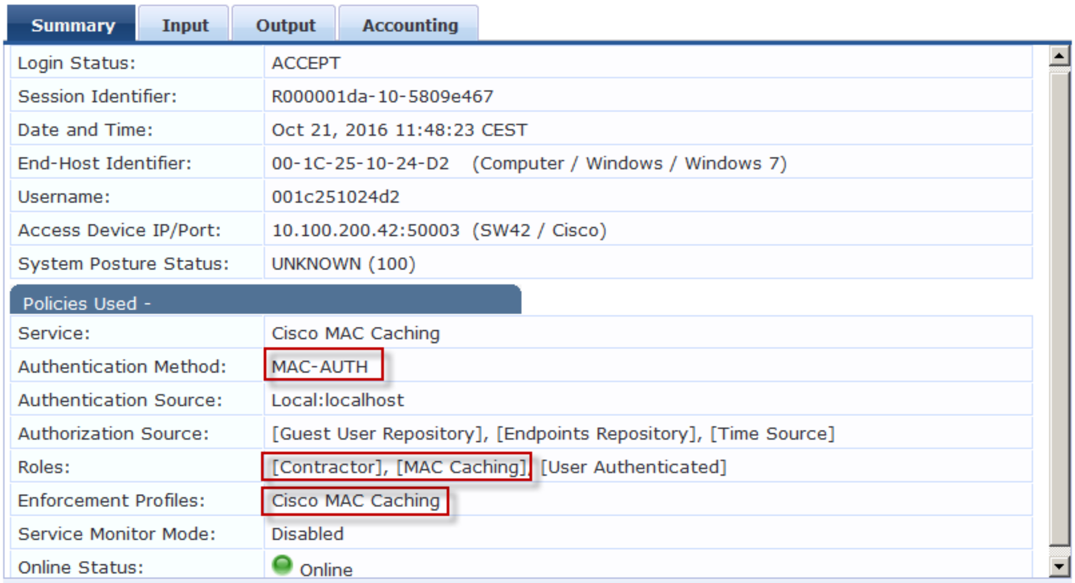
Access-tracker

Before provision



Login Status:	ACCEPT
Session Identifier:	R000001d9-10-5809e426
Date and Time:	Oct 21, 2016 11:47:18 CEST
End-Host Identifier:	00-1C-25-10-24-D2 (Computer / Windows / Windows 7)
Username:	001c251024d2
Access Device IP/Port:	10.100.200.42:50003 (SW42 / Cisco)
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	Cisco MAC Caching
Authentication Method:	MAC-AUTH
Authentication Source:	None
Authorization Source:	[Guest User Repository], [Endpoints Repository], [Time Source]
Roles:	[Guest], [User Authenticated]
Enforcement Profiles:	Cisco Captive Portal
Service Monitor Mode:	Disabled
Online Status:	● Online

