

Proteggere una porta di commutazione AP Flexconnect con Dot1x

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazione AP:](#)

[Configurazione degli switch](#)

[Configurazione di ISE:](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Riferimenti](#)

Introduzione

Questo documento descrive la configurazione per proteggere le porte di switching su cui i punti di accesso FlexConnect (AP) eseguono l'autenticazione con Dot1x.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- FlexConnect su controller WLC (Wireless Lan Controller)
- 802.1x sugli switch Cisco
- Topologia NEAT (Network Edge Authentication Topology)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

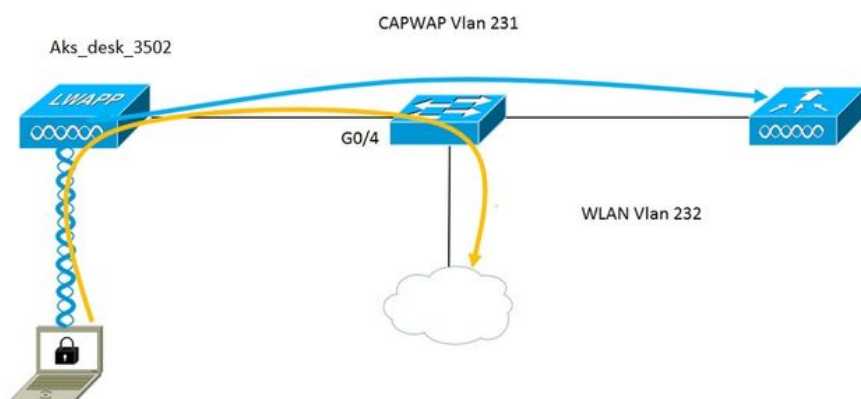
- WS-C3560CX-8PC-S, 15.2(4)E1
- AIR-CT-2504-K9, 8.2.141.0
- Identity Service Engine (ISE) 2.0
- Access point basati su IOS (serie x500,x600,x700).

I punti di accesso Wave 2 basati su sistema operativo AP non supportano flexconnect trunk dot1x al momento della scrittura.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Esempio di rete



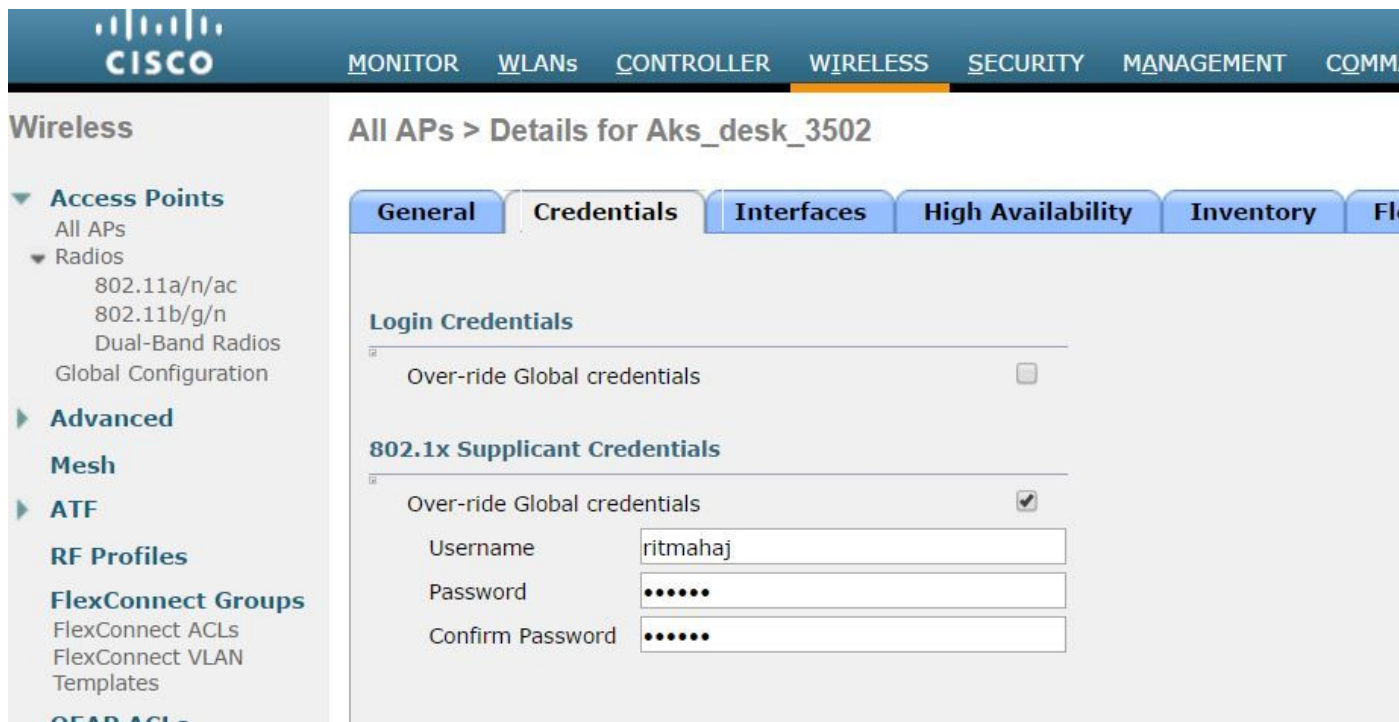
In questa configurazione, l'access point agisce come supplicant 802.1x ed è autenticato dallo switch contro ISE con EAP-FAST. Dopo aver configurato la porta per l'autenticazione 802.1x, lo switch non consente il passaggio di traffico diverso dal traffico 802.1x attraverso la porta finché il dispositivo connesso alla porta non esegue correttamente l'autenticazione.

