

# IPS 7.X: Esempio di autenticazione di accesso utente con ACS 5.X come configurazione del server Radius

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Configurazione](#)

[Configurare IPS per l'autenticazione dal server ACS tramite IME](#)

[Configurazione di ACS come server RADIUS](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

## [Introduzione](#)

In questo documento viene illustrato come configurare Cisco Intrusion Prevention System (IPS) per l'autenticazione dell'accesso utente tramite un server RADIUS. ACS viene utilizzato come server RADIUS.

## [Prerequisiti](#)

### [Requisiti](#)

In questo documento si presume che Cisco Intrusion Prevention System (IPS) sia completamente operativo e configurato per consentire a Cisco Intrusion Prevention System Manager Express (IME) o CLI di apportare modifiche alla configurazione. Oltre all'autenticazione AAA locale, è ora possibile configurare i server RADIUS per eseguire l'autenticazione dell'utente con sensore. La possibilità di configurare l'IPS in modo che utilizzi l'autenticazione AAA RADIUS per gli account utente, che facilita il funzionamento di distribuzioni IPS di grandi dimensioni, è disponibile in Cisco Intrusion Prevention System 7.0(4)E4 e versioni successive.

**Nota:** non è disponibile alcuna opzione per abilitare l'accounting su IPS. IPS 7.04 supporta l'autenticazione RADIUS, ma TACACS o Authorization o Accounting non sono supportati.

## [Componenti usati](#)

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

- Cisco Intrusion Prevention System versione 7.0(4)E4 e successive
- Intrusion Prevention System Manager Express versione 7.1(1) e successive
- Cisco Secure Access Control Server 5.x

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

Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

## Configurazione

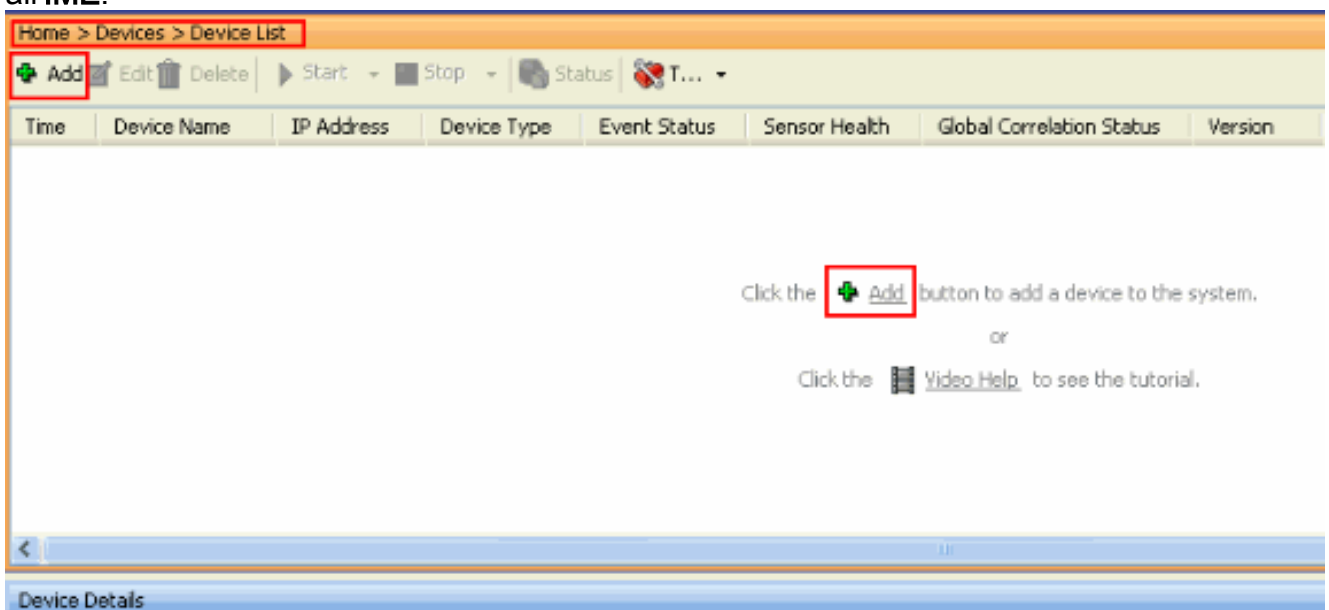
In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

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

### Configurare IPS per l'autenticazione dal server ACS tramite IME

Completare questa procedura per aggiungere l'IPS all'IME e quindi configurare l'IPS per l'autenticazione dal server ACS:

