

# Politiche ISE basate su esempi di configurazione SSID

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Configurazione](#)

[Configurazioni](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

## [Introduzione](#)

In questo documento viene descritto come configurare i criteri di autorizzazione in Cisco Identity Services Engine (ISE) per distinguere tra diversi identificatori di set di servizi (SSID). È molto comune per un'organizzazione avere più SSID nella propria rete wireless per vari scopi. Uno degli scopi più comuni è disporre di un SSID aziendale per i dipendenti e di un SSID ospite per i visitatori dell'organizzazione.

La presente guida presuppone che:

1. Il controller WLC (Wireless LAN Controller) è configurato e funziona per tutti gli SSID coinvolti.
2. L'autenticazione funziona su tutti gli SSID coinvolti nell'ISE.

### Altri documenti di questa serie

- [Esempio di autenticazione Web centrale con uno switch e configurazione di Identity Services Engine](#)
- [Esempio di autenticazione Web centralizzata su WLC e ISE](#)
- [Esempio di configurazione degli account ISE Guest per l'autenticazione RADIUS/802.1x](#)
- [VPN Inline Posture con iPEP ISE e ASA](#)

## [Prerequisiti](#)

### [Requisiti](#)

Nessun requisito specifico previsto per questo documento.

## Componenti usati

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

- Controller LAN wireless release 7.3.101.0
- Identity Services Engine release 1.1.2.145

Le versioni precedenti presentano entrambe queste caratteristiche.

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 [Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti](#).

## Configurazione

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

**Nota:** per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo [strumento di ricerca](#) dei comandi (solo utenti [registrati](#)).

## Configurazioni

Nel documento vengono usate queste configurazioni:

- Metodo 1: Airespace-Wlan-Id
- Metodo 2: Called-Station-ID

Utilizzare un solo metodo di configurazione alla volta. Se entrambe le configurazioni vengono implementate contemporaneamente, la quantità elaborata da ISE aumenta e influisce sulla leggibilità delle regole. In questo documento vengono esaminati i vantaggi e gli svantaggi di ciascun metodo di configurazione.

### **Metodo 1: Airespace-Wlan-Id**

Ogni rete WLAN (Wireless Local Area Network) creata sul WLC ha un ID WLAN. L'ID WLAN viene visualizzato nella pagina di riepilogo WLAN.

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	Corporate	Corporate	Enabled	[WPA2][Auth(802.1X)]
2	WLAN	Guest	Guest	Enabled	MAC Filtering

Quando un client si connette al SSID, la richiesta RADIUS a ISE contiene l'attributo Airespace-WLAN-ID. Questo semplice attributo viene utilizzato per prendere decisioni relative alle policy ad ISE. Uno svantaggio di questo attributo è che l'ID WLAN non corrisponde su un SSID distribuito su più controller. Se in questo modo viene descritta la distribuzione, passare al metodo 2.

In questo caso, come condizione viene usato Airespace-Wlan-Id. Può essere utilizzato come condizione semplice (da sola) o in una condizione composta (insieme a un altro attributo) per ottenere il risultato desiderato. Questo documento descrive entrambi i casi di utilizzo. Con i due SSID sopra indicati è possibile creare queste due regole.

- A) Gli utenti guest devono accedere al SSID guest.
- B) Gli utenti aziendali devono appartenere al gruppo "Domain Users" di Active Directory (AD) e devono accedere al SSID aziendale.

### Regola A

La regola A prevede un solo requisito, pertanto è possibile creare una condizione semplice (basata sui valori indicati in precedenza):

1. Ad ISE, vai a **Policy > Policy Elements > Conditions > Authorization > Simple Conditions** (Policy > Elementi della policy > Condizioni > Autorizzazione > Condizioni semplici) e crea una nuova condizione.
2. Nel campo Nome immettere un nome di condizione
3. Nel campo Descrizione immettere una descrizione (facoltativo).
4. Dall'elenco a discesa Attributo, scegliere **Airespace > Airespace-Wlan-Id—[1]**.
5. Dall'elenco a discesa Operatore, scegliere **Uguale a**.
6. Dall'elenco a discesa Valore (Value), selezionate **2**.
7. Fare clic su **Salva**.

