

# Configurazione dell'autenticazione TACACS Prime 3.1 per ISE 2.x

## Sommario

[Introduzione](#)

[Requisiti](#)

[Configurazione](#)

[Prime Configuration](#)

[Configurazione di ISE](#)

[Risoluzione dei problemi](#)

## Introduzione

Questo documento descrive come configurare Prime Infrastructure per l'autenticazione tramite TACACS con ISE 2.x.

## Requisiti

Cisco raccomanda la conoscenza di base dei seguenti argomenti:

- Identity Services Engine (ISE)
- Prime Infrastructure

## Configurazione

Cisco Prime Network Control System 3.1

Cisco Identity Service Engine 2.0 o versione successiva.

(Nota: ISE supporta solo TACACS a partire dalla versione 2.0, ma è possibile configurare Prime per l'utilizzo di Radius. Prime include l'elenco degli attributi Radius oltre a TACACS se si preferisce utilizzare Radius, con una versione precedente di ISE o una soluzione di terze parti.)

## Prime Configuration

Passare alla schermata seguente: Amministrazione / Utenti/ Utenti, Ruoli & AAA come mostrato di seguito.

Quindi, selezionare la scheda TACACS+ Server, selezionare l'opzione Add TACACS+ Server (Aggiungi server TACACS+) nell'angolo in alto a destra e selezionare go (Vai).

Nella schermata successiva è disponibile la configurazione della voce relativa al server TACACS (questa operazione deve essere eseguita per ciascun server TACACS).

Administration / Users / Users, Roles & AAA

AAA Mode Settings

Active Sessions

Change Password

Local Password Policy

RADIUS Servers

SSO Server Settings

SSO Servers

TACACS+ Servers

User Groups

Users

Add TACACS+ Server

IP Address

DNS Name

\* Port

Shared Secret Format

\* Shared Secret

\* Confirm Shared Secret

\* Retransmit Timeout  (secs)

\* Retries

Authentication Type

Local Interface IP

Immettere l'indirizzo IP o l'indirizzo DNS del server, nonché la chiave privata condivisa. Notare anche l'indirizzo IP dell'interfaccia locale che si desidera usare, poiché questo stesso indirizzo IP deve essere usato per il client AAA ad ISE.

Per completare la configurazione su Prime. È necessario abilitare TACACS in Amministrazione / Utenti / Utenti, Ruoli & AAA nella scheda Impostazioni modalità AAA.

(Nota: Si consiglia di selezionare l'opzione Abilita fallback su locale, con l'opzione SOLO su nessuna risposta del server o L'opzione Su nessuna risposta o errore, in particolare durante il test della configurazione.

Administration / Users / Users, Roles & AAA

AAA Mode Settings

Active Sessions

Change Password

Local Password Policy

RADIUS Servers

SSO Server Settings

SSO Servers

TACACS+ Servers

User Groups

Users

AAA Mode  Local  RADIUS  TACACS+  SSO

Enable fallback to Local

## Configurazione di ISE

Configurazione di Prime come client AAA su ISE, centri di lavoro / amministrazione dispositivi / risorse di rete / dispositivi di rete / aggiunta

Identity Services Engine

Home Context Visibility Operations Policy Administration Work Centers License Warning

Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration

Overview Identities User Identity Groups Ext Id Sources Network Resources Network Device Groups Policy Elements Device Admin Policy Sets Reports Settings

Network Devices

Default Devices

TACACS External Servers

TACACS Server Sequence

Network Devices

Selected 0 | Total 0

Show

Name	IP/Mask	Profile Name	Location	Type	Description
No data available					

Immettere le informazioni per il server Prime. Gli attributi obbligatori da includere sono Nome, Indirizzo IP, selezionare l'opzione per TACACS e il segreto condiviso. È inoltre possibile aggiungere un Tipo di dispositivo, specificatamente per Prime, da utilizzare successivamente come Condizione per la Regola di autorizzazione o altre informazioni, anche se questa operazione è facoltativa.