1. Scegliere **Home > Dispositivi > Elenco dispositivi > Aggiungi** per aggiungere un IPS all'IME.



2. Completare i campi nella finestra **Add Device** (Aggiungi dispositivo), come mostrato di seguito, per fornire i dettagli sull'IPS. Il nome del sensore utilizzato è **IPS**. Fare clic su

**Add Device**

Sensor Name:

Sensor IP Address:

Web Server Port:

Communication protocol

Use encrypted connection (https)

Use non-encrypted connection (http)

Authentication

Configuration User Name:  ⓘ

Configuration Password:

Use the Same Account for Configuration and Event Subscription (This is not recommended):

Event Subscription User Name:  ⓘ

Event Subscription Password:

Event Start Time (UTC)

Most Recent Alerts

Start Date (YYYY:MM:DD):  :  :

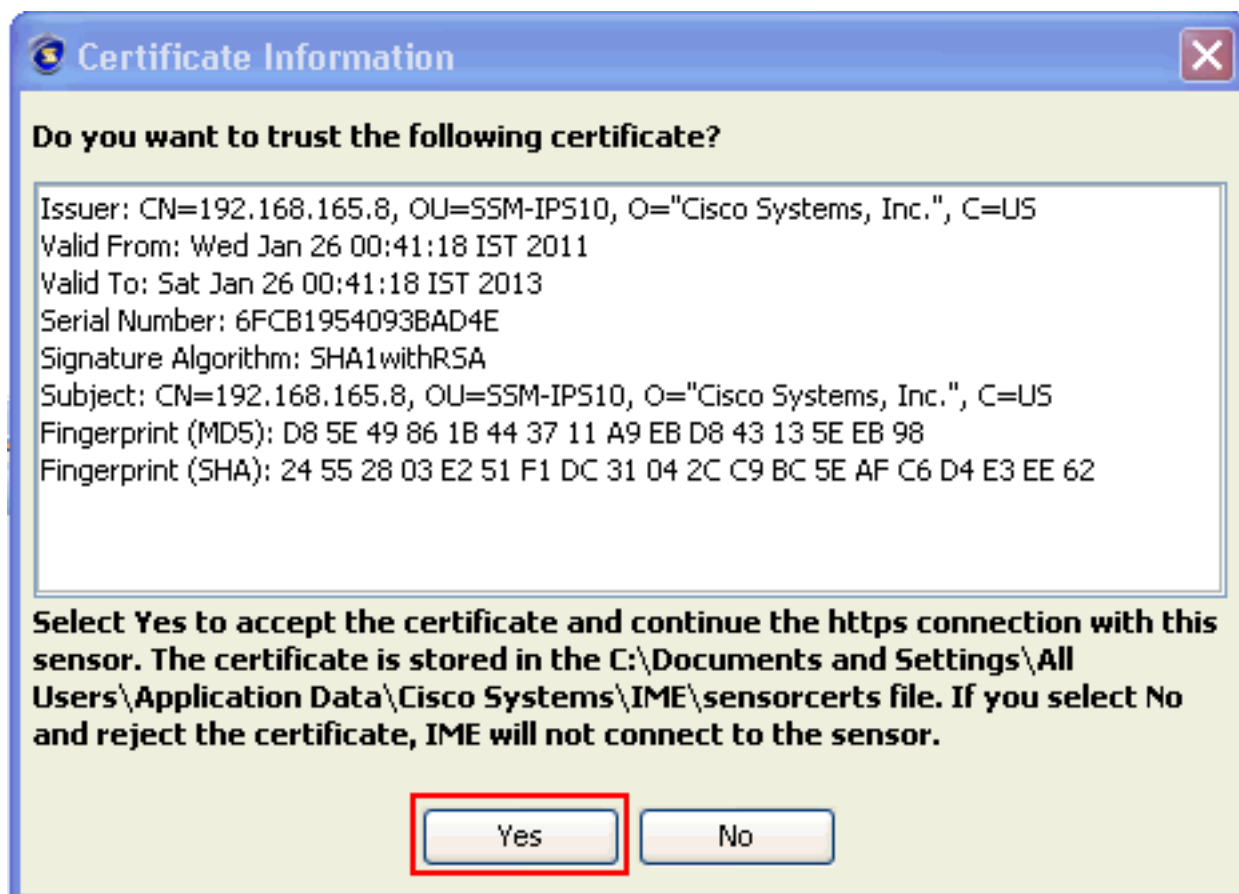
Start Time (HH:MM:SS):  :  :

