

Configuración de la autenticación TACACS+ en el switch Arista con ISE

Contenido

[Introducción](#)

[Prerequisites](#)

[Componentes Utilizados](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Configuración de TACACS+ en ISE](#)

[Configurar el switch Arista](#)

[Paso 1. Habilitar autenticación TACACS+](#)

[Paso 2. Guarde la configuración](#)

[Verificación](#)

[Revisión de ISE](#)

[Resolución de problemas](#)

[Problema 1](#)

[Posibles Causas](#)

[Problema 2](#)

[Posibles Causas](#)

[Solución](#)

Introducción

Este documento describe cómo integrar Cisco ISE TACACS+ con un switch Arista para obtener acceso de administrador a AAA centralizado.

Prerequisites

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco ISE y protocolo TACACS+.
- Switches Arista

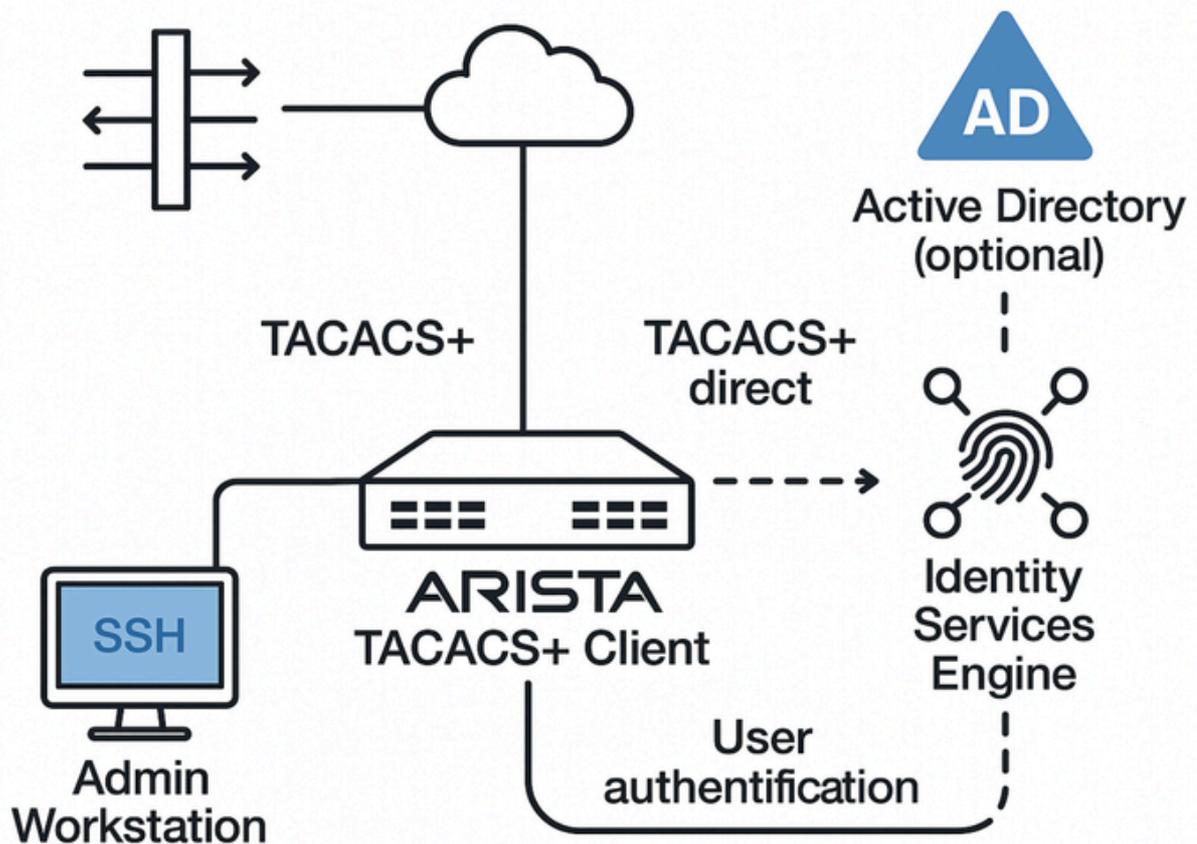
Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versión de imagen de software del switch Arista: 4.33.2F
- Parche 4 de Cisco Identity Services Engine (ISE) versión 3.3