Network Devices List > New Network Device

Network Devices

Name

Description

\* IP Address:  /  32

\* Device Profile

Model Name

Software Version

\* Network Device Group

Device Type

Location

RADIUS Authentication Settings

TACACS Authentication Settings

Shared Secret

Enable Single Connect Mode

Legacy Cisco Device

TACACS Draft Compliance Single Connect Support

SNMP Settings

Advanced TrustSec Settings

Quindi creare un risultato del profilo TACACS per inviare gli attributi richiesti da ISE a Prime, in modo da fornire il corretto livello di accesso. Passare a Centri di lavoro / Risultati criteri / Profili TACACS e selezionare l'opzione Aggiungi.

Identity Services Engine

Home > Operations > Policy > Guest Access > Administration > Work Centers

TrustSec > Device Administration

Overview > Identities > User Identity Groups > Network Resources > Network Device Groups > Policy Conditions > Policy Results > Device Admin Policy Sets > Reports > Settings

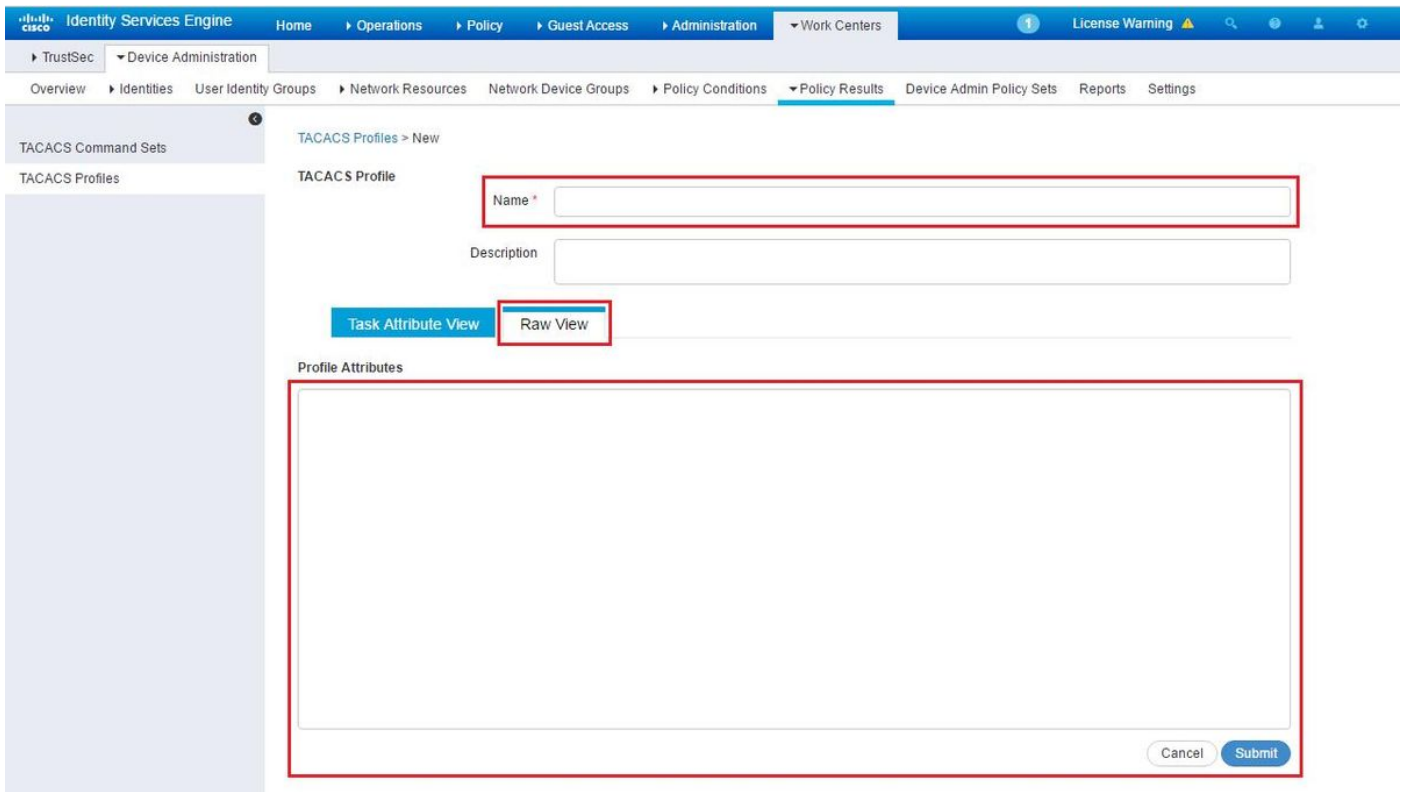
TACACS Profiles

Rows/Page 6 1 / 1 Go 6 Total Rows

Refresh Add Duplicate Trash Edit Filter

Name	Description
------	-------------

Configurare il nome e utilizzare l'opzione Visualizzazione non elaborata per immettere gli attributi nella casella Attributi profilo. Gli attributi provengono dal server di base stesso.



