# Configurazione di ACS 5.2 per l'autenticazione basata sulla porta con un LAP

# Sommario

Introduzione **Prerequisiti** Requisiti Componenti usati Convenzioni Premesse Configurazione Esempio di rete Presupposti Procedura di configurazione Configurazione LAP Configura switch Configura server RADIUS Configura risorse di rete Configura utenti Definizione degli elementi dei criteri Applica criteri di accesso Verifica Risoluzione dei problemi Informazioni correlate

# **Introduzione**

In questo documento viene descritto come configurare un Lightweight Access Point (LAP) come supplicant 802.1x per l'autenticazione su un server RADIUS come Access Control Server (ACS) 5.2.

# **Prerequisiti**

## Requisiti

Prima di provare la configurazione, verificare che siano soddisfatti i seguenti requisiti:

- Conoscere a fondo il controller WLC (Wireless LAN Controller) e i LAP.
- Avere una conoscenza funzionale del server AAA.
- Conoscere a fondo le reti wireless e i problemi di sicurezza wireless.

## Componenti usati

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

- Cisco 5508 WLC con firmware versione 7.0.20.0
- Cisco serie 3502 LAP
- Cisco Secure ACS con versione 5.2
- Cisco serie 3560 Switch

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.

## **Convenzioni**

Fare riferimento a <u>Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.</u>

## **Premesse**

I LAP dispongono di certificati X.509 preinstallati (firmati da una chiave privata) che vengono masterizzati nel dispositivo al momento della produzione. I LAP utilizzano questo certificato per autenticarsi al WLC nel processo di join. Questo metodo descrive un altro modo per autenticare i LAP. Con il software WLC, è possibile configurare l'autenticazione 802.1x tra un Cisco Aironet Access Point (AP) e uno switch Cisco. In questo caso, l'access point agisce come supplicant 802.1x ed è autenticato dallo switch su un server RADIUS (ACS) che usa EAP-FAST con provisioning PAC anonimo. Dopo aver configurato la porta per l'autenticazione 802.1x, lo switch non consente il passaggio di traffico diverso dal traffico 802.1x fino a quando il dispositivo connesso alla porta non esegue correttamente l'autenticazione. Un access point può essere autenticato prima di essere aggiunto a un WLC o dopo essere stato aggiunto a un WLC, nel qual caso è possibile configurare 802.1x sullo switch dopo che il LAP si è unito al WLC.

# **Configurazione**

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

## Esempio di rete

Nel documento viene usata questa impostazione di rete:



Di seguito sono riportati i dettagli di configurazione dei componenti utilizzati nel diagramma:

- L'indirizzo IP del server ACS (RADIUS) è 192.168.150.24.
- L'indirizzo dell'interfaccia di gestione e AP-manager del WLC è 192.168.75.44.
- L'indirizzo dei server DHCP è 192.168.150.25.
- II LAP viene inserito nella VLAN 253.
- VLAN 253: 192.168.153.x/24. Gateway: 192.168.153.10
- VLAN 75: 192.168.75.x/24. Gateway: 192.168.75.1

## **Presupposti**

- Gli switch sono configurati per tutte le VLAN di layer 3.
- Al server DHCP viene assegnato un ambito DHCP.
- Esiste una connettività di livello 3 tra tutti i dispositivi della rete.
- II LAP è già unito al WLC.
- Ogni VLAN ha una maschera /24.
- In ACS 5.2 è installato un certificato autofirmato.

# Procedura di configurazione

Questa configurazione è suddivisa in tre categorie:

- 1. Configurare il LAP.
- 2. Configurare lo switch.
- 3. Configurare il server RADIUS.

#### **Configurazione LAP**

Presupposti:

Il LAP è già registrato sul WLC con l'opzione 43, il DNS o l'IP dell'interfaccia di gestione del WLC configurato staticamente.

Attenersi alla seguente procedura:

1. Per verificare la registrazione dei LAP sul WLC, selezionare Wireless > Access Point > Tutti ali

AP.								
cisco	MONITOR MLANS	CONTROLLER WORELESS SECU	KUTY MANADEMENT O	OMMANOS HELP (EEDEA	Say ICX	e Configuration	Bing   Logos	d Befred
Wireless	All APs						Entries 1	-1 of 1
* Access Points All APU	Current Filter	Rone	(Change Fit	arl [Clear.Fiber]				
602.11a/n 802.11b/g/h Global Configuration	Number of APs	1						
<ul> <li>&gt; Advanced</li> <li>Mesh</li> <li>HREAP Groups</li> <li>&gt; 802.11a/n</li> <li>&gt; 902.11b/g/n</li> <li>&gt; Media Stream</li> <li>Country</li> <li>Timers</li> <li>&gt; QoS</li> </ul>	A9 Name 33526	AP Hodel AIR-CAP3502E-A-K5	AP HAC cc.ef+45.fe:33:13	AP Up Time 1 d, 62 h 32 m 42 s	Admin Status Enabled	Operational Statuc REG	Port AU	P Mode cel