Exclude alerts of the following severity level(s)

Informational  Low  Medium  High

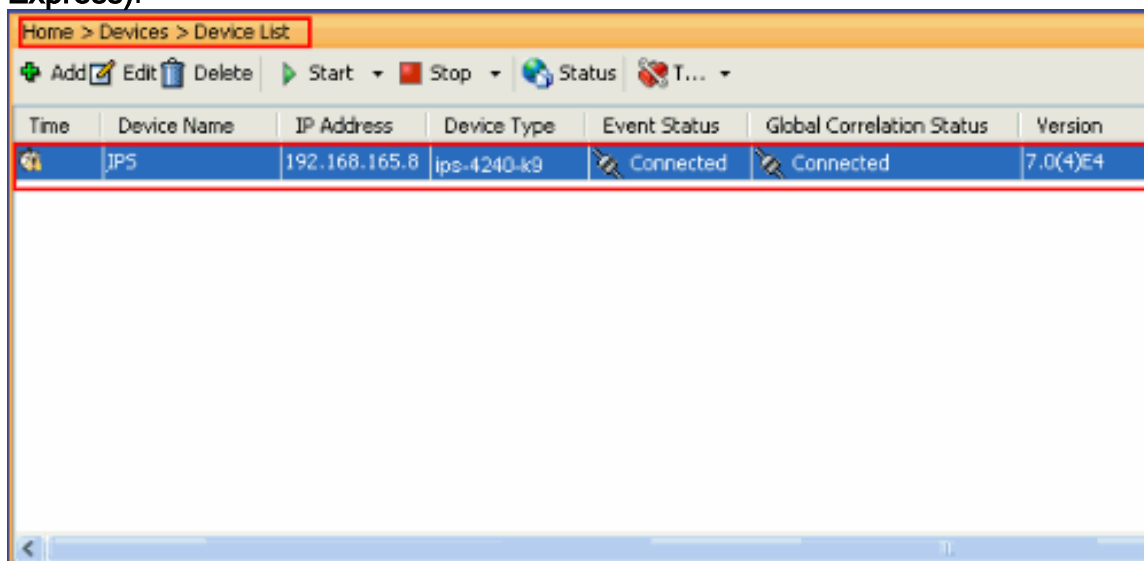
OK.

3. Fare clic su **Sì** per accettare il certificato e continuare la connessione https al sensore. È necessario accettare il certificato per connettersi al sensore e accedervi.



L'IP

S denominato **IPS** viene aggiunto all'**IME (Intrusion Prevention System Manager Express)**.



4. Scegliere **Configurazione > IPS > Impostazione sensore > Autenticazione**, quindi attenersi alla seguente procedura: Per selezionare il server RADIUS come dispositivo di autenticazione, fare clic sul pulsante di opzione **Server RADIUS**. Specificare i parametri di **autenticazione RADIUS**, come mostrato. Scegliere **Locale e RADIUS** come autenticazione della console, in modo che venga utilizzata l'autenticazione locale quando il server RADIUS non è disponibile. Fare clic su **Apply** (Applica).

Configuration > IPS > Sensor Setup > Authentication

User Authentication:  Local  Radius Server

**Local Authentication**  
Specify the users that have access to the sensor. The service role is a special role that allows you to bypass the CLI if needed. Only one service account is allowed.

Username	Role	Status
disco	Administrator	Active
service	Service	Active

Add Edit Delete

**Radius Authentication**

Network Access ID:  Default User Role:

Allow Local Authentication if all Radius Servers are Unresponsive

**Primary Radius Server**

Server IP Address:   
 Authentication Port:   
 Timeout (seconds):   
 Shared Secret:

**Secondary Radius Server (optional)**

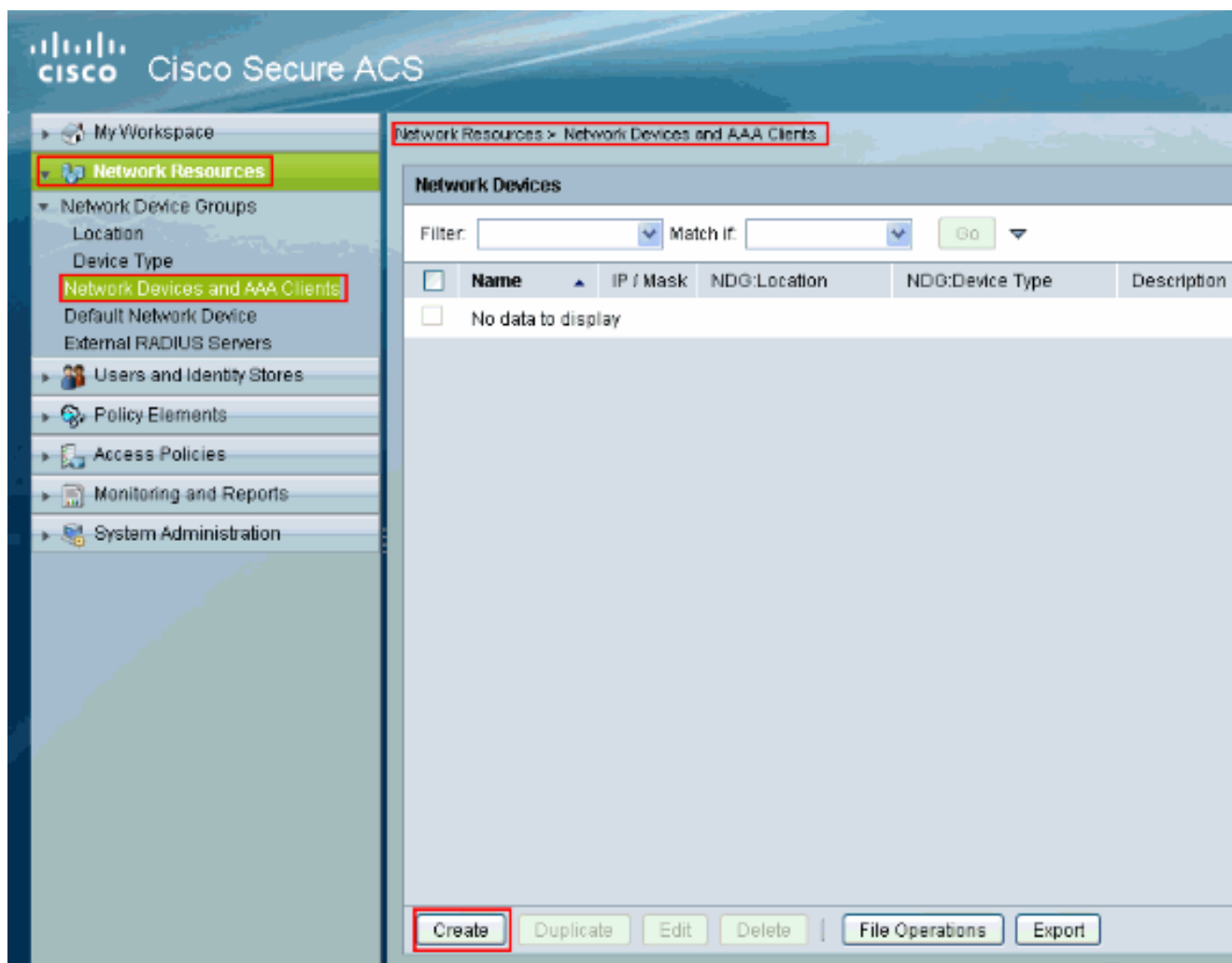
**Console Authentication**  
Console Authentication:

Apply Reset

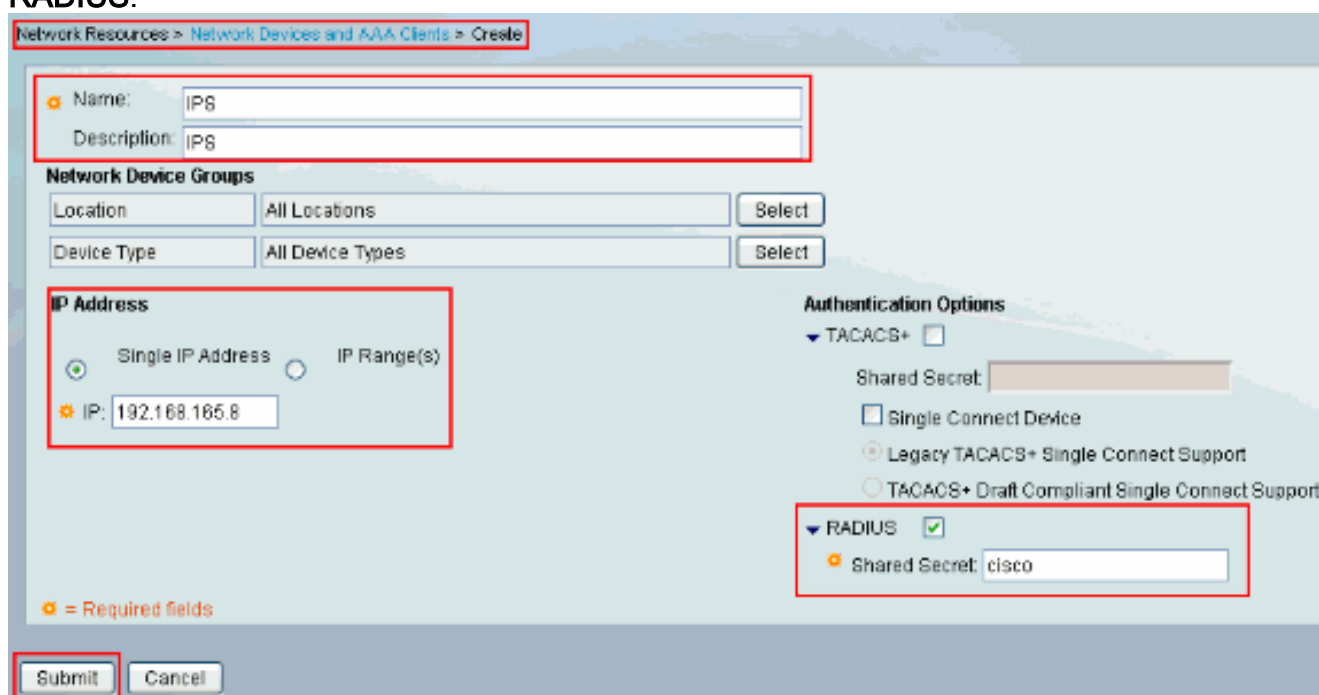
## Configurazione di ACS come server RADIUS

Per configurare il server ACS come server RADIUS, completare la procedura seguente:

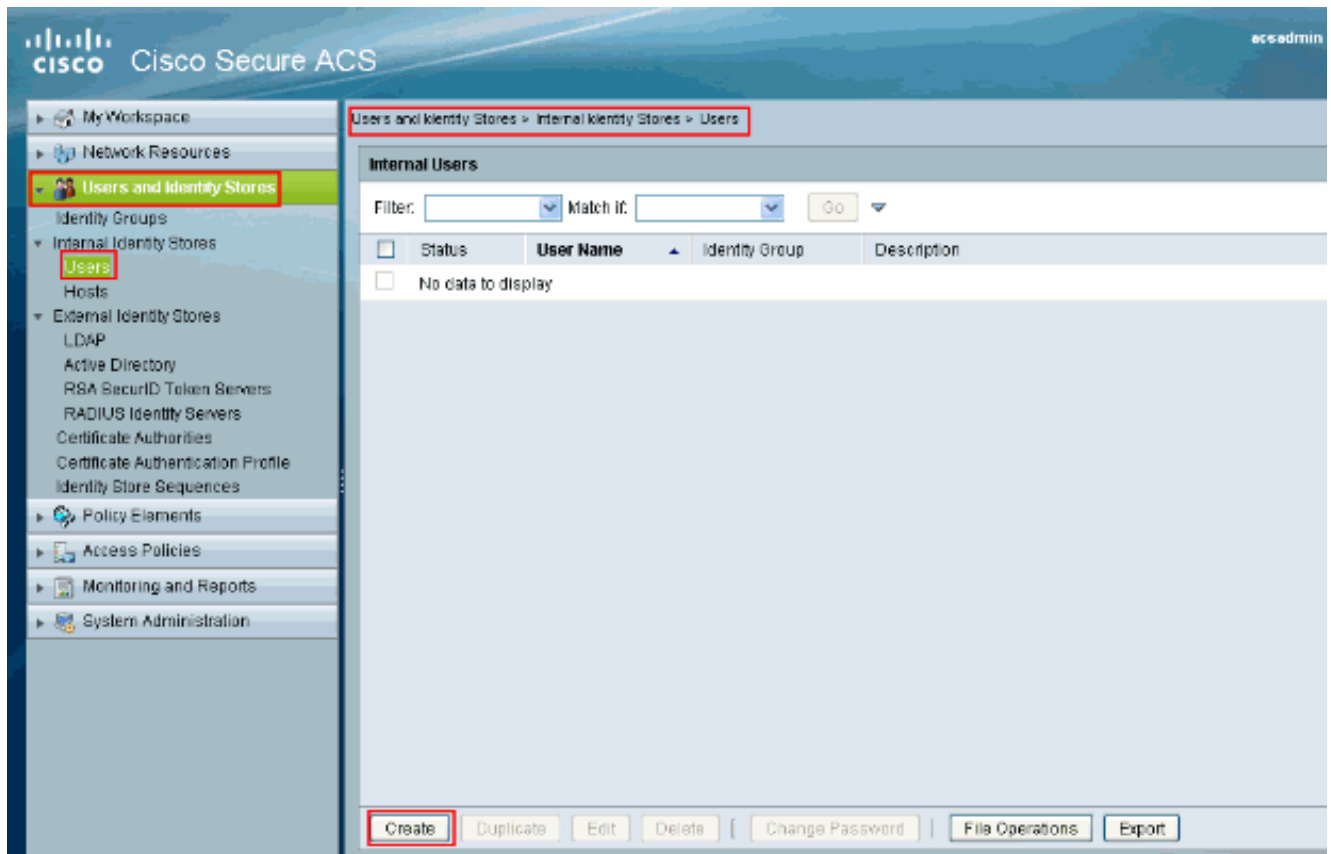
1. Scegliere **Risorse di rete > Dispositivi di rete e client AAA**, quindi fare clic su **Crea** per aggiungere l'IPS al server ACS.