Authorization Simple Condition List > GuestSSID

**Simple Condition**

\* Name: GuestSSID

Description: Airespace:Airespace-Wlan-Id EQUALS 1

\* Attribute: Airespace:Airespace-Wlan-Id    \* Operator: Equals    \* Value: 2

Save    Reset

## Regola B

La regola B prevede due requisiti, pertanto è possibile creare una condizione composta in base ai valori riportati sopra:

1. Ad ISE, vai a **Policy > Policy Elements > Conditions > Authorization > Compound Conditions** e crea una nuova condizione.
2. Nel campo Nome immettere un nome di condizione.
3. Nel campo Descrizione immettere una descrizione (facoltativo).
4. Scegliere **Crea nuova condizione (opzione avanzata)**.
5. Dall'elenco a discesa Attributo, scegliere **Airespace > Airespace-Wlan-Id—[1]**.
6. Dall'elenco a discesa Operatore, scegliere **Uguale a**.
7. Dall'elenco a discesa Valore (Value), selezionate **1**.
8. Fare clic sull'ingranaggio a destra e scegliere **Aggiungi attributo/valore**.
9. Dall'elenco a discesa Attributo, scegliere **AD1 > Gruppi esterni**.
10. Dall'elenco a discesa Operatore, scegliere **Uguale a**.
11. Dall'elenco a discesa Valore (Value), selezionate il gruppo desiderato. In questo esempio viene impostato su Domain Users.
12. Fare clic su **Salva**.

The screenshot shows the Cisco Identity Services Engine (ISE) interface for creating a new Authorization Compound Condition. The breadcrumb navigation is 'Authorization Compound Condition List > New Authorization Compound Condition'. The form includes the following fields:

- \* Name:** CorporateSSID
- Description:** (empty text area)
- \*Condition Expression:** A table with two rows and three columns: Condition Name, Expression, and Operator. The first row contains 'Airespace:Airespace', 'Equals', and '1'. The second row contains 'AD1:ExternalGroups', 'Equals', and 'Domain Users'. The table is connected by an 'AND' operator.

Buttons for 'Submit' and 'Cancel' are located at the bottom of the form.

**Nota:** in questo documento vengono utilizzati semplici profili di autorizzazione configurati in Criteri > Elementi criteri > Risultati > Autorizzazione > Profili di autorizzazione. Sono impostate su Consenti accesso, ma possono essere adattate alle esigenze dell'installazione.

Ora che abbiamo le condizioni, possiamo applicarle alla politica di autorizzazione. Andare a **Criteri > Autorizzazione**. Determinare dove inserire la regola nell'elenco o modificare la regola esistente.

## Regola Guest

1. Fare clic sulla freccia rivolta verso il basso a destra di una regola esistente e scegliere **Inserisci nuova regola**.
2. Immettere un nome per la regola ospite e lasciare il campo Gruppi di identità impostato su Qualsiasi.
3. In Condizioni, fare clic sul segno più e fare clic su **Seleziona condizione esistente dalla**

libreria.

4. In Nome condizione scegliere **Condizione semplice > GuestSSID**.
5. In Autorizzazioni, scegliere il profilo di autorizzazione appropriato per gli utenti guest.
6. Selezionate **Fatto (Done)**.

### Regola aziendale

1. Fare clic sulla freccia rivolta verso il basso a destra di una regola esistente e scegliere **Inserisci nuova regola**.
2. Immettere un nome per la regola aziendale e lasciare il campo Gruppi di identità impostato su Qualsiasi.
3. In Condizioni, fare clic sul segno più e fare clic su **Seleziona condizione esistente dalla libreria**.
4. In Nome condizione scegliere **Condizione composta > CorporateSSID**.
5. In Autorizzazioni scegliere il profilo di autorizzazione appropriato per gli utenti aziendali.
6. Selezionate **Fatto (Done)**.