Una volta che l'autenticazione del punto di accesso ha esito positivo sull'ISE, lo switch riceve l'attributo Cisco VSA "device-traffic-class=switch" e sposta automaticamente la porta sul trunk.

Ciò significa che, se l'access point supporta la modalità FlexConnect e ha configurato SSID commutati localmente, può inviare traffico con tag. Verificare che il supporto vlan sia abilitato sull'access point e che sia configurata la vlan nativa corretta.

Configurazione AP:

1. Se l'access point è già collegato al WLC, vai alla scheda Wireless e fai clic sul punto di accesso. Passare al campo Credenziali e sotto l'intestazione Credenziali richieste 802.1x selezionare la casella Ignora credenziali globali per impostare il nome utente e la password 802.1x per questo punto di accesso.



The screenshot shows the Cisco Wireless LAN Controller (WLC) configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', and 'COMM'. The left sidebar shows the 'Wireless' menu with options like 'Access Points', 'Radios', 'Advanced', 'Mesh', 'ATF', 'RF Profiles', and 'FlexConnect Groups'. The main content area is titled 'All APs > Details for Aks_desk_3502' and has tabs for 'General', 'Credentials', 'Interfaces', 'High Availability', 'Inventory', and 'Flex'. The 'Credentials' tab is active, showing the 'Login Credentials' section with an unchecked 'Over-ride Global credentials' checkbox. Below it, the '802.1x Supplicant Credentials' section has a checked 'Over-ride Global credentials' checkbox and three input fields: 'Username' (ritmahaj), 'Password' (masked with dots), and 'Confirm Password' (masked with dots).

Inoltre, è possibile impostare un nome utente e una password di comando per tutti i punti di accesso che vengono aggiunti al WLC con il menu Global Configuration.

The screenshot shows the Cisco Wireless configuration interface. The left sidebar contains a navigation menu with 'Global Configuration' highlighted. The main content area is divided into several sections:

- Ethernet Interface# CDP State:** A table with columns for Ethernet Interface# and CDP State. Values for interfaces 0-4 are all checked.
- Radio Slot# CDP State:** A table with columns for Radio Slot# and CDP State. Values for slots 0-2 are all checked.
- Login Credentials:** Fields for Username, Password, and Enable Password.
- 802.1x Supplicant Credentials:** A checkbox for 802.1x Authentication (checked) and fields for Username, Password, and Confirm Password.
- TCP MSS:** A section for Global TCP Adjust MSS (IPv4: 536 - 1363, IPv6: 1220 - 1331).
- AP Retransmit Config Parameters:** Fields for AP Retransmit Count (5) and AP Retransmit Interval (3).
- OEAP Config Parameters:** A checkbox for Disable Local Access.