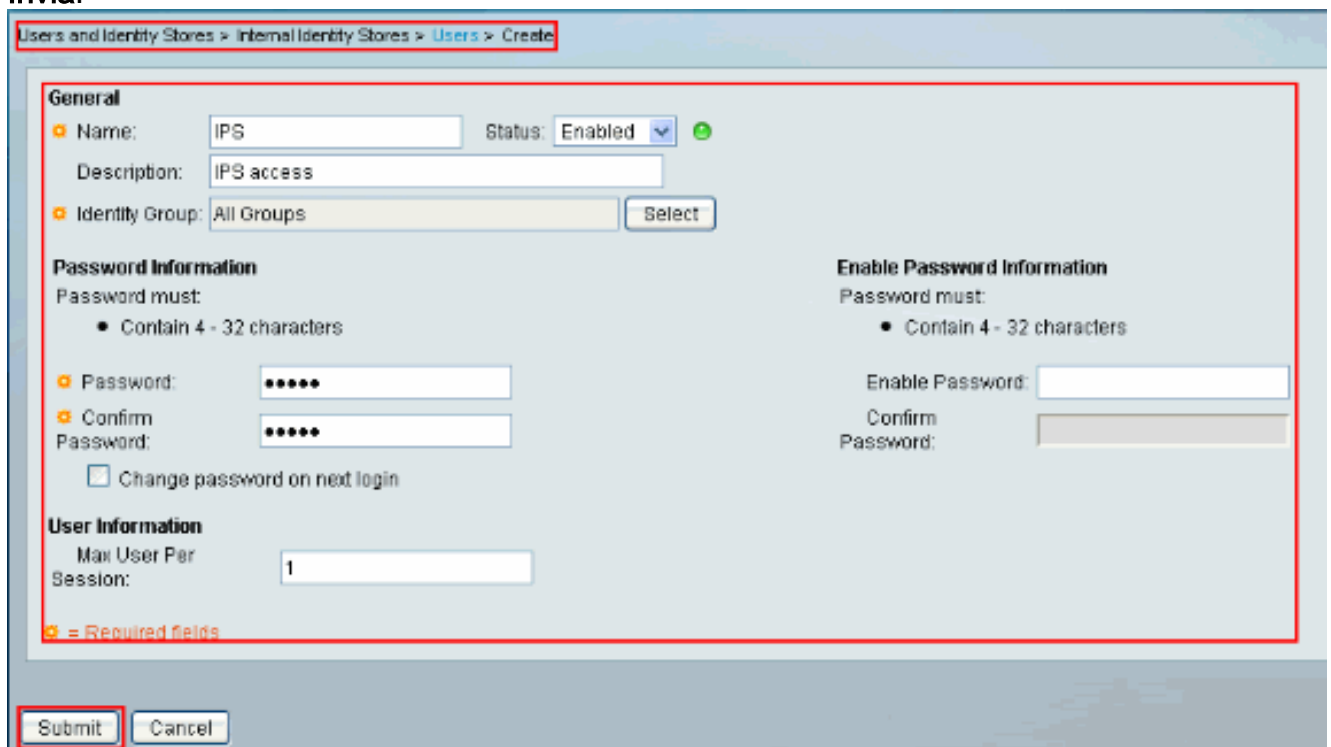
2. Fornire le informazioni richieste sul **client** (IPS è il client qui) e fare clic su **Invia**. In questo modo l'IPS viene aggiunto al server ACS. I dettagli includono l'**indirizzo IP** dell'IPS e i dettagli del **server RADIUS**.



