

# Autenticación de TACACS de la prima 3.1 de la configuración contra ISE 2.x

## Contenido

[Introducción](#)

[Requisitos](#)

[Configurar](#)

[Configuración primera](#)

[Configuración ISE](#)

[Troubleshooting](#)

## Introducción

Este documento describe cómo configurar la infraestructura primera para autenticar vía el TACACS con ISE 2.x.

## Requisitos

Cisco recomienda que usted tiene un conocimiento básico de estos temas:

- Identity Services Engine (ISE)
- Infraestructura primera

## Configurar

Sistema de control de redes 3.1 de la prima de Cisco

Motor 2.0 del servicio de la identidad de Cisco o más adelante.

(Nota: El ISE soporta solamente el TACACS que comienza con la versión 2.0, sin embargo es posible configurar la prima para utilizar el radio. La prima incluye la lista de atributos de RADIUS además del TACACS si usted preferiría utilizar el radio, con una versión anterior del ISE o de una solución del otro vendedor.)

## Configuración primera

Navigate a la pantalla siguiente: La administración/usuarios, papeles y AAA de los usuarios según lo visto abajo.

Una vez que, selecciona el lengüeta de los servidores TACACS+, después seleccione la opción del servidor del agregar TACACS+ en la esquina derecha superior y selecto vaya.

En la siguiente pantalla la configuración de la entrada del servidor TACACS está disponible (ésta

tendrá que ser hecha para cada servidor TACACS individual)

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: 49

Shared Secret Format: ASCII

\* Shared Secret

\* Confirm Shared Secret

\* Retransmit Timeout: 5 (secs)

\* Retries: 1

Authentication Type: PAP

Local Interface IP: 192.168.10.154

Save Cancel

Aquí usted necesitará ingresar el IP Address o la dirección de DNS del servidor, así como la clave secreta compartida. También satisfaga observan el IP de la interfaz local que usted quisiera utilizar, como esta misma dirección IP necesita ser utilizada para el cliente AAA en el ISE después.

Para completar la configuración en la prima. Usted necesitará habilitar el TACACS bajo la administración/los usuarios/los usuarios, los papeles y el AAA bajo lengüeta de las configuraciones de modo AAA.

(Nota: Se recomienda para marcar el retraso del permiso a la opción local, con SOLAMENTE en ninguna respuesta del servidor o encendido la ninguna opción de la respuesta o del error, especialmente mientras que prueba la configuración)

Administration / Users / Users, Roles & AAA

AAA Mode Settings

AAA Mode

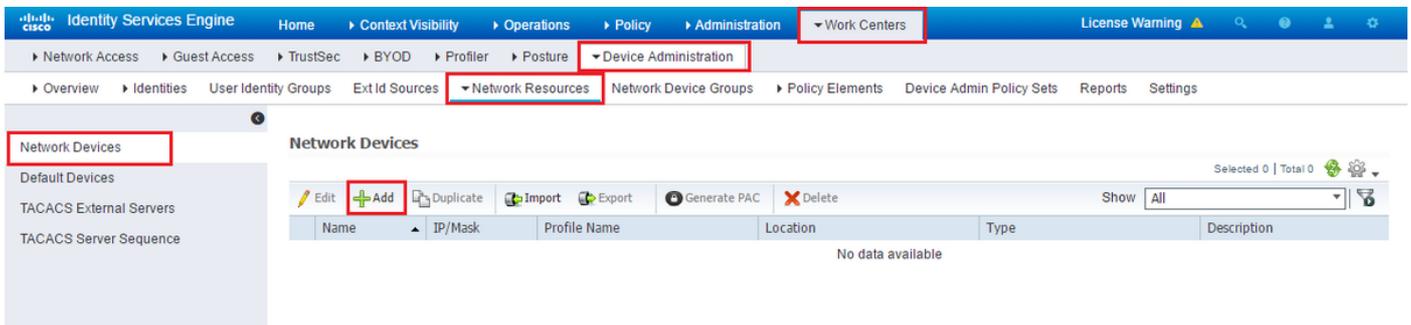
Local  RADIUS  TACACS+  SSO

Enable fallback to Local ONLY on no server respons:

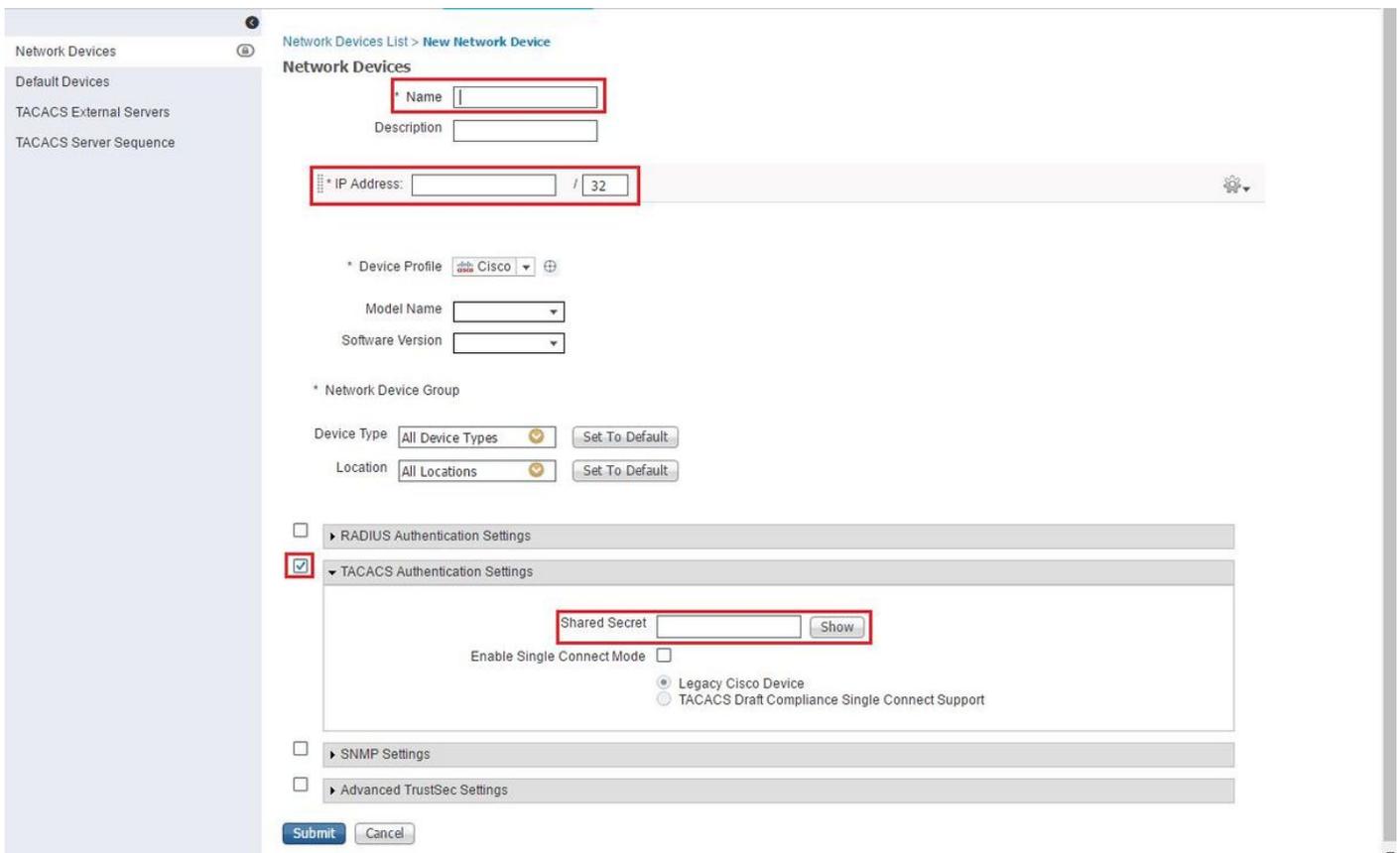
Save

## Configuración ISE

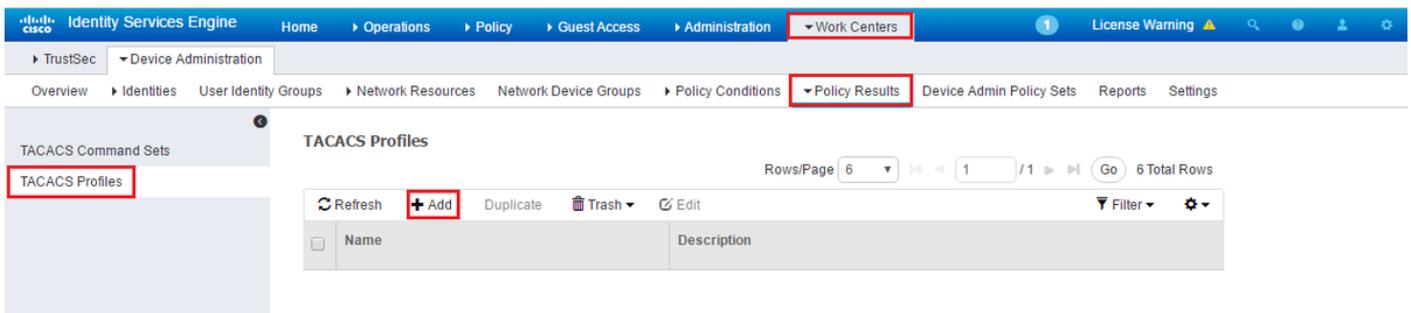
Configure la prima como cliente AAA en el ISE en los centros de trabajo/Device Administration (Administración del dispositivo) los dispositivos del /Network de los recursos del /Network/agregue



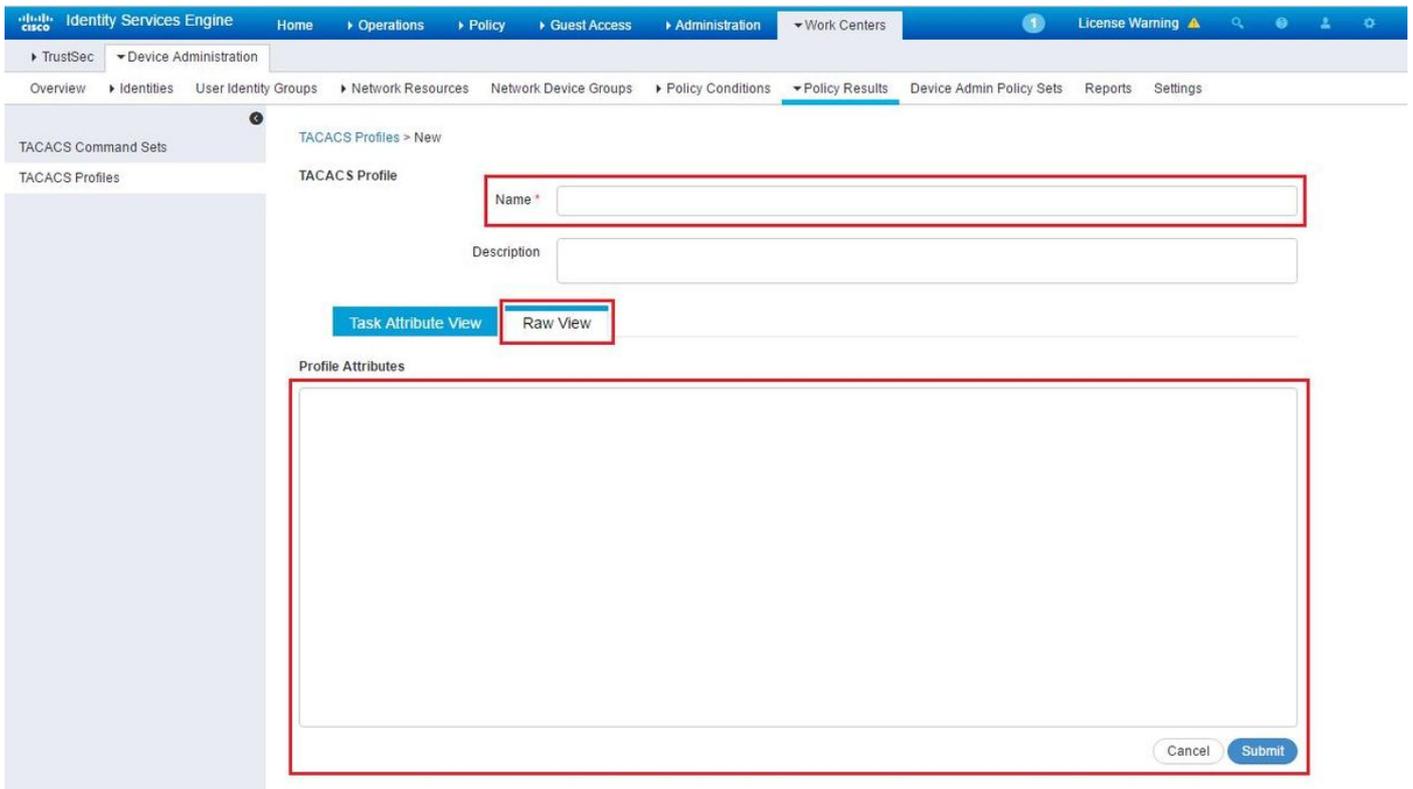
Ingrese la información para el servidor primero. Los atributos requeridos que usted necesita incluir son nombre, dirección IP, seleccionan la opción para el TACACS y el secreto compartido. Usted puede desear además agregar un tipo de dispositivo, específicamente para la prima, para utilizar después como condición para la regla de la autorización o la otra información, no obstante ésta es opcional.