 Èpossibile configurare le credenziali 802.1x (nome utente/password) per tutti i LAP in due modi:GlobalmentePer un LAP già aggiunto, è possibile impostare le credenziali a livello globale in modo che ogni LAP aggiunto al WLC erediti tali credenziali.

uluilu cisco	HONETOR WLAND CON	TROLLER WIRELESS	SECONELLA MIRVAGEMENT	COMMANDS HELP (EEDBACK	Saye Configuration   Bing   Legout Belie
Wireless	Global Configuration				Apply
<ul> <li>★ Access Points         <ul> <li>Al APs</li> <li>★ Ratios</li> <li>± 02.33s/n</li> <li>± 02.415s/n</li> <li>± 02.415s/n</li> </ul> </li> <li>Dead Canfiguration</li> </ul>	CDP CDP State	ų		High Availability A# Heartbeat Timesut(1-33)	50
Advanced Hesh HBEAP Groups 902.31a/n 902.31b/g/n Hedia Stream Gradin	Ethernet Interface# 0 1 2 3 Redio Slot# 0 1 2 2 2 3 1 2 2 3 2 3 2 3 2 3 3 4 3 4 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	COP State		Local Mode AP Test Heartbeet Time 30 H-REAP Mode AP Feat Heartbeet Timer AP Primery Discovery Timeout(30 to 3 Back-up Primary Controller PAddress Back-up Primary Controller name Back-up Secondary Controller IP Addr Back-up Secondary Controller name	Balance Disable Control Contro
Timers	3	P		TCP MSS	
+ QeS	Login Credentials			Globel TCP Adjust MSS	
	Disername Passaord Enable Password			AP Retransmit Config Parameters AP Retransmit Count AP Retransmit Interval	8
	802.1x Supplicant Cre 902.1x Authentication Username Password Canfirm Password	dentials			
	AP Failover Priority Gobal AP Failover Priorit AP Image Pre-downlos	ty Disable •			
	Download Primary Interchange Image	Develo	ad Backup		

**Singolarmente**Configurare i profili 802.1 x per access point. Nell'esempio riportato sotto, le credenziali verranno configurate per ciascun access point.Selezionare **Wireless > All AP** (Tutti gli access point), quindi selezionare l'access point in questione.Aggiungere il nome utente e la password nei campi **Credenziali richiedente** 



**Nota:** le credenziali di accesso vengono utilizzate per Telnet, SSH o console nell'access point.

3. Configurare la sezione Alta disponibilità e fare clic su **Applica**.

 cisco	MONITOR MUANS CONTROLLER WIRELESS SECURITY MUNAGEMENT COMMANDS HELP EEEDBACK	Days Configuration   Brig	Logout   Beives
Wireless	All APs > Details for 3502e	< Seck	Apply
<ul> <li>Access Points         All APs         Radios         392.118/m         S92.118/m         S92.118/m         S02.118/m         Bobel Configuration         Advanced         Hesh         HREAP Groups         S02.118/m         S02.118/m         S02.118/m         S02.118/m         Redia Stream         Country     </li> </ul>	General     Credentials     Interfaces     High Availability     Inventory     Advanced       Nome     Neme     Neme     Neme     Neme       Primary Controller     5566-3     192.268.75.44       Secondary Centreller     Image: Secondary Centreller       Tertiary Controller     Image: Secondary Centreller		
Timers > QuS			

Nota: una volta salvate, queste credenziali vengono conservate nel WLC e l'access point viene riavviato. Le credenziali cambiano solo quando il LAP si unisce a un nuovo WLC. Il LAP presume il nome utente e la password configurati sul nuovo WLC.Se l'access point non è ancora stato aggiunto a un WLC, è necessario eseguire la console nel LAP per impostare le credenziali. Usare questo comando CLI in modalità di abilitazione:LAP#Iwapp ap dot1x nomeutente <nomeutente>password <password> oLAP#capwap dot1x nomeutente

