

# Configurazione e risoluzione dei problemi dei server TACACS esterni su ISE

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurare ISE](#)

[Configurazione di ACS](#)

[Verifica](#)

[Risoluzione dei problemi](#)

---

## Introduzione

Questo documento descrive la funzionalità per utilizzare il server TACACS+ esterno in una distribuzione utilizzando Identity Service Engine (ISE) come proxy.

## Prerequisiti

### Requisiti

- Conoscenze base di Amministrazione dispositivi su ISE.
- Questo documento è basato su Identity Service Engine versione 2.0, applicabile a qualsiasi versione di Identity Service Engine successiva alla versione 2.0.

### Componenti usati

---

Nota: tutti i riferimenti ad ACS in questo documento possono essere interpretati come riferimenti a qualsiasi server TACACS+ esterno. Tuttavia, la configurazione sull'ACS e la configurazione su qualsiasi altro server TACACS possono variare.

---

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

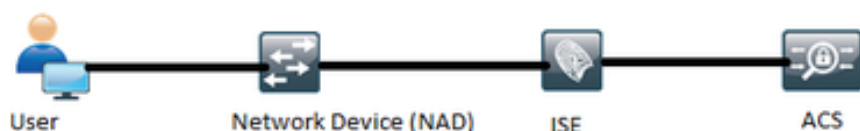
- Identity Service Engine 2.0
- Access Control System (ACS) 5.7

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 modifiche alla configurazione.

## Configurazione

In questa sezione viene spiegato come configurare ISE in modo che proxy le richieste TACACS+ ad ACS.

### Esempio di rete



## Configurare ISE

1. Più server TACACS esterni possono essere configurati su ISE e utilizzati per autenticare gli utenti. Per configurare il server TACACS+ esterno su ISE, selezionare Work Center > Device Administration > Network Resources > TACACS External Servers (Centri di lavoro > Amministrazione dispositivi > Risorse di rete > Server esterni TACACS). Fare clic su Add (Aggiungi) e specificare i dettagli di External Server Details (Dettagli server esterno).

Lo screenshot mostra l'interfaccia di configurazione di ISE. La barra superiore indica "Identity Services Engine" con menu per Home, Operations, Policy, Guest Access, Administration e Work Centers. Sotto, la navigazione include TrustSec, Device Administration, Overview, Identities, User Identity Groups, Network Resources (selezionato), Network Device Groups, Policy Conditions, Policy Results, Device Admin Policy Sets, Reports e Settings. Il pannello di sinistra mostra una gerarchia di menu: Network Devices, Default Devices, TACACS External Servers e TACACS Server Sequence. L'area principale è intitolata "TACACS External Servers > External\_Server" e contiene i seguenti campi di configurazione:

- Name: External\_Server
- Description: External TACACS Server
- Host IP: 10.127.196.237
- Connection Port: 49 (1-65,535)
- Timeout: 20 Seconds (1-999)
- Shared Secret: \*\*\*\*\* (con pulsante Show Secret)
- Use Single Connect:

In basso a destra sono presenti i pulsanti "Cancel" e "Save".

Il segreto condiviso fornito in questa sezione deve essere lo stesso segreto utilizzato in ACS.

2. Per utilizzare il server TACACS esterno configurato, è necessario aggiungerlo in una sequenza di server TACACS da utilizzare nei set di criteri. Per configurare la sequenza del server TACACS, selezionare Centri di lavoro > Amministrazione dispositivi > Risorse di rete > Sequenza server TACACS. Fare clic su Add (Aggiungi), immettere i dettagli e scegliere i server da utilizzare nella sequenza.

The screenshot shows the 'Server Sequence' configuration page in the Identity Services Engine (ISE) interface. The page is titled 'Server Sequence' and has a breadcrumb trail: Home > Operations > Policy > Guest Access > Administration > Work Centers > TrustSec > Device Administration > Network Resources > Network Device Groups > Policy Conditions > Policy Results > Device Admin Policy Sets > Reports > Settings.