**Nota:** finché non si fa clic su Salva in fondo all'elenco dei criteri, alla distribuzione non verrà applicata alcuna modifica apportata in questa schermata.

The screenshot displays the Cisco Identity Services Engine (ISE) interface for configuring an Authorization Policy. The page title is "Authorization Policy" and it includes instructions: "Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order." A dropdown menu shows "First Matched Rule Applies". Below this, there is an "Exceptions (0)" section and a "Standard" section containing a table of rules.

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	CorporateWireless	if CorporateSSID	then CorporateWireless
<input checked="" type="checkbox"/>	GuestWireless	if GuestSSID	then GuestWireless
<input checked="" type="checkbox"/>	Default	if no matches, then	PermitAccess

At the bottom of the table, there are "Save" and "Reset" buttons.

### Metodo 2: Called-Station-ID

Il WLC può essere configurato per inviare il nome SSID nell'attributo RADIUS Called-Station-ID, che a sua volta può essere utilizzato come condizione su ISE. Il vantaggio di questo attributo è che può essere utilizzato indipendentemente dall'ID WLAN impostato sul WLC. Per impostazione predefinita, il WLC non invia il SSID nell'attributo Called-Station-ID. Per abilitare questa funzione sul WLC, selezionare **Security > AAA > RADIUS > Authentication** (Sicurezza > AAA > RADIUS > Autenticazione) e impostare Call Station ID Type (Tipo di ID stazione di chiamata) su AP MAC Address:SSID (Indirizzo MAC AP:SSID). In questo modo il formato dell'ID stazione chiamata viene impostato su *<MAC dell'access point a cui l'utente si sta connettendo>:<SSID Name>*.



Dalla pagina di riepilogo della WLAN è possibile visualizzare il nome SSID che verrà inviato.



Poiché l'attributo Called-Station-Id contiene anche l'indirizzo MAC dell'access point, viene utilizzata un'espressione regolare (REGEX) per far corrispondere il nome SSID nella policy ISE. L'operatore 'Corrispondenze' nella configurazione della condizione può leggere un REGEX dal campo Valore.

## Esempi di REGEX

**'Inizia con'**—ad esempio, utilizzare il valore REGEX di **^(Acme).\***—questa condizione è configurata come CERTIFICATE:Organization MATCHES 'Acme' (qualsiasi corrispondenza con una condizione che inizia con "Acme").

**'Termina con'**—ad esempio, utilizzare il valore REGEX **.\*(mktg)\$**—questa condizione è configurata come CERTIFICATE:Organization MATCHES 'mktg' (qualsiasi corrispondenza con una condizione che termina con "mktg").

**'Contiene'**—ad esempio, utilizzare il valore REGEX **.\*(1234).\***—questa condizione è configurata come CERTIFICATE:L'organizzazione CORRISPONDE a '1234' (qualsiasi corrispondenza con una condizione che contiene "1234", ad esempio Eng1234, 1234Dev e Corp1234Mktg).

**'Non inizia con'**—ad esempio, utilizzare il valore REGEX di **^(?!LDAP).\***—questa condizione è configurata come CERTIFICATE:Organization MATCHES 'LDAP' (qualsiasi corrispondenza con una condizione che non inizia con "LDAP", come usLDAP o CorpLDAPmktg).

L'ID della stazione chiamata termina con il nome SSID, quindi il REGEX da utilizzare nell'esempio è **.\*(<NOME SSID>)\$**. Tenere presente questa condizione durante la configurazione.