## **Configura switch**

Lo switch funge da autenticatore per il LAP e autentica il LAP su un server RADIUS. Se lo switch non dispone di software compatibile, aggiornarlo. Nella CLI dello switch, usare questi comandi per abilitare l'autenticazione 802.1x su una porta dello switch:

```
switch#configure terminal
switch(config)#dot1x system-auth-control
switch(config)#aaa new-model
!--- Enables 802.1x on the Switch. switch(config)#aaa authentication dot1x default group radius
switch(config)#radius server host 192.168.150.24 key cisco
!--- Configures the RADIUS server with shared secret and enables switch to send !--- 802.1x
information to the RADIUS server for authentication. switch(config)#ip radius source-interface
vlan 253
!--- We are sourcing RADIUS packets from VLAN 253 with NAS IP: 192.168.153.10.
switch(config)interface gigabitEthernet 0/11 switch(config-if)switchport mode access
switch(config-if)switchport access vlan 253 switch(config-if)mls qos trust dscp switch(config-
if)spanning-tree portfast !--- gig0/11 is the port number on which the AP is connected.
switch(config-if)dot1x pae authenticator !--- Configures dot1x authentication. switch(config-
if)dot1x port-control auto !--- With this command, the switch initiates the 802.1x
authentication.
```

**Nota:** se si hanno altri access point sullo stesso switch e non si desidera che utilizzino 802.1x, è possibile lasciare la porta non configurata per 802.1x o usare questo comando:

switch(config-if)authentication port-control force-authorized

LAP è autenticato con EAP-FAST. Se non si utilizza Cisco ACS 5.2, verificare che il server RADIUS in uso supporti questo metodo EAP.

La configurazione del server RADIUS è suddivisa in quattro passaggi:

- 1. Configurare le risorse di rete.
- 2. Configurare gli utenti.
- 3. Definire gli elementi dei criteri.
- 4. Applicare i criteri di accesso.

ACS 5.x è un ACS basato su regole. In altre parole, ACS 5.x utilizza un modello di criteri basato su regole anziché il modello basato su gruppi utilizzato nelle versioni 4.x.

Il modello di policy basato su regole ACS 5.x offre un controllo dell'accesso più potente e flessibile rispetto al precedente approccio basato su gruppi.

Nel modello basato su gruppi meno recente, un gruppo definisce i criteri in quanto contiene e associa tre tipi di informazioni:

- Informazioni sull'identità: queste informazioni possono essere basate sull'appartenenza a gruppi AD o LDAP oppure su un'assegnazione statica per gli utenti ACS interni.
- Altre restrizioni o condizioni restrizioni temporali, restrizioni di dispositivo e così via.
- Autorizzazioni VLAN o livelli di privilegio Cisco IOS<sup>®</sup>.

Il modello di policy di ACS 5.x si basa sulle seguenti regole:

If condition then result

Ad esempio, vengono utilizzate le informazioni descritte per il modello basato su gruppi:

If identity-condition, restricted-condition e authorization-profile.

Di conseguenza, questo ci offre la flessibilità di limitare le condizioni in base alle quali l'utente può accedere alla rete e anche il livello di autorizzazione consentito quando sono soddisfatte condizioni specifiche.

#### Configura risorse di rete

In questa sezione viene configurato il client AAA per lo switch sul server RADIUS.

In questa procedura viene illustrato come aggiungere lo switch come client AAA sul server RADIUS in modo che lo switch possa passare le credenziali utente del LAP al server RADIUS.

Attenersi alla seguente procedura:

- 1. Dall'interfaccia utente di ACS, fare clic su **Risorse di rete**.
- 2. Fare clic su Gruppi di dispositivi di rete.
- 3. Selezionare Posizione > Crea (in basso

+ 🛞 My Workspace	Network Resources > Network Device Groups > Location
Seturork Resources	Network Device Groups
<ul> <li>Network Device Groups</li> <li>Location</li> </ul>	Filter. Vlatch it Go
Network Devices and AAA Clients Default Network Device External RADIUS Servers	Name Description

4. Aggiungere i campi obbligatori e fare clic su **Invia**.

cisco Cisco Secure A	ics	
+ 🛞 My Workspace	Network Resources > Network Device Groups > Location > Create	
Vetwork Resources     Network Device Groups     Location     Device Type     Notwork Devices and AAA Clients     Default Network Device     External RADIUS Servers	Device Group - General         o Name:       LAB         Description:       LAB Devices         o Parent       All Locations         0 = Required fields	Select
<ul> <li>Users and identity Stores</li> </ul>		
Policy Elements		
Access Policies		
Monitoring and Reports		
System Administration		