The configuration fields are as follows:

- Name:** External\_Server\_Sequence
- Description:** Sequence for External Servers
- Server List:** The TACACS Proxy Servers selected will be tried in order. It consists of two panes: 'Available' (empty) and 'Chosen' (containing 'External\_Server'). There are blue arrows between the panes for adding and removing servers. Below the panes are buttons for 'Choose all' and 'Clear all'.
- Logging Control:** Accounting requests should be handled. It includes checkboxes for 'Local Accounting' and 'Remote Accounting'.
- Username Stripping:** It includes checkboxes for 'Prefix Strip' and 'Suffix Strip'. The 'Prefix Strip' field contains the character '\', and the 'Suffix Strip' field contains '@'. Descriptions for both fields indicate they strip the start or end of the subject name up to the first or last occurrence of the separator, respectively.

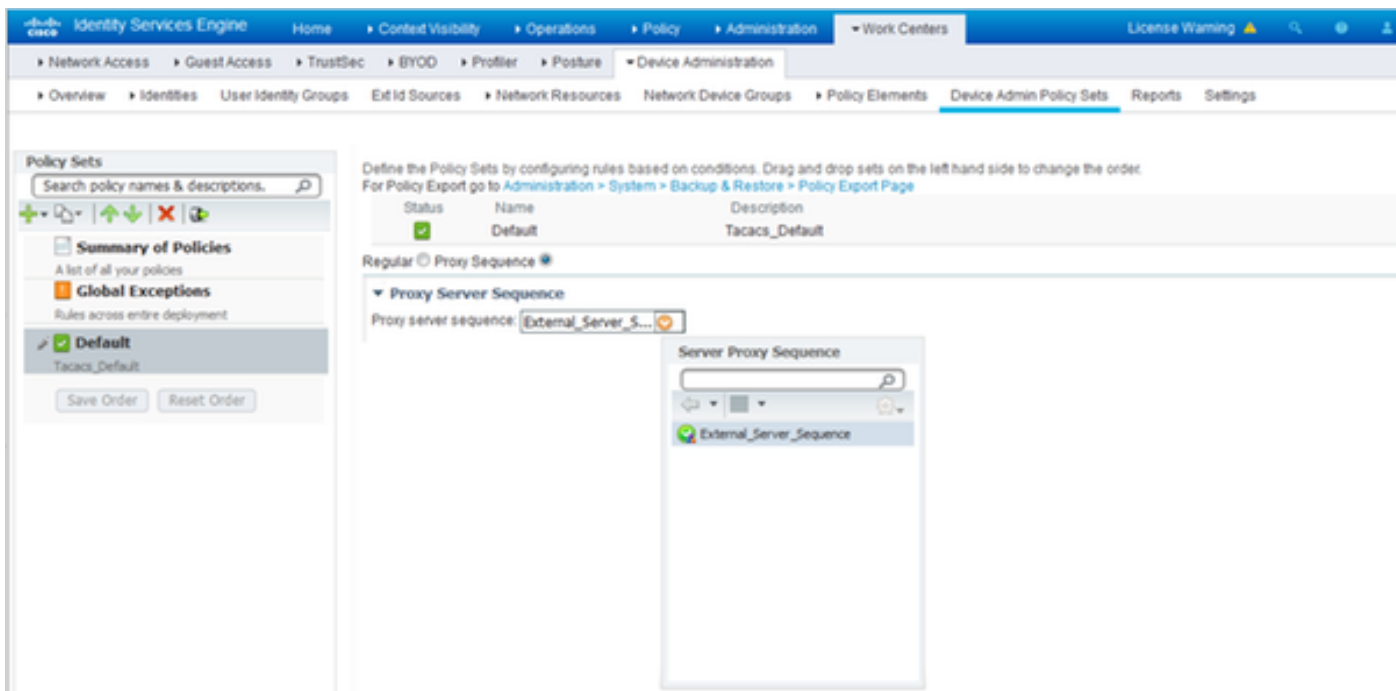
At the bottom right, there are 'Cancel' and 'Submit' buttons.

Oltre alla sequenza del server, sono disponibili altre due opzioni. Controllo registrazione e rimozione nome utente.