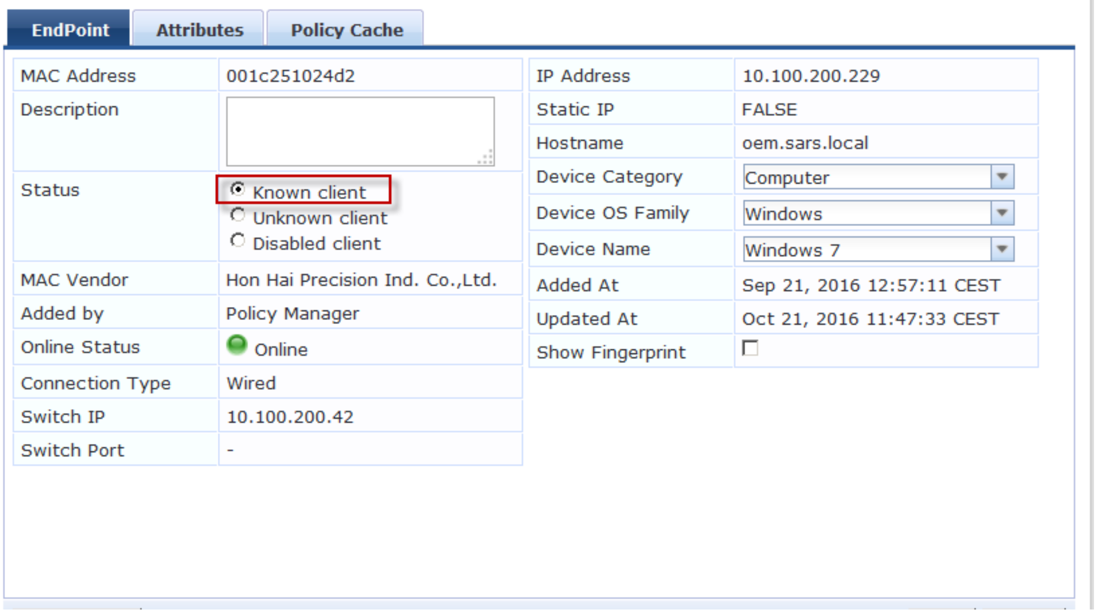
After provision



Login Status:	ACCEPT
Session Identifier:	R000001da-10-5809e467
Date and Time:	Oct 21, 2016 11:48:23 CEST
End-Host Identifier:	00-1C-25-10-24-D2 (Computer / Windows / Windows 7)
Username:	001c251024d2
Access Device IP/Port:	10.100.200.42:50003 (SW42 / Cisco)
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	Cisco MAC Caching
Authentication Method:	MAC-AUTH
Authentication Source:	Local:localhost
Authorization Source:	[Guest User Repository], [Endpoints Repository], [Time Source]
Roles:	[Contractor], [MAC Caching], [User Authenticated]
Enforcement Profiles:	Cisco MAC Caching
Service Monitor Mode:	Disabled
Online Status:	● Online

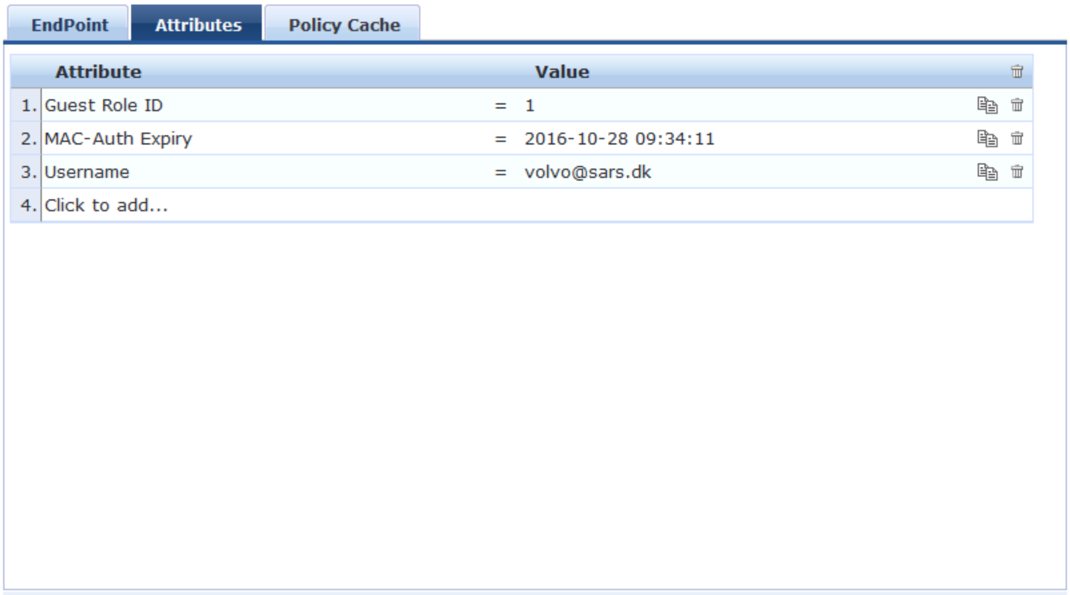
Endpoint

After provision



MAC Address	001c251024d2
Description	
Status	● Known client ○ Unknown client ○ Disabled client
MAC Vendor	Hon Hai Precision Ind. Co.,Ltd.
Added by	Policy Manager
Online Status	● Online
Connection Type	Wired
Switch IP	10.100.200.42
Switch Port	-

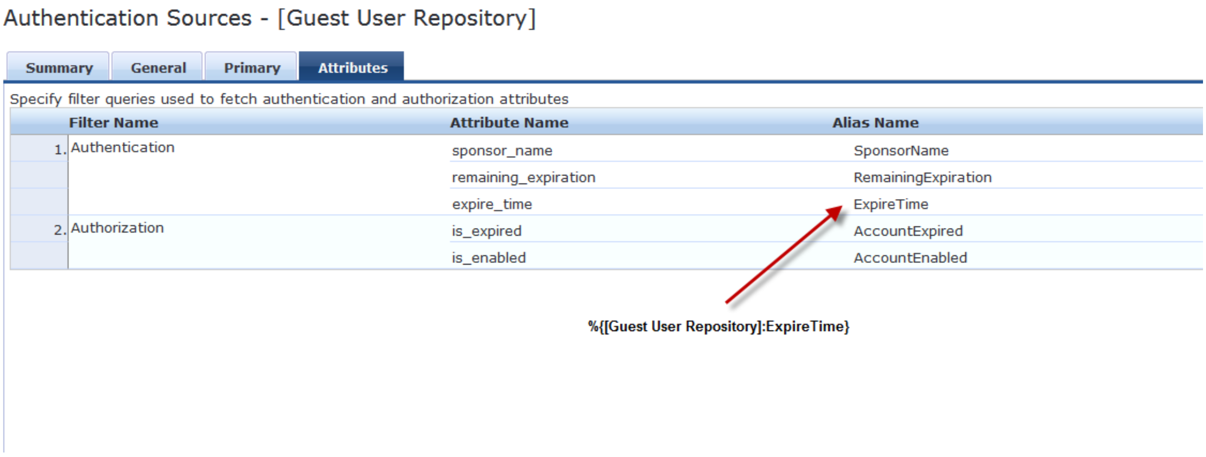
IP Address	10.100.200.229
Static IP	FALSE
Hostname	oem.sars.local
Device Category	Computer
Device OS Family	Windows
Device Name	Windows 7
Added At	Sep 21, 2016 12:57:11 CEST
Updated At	Oct 21, 2016 11:47:33 CEST
Show Fingerprint	□