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando

Diagrama de la red

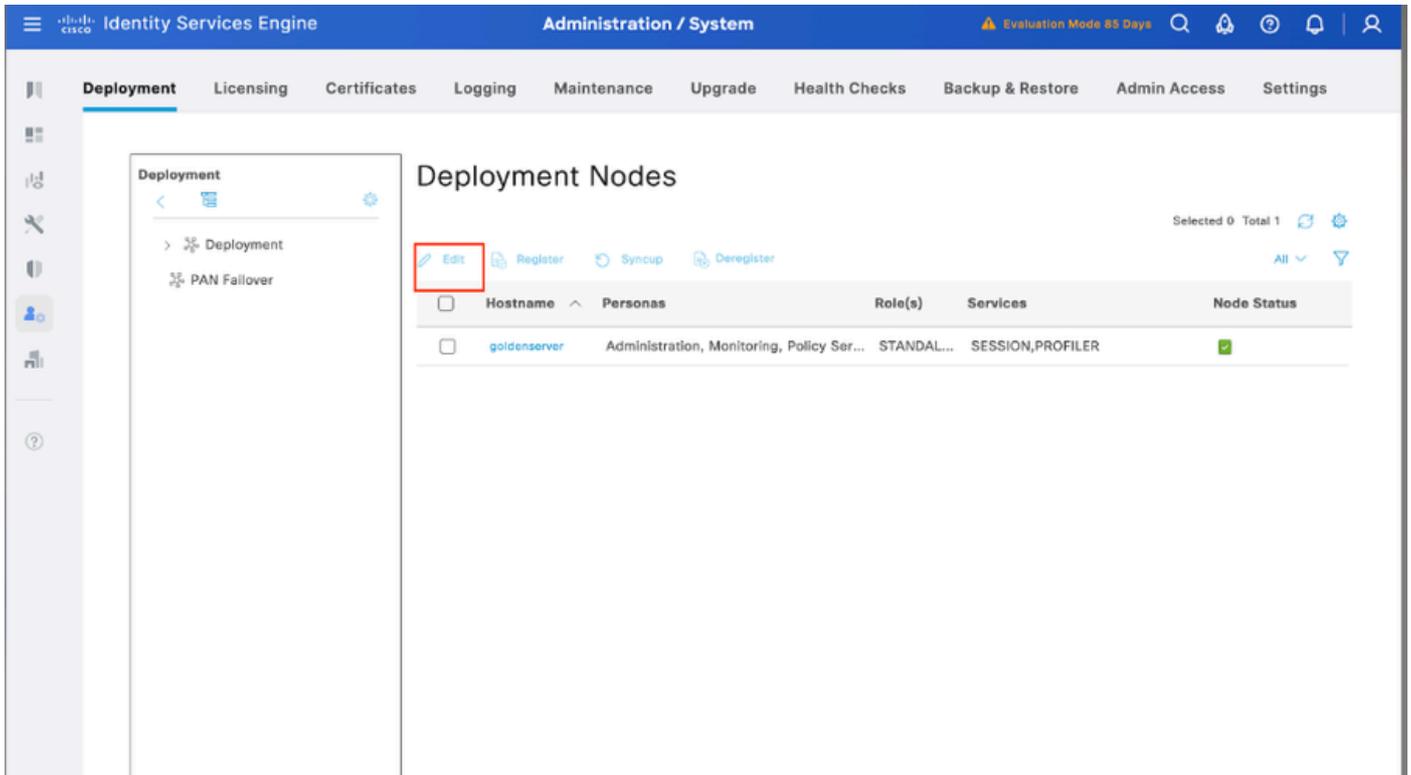


Configuraciones

Configuración de TACACS+ en ISE

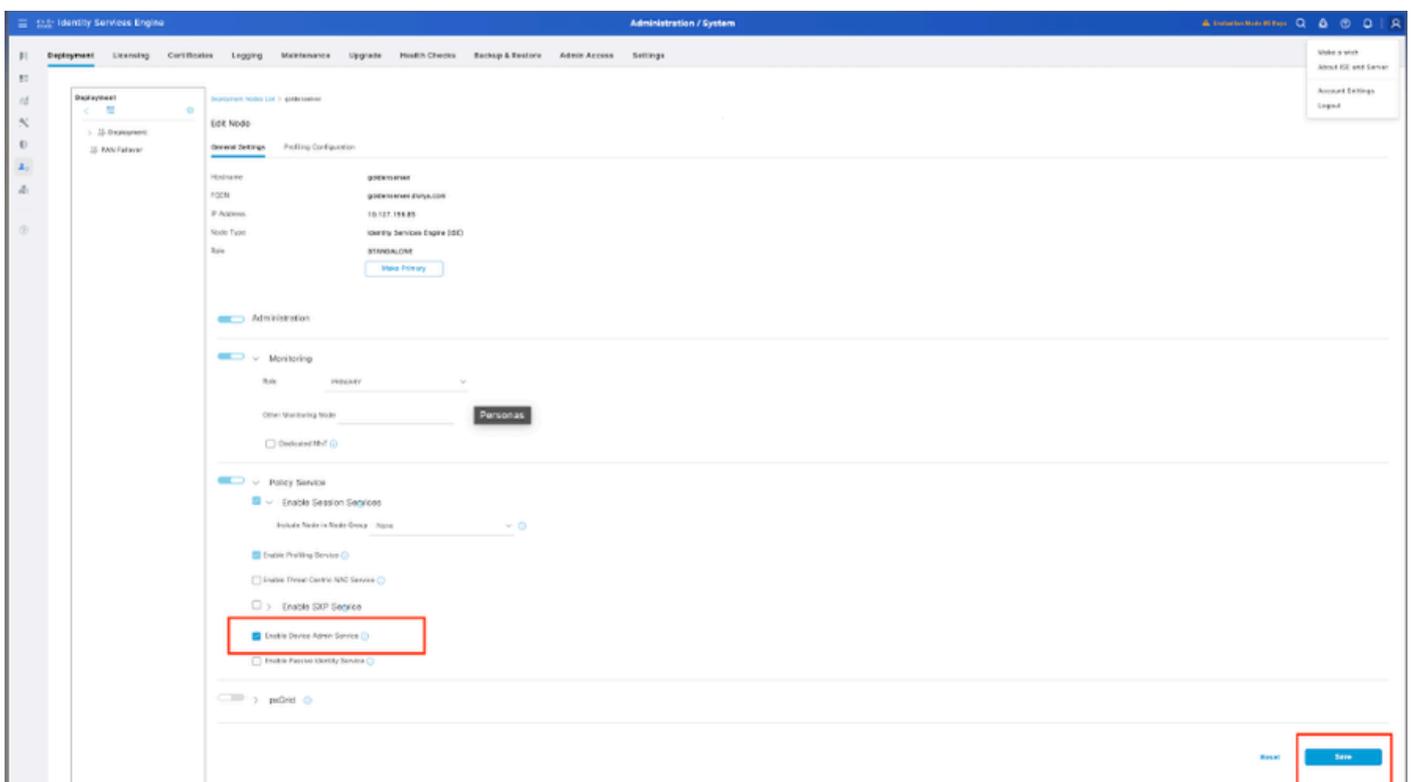
Paso 1. El paso inicial es verificar si Cisco ISE cuenta con las capacidades necesarias para gestionar la autenticación TACACS+. Para ello, confirme que el nodo de servicios de directivas (PSN) deseado tiene activada la función Device Admin Service.

Vaya a Administration > System > Deployment, seleccione el nodo adecuado donde ISE procesa la autenticación TACACS+ y haga clic en Edit para revisar su configuración.



Paso 2. Desplácese hacia abajo para localizar la función Device Administration Service. Tenga en cuenta que para activar esta función es necesario que el usuario del servicio de políticas esté activo en el nodo, junto con las licencias TACACS+ disponibles en la implementación.

Seleccione la casilla de verificación para activar la función y, a continuación, guarde la configuración.



Paso 3. Obtención del perfil de dispositivo de red de Arista para Cisco ISE.