Logging Control consente di registrare le richieste di accounting localmente su ISE o di registrare le richieste di accounting sul server esterno che gestisce anche l'autenticazione.

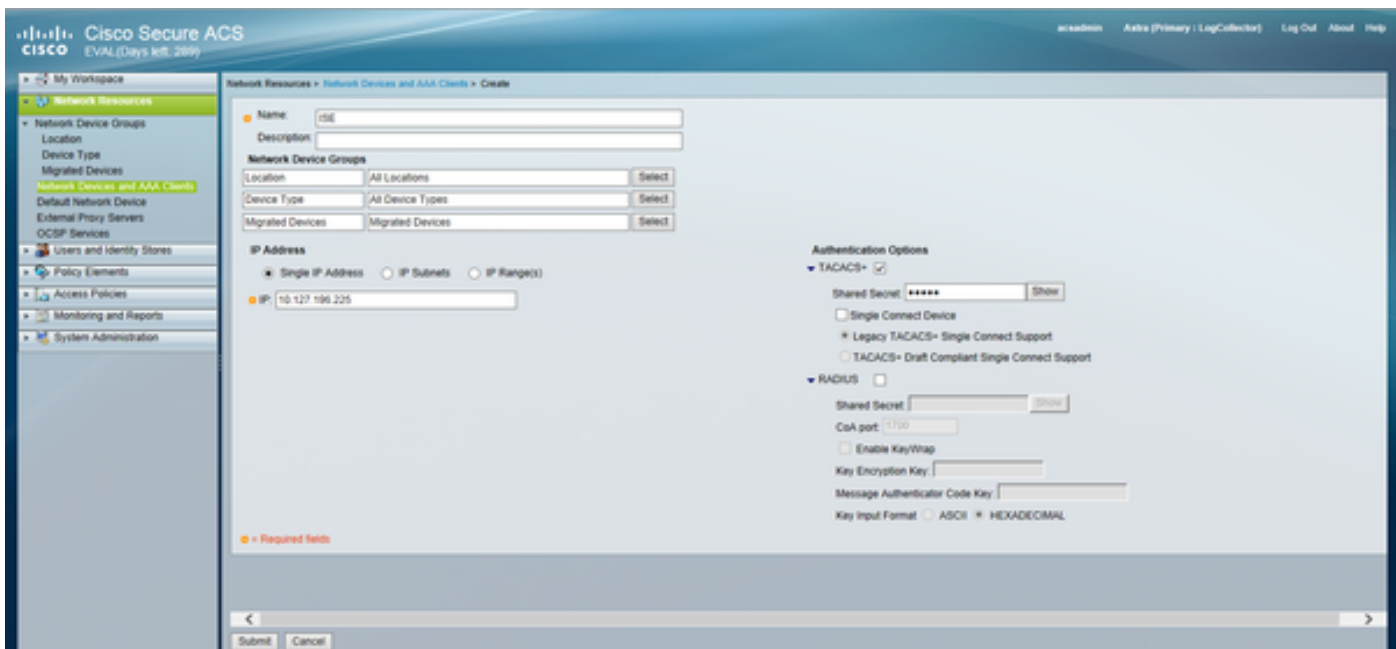
Username Stripping è usato per rimuovere il prefisso o il suffisso specificando un delimitatore prima di inoltrare la richiesta a un server TACACS esterno.

3. Per utilizzare la sequenza di server TACACS esterno configurata, è necessario configurare i set di criteri in modo da utilizzare la sequenza creata. Per configurare i set di criteri in modo da utilizzare la sequenza di server esterni, passare a Centri di lavoro > Amministrazione dispositivi > Set di criteri di amministrazione dispositivi > [selezionare il set di criteri]. Pulsante di opzione che indica Sequenza proxy. Scegliere la sequenza di server esterni creata.