3. Scegliere **Utenti e archivi identità > Archivi identità interni > Utenti**, quindi fare clic su **Crea** per creare un nuovo utente.



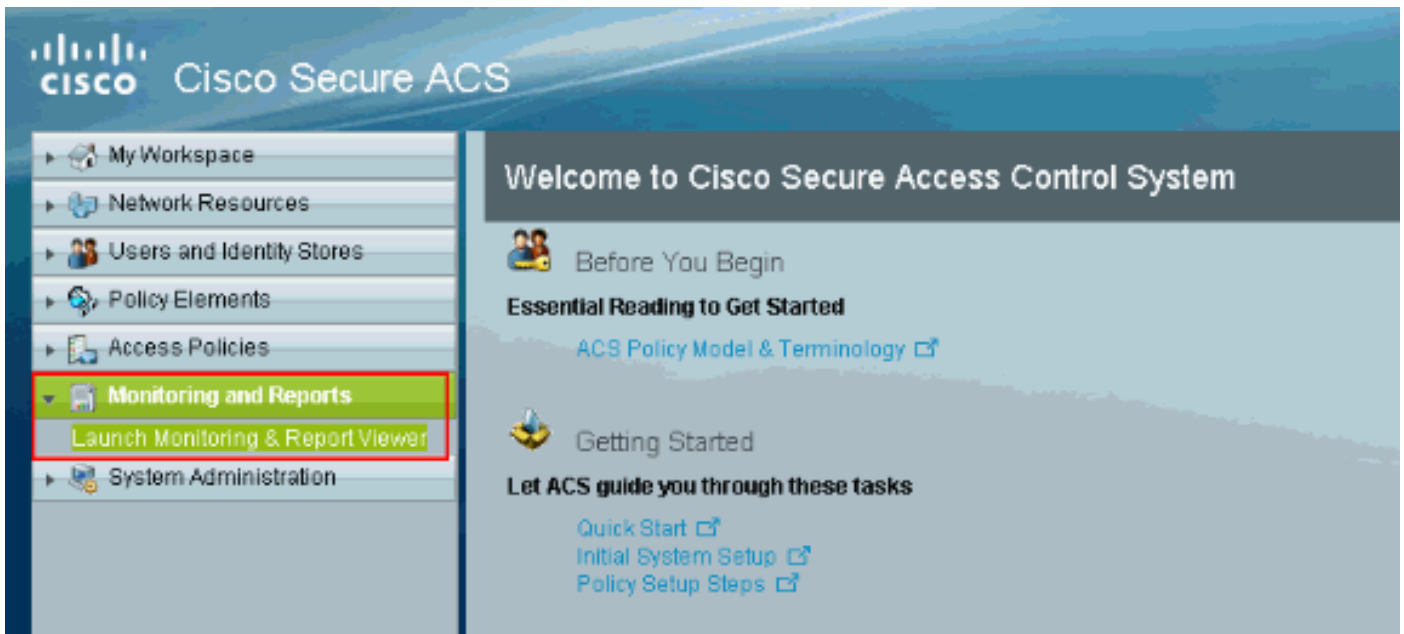
4. Specificare il nome e la password. Al termine, fare clic su **Invia**.