Con i due SSID sopra indicati, è possibile creare due regole con i seguenti requisiti:

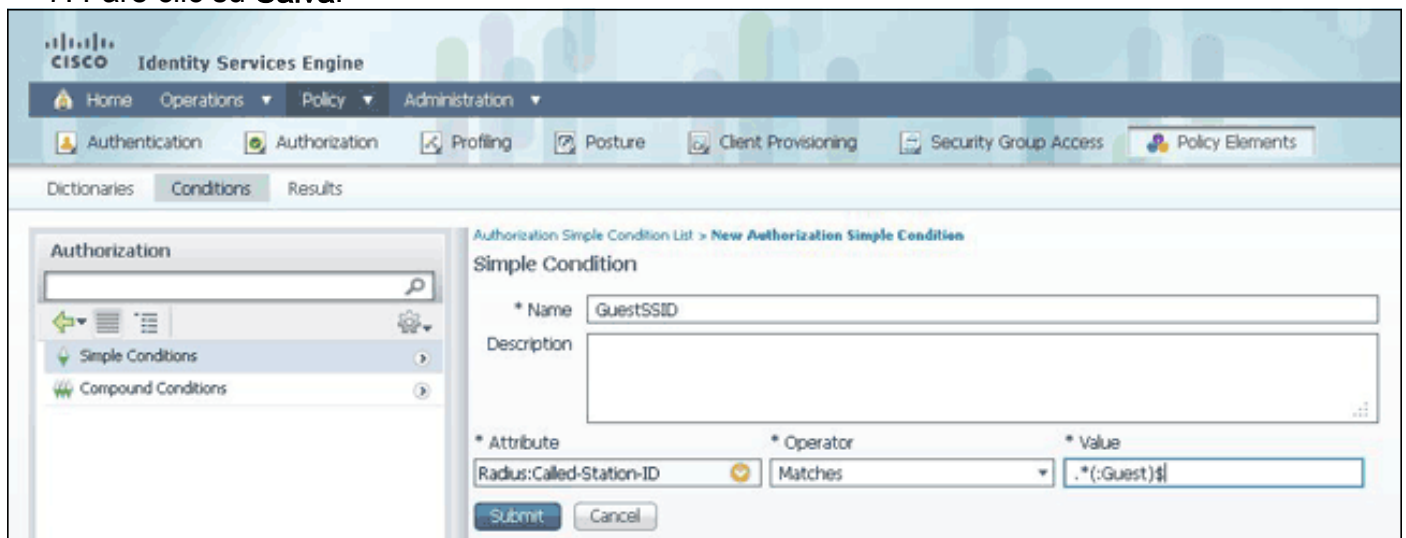
A) Gli utenti guest devono accedere al SSID guest.

B) Gli utenti aziendali devono appartenere al gruppo AD "Utenti del dominio" e devono accedere al SSID aziendale.

## Regola A

La regola A prevede un solo requisito, pertanto è possibile creare una condizione semplice (basata sui valori indicati in precedenza):

1. Ad ISE, vai a **Policy > Policy Elements > Conditions > Authorization > Simple Conditions** (Policy > Elementi della policy > Condizioni > Autorizzazione > Condizioni semplici) e crea una nuova condizione.
2. Nel campo Nome immettere un nome di condizione.
3. Nel campo Descrizione immettere una descrizione (facoltativo).
4. Dall'elenco a discesa Attributo (Attribute), selezionate **Raggio (Radius) -> ID stazione chiamata (Called-Station-ID)-[30]**.
5. Dall'elenco a discesa Operatore, scegliere **Corrispondenze**.
6. Dall'elenco a discesa Valore, scegliere **.\*(:Guest)\$**. Questa operazione fa distinzione tra maiuscole e minuscole.
7. Fare clic su **Salva**.



The screenshot displays the Cisco Identity Services Engine (ISE) web interface. The top navigation bar shows 'Home', 'Operations', 'Policy', and 'Administration'. Below this, there are tabs for 'Authentication', 'Authorization', 'Profiling', 'Posture', 'Client Provisioning', 'Security Group Access', and 'Policy Elements'. The 'Policy Elements' tab is active, and the 'Conditions' sub-tab is selected. The main content area is titled 'Authorization Simple Condition List > New Authorization Simple Condition'. It features a search bar and a list of conditions. The 'Simple Conditions' list is expanded, showing a search bar and a list of conditions. The 'Simple Condition' configuration form is visible, with the following fields: 'Name' (GuestSSID), 'Description' (empty), 'Attribute' (Radius:Called-Station-ID), 'Operator' (Matches), and 'Value' (.\*(:Guest)\$). There are 'Submit' and 'Cancel' buttons at the bottom of the form.

