Brocade with Cisco Identity Services Engine 2.0+ / Multi-Auth Configuration with Phone and PC w/Dynamic VLAN assignment

Chad Mitchell CCIE#44090 chadmi@cisco.com

```
ICX6450-24P Switch#sh flash
Stack unit 1:
  Compressed Pri Code size = 10029540, Version:07.4.00jT311 (ICX64S07400j.bin)
  Compressed Sec Code size = 8310988, Version:08.0.20aT311 (ICX64S08020a.bin)
  Compressed Boot-Monitor Image size = 786944, Version:10.1.05T310
  Code Flash Free Space = 32587776
ICX6450-24P Switch#
```

****

ISE needs to tell the switch when to use 802.1X using the Foundry-MAC-Authent-needs-802.1X attribute set to 1 or 0. The Authorization Policy must be set to send this attribute = 1 if MAC auth does not match a Identity Group policy in the ISE AuthZ list. The switch will then try 802.1X for the session in question and allow the VLAN assignment if match is then found. For endpoints that match and Identity Group policy you must send the attribute = 0 to tell the switch to stop trying to authenticate and assign the VLAN specified along with the 0 attribute.

SW: Version 07.4.00jT311

```
ICX6450-24P Switch#sh run
Current configuration:
!
ver 07.4.00jT311
!
stack unit 1
  module 1 icx6450-24p-poe-port-management-module
  module 2 icx6450-sfp-plus-4port-40g-module
!
!
!
!
vlan 1 name DEFAULT-VLAN by port
!
vlan 2 by port
!
vlan 3 name VOICE by port
 tagged ethe 1/1/1 to 1/1/2 ethe 1/1/23 to 1/1/24
!
vlan 252 name ACCESS by port
 tagged ethe 1/1/1 to 1/1/2 ethe 1/1/23 to 1/1/24
!
vlan 254 name MANAGEMENT by port
 tagged ethe 1/1/23 to 1/1/24
 management-vlan
 default-gateway  10.99.254.2 1
!
vlan 999 name AUTHFAILVLAN by port
 tagged ethe 1/1/23 to 1/1/24
!
!
!
!
dot1x-enable
```

```
 re-authentication
 auth-fail-action restricted-vlan
 auth-fail-vlanid 999
 mac-session-aging no-aging permitted-mac-only
 enable ethe 1/1/1 to 1/1/2
!
!
!
!
!
aaa authentication dot1x default radius
boot sys fl pri
ip address 10.99.254.15 255.255.255.0
no ip dhcp-client enable
logging console
radius-server host 10.99.10.15 auth-port 1812 acct-port 1813 default key 1 $d=-dsZ|8 dot1x
cdp run
fdp run

mac-authentication enable
mac-authentication mac-vlan-dyn-activation
mac-authentication disable-aging permitted-mac-only
mac-authentication auth-passwd-format xx-xx-xx-xx-xx-xx
interface ethernet 1/1/1
 dot1x port-control auto
 dual-mode
 mac-authentication enable
 mac-authentication auth-timeout-action failure
 mac-authentication enable-dynamic-vlan
 inline power
 voice-vlan 3
!
interface ethernet 1/1/2
 dot1x port-control auto
 dual-mode
 mac-authentication enable
 mac-authentication auth-timeout-action failure
 mac-authentication enable-dynamic-vlan
 inline power
 voice-vlan 3
!
interface ethernet 1/1/23
 link-aggregate active
!
interface ethernet 1/1/24
 link-aggregate active
!
!
!
!
!
!
!
end
```

```
ICX6450-24P Switch#

********************************************************************************************************************************
********************************************************************************************************************************

        SW: Version 08.0.20aT311

ICX6450-24P Switch#sh run
Current configuration:
!
ver 08.0.20aT311
!
stack unit 1
  module 1 icx6450-24p-poe-port-management-module
  module 2 icx6450-sfp-plus-4port-40g-module
!
!
!
lag LAG_1 dynamic id 1
 ports ethernet 1/1/23 to 1/1/24
 primary-port 1/1/23
 deploy
!
!
vlan 1 name DEFAULT-VLAN by port
!
vlan 2 by port
!
vlan 3 name VOICE by port
 tagged ethe 1/1/23 to 1/1/24
!
vlan 252 name ACCESS by port
 tagged ethe 1/1/23 to 1/1/24
!
vlan 254 name MANAGEMENT by port
 tagged ethe 1/1/23 to 1/1/24
 management-vlan
 default-gateway  10.99.254.2 1
!
vlan 998 name AUTHDEFAULT by port
!
vlan 999 name AUTHFAILVLAN by port
 tagged ethe 1/1/23 to 1/1/24
!
!
!
!
authentication
 auth-order mac-auth dot1x
 auth-default-vlan 998
 restricted-vlan 999
 auth-fail-action restricted-vlan
 re-authentication
```