Ottenere gli attributi nella schermata Amministrazione / Utenti/ Utenti, Ruoli & AAA e selezionare la scheda Gruppi di utenti. Selezionare il livello di accesso Gruppo che si desidera fornire. In questo esempio l'accesso come amministratore viene fornito selezionando l'elenco di task appropriato sul lato sinistro.

Administration / Users / Users, Roles & AAA

AAA Mode Settings	User Groups			
Active Sessions	Group Name	Members	Audit Trail	View Task
Change Password	Admin	JP		<b>Task List</b>
Local Password Policy	Config Managers			Task List
RADIUS Servers	Lobby Ambassador	User1 , CostaRica , Yita		Task List
SSO Server Settings	Monitor Lite			Task List
SSO Servers	NBI Credential			Task List
TACACS+ Servers	NBI Read			Task List
<b>User Groups</b>	NBI Write			Task List
Users	North Bound API			Task List
	Root	root		Task List
	Super Users			Task List
	System Monitoring			Task List
	User Assistant			Task List
	User Defined 1			Task List
	User Defined 2			Task List
	User Defined 3			Task List
	User Defined 4			Task List
	mDNS Policy Admin			Task List

Copiare tutti gli attributi personalizzati TACACS.

- AAA Mode Settings
- Active Sessions
- Change Password
- Local Password Policy
- RADIUS Servers
- SSO Server Settings
- SSO Servers
- TACACS+ Servers
- User Groups**
- Users

Task List

Please copy and paste the appropriate protocol data below into the custom/vendor-specific attribute field in your AAA server.

TACACS+ Custom Attributes

```
role0=Admin
task0=Discovery Schedule Privilege
task1=Mesh Reports
task2=Saved Reports List
task3=Monitor Menu Access
task4=Device WorkCenter
task5=Inventory Menu Access
task6=Add Device Access
task7=Config Audit Dashboard
task8=Custom NetFlow Reports
task9=Apic Controller Read Access
task10=Configuration Templates Read Access
task11=Alarm Policies Edit Access
task12=High Availability Configuration
task13=View Job
task14=Incidents Alarms Events Access
task15=TAC Case Management Tool
task16=Configure Autonomous Access Point
Templates
task17=Import Policy Update
task18=PnP Profile Read-Write Access
task19=SSO Server AAA Mode
task20=Alarm Resource Access
```

RADIUS Custom Attributes

If the size of the RADIUS attributes on your AAA server is more than 4096 bytes, Please copy ONLY role attributes, application will retrieve the associated TASKS

```
NCS:role0=Admin
NCS:task0=Discovery Schedule Privilege
NCS:task1=Mesh Reports
NCS:task2=Saved Reports List
NCS:task3=Monitor Menu Access
NCS:task4=Device WorkCenter
NCS:task5=Inventory Menu Access
NCS:task6=Add Device Access
NCS:task7=Config Audit Dashboard
NCS:task8=Custom NetFlow Reports
NCS:task9=Apic Controller Read Access
NCS:task10=Configuration Templates Read Access
NCS:task11=Alarm Policies Edit Access
NCS:task12=High Availability Configuration
NCS:task13=View Job
NCS:task14=Incidents Alarms Events Access
NCS:task15=TAC Case Management Tool
NCS:task16=Configure Autonomous Access Point
Templates
NCS:task17=Import Policy Update
NCS:task18=PnP Profile Read-Write Access
NCS:task19=SSO Server AAA Mode
NCS:task20=Alarm Resource Access
```

Virtual Domain custom attributes are mandatory. To add custom attributes related to Virtual Domains, please click here.

Quindi incollale nella sezione "Visualizzazione raw" del Profilo su ISE.