La comunidad de Cisco ha compartido un perfil NAD dedicado para los dispositivos Arista. Este perfil, junto con los archivos de diccionario necesarios, se puede encontrar en el artículo [Arista CloudVision WiFi Dictionary y NAD Profile for ISE Integration](#). La descarga e importación de este perfil en la configuración de ISE facilita una integración más fluida

Pasos para importar el perfil de Arista NAD a Cisco ISE:

1. Descargue el perfil:

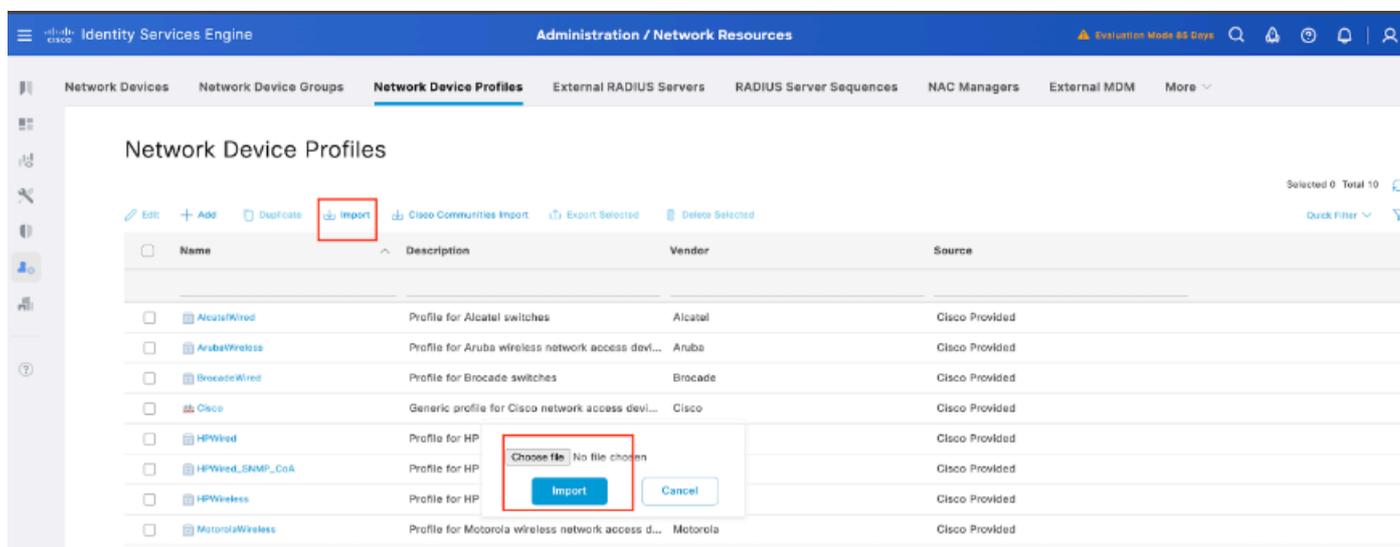
- Obtenga el perfil de Arista NAD del enlace de la comunidad de Cisco proporcionado anteriormente. [Comunidad de Cisco](#)

2. Acceda a Cisco ISE:

- Inicie sesión en la consola administrativa de Cisco ISE

3. Importar el perfil NAD:

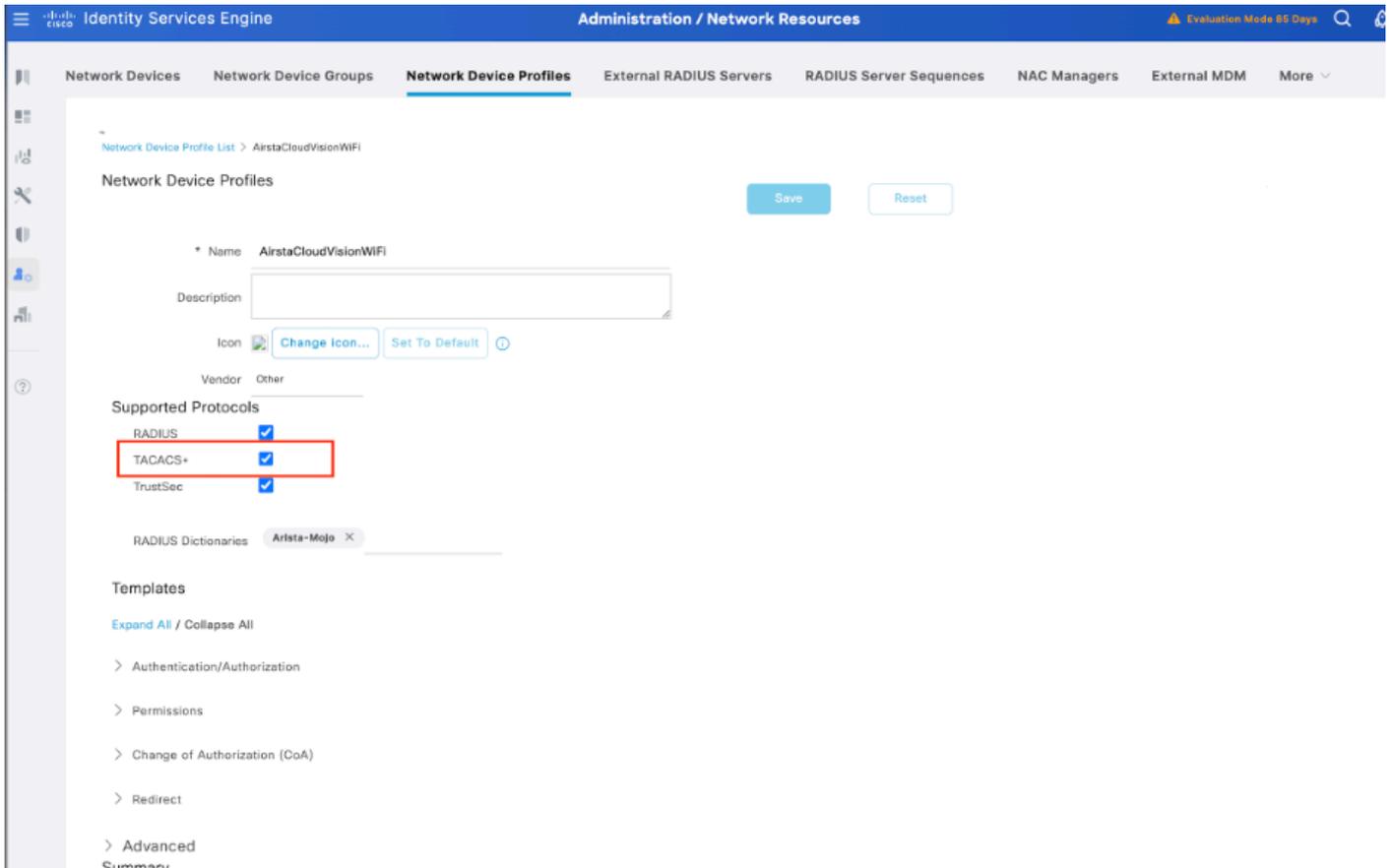
- Vaya a Administration > Network Resources > Network Device Profiles.
- Haga clic en el botón Importar
- Cargue el archivo de perfil de Arista NAD descargado.