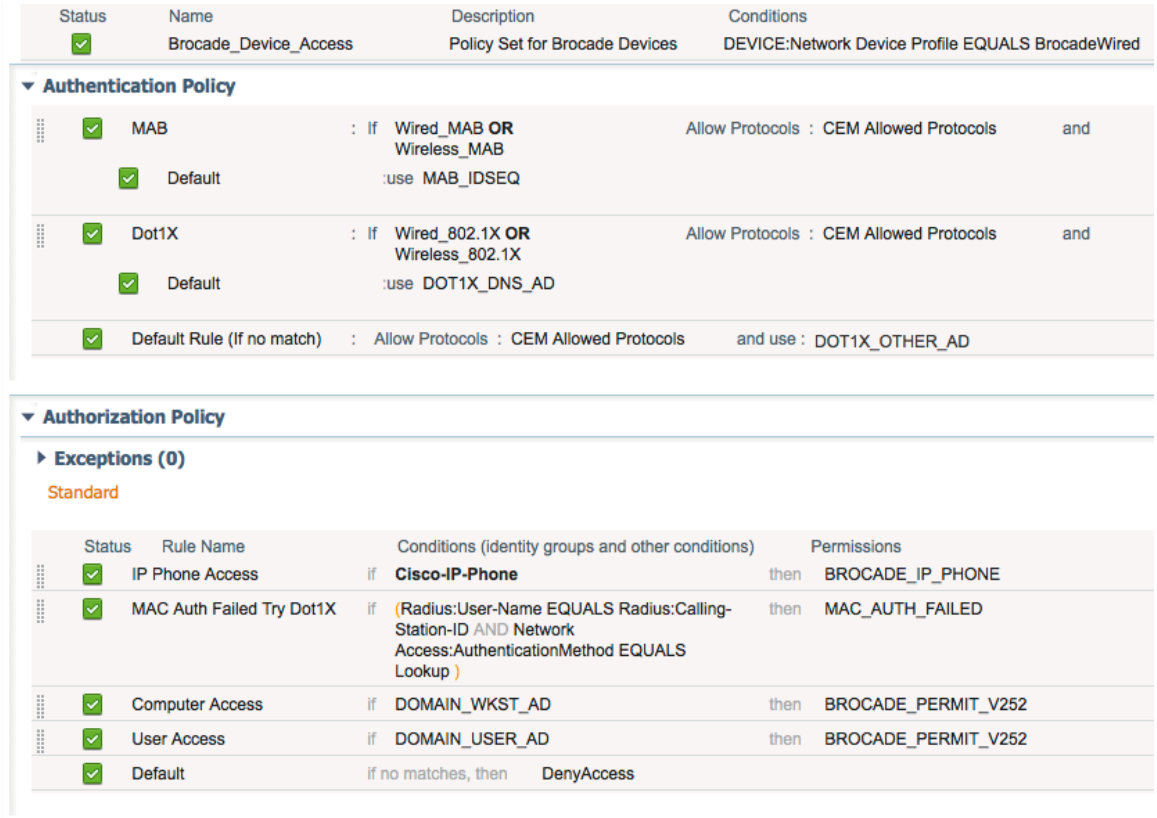
```
 disable-aging permitted-mac
 dot1x enable
 dot1x enable ethe 1/1/1 to 1/1/2
 mac-authentication enable
 mac-authentication enable ethe 1/1/1 to 1/1/2
 mac-authentication password-format xx-xx-xx-xx-xx-xx
!
aaa authentication dot1x default radius
aaa authorization coa enable
boot sys fl sec
ip address 10.99.254.15 255.255.255.0
no ip dhcp-client enable
!
logging console
radius-server host 10.99.10.15 auth-port 1812 acct-
port 1813 default key 2 $ZD0tZHNafDg= dot1x
cdp run
fdp run
!
!
interface ethernet 1/1/1
 dot1x port-control auto
 inline power
!
interface ethernet 1/1/2
 dot1x port-control auto
 inline power
!
!
!
!
!
!
!
!
end

ICX6450-24P Switch#
```