TACACS Profiles > New

TACACS Profile

Name \* Prime

Description

Task Attribute View Raw View

Profile Attributes

```
role0=Admin
task0=Discovery Schedule Privilege
task1=Mesh Reports
task2=Saved Reports List
task3=Monitor Menu Access
task4=Device WorkCenter
task5=Inventory Menu Access
task6=Add Device Access
task7=Config Audit Dashboard
task8=Custom NetFlow Reports
task9=Apic Controller Read Access
task10=Configuration Templates Read Access
task11=Alarm Policies Edit Access
task12=High Availability Configuration
task13=View Job
```

Cancel Submit

Gli attributi personalizzati del dominio virtuale sono obbligatori. Le informazioni sul dominio principale sono disponibili in Amministrazione principale -> Domini virtuali.

Cisco Prime Infrastructure

Virtual Domain ROOT-DOMAIN | root

Administration > Virtual Domains

Virtual Domains

Virtual Domains > ROOT-DOMAIN

ROOT-DOMAIN

Virtual domains are logical groupings of devices and are used to control who can administer a group. After you add devices to Prime Infrastructure, you can configure virtual domains. Virtual domain filters allow users to configure devices, view alarms, and generate reports their assigned part of the network only.

\* Name ROOT-DOMAIN

Time Zone -- Select Time Zone --

Email Address

Description ROOT-DOMAIN

Submit Cancel

Il nome del dominio virtuale principale deve essere aggiunto come attributo **virtual-domain0="nome dominio virtuale"**

TACACS Profiles > Prime Access

**TACACS Profile**

Name: Prime Access

Description:

Task Attribute View | **Raw View**

**Profile Attributes**

```
task162=Monitor Mobility Devices
task163=Context Aware Reports
task164=Voice Diagnostics
task165=Configure Choke Points
task166=RRM Dashboard
task167=Swim Delete
task168=Theme Changer Access
task169=Import Policy Update
task170=Design Endpoint Site Association Access
task171=Planning Mode
task172=Pick and Unpick Alerts
task173=Configure Menu Access
task174=Ack and Unack Security Index Issues
task175=Ack and Unack Alerts
task176=Auto Provisioning
virtual-domain0=ROOT-DOMAIN
```

Cancel Save

Al termine, è sufficiente creare una regola per assegnare il profilo di shell creato nel passaggio precedente, in Centri di lavoro / Amministrazione dispositivi / Set di criteri di amministrazione dispositivi

(Nota: Le "Condizioni" variano a seconda della distribuzione, tuttavia è possibile utilizzare "Tipo di dispositivo" specificatamente per Prime o un altro tipo di filtro, ad esempio l'indirizzo IP di Prime, come una delle "Condizioni" in modo che questa regola filtri correttamente le richieste)

Define the Policy Sets by configuring rules based on conditions. Drag and drop sets on the left hand side to change the order. For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Status	Name	Description
<input checked="" type="checkbox"/>	Default	Tacacs_Default

Regular Proxy Sequence

**Authentication Policy**

Default Rule (if no match) : Allow Protocols : Default Device Admin and use : Internal Users [Edit](#)

**Authorization Policy**

**Exceptions (0)**

Standard

Status	Rule Name	Conditions (Identity groups and other conditions)	Command Sets	Shell Profiles
<input checked="" type="checkbox"/>	Prime Rule	if DEVICE Device Type EQUALS All Device Types#Prime	then PermitAll AND	Prime
<input checked="" type="checkbox"/>	Tacacs_Default	if no matches, then	Select Profile(s) Deny All Shell Profile	

A questo punto la configurazione deve essere completa.



## Risoluzione dei problemi

Se questa configurazione non ha esito positivo e l'opzione di fallback locale è stata abilitata su Prime, è possibile forzare il failover da ISE, rimuovendo l'indirizzo IP di Prime. In questo modo ISE non risponderà e verrà forzato l'uso delle credenziali locali. Se il fallback locale è configurato per essere eseguito su un rifiuto, gli account locali continueranno a funzionare e forniranno l'accesso al cliente.

Se ISE ha completato l'autenticazione e soddisfa la regola corretta, ma Prime rifiuta comunque la richiesta. Verificare che gli attributi siano configurati correttamente nel profilo e che non siano stati inviati attributi aggiuntivi.