

# Configurar la política de autorización basada en el atributo vlan-id en ISE

## Contenido

[Introducción](#)

[Caso de uso](#)

[Configuration Steps](#)

[lado NAD](#)

[lado ISE](#)

[Prueba](#)

[lado NAD](#)

[lado ISE](#)

## Introducción

En este artículo se describen los pasos para configurar la política de autorización de ISE basada en el atributo de ID de VLAN enviado desde el NAD. Esta función sólo está disponible con IBNS 2.0.

## Caso de uso

Los clientes desean rellenar el ID de VLAN configurado en la interfaz de acceso y utilizarlo posteriormente para proporcionar acceso en ISE.

## Configuration Steps

### lado NAD

1. Configure el switch para enviar atributos de radio VLAN en la solicitud de acceso.

```
Device# configure terminal Device(config)# access-session attributes filter-list list TEST
Device(config-com-filter-list)# vlan-id Device(config-com-filter-list)# exit Device(config)#
access-session accounting attributes filter-spec include list TEST Device(config)# access-
session authentication attributes filter-spec include list TEST Device(config)# end
```

**NOTE:** Puede recibir una advertencia al ingresar el comando *"access-session accounting Attributes filter-spec include list TEST"* para aceptar la migración a IBNS 2.

```
Switch(config)#access-session accounting attributes filter-spec include list TEST This operation
will permanently convert all relevant authentication commands to their CPL control-policy
equivalents. As this conversion is irreversible and will disable the conversion CLI
'authentication display [legacy|new-style]', you are strongly advised to back up your current
configuration before proceeding. Do you wish to continue? [yes]:
```

Consulte la siguiente guía para obtener más información: [Guía de configuración de atributos de Vlan-id radius](#)

## lado ISE

1. Cree una política de autenticación basada en sus necesidades (MAB/DOT1X).
2. La política de autorización incluirá el siguiente tipo de condición, asegúrese de coincidir con la sintaxis exacta

Radius-Tunnel-Private-Group-ID EQUALS (tag=1)

Ejemplo:

Para un VLAN-ID = 77

Authorization Policy (21)

Status	Rule Name	Conditions	Results
+	Vlan-Id test	Radius-Tunnel-Private-Group-ID EQUALS (tag=1) 77	PermitAccess

## Prueba

### lado NAD

```
Switch#sh run interface Tw1/0/3 Building configuration... Current configuration : 336 bytes !
interface TwoGigabitEthernet1/0/3 switchport access vlan 77 switchport mode access device-
tracking attach-policy DT_POLICY access-session host-mode multi-host access-session closed
access-session port-control auto mab dot1x pae authenticator spanning-tree portfast service-
policy type control subscriber POLICY_Tw1/0/3 end Switch#
```

```
Switch#sh auth sess inter Tw1/0/3 details Interface: TwoGigabitEthernet1/0/3 IIF-ID: 0x1FA6B281
MAC Address: c85b.768f.51b4 IPv6 Address: Unknown IPv4 Address: 10.4.18.167 User-Name: C8-5B-76-
8F-51-B4 Status: Authorized Domain: DATA Oper host mode: multi-host Oper control dir: both
Session timeout: N/A Common Session ID: 33781F0A00000AE958E57C9D Acct Session ID: 0x0000000e
Handle: 0x43000019 Current Policy: POLICY_Tw1/0/3 Local Policies: Service Template:
DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150) Security Policy: Should Secure Server
Policies: Method status list: Method State mab Authc Success Switch#
```

### lado ISE

## Overview

Event	5200 Authentication succeeded
Username	C8:5B:76:8F:51:B4
Endpoint Id	C8:5B:76:8F:51:B4 ⓘ
Endpoint Profile	Unknown
Authentication Policy	Default >> MAB
Authorization Policy	Default >> Vlan-id test
Authorization Result	PermitAccess

## Authentication Details

Source Timestamp	2021-11-25 21:06:55.187
Received Timestamp	2021-11-25 21:06:55.187
Policy Server	ise30baaamex
Event	5200 Authentication succeeded
Username	C8:5B:76:8F:51:B4
User Type	Host

## Steps

11001 Received RADIUS Access-Request  
11017 RADIUS created a new session  
11027 Detected Host Lookup UseCase (Service-Type = Call Check (10)) **System Scan**  
15049 Evaluating Policy Group  
15008 Evaluating Service Selection Policy  
15041 Evaluating Identity Policy  
15048 Queried PIP - Normalised Radius.RadiusFlowType  
15013 Selected Identity Source - Internal Endpoints  
24209 Looking up Endpoint in Internal Endpoints IDStore - C8:5B:76:8F:51:B4  
24211 Found Endpoint in Internal Endpoints IDStore  
22037 Authentication Passed  
24715 ISE has not confirmed locally previous successful machine authentication for user in Active Directory  
15036 Evaluating Authorization Policy  
15048 Queried PIP - Radius.Tunnel-Private-Group-ID  
15016 Selected Authorization Profile - PermitAccess  
24209 Looking up Endpoint in Internal Endpoints IDStore - C8:5B:76:8F:51:B4  
24211 Found Endpoint in Internal Endpoints IDStore  
11002 Returned RADIUS Access-Accept

CiscoAVPair

```
cts-pac-opaque=****,  
service-type=Call Check,  
audit-session-id=33781F0A00000AEA58E88DB4,  
method=mab,  
client-iif-id=491113166,  
vlan-id=77
```