****

****

ISE Configuration

Policy Set Configuration



Status	Name	Description	Conditions
✓	Brocade_Device_Access	Policy Set for Brocade Devices	DEVICE:Network Device Profile EQUALS BrocadeWired

Authentication Policy

✓	MAB	: If	Wired_MAB **OR** Wireless_MAB	Allow Protocols :	CEM Allowed Protocols	and
✓	Default	:use	MAB_IDSEQ			
✓	Dot1X	: If	Wired_802.1X **OR** Wireless_802.1X	Allow Protocols :	CEM Allowed Protocols	and
✓	Default	:use	DOT1X_DNS_AD			
✓	Default Rule (If no match)	:	Allow Protocols : CEM Allowed Protocols	and use :	DOT1X_OTHER_AD	

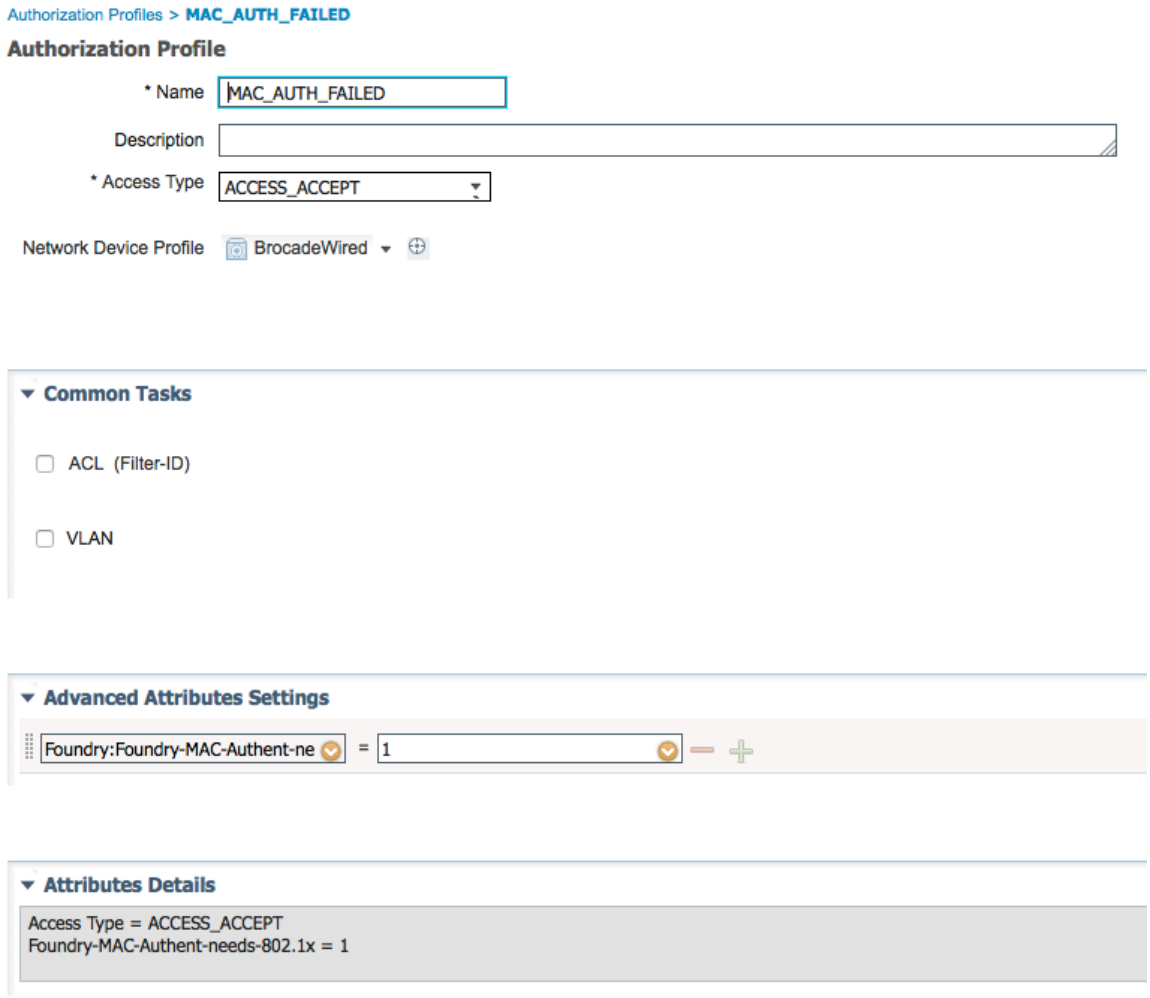
Authorization Policy

Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)		Permissions
✓	IP Phone Access	if **Cisco-IP-Phone**	then	BROCADE_IP_PHONE
✓	MAC Auth Failed Try Dot1X	if (Radius:User-Name EQUALS Radius:Calling-Station-ID AND Network Access:AuthenticationMethod EQUALS Lookup)	then	MAC_AUTH_FAILED
✓	Computer Access	if DOMAIN_WKST_AD	then	BROCADE_PERMIT_V252
✓	User Access	if DOMAIN_USER_AD	then	BROCADE_PERMIT_V252
✓	Default	if no matches, then DenyAccess		

Authorization Profiles



Authorization Profiles > **BROCADE_IP_PHONE**