## Regola B

La regola B prevede due requisiti, pertanto è possibile creare una condizione composta in base ai valori riportati sopra:

1. Ad ISE, vai a **Policy > Policy Elements > Conditions > Authorization > Compound Conditions** e crea una nuova condizione.
2. Nel campo Nome immettere un nome di condizione.
3. Nel campo Descrizione immettere una descrizione (facoltativo).
4. Scegliere **Crea nuova condizione (opzione avanzata)**.
5. Dall'elenco a discesa Attributo (Attribute), selezionate **Raggio (Radius) -> Id stazione chiamata (Called-Station-Id)—[30]**.
6. Dall'elenco a discesa Operatore, scegliere **Corrispondenze**.
7. Dall'elenco a discesa Valore, scegliere **.\*(:Aziendale)\$**. Questa operazione fa distinzione tra maiuscole e minuscole.
8. Fare clic sull'ingranaggio a destra e scegliere **Aggiungi attributo/valore**.
9. Dall'elenco a discesa Attributo, scegliere **AD1 > Gruppi esterni**.
10. Dall'elenco a discesa Operatore, scegliere **Uguale a**.
11. Dall'elenco a discesa Valore (Value), selezionate il gruppo desiderato. In questo esempio

viene impostato su Domain Users.

## 12. Fare clic su **Salva**.

The screenshot displays the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes 'Home', 'Operations', 'Policy', and 'Administration'. Below this, there are tabs for 'Authentication', 'Authorization', 'Profiling', 'Posture', 'Client Provisioning', 'Security Group Access', and 'Policy Elements'. The 'Conditions' tab is selected, and the 'Authorization' section is active. The main content area shows the 'Compound Condition List' with a 'New Authorization Compound Condition' button. The configuration form includes fields for 'Name' (CorporateSSID), 'Description', and '\*Condition Expression'. The expression is configured as 'AND (Radius:Called-Station Matches \*(Corporate)\$ AND AD1:ExternalGroups Equals main Users)'. There are 'Submit' and 'Cancel' buttons at the bottom.

**Nota:** in questo documento vengono utilizzati semplici profili di autorizzazione configurati in Criteri > Elementi criteri > Risultati > Autorizzazione > Profili di autorizzazione. Sono impostate su Consenti accesso, ma possono essere adattate alle esigenze dell'installazione.

Dopo aver configurato le condizioni, applicarle a un criterio di autorizzazione. Andare a **Criteri > Autorizzazione**. Inserire la regola nell'elenco nella posizione appropriata o modificare una regola esistente.

### Regola Guest

1. Fare clic sulla freccia rivolta verso il basso a destra di una regola esistente e scegliere **Inserisci nuova regola**.
2. Immettere un nome per la regola ospite e lasciare il campo Gruppi di identità impostato su Qualsiasi.
3. In Condizioni, fare clic sul segno più e fare clic su **Seleziona condizione esistente dalla libreria**.
4. In Nome condizione scegliere **Condizione semplice > GuestSSID**
5. In Autorizzazioni, scegliere il profilo di autorizzazione appropriato per gli utenti guest.
6. Selezionate **Fatto (Done)**.