The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The page title is "Network Device Profiles" under the "Administration / Network Resources" section. The "Import" button in the top toolbar is highlighted with a red box. A file selection dialog is open over the "HPWired" profile, showing "Choose file", "No file chosen", "Import", and "Cancel" buttons.

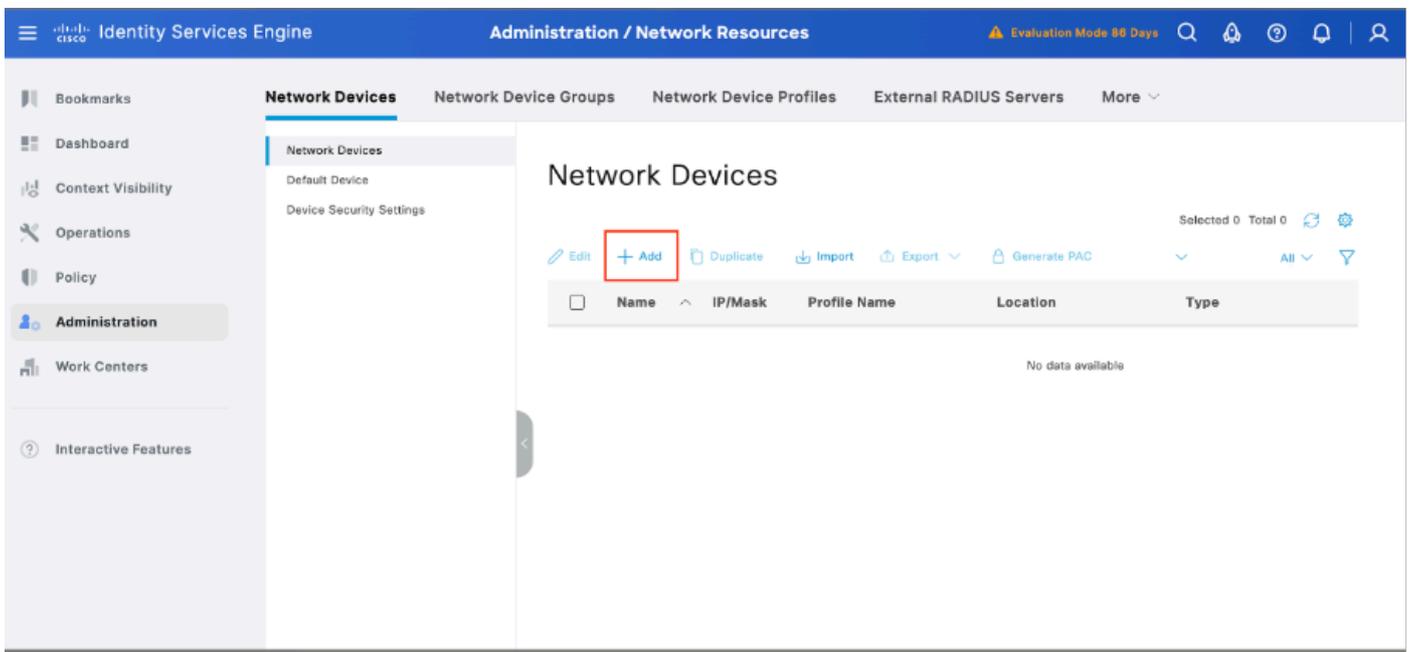
Name	Description	Vendor	Source
AlcatelWired	Profile for Alcatel switches	Alcatel	Cisco Provided
ArubaWireless	Profile for Aruba wireless network access devi...	Aruba	Cisco Provided
BrocadeWired	Profile for Brocade switches	Brocade	Cisco Provided
Cisco	Generic profile for Cisco network access devi...	Cisco	Cisco Provided
HPWired	Profile for HP		Cisco Provided
HPWired_SKMP_CoA	Profile for HP		Cisco Provided
HPWireless	Profile for HP		Cisco Provided
MotorolaWireless	Profile for Motorola wireless network access d...	Motorola	Cisco Provided

Una vez completada la carga, navegue hasta la opción Edit y habilite TACACS+ como protocolo soportado.



Paso 2: Agregue el switch Arista como dispositivo de red.