5. La finestra viene aggiornata:

cisco Cisco Secure A	CS
🖌 💮 My Workspace	Network Resources > Network Device Groups > Location
🗸 🕼 Network Resources	Network Device Groups
<ul> <li>Network Device Groups</li> <li>Location</li> </ul>	Filter: 💽 Match if: 💽 Go 🗢
Device Type Network Devices and AAA Clients Default Network Device External RADIUS Servers	Name      Description     * <u>All Locations</u>
B Users and Identity Stores	LAB LAB Devices
► Step Policy Elements	
Access Policies	
Monitoring and Reports	
🖌 🍓 System Administration	

6. Selezionate Tipo periferica (Device Type) > Crea (Create).

cisco Cisco Secure A	CS
<ul> <li>My Workspace</li> </ul>	Network Resources > Network Device Groups > Device Type > Edit "Device Type:Al Device Types:Switche
Ketwork Resources     Network Device Groups     Location     Device Type     Network Devices and AAA Clients     Default Network Device     External RADIUS Servers	Device Group - General         Ø Name:       Switches         Description:       Switch where LAP is connected         Ø Parent:       All Device Types         Ø = Required fields
Users and Identity Stores	
Policy Elements	
+ 🛴 Access Policies	
Monitoring and Reports	Aller Willing the second states and
+ 🧏 System Administration	Carles and the second of the second

7. Fare clic su Invia. Al termine, la finestra viene

cisco Cisco Secure A	CS
▶ 💮 My Workspace	Network Resources > Network Device Groups > Device Type
🗸 🕼 Network Resources	Network Device Groups
<ul> <li>Network Device Groups</li> <li>Location</li> </ul>	Filter. Match it: Go 🗢
Device Type	
Network Devices and AAA Clients	🗖 Name 🔺 Description
External RADIUS Servers	All Device Types All Device Types
<ul> <li>Business and Identity Stores</li> </ul>	Switches Switch where LAP is connected
Policy Elements	
Access Policies	
Monitoring and Reports	
🔹 🍇 System Administration	

aggiornata:

- 8. Selezionare Risorse di rete > Dispositivi di rete e client AAA.
- 9. Fare clic su **Create** (Crea) e immettere i dettagli come illustrato di seguito:

+ 🛃 Ny Workspace	Network Resources > Network Devices and AAA Clerks > Create	
Ign Retwork Reserves     Network/Device Groups     Location     Device Tros     Network Devices and AuAClevits     Default Network Device     External RADUS Barvers	Nama: 2500-Switch-LAP     Description: Switch where LAP is connected     Network Device Groups     Location	Select
W. Users and Identity Stores     Policy Elements     Corece Policies     Nontoring and Reports     System Administration	P Address P Single IP Address (* IP Range(s) o IP [192:168.153.10]	Aethentication Options TAGACB+ RADUS Ghared Secret clacs CsApart 1790
		F Enable KeyWrap Key Encryption Key Message Aethenticator Cede Key Key Input Format C ASCI P HEXADECIMA

10. Fare clic su **Invia**. La finestra viene aggiornata:

cisco Cisco Secure A	s				ecostran	SAUL-AC
+ 🔂 Mr Workspace	Network Resources > Net	work Devises and AAA Clent	8			
<ul> <li>An Network Resources</li> </ul>	Network Devices					Showin
Network Device Groups     Location	Filter:	💌 Match itt.	▼ Go	v		
Network Devices and AM-Clients	T Name	▲ IP/Mask	NDG:Location	NDG:Device Type	Description	
Detault Network Device External RADIUS Servers	C 3560-Switch-	LAP 192.168.153.10/32	All Locations:LAB	All Device Types:Switches	Switch where LAP is connected	1
· S Users and identity stores						
Policy Elements						
Access Polices						

## Configura utenti

In questa sezione viene illustrato come creare un utente sul server ACS configurato in precedenza. L'utente verrà assegnato a un gruppo denominato "utenti LAP".

Attenersi alla seguente procedura:

1. Andare a Utenti e archivi identità > Gruppi di identità >

#### Crea.

Cisco Secure /     MyWorkspace	ACS Users and Identity Stores > Identity Groups > Edit: "IdentityGroup:All Groups:Wireless Users"
Interwork Resources     Identity Stores     Identity Groups     Internal Identity Stores     External Identity Stores     LDAP	General Vame: LAP users Description: LAPs authenticating over wired Network. Value Parent All Groups Select Call = Required fields
Active Directory RSA SecuriD Token Servers RADIUS Identity Servers Certificate Authorities Certificate Authentication Profile Identity Store Sequences	