Entonces cree un resultado del perfil TACACS para enviar los atributos requeridos del ISE para preparar, proporcionar el nivel correcto de acceso. Navegue a los centros de trabajo/a los resultados de la directiva/a los perfiles de Tacacs y seleccione la opción del agregar.



Configure el nombre, y utilice la opción sin procesar de la visión para ingresar los atributos bajo el rectángulo de los atributos del perfil. Los atributos vendrán del servidor sí mismo de la cartilla.



Consiga los atributos bajo la administración/los usuarios de los usuarios, los papeles y la pantalla AAA, y seleccione la lengüeta de los grupos de usuarios. Aquí usted selecciona el nivel de grupo de acceso que usted desea proporcionar. En este admin de ejemplo el acceso es proporcionado seleccionando la lista de tareas apropiada en el lado izquierdo.

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

Copie todos los atributos personalizados 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.

Entonces pegúelos en la sección sin procesar de la visión del perfil en el ISE.

The screenshot shows the 'TACACS Profile' configuration page in Cisco ISE. The profile name is 'Prime'. The 'Raw View' tab is active, displaying a list of task 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, and task13=View Job. This list is enclosed in a red box.

Los atributos personalizados del dominio virtual son obligatorios. La información del Raíz-dominio se puede encontrar bajo administración primera -> los dominios virtuales.

The screenshot shows the 'Virtual Domains' configuration page in Cisco Prime Infrastructure. The virtual domain name is 'ROOT-DOMAIN'. The 'Name' field is highlighted with a red box. Other fields include 'Email Address', 'Time Zone' (set to '-- Select Time Zone --'), and 'Description' (set to 'ROOT-DOMAIN').

El nombre del dominio virtual primero tiene que ser agregado como Domain Name del atributo `virtual-domain0="virtual"`

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

Una vez que eso se hace todos ustedes necesita hacer debe crear una regla para asignar el perfil del shell creado en el paso anterior, bajo los centros de trabajo/Device Administration (Administración del dispositivo)/directiva Admin del dispositivo fija

(Nota: Las “condiciones” variarán dependiendo del despliegue, no obstante usted puede utilizar el “tipo de dispositivo” específicamente para la prima u otro tipo de filtro tal como dirección IP de la prima, como una de “condicionan” de modo que esta regla filtre correctamente las peticiones)

Policy Sets

Search policy names & descriptions.

Summary of Policies

Global Exceptions

Default

Tacacs\_Default

Save Order Reset Order

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
✓	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
✓	Prime Rule	if DEVICE Device Type EQUALS All Device Types#Prime	PermitAll AND	Prime
✓	Tacacs_Default	if no matches, then	Select Profile(s) Deny All Shell Profile	

En este momento la configuración debe ser completa.

# Troubleshooting

Si esta configuración es fracasada y si bajan el locales opción eran permiso en la prima, usted puede forzar un fall encima del ISE, quitando la dirección IP de la prima. Esto hará el ISE no responder y forzar el uso de las credenciales locales. Si el retraso local se configura para ser realizado en un rechazo, las cuentas locales todavía trabajarán y proporcionarán el acceso al cliente.

Si el ISE muestra una autenticación satisfactoria y está correspondiendo con la regla correcta sin embargo la prima todavía está rechazando la petición que usted puede desear para comprobar los atributos con minuciosidad se configura correctamente en el perfil y no se está enviando ningunos atributos adicionales.