2. Se l'access point non è ancora stato aggiunto a un WLC, è necessario eseguire la console nel LAP per impostare le credenziali e usare questo comando CLI:

Cli console LAP#debug capwap

LAP#capwap dot1x nomeutente <nomeutente> password <password>

Configurazione degli switch

1. Abilitare dot1x sullo switch a livello globale e aggiungere il server ISE allo switch

aaa new-model

!

raggio gruppo predefinito dot1x autenticazione aaa

!

raggio gruppo predefinito rete di autorizzazione aaa

!

dot1x system-auth-control

!

server radius ISE

indirizzo ipv4 10.48.39.161 porta auth 1645 porta acct 1646

chiave 7 123A0C0411045D5679

2. Configurare ora la porta dello switch AP

```
interfaccia Gigabit Ethernet0/4
switchport access vlan 231
switchport trunk consentita vlan 231.232
accesso in modalità switchport
autenticazione host-mode multi-host
ordine di autenticazione dot1x
authentication port-control auto
autenticatore pagina dot1x
spanning-tree portfast edge
```

Configurazione di ISE:

1. Con ISE, è possibile abilitare semplicemente NEAT per il profilo di autorizzazione AP per impostare l'attributo corretto; tuttavia, sugli altri server RADIUS, è possibile configurare manualmente.

Authorization Profiles > AP_Flex_Trunk

Authorization Profile

* Name

Description

* Access Type

Network Device Profile 

Service Template

Track Movement 

Common Tasks

NEAT

Attributes Details

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = device-traffic-class=switch
```

2. Su ISE, è necessario configurare anche la policy di autenticazione e la policy di autorizzazione. In questo caso abbiamo raggiunto la regola di autenticazione predefinita che è il dot1x cablato ma si può personalizzare secondo il requisito.

Per quanto riguarda il criterio di autorizzazione (Port_AuthZ), in questo caso abbiamo aggiunto le credenziali dell'access point a un gruppo di utenti (AP) e abbiamo eseguito il push del profilo di autorizzazione (AP_Flex_Trunk) in base a questo.

Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.
For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

First Matched Rule Applies

▶ Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
	Port_AuthZ	if APs AND Wired_802.1X	then AP_Flex_Trunk

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

1. Sullo switch, è possibile usare il comando "debug authentication feature autocfg all" per verificare se la porta viene spostata sulla porta trunk o meno.

```
20 feb 12:34:18.119: %LINK-3-UPDOWN: interfaccia Gigabit Ethernet0/4, stato modificato in attivo
```

```
20 feb 12:34:19.122: %LINEPROTO-5-UPDOWN: protocollo di linea sull'interfaccia Gigabit Ethernet0/4, stato modificato in attivo
```

```
akshat_sw#
```

```
akshat_sw#
```

```
20 feb 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: In dot1x AutoCfg start_fn, epm_handle: 3372220456
```

```
20 feb 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [588d.0997.061d, Gi0/4] Tipo di dispositivo = Switch
```

```
20 feb 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [588d.0997.061d, Gi0/4] nuovo client
```

```
20 feb 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Stato applicazione macro autocfg interna : 1
```

```
20 feb 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Tipo di dispositivo: 2
```

```
20 feb 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Auto-config: stp ha port_config 0x85777D8
```

```
20 feb 12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Configurazione automatica: stp port_config con bpdu guard_config 2
```

```
20 feb 12:38:11.116: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Applicazione di auto-cfg sulla porta.
```

```
20 feb 12:38:11.116: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Vlan: 231 Vlan-Str: 231
```

```
20 feb 12:38:11.116: AUTH-FEAT-AUTOCFG-EVENT: [Gi0/4] Applicazione della macro dot1x_autocfg_supp
```

```
20 feb 12:38:11.116: Applicazione del comando in corso... 'no switchport access vlan 231' in Gi0/4
```

```
20 feb 12:38:11.127: Applicazione del comando in corso... 'no switchport nonegotiate' in Gi0/4
```

```
20 feb 12:38:11.127: Applicazione del comando in corso... 'switchport mode trunk' in Gi0/4
```

```
20 feb 12:38:11.134: Applicazione del comando in corso... 'switchport trunk native vlan 231' in Gi0/4
```

```
20 feb 12:38:11.134: Applicazione del comando in corso... 'spanning-tree portfast trunk' in Gi0/4
```

```
20 feb 12:38:12.120: %LINEPROTO-5-UPDOWN: protocollo di linea sull'interfaccia Gigabit Ethernet0/4, stato modificato in inattivo
```

```
20 feb 12:38:15.139: %LINEPROTO-5-UPDOWN: protocollo di linea sull'interfaccia Gigabit
```

Ethernet0/4, stato modificato in attivo

2. L'output del comando "show run int g0/4" mostra che la porta è stata trasformata in porta trunk.

Configurazione corrente: 295 byte

!