2. Fare clic su

Invia.
--------

Cisco Secure A	CS
My Workspace	Users and Identity Stores > Identity Groups
Network Resources	Identity Groups
Signature and Identity Stores  Identity Groups	Filter: Go 👻
<ul> <li>Internal Identity Stores</li> <li>External Identity Stores         <ul> <li>LDAP</li> <li>Active Directory</li> <li>RSA SecurID Token Servers</li> <li>RADIUS Identity Servers</li> </ul> </li> </ul>	Name       Description         All Groups       Identity Group Root         LAP users       LAPs authenticating over wired Network.
Certificate Authorities Certificate Authentication Profile Identity Store Sequences	

- 3. Creare lo switch 3502e assegnarlo al gruppo "utenti LAP".
- 4. Andare a Utenti e archivi identità > Gruppi di identità > Utenti >



- Crea.
- 5. Verranno visualizzate le informazioni aggiornate:

🚭 My Workspace	Users and	Identity Store	s > Internal Identity Sto	nes >	Users	
(b) Network Resources	Interna	Users				
Users and Identity Stores	Filter:	[	Match if:		• G0 •	~
Internal identity Stores	Г	Status	User Name		Identity Group	Description
Usars			35024		All Groups:LAP users	LAP 3502e in vian 253

## Definizione degli elementi dei criteri

Verificare che l'opzione Permit Access sia impostata.

cisco Cisco Secure A	ICS III III III III III III III III III
+ 💮 My Workspace	Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles
Network Resources	Authorization Profiles
Users and identity Stores	Eltar 🔹 Match if 💽 🛃 🚱 🕱
<ul> <li>Q: Policy Elements</li> </ul>	
Session Conditions     Authorization and Permissions	Permit Access
<ul> <li>Network Access Authorization Profiles         </li> </ul>	
Device Administration     Named Permission Objects	
+ 🔂 Access Policies	
<ul> <li>Monitoring and Reports</li> </ul>	
🕨 🍓 System Administration	

## Applica criteri di accesso

In questa sezione, selezionare EAP-FAST come metodo di autenticazione usato per i LAP per l'autenticazione. Le regole verranno quindi create in base ai passaggi precedenti.

Attenersi alla seguente procedura:

 Selezionare Access Policies > Access Services > Default Network Access > Edit: "Default Network Access".

A H W I I		
<ul> <li>My Workspace</li> </ul>	Access Policies > Access Services > Default Network Access > Edit "Defau	t Network Acc
Network Resources		
🔐 Users and Identity Stores	General Allowed Protocols	
Sp. Policy Elements	Name: Default Network Access	
🐁 Access Policies	Description: Default Network Access Service	
Access Services	Service Type : Network Access	
Default Device Admin	Policy Structure	
Default Network Access	Identity	
▶ Ø deleteme	Group Mapping	
Monitoring and Reports		

2. Accertarsi di aver abilitato EAP-FAST e la preparazione anonima della PAC in banda.



• 🛃 Access Policies	► E Allow LEAP
Access Services     If Service Selection Rules     O Default Device Admin     O Default Network Access     Idently     Authorization     Ø deleteme     Monitoring and Reports     Ø System Administration	<ul> <li>▼ Allow PEAP</li> <li>PEAP Inner Methods</li> <li>▼ Allow EAP-MS-CHAPv2</li> <li>▼ Allow Password Change Retries: 1</li> <li>▼ Allow EAP-GTC</li> <li>▼ Allow Password Change Retries: 1</li> </ul>
	<ul> <li>Allow EAP-FAST</li> <li>EAP-FAST Inner Methods</li> <li>Allow EAP-MS-CHAPv2</li> <li>Allow Password Change Retries: 3</li> <li>Allow EAP-GTC</li> <li>Allow TL3-Renegotiation</li> <li>Use PACs Don't Use PACs</li> <li>Tunnel PAC Time To Live: 90</li> <li>Proactive PAC update will occur after 10</li> <li>% of PAC Time To Live has expired</li> <li>Allow Authenticated In-Band PAC Provisioning</li> <li>Server Returns Access Accept After Authenticated Provisioning</li> <li>Allow Nachine Authentication</li> <li>Machine PAC Time To Live: 1</li> <li>Weeks </li> <li>Enable Stateless Session Resume</li> <li>Authorization PAC Time To Live: 1</li> <li>Hours </li> </ul>
	Submit Cancel

- 3. Fare clic su Invia.
- 4. Verificare il gruppo di identità selezionato. In questo esempio, utilizzare **Internal Users** (creato su ACS) e salvare le modifiche.