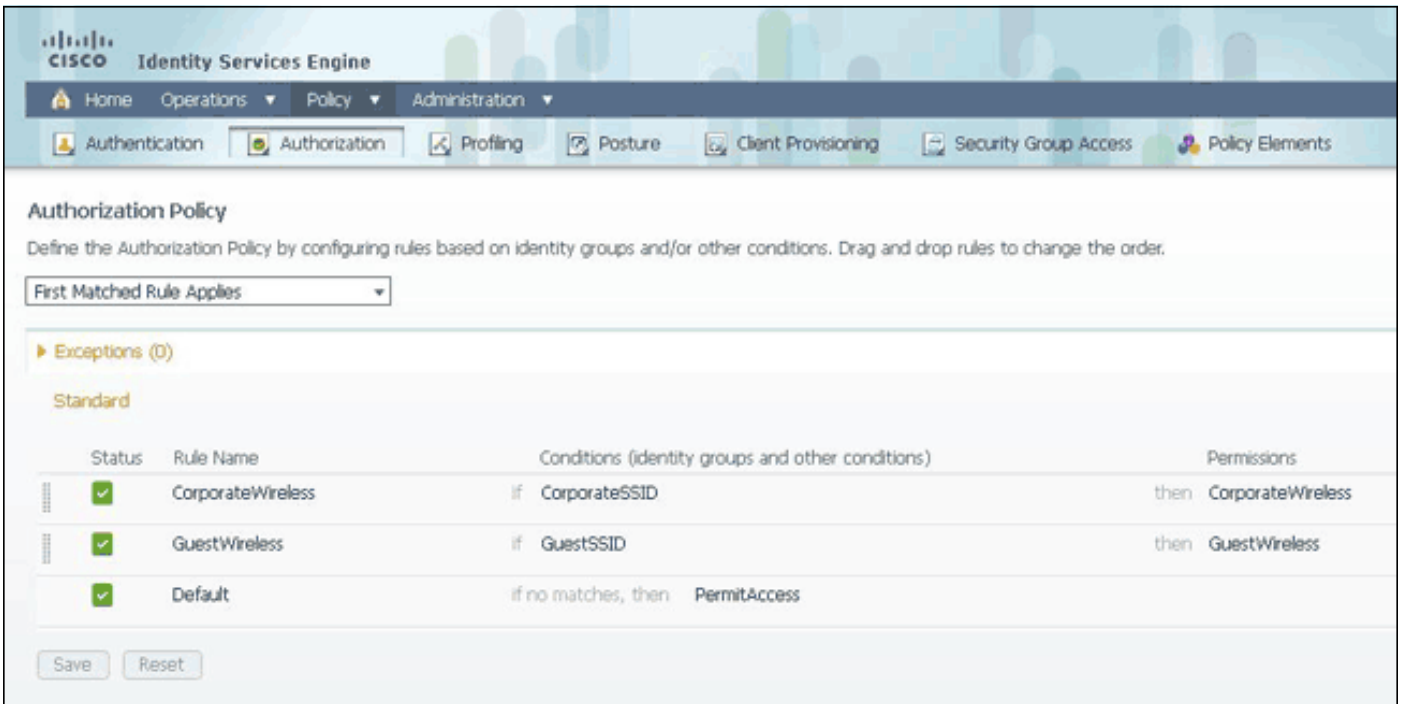
### Regola aziendale

1. Fare clic sulla freccia rivolta verso il basso a destra di una regola esistente e scegliere **Inserisci nuova regola**.
2. Immettere un nome per la regola aziendale e lasciare il campo Gruppi di identità impostato su Qualsiasi.
3. In Condizioni, fare clic sul segno più e fare clic su **Seleziona condizione esistente dalla libreria**.
4. In Nome condizione scegliere **Condizione composta > CorporateSSID**.
5. In Autorizzazioni scegliere il profilo di autorizzazione appropriato per gli utenti aziendali.
6. Selezionate **Fatto (Done)**.



7. Fare clic su **Salva** in fondo all'elenco dei criteri.

**Nota:** finché non si fa clic su Salva in fondo all'elenco dei criteri, alla distribuzione non verrà applicata alcuna modifica apportata in questa schermata.