Authorization Profile

* Name: BROCADE_IP_PHONE

Description: Default profile used for Cisco Phones.

* Access Type: ACCESS_ACCEPT

Network Device Profile: BrocadeWired

Common Tasks

- [ ] ACL (Filter-ID)
- [ ] VLAN

Advanced Attributes Settings

Foundry:Foundry-MAC-Authent-ne	=	0		
Radius:Tunnel-Medium-Type	=	802	Tag ID 1	Edit Tag
Radius:Tunnel-Private-Group-ID	=	U:3	Tag ID 1	Edit Tag
Radius:Tunnel-Type	=	VLAN	Tag ID 1	Edit Tag

Attributes Details

```
Access Type = ACCESS_ACCEPT
Foundry-MAC-Authent-needs-802.1x = 0
Tunnel-Medium-Type = 1:6
Tunnel-Private-Group-ID = 1:U:3
Tunnel-Type = 1:13
```

Authorization Profiles > **BROCADE_PERMIT_V252**

Authorization Profile

* Name: BROCADE_PERMIT_V252

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: BrocadeWired

Common Tasks

- [ ] ACL (Filter-ID)
- [ ] VLAN

Advanced Attributes Settings

Radius:Tunnel-Private-Group-ID	=	U:252	Tag ID 1	Edit Tag
Radius:Tunnel-Medium-Type	=	802	Tag ID 1	Edit Tag
Radius:Tunnel-Type	=	VLAN	Tag ID 1	Edit Tag

Attributes Details

```
Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:U:252
Tunnel-Medium-Type = 1:6
Tunnel-Type = 1:13
```