cisco Cisco Secure A	CS academin SAL
<ul> <li>My Workspace</li> <li>My Network Resources</li> </ul>	Access Policies > Access Services > Default Network Access > Mently
B Users and Identity Stores     S Policy Elements	Nonthly Source: Internal Users Select
C. Access Policies     Access Services     Service Selection Rules     O Detault Device Admin     O Detault Network Access	Absanced options     If authentication failed Reject     If user notifound Reject     If process failed Drop     Note: For authentications using PEAP, LEAP, EAP-PAST or RADIUS MSCHAP is is not possible to continue
Authorization	processing when authentication fails or user is not found. If continue option is selected in these cases, requests will be rejected

5. Per verificare il profilo di autorizzazione, selezionare Access Policies > Access Services > Default Network Access > Authorization (Policy di accesso > Servizi di accesso > Accesso di rete predefinito > Autorizzazione).Èpossibile personalizzare in base a quali condizioni si consentirà a un utente l'accesso alla rete e a quali profili di autorizzazione (attributi) si

passerà dopo l'autenticazione. Questa granularità è disponibile solo in ACS 5.x. Nell'esempio sono selezionati Location, **Device Type**, **Protocol**, **Identity Group** e **EAP Authentication Method**.



- 6. Fare clic su OK, quindi su Salva modifiche.
- 7. Il passaggio successivo consiste nella creazione di una regola. Se non viene definita alcuna regola, è consentito l'accesso LAP senza condizioni.
- Selezionate Crea (Create) > Regola-1 (Rule-1). Questa regola è destinata agli utenti del gruppo "utenti

LAP".

cisco Cisco Secure Al	S					
+ 🕀 My Workspace	Access Palkies > Acce	ess Services > Defaul	Network Access > Authoriz	ation		
+ 🞲 Network Resources	Standard Policy Ex	caption Policy				
+ 🎎 Users and identity Stores	Net Care Serute	ACS - Movilla Finairea				×
<ul> <li>Q. Policy Elements</li> </ul>	[ [ ]	No Martin Martin				-
- 🕵 Access Policies	192,168	150.24 https://192.	168-150-24/acsadmin/Polic	yinputAction.de		17
Access Services     E Service Selection Rules     Ø Default Device Admin     O Default Network Access     Identity     Constants	1 General Name	Rule-1 The Customize policy condition	Status: Enabled	the policy rules screen liable here for use in policy rules.	controts which	
Monitoring and Reports		point, construction				
System Administration	Conditio	188				
	M NDA	SiLocation:	in line	All Locations:LAB	Select	
	M ND	G:Device Type:	in in	All Device Types Switches	Select	
	Prof	locol:	maton	• Radus	Select	
	M Ider	ntty Group:		- All Groups DAP users	Select Q	
	Results Authoriz Sele	ation Profiles: Access at Deselect		You may select multiple authorization defined in multiple profiles will use th profile defined.	profiles. Attributes le value from the first	
		ancel auti Free licate   • ] Elda ]	tules defined or no enabl	• ied rule matches. 	He	etp

9. Fare clic su **Salva modifiche**. Se si desidera negare agli utenti che non soddisfano le condizioni, modificare la regola predefinita in "Nega accesso".

cisco Cisco Secure A	CS SALE ACSU IN	renery) Lig Dut About He
	Access Pilicies > Access Services > Default lintwork Access > Authorization Standoord Policy <u>Exception Policy</u> Network Access Authorization Policy Filter Status • Match it Equals • Enabled • Crear Filter Go ▼	
Access Services     Envice Selecton Rules     Orfeet Dovice Admin     Orfeet Network Access     Incents     OrdestEnte     Montseng and Reports     Montseng and Reports     Montseng and Reports	Status         Name         Conditions           Status         NDGLocation         NDGDevice Type         Protocol         Homely Group         Eao Authentication Method           @         Butch         M All LocationessLAB         In All Device Types Dwtches         match Radua         In All Droups LAP users         -All'entication Method	Results Hi Actholoxion Profiles Permit Access 0
	Extant     Ene rules defined or no enabled rule matches.      Create I = Dusticate I = Edit Define	Permit Access Custemize HttCount

10. L'ultimo passo consiste nel definire le regole di selezione del servizio. Utilizzare questa pagina per configurare un criterio semplice o basato su regole per determinare il servizio da

applicare alle richieste in ingresso. Ad esempio:

A My Workspace	Access P	uicies > A	ccess Services >	Service Selection Rules		
Network Resources	C Sr	de result	selection @ F	Rule based result selection		
🚜 Users and Identity Stores	Servic	e Salecti	on Policy			
Sy Policy Elements	Filter	Status	w Match it	Equals + Enabled + Clea	ar Filter   Go   🖛	
Access Policies		C S	tatus Name	Conditions	Resulta Service	Hit Count
Default Device Admin	1		B Rule-1	match Radius	Default Network Access	0
O Detault Network Access     Identity     Authorization     Ø determe	2	-	Rule-2	match Tacacs	Detault Device Admin	0
Replace and Reports						

# **Verifica**

Dopo aver abilitato 802.1x sulla porta dello switch, tutto il traffico, ad eccezione del traffico 802.1x, viene bloccato tramite la porta. Il LAP, già registrato sul WLC, viene dissociato. Solo dopo un'autenticazione 802.1x riuscita è consentito il passaggio di altro traffico. La corretta registrazione del LAP sul WLC dopo l'abilitazione della versione 802.1x sullo switch indica che l'autenticazione LAP è riuscita.

Console AP:

```
*Jan 29 09:10:24.048: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to
  192.168.75.44:5246
*Jan 29 09:10:27.049: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to
   192.168.75.44:5247
!--- AP disconnects upon adding dot1x information in the gig0/11. *Jan 29 09:10:30.104: %WIDS-5-
DISABLED: IDS Signature is removed and disabled. *Jan 29 09:10:30.107: %CAPWAP-5-CHANGED: CAPWAP
changed state to DISCOVERY *Jan 29 09:10:30.107: %CAPWAP-5-CHANGED: CAPWAP changed state to
DISCOVERY *Jan 29 09:10:30.176: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
administratively down *Jan 29 09:10:30.176: %LINK-5-CHANGED: Interface Dotl1Radio1, changed
state to administratively down *Jan 29 09:10:30.186: %LINK-5-CHANGED: Interface Dot11Radio0,
changed state to reset *Jan 29 09:10:30.201: %LINK-3-UPDOWN: Interface Dot11Radio1, changed
state to up *Jan 29 09:10:30.211: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Jan 29 09:10:30.220: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to reset Translating
"CISCO-CAPWAP-CONTROLLER"...domain server (192.168.150.25) *Jan 29 09:10:36.203: status of
voice_diag_test from WLC is false
*Jan 29 09:11:05.927: %DOT1X_SHIM-6-AUTH_OK: Interface GigabitEthernet0 authenticated [EAP-FAST]
*Jan 29 09:11:08.947: %DHCP-6-ADDRESS_ASSIGN: Interface GigabitEthernet0 assigned DHCP address
192.168.153.106, mask 255.255.255.0, hostname 3502e
!--- Authentication is successful and the AP gets an IP. Translating "CISCO-CAPWAP-
CONTROLLER.Wlab"...domain server (192.168.150.25) *Jan 29 09:11:37.000: %CAPWAP-5-DTLSREQSEND:
DTLS connection request sent peer_ip: 192.168.75.44 peer_port: 5246 *Jan 29 09:11:37.000:
%CAPWAP-5-CHANGED: CAPWAP changed state to *Jan 29 09:11:37.575: %CAPWAP-5-DTLSREQSUCC: DTLS
connection created successfully peer_ip: 192.168.75.44 peer_port: 5246 *Jan 29 09:11:37.578:
%CAPWAP-5-SENDJOIN: sending Join Request to 192.168.75.44 *Jan 29 09:11:37.578: %CAPWAP-5-
CHANGED: CAPWAP changed state to JOIN
*Jan 29 09:11:37.748: %CAPWAP-5-CHANGED: CAPWAP chan
```

wmmAC status is FALSEged state to CFG \*Jan 29 09:11:38.890: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to

```
down
*Jan 29 09:11:38.900: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
  reset
*Jan 29 09:11:38.900: %CAPWAP-5-CHANGED: CAPWAP changed state to UP
*Jan 29 09:11:38.956: %CAPWAP-5-JOINEDCONTROLLER: AP has joined controller
   5508-3
*Jan 29 09:11:39.013: %CAPWAP-5-DATA_DTLS_START: Starting Data DTLS handshake.
  Wireless client traffic will be blocked until DTLS tunnel is established.
*Jan 29 09:11:39.013: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Jan 29 09:11:39.016: %LWAPP-3-CLIENTEVENTLOG: SSID goa added to the slot[0]
*Jan 29 09:11:39.028: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to
  down
*Jan 29 09:11:39.038: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to
  reset
*Jan 29 09:11:39.054: %LINK-3-UPDOWN: Interface Dot11Radiol, changed state to up
*Jan 29 09:11:39.060: %LINK-3-UPDOWN: Interface DotllRadio0, changed state to
  down
*Jan 29 09:11:39.069: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
  reset
*Jan 29 09:11:39.085: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Jan 29 09:11:39.135: %LWAPP-3-CLIENTEVENTLOG: SSID goa added to the slot[1]DTLS
  keys are plumbed successfully.
*Jan 29 09:11:39.151: %CAPWAP-5-DATA_DTLS_ESTABLISHED: Data DTLS tunnel
  established.
*Jan 29 09:11:39.161: %WIDS-5-ENABLED: IDS Signature is loaded and enabled
!--- AP joins the 5508-3 WLC.
Log ACS:
```