	Attribute		Value
1.	Guest Role ID	=	1
2.	MAC-Auth Expiry	=	2016-10-28 09:34:11
3.	Username	=	volvo@sars.dk
4.	Click to add...		

Appendix system variables

Expire time



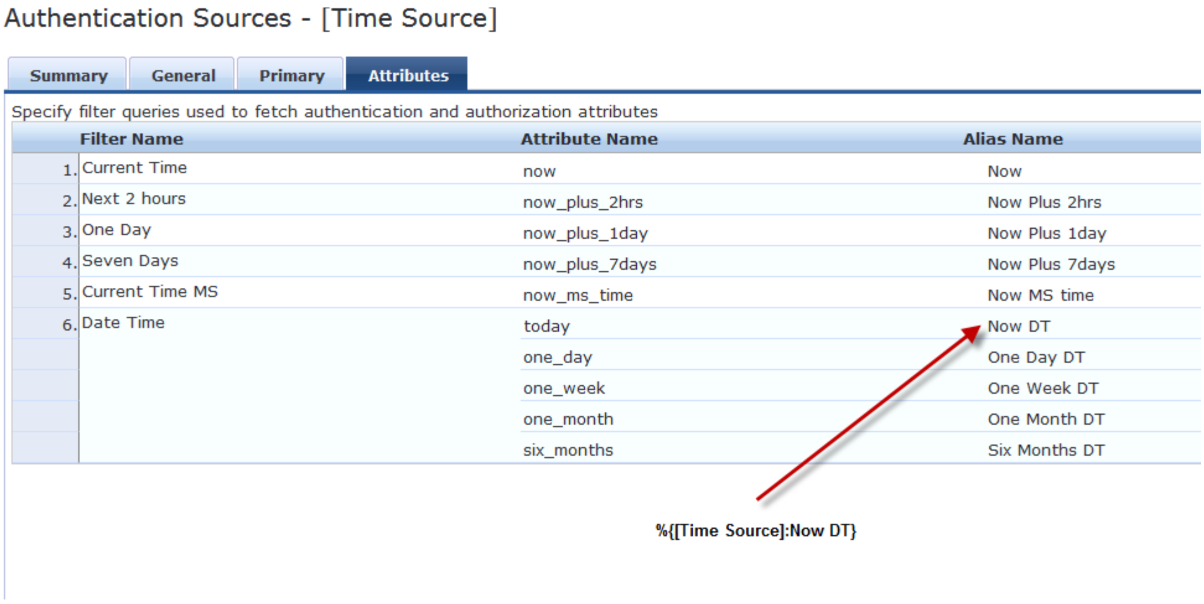
Authentication Sources - [Guest User Repository]

Specify filter queries used to fetch authentication and authorization attributes

	Filter Name	Attribute Name	Alias Name
1.	Authentication	sponsor_name	SponsorName
		remaining_expiration	RemainingExpiration
		expire_time	ExpireTime
2.	Authorization	is_expired	AccountExpired
		is_enabled	AccountEnabled

%{[Guest User Repository]:ExpireTime}

Current time



Authentication Sources - [Time Source]

Specify filter queries used to fetch authentication and authorization attributes

	Filter Name	Attribute Name	Alias Name
1.	Current Time	now	Now
2.	Next 2 hours	now_plus_2hrs	Now Plus 2hrs
3.	One Day	now_plus_1day	Now Plus 1day
4.	Seven Days	now_plus_7days	Now Plus 7days
5.	Current Time MS	now_ms_time	Now MS time
6.	Date Time	today	Now DT
		one_day	One Day DT
		one_week	One Week DT
		one_month	One Month DT
		six_months	Six Months DT

%{[Time Source]:Now DT}