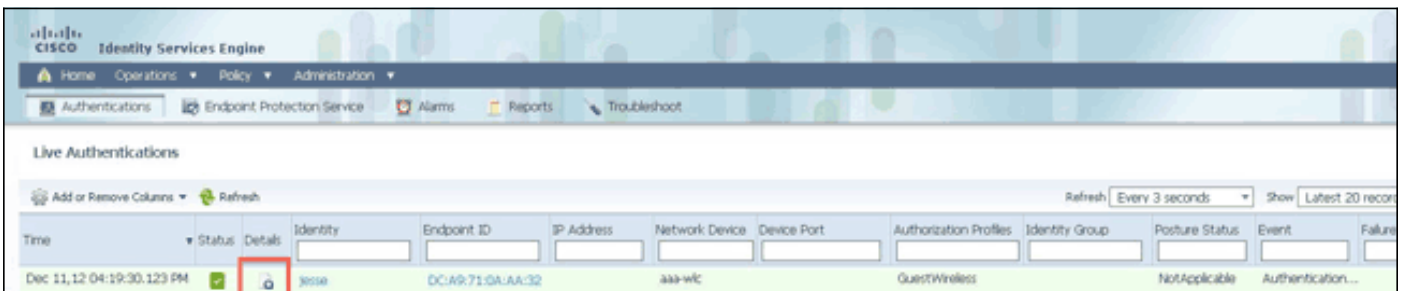
## Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

## Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Per verificare se il criterio è stato creato correttamente e per accertarsi che ISE riceva gli attributi corretti, esaminare il rapporto di autenticazione dettagliato per verificare se l'autenticazione per l'utente è stata superata o non è riuscita. Scegliere **Operazioni > Autenticazioni**, quindi fare clic sull'icona **Dettagli** per un'autenticazione.



Controllare innanzitutto il riepilogo dell'autenticazione. In questo modo vengono illustrate le nozioni di base dell'autenticazione che includono il profilo di autorizzazione fornito all'utente.

Authentication Summary	
Logged At:	December 11, 2012 4:19:30.123 PM
RADIUS Status:	Authentication succeeded
NAS Failure:	
Username:	jesse
MAC/IP Address:	DC:A9:71:0A:AA:32
Network Device:	aaa-wlc : 14.36.14.254 :
Allowed Protocol:	Default Network Access
Identity Store:	AD1
Authorization Profiles:	GuestWireless
SGA Security Group:	
Authentication Protocol :	PEAP(EAP-MSCHAPv2)

Se il criterio non è corretto, i dettagli di autenticazione mostreranno l'ID Aireospace-Wlan e l'ID della stazione chiamata inviato dal WLC. Regolare le regole di conseguenza. La regola di corrispondenza dei criteri di autorizzazione conferma se l'autenticazione corrisponde o meno alla regola desiderata.

Authorization Policy Matched Rule:	GuestWireless
SGA Security Group:	
AAA Session ID:	jedubois-ise1/144529641/233
Audit Session ID:	0x240def000011660c75d0f
Tunnel Details:	Tunnel-Type=(tag=0) VLAN, Tunnel-Medium-Type=(tag=0) 802, Tunnel-Private-Group-ID=(tag=0) 36
Cisco-AVPairs:	audit-session-id=0x240def000011660c75d0f
Other Attributes:	ConfigSessionId=13, DestinationPort=1812, Protocol=Radius, Framed-MTU=1300, State=37, CPMSessionId=0x240def000011660c75d0f, 37SessionId=jedubois-ise1/144529641/233, Aireospace-Wlan-Ip=? , PMSessionId=0x240def000011660c75d0f, Called-Station-Id=00-1b-2b-6b-67-30, Guest-Address=DC-A9-71-0A-AA-32, Device Type=Device Type#All Device Types, Location=Location#All Location, AccessRestricted=false, Device Address=14.36.14.254

Queste regole sono in genere configurate in modo errato. Per individuare il problema di configurazione, confrontare la regola con quanto riportato nei dettagli di autenticazione. Se gli attributi non vengono visualizzati nel campo Altri attributi, verificare che il WLC sia configurato correttamente.

## [Informazioni correlate](#)

- [Documentazione e supporto tecnico – Cisco Systems](#)