 Visualizza il numero di accessi:Se si stanno controllando i registri entro 15 minuti dall'autenticazione, assicurarsi di aggiornare il numero di accessi. Nella stessa pagina, nella parte inferiore è presente la scheda Conteggio visite.

cisco Cisco Secure Ad	CS						ace			
+ 🛞 My Workspace	Access	Policies	> Access	Services >	Service Selection Rules					
+ 🎲 Network Resources	0.9	Sincle result selection 🔎 Rule based result selection								
+ 🏭 Users and Identity Stores	Serv	Service Selection Policy								
+ Q. Policy Elements	Filte	: Stat	.is •	Match if:	Equals - Enabled -	Clear Filter   Go   👻				
f. Access Policies     Access Services		-	Status	Name	Conditions	Results Service	Hit Count			
Historie State Controlled      Historie Device Admin	1			Bule-1	match Radius	Default Network Access	1			
<ul> <li>Ø Default Network Access</li> </ul>	2			Rule-2	match Tacaca	Default Device Admin	0			
Authorization    Authorization										
<ul> <li>System Administration</li> </ul>										

- A B. Washington	URALLANDA AND AND AND AND AND AND AND AND AND										
a 25 mi un centre	Access Policies + Access Services + C	unaut Network Access + Authorizat	ian				1988				
» 15 Network Resources	Standard Daliesi Exception Delive										
> 😹 Users and Identity Stores	Statute for a function of the	envere Frenzy <u>Frenzy State</u>									
> 🕞 Policy Elements	NUCLORK ACCESS ADDICT/200011	NECHOFK ACCESS AUDIORIZATION PORCY									
- 📕 Access Polices	Filter   Diatus	Batch It Equals •	Enabled •	Clear Filter Co 🔻							
<ul> <li>Access Services</li> <li>T Revice Relation Relation</li> </ul>	Name NDGLocation	NDG Device Type	Conditions Protocol	Identity Group	Esp Authentication Method	Results Authorization Profiles	HE Count				
<ul> <li>Default Device Admin</li> </ul>	Rule-1 In Al Locations LAB	In All Device Types Switches	match Radius	In All Groups LAP users	-4017-	Permit Access	1				
Americanie • V dalataria											
<ul> <li>Monitoring and Reports</li> </ul>											
» 😽 Dydlem Administration											
	1 If nondes defined or Create 1 - Duplicate 1 - Ed	no esebled rule matches. 81 Detaile A Move to.	1.			Permit Access Customize	e 🗗				

2. Fare clic su **Monitoraggio e report** per visualizzare una nuova finestra popup. Fare clic su **Autenticazioni -RADIUS -Oggi**. È inoltre possibile fare clic su **Dettagli** per verificare quale regola di selezione del servizio è stata applicata.

🔁 🖻								Launch Interact	ive Warwar
Showing Page	e 1 of 1			I Gata i	lage: Ge				
AAA Protocol > RAD	US Authentication	n							
Authentication Status : Date :	Pass or Pail January 25, 2012 (La	ust 30 Minutes I Last Hi	tur i Last 12 Hours i To	day i <u>Yesferdar i Last 7 Das</u>	(Last 30 Days )				
Generated on January 2	29, 2012 9:15:01 PM E	ST							
Rebei	t → Click for details	9 -House over item	for additional informa	tion					
Logged At	RADUS NAS Status Failure	Details Usemame	MACIP Address	Access Service	Authentication Method	Network Device	NAS IP Address	NAS Port ID	CTS Security Gr
Jan 29,12 9 11:12 966	PM 🖌	S 3502e	CC-EF-48-FA-53-19	Default Network Access	EAP-FAST (EAP-NSCHAP\2)	3560-Switch-LAP	192.168,153.10	GicabtEthemet0/11	

# Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

# Informazioni correlate

- <u>Cisco Secure Access Control System</u>
- Documentazione e supporto tecnico Cisco Systems

#### 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).