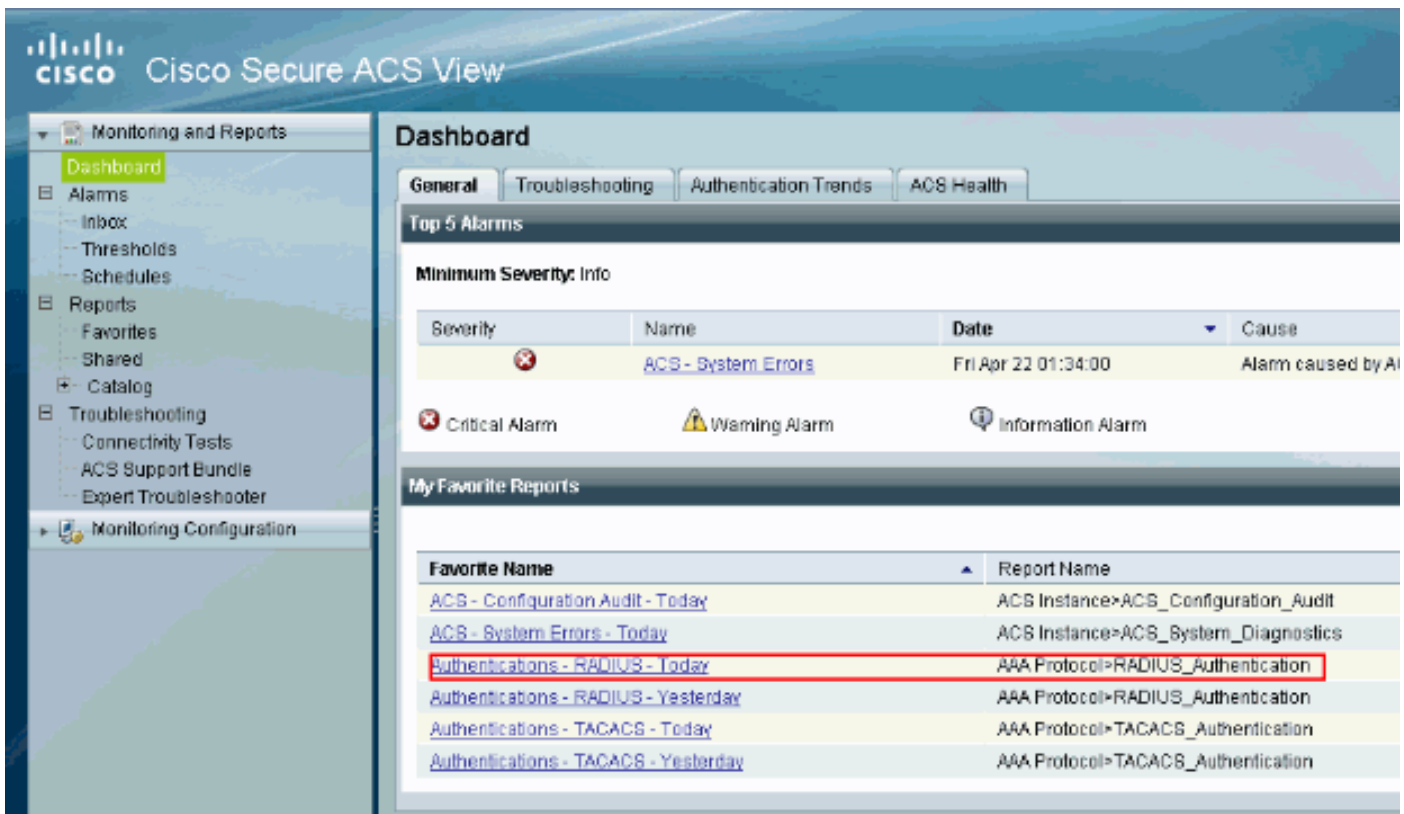
## Verifica

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

Provare ad accedere all'IPS con l'utente appena creato. Una volta autenticato l'utente, controllare il report su ACS.



Per visualizzare il report corrente, fare clic su **Authentication-RADIUS-Today**.



Nell'immagine viene mostrato come l'utente che si connette all'IPS venga autenticato dal server ACS.



**AAA Protocol > RADIUS Authentication**

Authentication Status: Pass or Fail

Date: April 29, 2011 ( [Last 30 Minutes](#) | [Last Hour](#) | [Last 12 Hours](#) | [Today](#) | [Yesterday](#) | [Last 7 Days](#) | [Last 30 Days](#) )

Generated on April 29, 2011 1:31:12 AM UTC

 Reload

✔=Pass   ✖=Fail   🔍=Click for details   🖱=Mouse over item for additional information

Logged At	RADIUS Status	NAS Failure	Details	Username	MAC/IP Address	Access Service	Authentication Method	Network Device	NAS IP Address
Apr 29,11 1:25:51.836 AM	✔			IPS	127.0.1.1	Default Network Access	PAP_ASCII	IPS	192.168.165.0

Lo [strumento Output Interpreter](#) (solo utenti [registrati](#)) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

## [Risoluzione dei problemi](#)

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

## [Informazioni correlate](#)

- [Pagina di supporto per i sensori Cisco IPS serie 4200](#)
- [Riferimenti per i comandi dei sensori Cisco IPS serie 4200](#)
- [Cisco IPS Manager Express](#)
- [Pagina di supporto per la negoziazione IPsec/i protocolli IKE](#)
- [Cisco Secure Access Control Server per Windows](#)
- [RFC \(Requests for Comments\)](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)