1. Vaya a Administration > Network Resources > Network Devices > +Add:

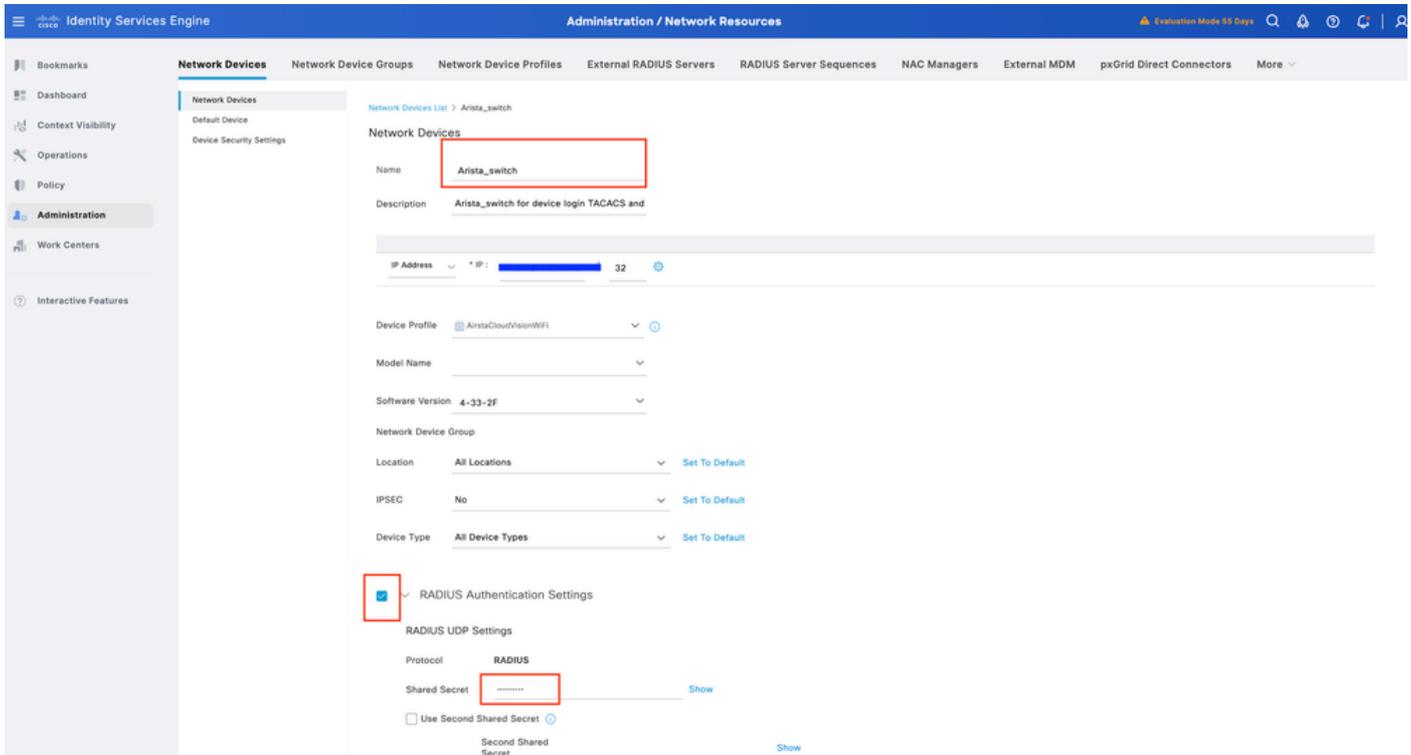


2. Haga clic en Agregar e ingrese estos detalles:

- IP Address: <Switch-IP>
- tipo de dispositivo: Seleccione Otro Cableado
- Perfil de dispositivo de red: seleccione AirstaCloudVisionWiFi.

- Configuración de autenticación RADIUS:
 - Habilite la autenticación RADIUS.
 - Ingrese el secreto compartido (debe coincidir con la configuración del switch).

3. Haga clic en Guardar:

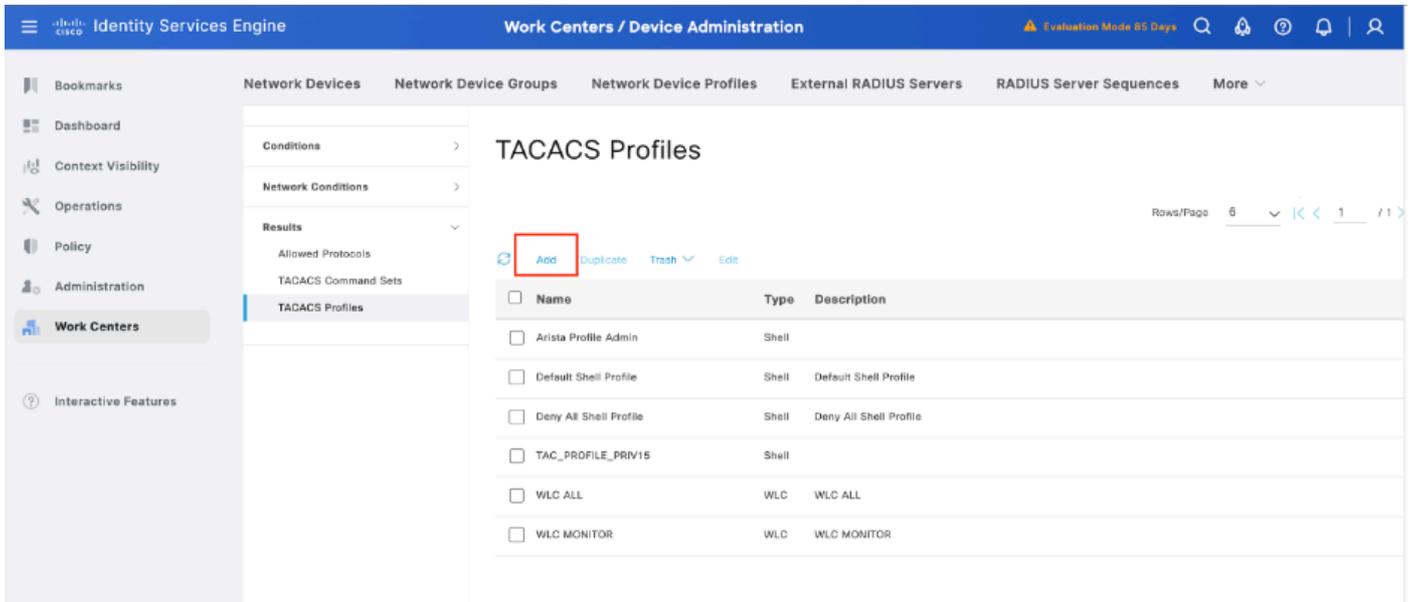


Paso 3. Validar el nuevo dispositivo se muestra en Dispositivos de red:

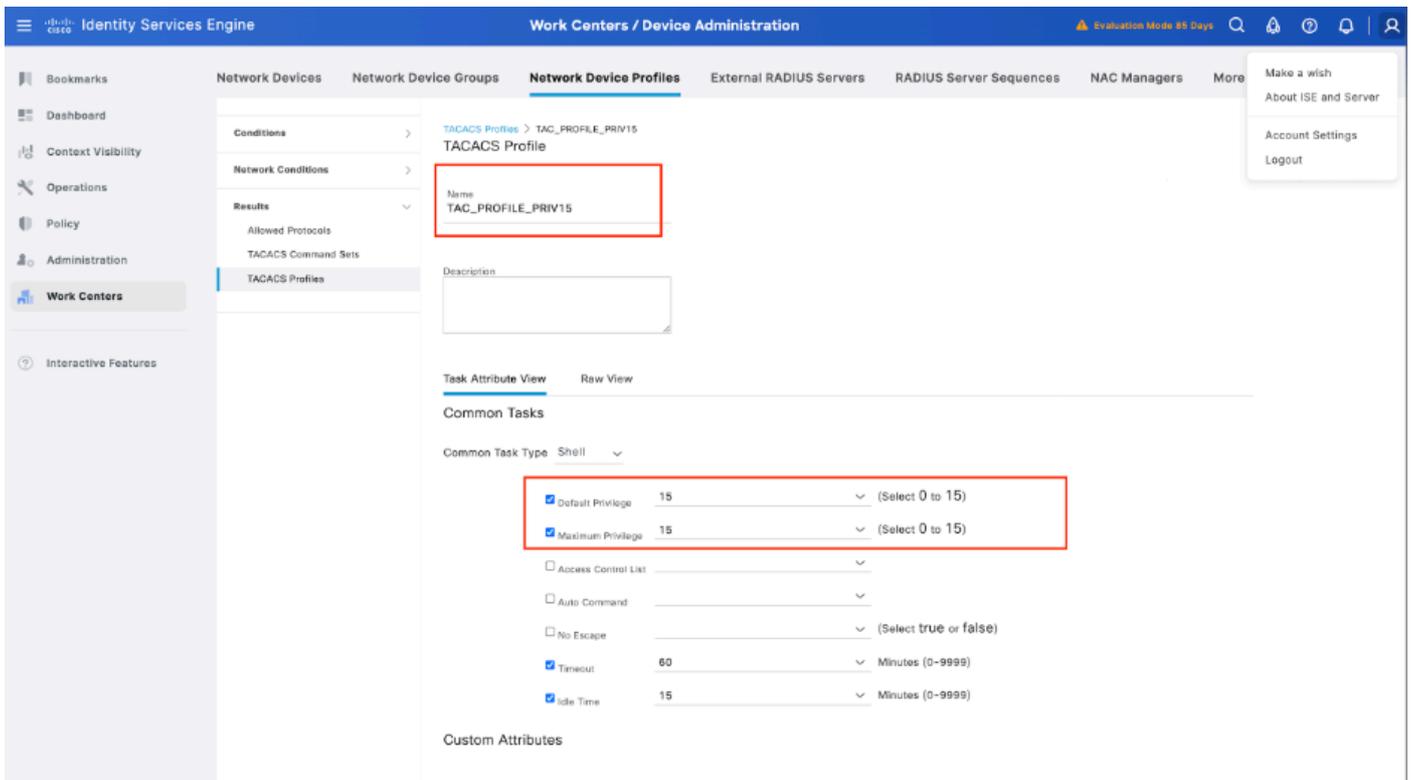


Paso 4. Configure el perfil TACACS.

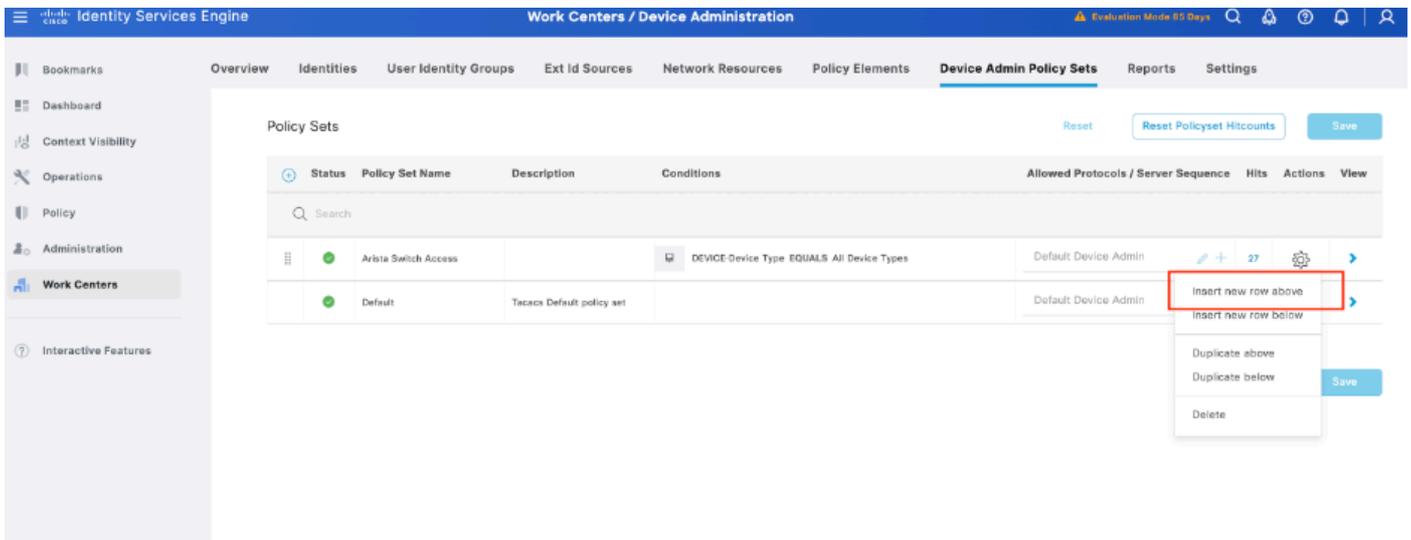
Cree un perfil TACACS, navegue hasta el menú Centros de trabajo > Administración de dispositivos > Elementos de política > Resultados > Perfiles TACACS, luego seleccione Agregar:



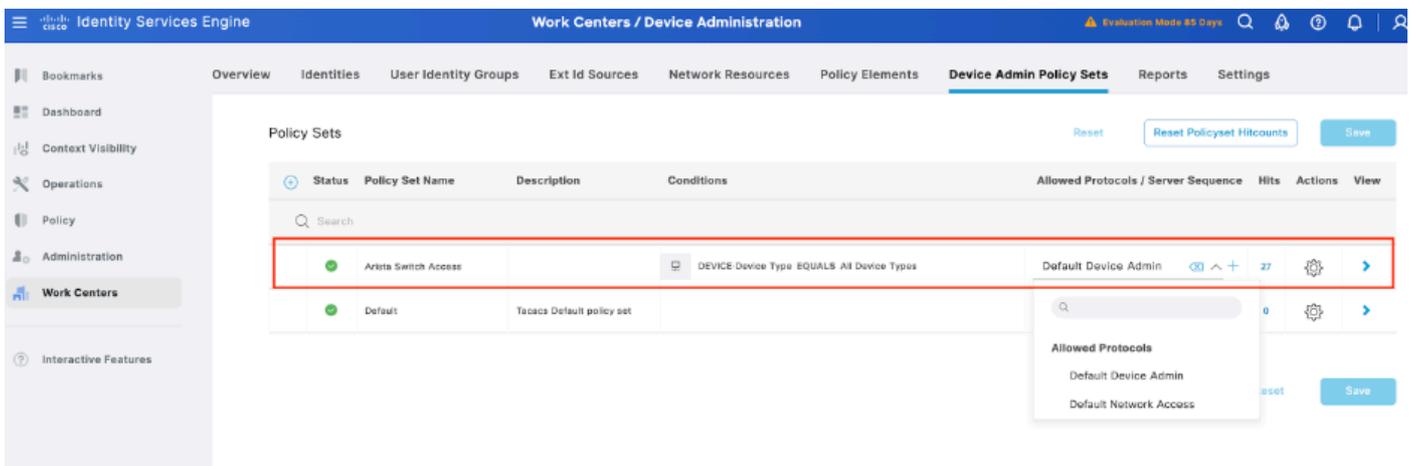
Introduzca un nombre, active la casilla de control Privilegio por Defecto y defina el valor en 15. Además, seleccione Privilegio Máximo, defina su valor en 15 y haga clic en Enviar:



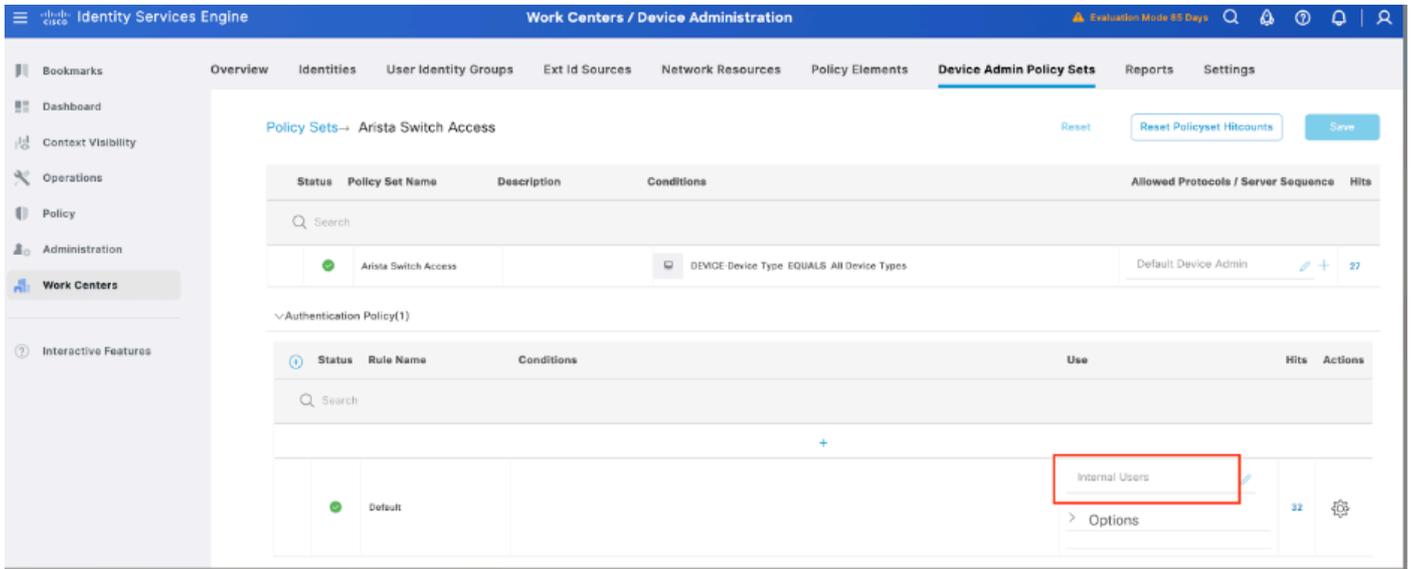
Paso 5. Cree un conjunto de políticas de administración de dispositivos para su switch Arista, navegue hasta el menú Centros de trabajo > Administración de dispositivos > Conjuntos de políticas de administración de dispositivos, luego desde un conjunto de políticas existente seleccione el icono de engranaje para luego seleccionar Insertar nueva fila arriba.



Paso 6. Dé un nombre a este nuevo conjunto de políticas, agregue condiciones en función de las características de las autenticaciones TACACS+ que se estén realizando desde el switch Arista y seleccione Allowed Protocols > Default Device Admin para guardar su configuración.