```
interfaccia Gigabit Ethernet0/4
switchport trunk consentita vlan 231.232.239
switchport trunk native vlan 231
switchport mode trunk
autenticazione host-mode multi-host
ordine di autenticazione dot1x
authentication port-control auto
autenticatore pagina dot1x
spanning-tree portfast edge trunk
fine
```

3. Su ISE, in Operations>>Radius Livelogs si può verificare il corretto completamento dell'autenticazione e la richiesta del profilo di autorizzazione.

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles
2017-02-20 15:05:48.991			0	ritmahaj	58:8D:09:97:06:1D	Cisco-Device	Default >> Dot1X >> D..	Default >> Port_AuthZ	AP_Flex_Trunk
2017-02-20 15:05:48.991				ritmahaj	58:8D:09:97:06:1D	Cisco-Device	Default >> Dot1X >> D..	Default >> Port_AuthZ	AP_Flex_Trunk
2017-02-20 15:04:49.272				ritmahaj	58:8D:09:97:06:1D	Cisco-Device	Default >> Dot1X >> D..	Default >> Port_AuthZ	

4. Se si connette un client dopo questo, il relativo indirizzo mac viene appreso sulla porta dello switch AP nella vlan del client 232.

```
akshat_sw#sh mac address-table int g0/4
```

Tabella indirizzi Mac

—

Porte Vlan Mac Address Type

— — —

```
231 588d.0997.061d STATICO Gi0/4 - AP
232 c0ee.fbd7.8824 DYNAMIC Gi0/4 - Client
```

Sul WLC, nei dettagli del client, si nota che il client appartiene alla vlan 232 e l'SSID è commutato localmente. Ecco un frammento.

```
(Cisco Controller) >show client detail c0:ee:fb:d7:88:24
Indirizzo MAC client..... c0:ee:fb:d7:88:24
Nome utente client..... N/D
Indirizzo MAC AP..... b4:14:89:82:cb:90
Nome AP..... Aks_desk_3502
ID slot radio AP..... 1
Stato cliente..... Associato
Gruppo di utenti client.....
Stato OOB NAC client..... Accesso
```

```

ID LAN wireless..... 2
Nome della rete LAN wireless (SSID)..... Port-Auth
Nome profilo LAN wireless..... Port-auth
Area sensibile
(802.11u).....
Non supportata
BSSID..... b4:14:89:82:cb:9f
Connesso per ..... 42 sec
Canale..... 44
Indirizzo IP..... 192.168.232.90
Indirizzo gateway..... 192.168.232.1
Maschera di rete..... 255.255.255.0
ID associazione..... 1
Algoritmo di autenticazione..... Apri sistema
Codice motivo..... 1
Codice di stato..... 0

Switching dei dati FlexConnect..... Locale
Stato Dhcp FlexConnect..... Locale
Switching centrale basato su Vlan FlexConnect..... No
Autenticazione FlexConnect..... Centrale
Associazione centrale FlexConnect..... No
NOME VLAN FlexConnect..... vlan 232
Quarantena VLAN..... 0
Accesso alla VLAN..... 232
VLAN di bridging locale..... 232

```

Risoluzione dei problemi

In questa sezione vengono fornite informazioni utili per risolvere i problemi di configurazione.

- Se l'autenticazione ha esito negativo, utilizzare i comandi debug dot1x, debug authentication.
- Se la porta non viene spostata nel trunk, immettere il comando debug authentication feature autocfg all.
- Accertarsi di aver configurato la modalità multi-host (modalità host di autenticazione multi-host). Per consentire gli indirizzi MAC wireless del client, è necessario abilitare Multi-Host.
- Affinché lo switch accetti e applichi gli attributi inviati da ISE, è necessario configurare il comando "aaa authorization network".

Gli access point Cisco IOS supportano solo TLS 1.0. Ciò può causare problemi se il server RADIUS è configurato per consentire solo le autenticazioni TLS 1.2.802.1X

Riferimenti

[Configurazione del supplicant dot1x con AP e WLC 9800](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).