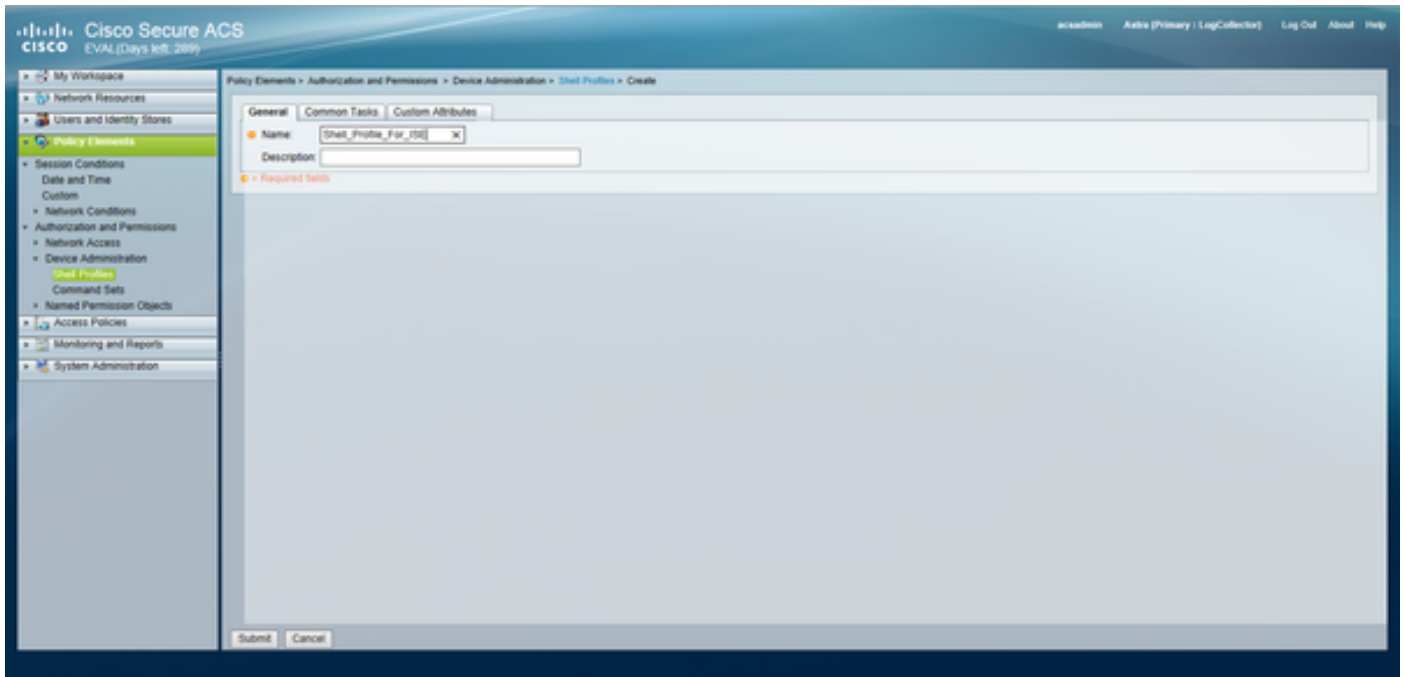


## Configurazione di ACS


Per il sistema ACS, ISE è solo un altro dispositivo di rete che invierà una richiesta TACACS. Per configurare ISE come dispositivo di rete in ACS, selezionare Risorse di rete > Dispositivi di rete e client AAA. Fare clic su Create (Crea) e specificare i dettagli del server ISE usando lo stesso segreto condiviso configurato sull'ISE.




Configurare i parametri di amministrazione dei dispositivi su ACS, ovvero i profili della shell e i set di comandi. Per configurare i profili di shell, selezionare Elementi criteri > Autorizzazione e autorizzazioni > Amministrazione dispositivi > Profili shell. Fare clic su Crea e configurare il nome, le attività comuni e gli attributi personalizzati in base al requisito.



Per configurare i set di comandi, selezionare Elementi dei criteri > Autorizzazione e autorizzazioni > Amministrazione dispositivi > Set di comandi. Fare clic su Crea e inserire i dettagli in base al requisito.

**General**  
Name:  Status:  

 The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

**Conditions**  
 Protocol:

**Results**  
Service:

Configurare il servizio di accesso selezionato nella regola di selezione del servizio in base ai requisiti. Per configurare le regole del servizio di accesso, selezionare Criteri di accesso > Servizi di accesso > Amministrazione predefinita dispositivi > Identità, in cui è possibile selezionare per l'autenticazione l'archivio identità da utilizzare. È possibile configurare le regole di autorizzazione selezionando Criteri di accesso > Servizi di accesso > Amministratore predefinito dispositivi > Autorizzazione.

---

Nota: la configurazione dei criteri di autorizzazione e dei profili della shell per dispositivi specifici può variare e non è inclusa nell'ambito del presente documento.

---

## Verifica

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

La verifica può essere effettuata sia sull'ISE che sull'ACS. Qualsiasi errore nella configurazione dell'ISE o dell'ACS causerà un errore di autenticazione. ACS è il server principale che gestirà l'autenticazione e le richieste di autorizzazione, ISE si assume la responsabilità di e dal server ACS e funge da proxy per le richieste. Poiché il pacchetto attraversa entrambi i server, la verifica dell'autenticazione o della richiesta di autorizzazione può essere eseguita su entrambi i server.

I dispositivi di rete sono configurati con ISE come server TACACS e non come server ACS. Pertanto, la richiesta raggiunge ISE per prima e, in base alle regole configurate, ISE decide se deve essere inoltrata a un server esterno. È possibile verificare questa condizione nei log di TACACS Live sull'ISE.

Per visualizzare i log attivi sull'ISE, selezionare Operations > TACACS > Live Log. In questa pagina è possibile visualizzare i report in tempo reale e controllare i dettagli di una richiesta specifica facendo clic sull'icona a forma di lente di ingrandimento relativa alla richiesta specifica desiderata.

## Steps

```
13020 Get TACACS+ default network device setting
13013 Received TACACS+ Authentication START Request
15049 Evaluating Policy Group
15008 Evaluating Service Selection Policy
15048 Queried PIP - Network Access.Protocol
15006 Matched Default Rule
13064 TACACS proxy received incoming request for forwarding.
13065 TACACS proxy received valid incoming authentication request.
13063 Start forwarding request to remote TACACS server.
13074 Finished to process TACACS Proxy request.
13020 Get TACACS+ default network device setting
13014 Received TACACS+ Authentication CONTINUE Request
13064 TACACS proxy received incoming request for forwarding.
13065 TACACS proxy received valid incoming authentication request.
13071 Continue flow (seq_no > 1).
13063 Start forwarding request to remote TACACS server.
13074 Finished to process TACACS Proxy request.
```

Per visualizzare i report di autenticazione sull'ACS, selezionare Monitoraggio e report > Avvia visualizzatore report e monitoraggio > Monitoraggio e report > Report > Protocollo AAA > Autenticazione TACACS. Come ISE, è possibile controllare i dettagli di una richiesta facendo clic

sull'icona con la lente di ingrandimento relativa alla richiesta desiderata



## Risoluzione dei problemi

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

1. Se i dettagli del report su ISE mostrano il messaggio di errore mostrato nella figura, allora indica un segreto condiviso non valido configurato sull'ISE o sul dispositivo di rete (NAD).

Message Text

**TACACS: Invalid TACACS+ request packet - possibly mismatched Shared Secrets**

2. Se non è disponibile alcun report di autenticazione per una richiesta sull'ISE ma viene negato all'utente finale l'accesso a un dispositivo di rete, ciò indica in genere diversi elementi.

- La richiesta non ha raggiunto il server ISE.
- Se l'amministratore del dispositivo è disabilitato su ISE, qualsiasi richiesta TACACS+ ad ISE verrà eliminata in modo invisibile all'utente. Nei report o nei Live Log non verrà visualizzato alcun log che indica la stessa condizione. Per verificare questa condizione, passare ad Amministrazione > Sistema > Distribuzione > [selezionare il nodo]. Fare clic su Edit (Modifica) e notare la casella di controllo "Enable Device Admin Service" (Abilita servizio di amministrazione dispositivi) nella scheda General Settings (Impostazioni generali), come mostrato nella figura. Affinché Device Administration funzioni su ISE, è necessario selezionare questa casella di controllo.



**Personas**

Administration      Role **PRIMARY**     

Monitoring      Role PRIMARY      Other Monitoring Node

Policy Service

Enable Session Services      Include Node in Node Group None

Enable Profiling Service

Enable Threat Centric NAC Service

Enable SXP Service      Use Interface GigabitEthernet 0

Enable Device Admin Service

Enable Passive Identity Service

pxGrid

- Se non è presente una licenza di amministrazione del dispositivo scaduta, tutte le richieste TACACS+ vengono eliminate automaticamente. Nell'interfaccia utente non viene visualizzato alcun log per lo stesso motivo. Selezionare Amministrazione > Sistema > Licenze per controllare la licenza di amministrazione del dispositivo.

**Licenses** How do I register/modify or lookup my licenses?

License File	Quantity	Term	Expiration Date
EVALUATION.lic			
Base	100	90 days	22-Jan-2017 (43 days remaining)
Plus	100	90 days	22-Jan-2017 (43 days remaining)
Apex	100	90 days	22-Jan-2017 (43 days remaining)
Wired	100	90 days	22-Jan-2017 (43 days remaining)
Device Admin	Uncounted	90 days	22-Jan-2017 (43 days remaining)

- Se il dispositivo di rete non è configurato o se sull'ISE è configurato un IP di dispositivo di rete errato, ISE scarta il pacchetto senza avvisare. Non viene inviata alcuna risposta al client e non viene visualizzato alcun log nella GUI. Si tratta di un cambiamento di comportamento in ISE per TACACS+ rispetto a quello di ACS che informa che la richiesta proviene da un dispositivo di rete o da un client AAA sconosciuto.
- La richiesta ha raggiunto l'ACS, ma la risposta non è arrivata all'ISE. Questo scenario può essere controllato dai report sull'ACS come mostrato nella figura. In genere ciò è dovuto a un segreto condiviso non valido sull'ACS configurato per ISE o sull'ISE configurato per l'ACS.

Steps

Message

```
Received TACACS+ Authentication START Request
Invalid TACACS+ request packet - possibly mismatched Shared Secrets
```

- La risposta non verrà inviata anche se l'ISE non è configurato o se l'indirizzo IP dell'interfaccia di gestione di ISE non è configurato sull'ACS nella configurazione del dispositivo di rete. In questo scenario, il messaggio nella figura può essere osservato sul

ACS.



- Se il report di autenticazione sull'ACS ha esito positivo, ma l'ISE non include alcun report e l'utente viene rifiutato, il problema potrebbe riguardare la rete. È possibile verificare questa condizione tramite l'acquisizione di un pacchetto su ISE con i filtri necessari. Per raccogliere un'acquisizione di pacchetto su ISE, selezionare Operations > Troubleshoot > Diagnostic Tools > General tools > TCP Dump.

## TCP Dump

Monitor the packet headers on the network and save to a file (up to 5 Minutes)

Status  Stopped  Start

Host Name

Network Interface

Promiscuous Mode  On  Off

Filter

Example: 'ip host helios and not iceberg'

Format

---

**Dump File** Last created on Fri Dec 09 20:51:18 IST 2016  
File size: 9,606 bytes  
Format: Raw Packet Data  
Host Name: tornado  
Network Interface: GigabitEthernet 0  
Promiscuous Mode: On

3. Se i report possono essere visualizzati su ISE ma non su ACS, potrebbe significare che la richiesta non ha raggiunto l'ACS a causa di una configurazione errata dei set di criteri per ISE che può essere risolta in base al report dettagliato sull'ISE o a causa di un problema di rete identificabile tramite un'acquisizione di pacchetti sull'ACS.

4. Se i report vengono visualizzati sia sull'ISE che sull'ACS, ma l'accesso viene ancora negato

all'utente, allora più spesso si tratta di un problema nella configurazione dei criteri di accesso sull'ACS, che può essere risolto basandosi sul report dettagliato sull'ACS. Inoltre, deve essere consentito il traffico di ritorno da ISE al dispositivo di rete.

## 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).