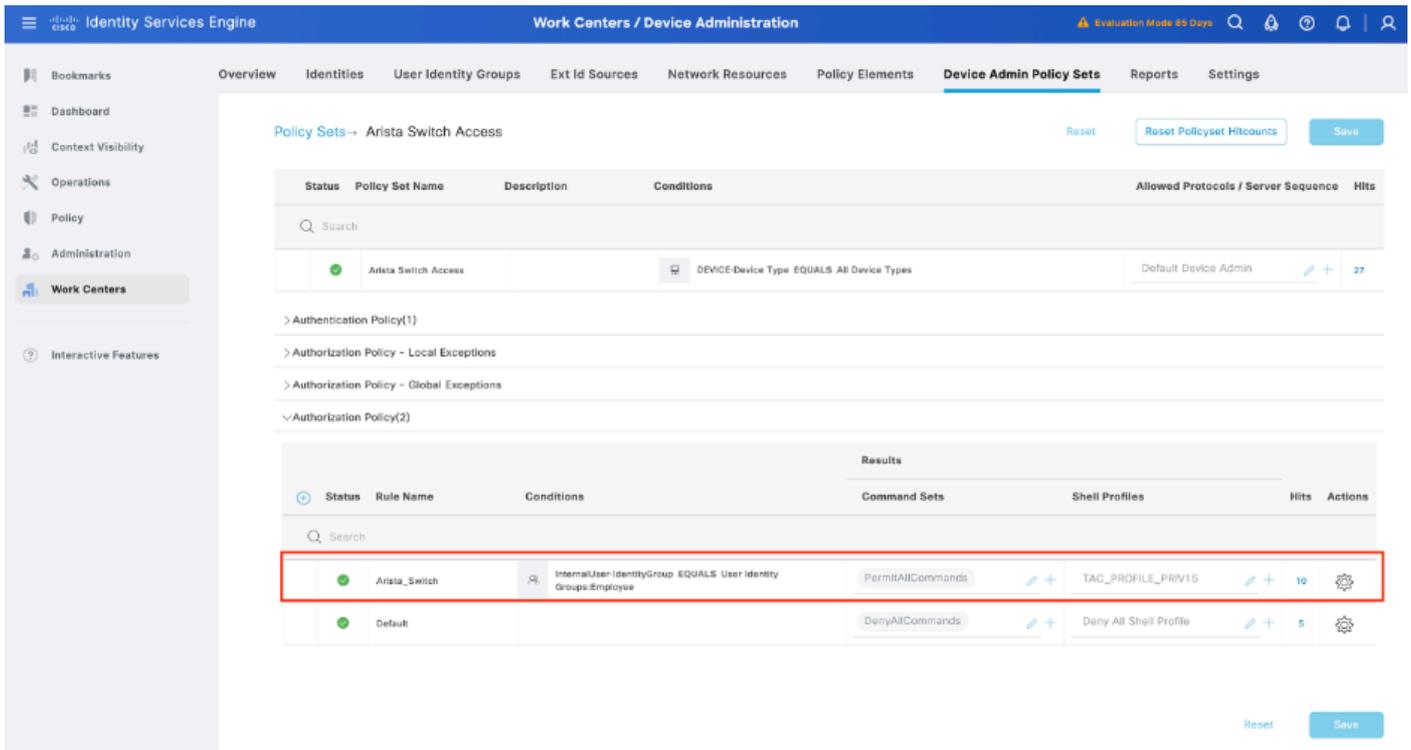


Paso 7. Seleccione la opción > view y, a continuación, en la sección Authentication Policy, seleccione el origen de identidad externo que Cisco ISE utiliza para consultar el nombre de usuario y las credenciales para la autenticación en el switch Arista. En este ejemplo, las credenciales corresponden a los usuarios internos almacenados en ISE.



Paso 8. Desplácese hacia abajo hasta la sección denominada Authorization Policy to Default policy, seleccione el icono de engranaje y luego inserte una regla arriba.

Paso 9. Asigne un nombre a la nueva regla de autorización, agregue condiciones relativas al usuario que ya se ha autenticado como miembro del grupo y, en la sección Perfiles de shell, agregue el perfil TACACS que configuró anteriormente y guarde la configuración.



Configurar el switch Arista

Paso 1. Habilitar autenticación TACACS+

Inicie sesión en el switch de Arista e ingrese al modo de configuración:

configurar

```
!  
tacacs-server host <ISE-IP> key <TACACS-SECRET>  
  
!  
aaa group server tacacs+ ISE_TACACS  
    server <ISE-IP>  
  
!  
aaa authentication login default group ISE_TACACS local  
aaa authorization exec default group ISE_TACACS local  
aaa accounting commands 15 default start-stop group ISE_TACACS  
  
!
```

Finalizar

Paso 2. Guarde la configuración

Para conservar la configuración durante los reinicios:

```
# write memory  
  
O  
  
# copy running-config startup-config
```

Verificación

Revisión de ISE

Paso 1. Revise si la capacidad de servicio de TACACS+ se está ejecutando, esto se puede registrar:

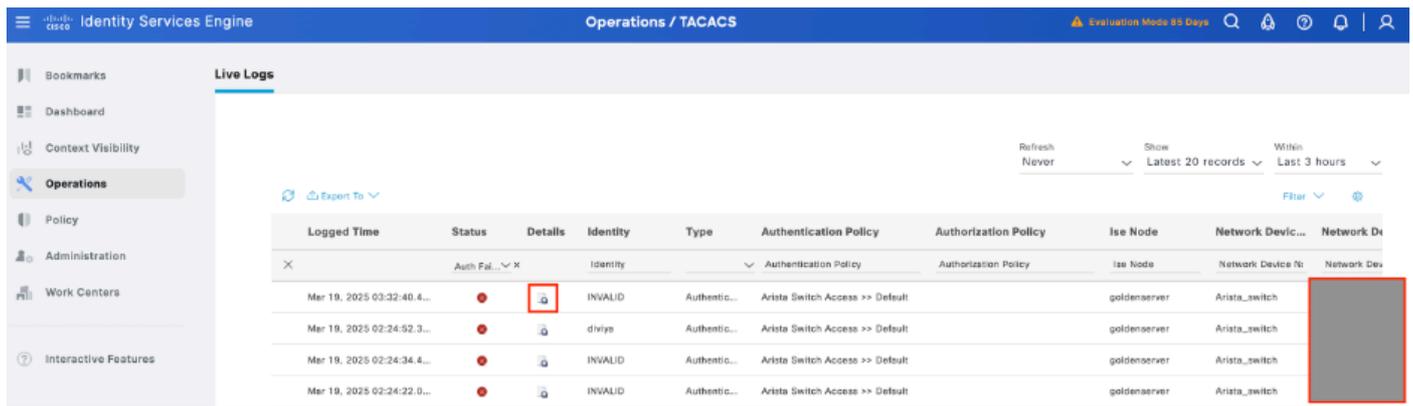
- GUI: Revise si el nodo aparece con el servicio DEVICE ADMIN en > System > Deployment.
- CLI: Ejecute el comando show ports | incluir 49 para confirmar que hay conexiones en el puerto TCP que pertenecen a TACACS+

```
goldenserver/admin#show ports | include 49
```

```
tcp: [REDACTED]
```

Paso 2. Confirme si hay registros de vida relacionados con intentos de autenticación TACACS+ : esto se puede verificar en el menú Operaciones > TACACS > Live logs,

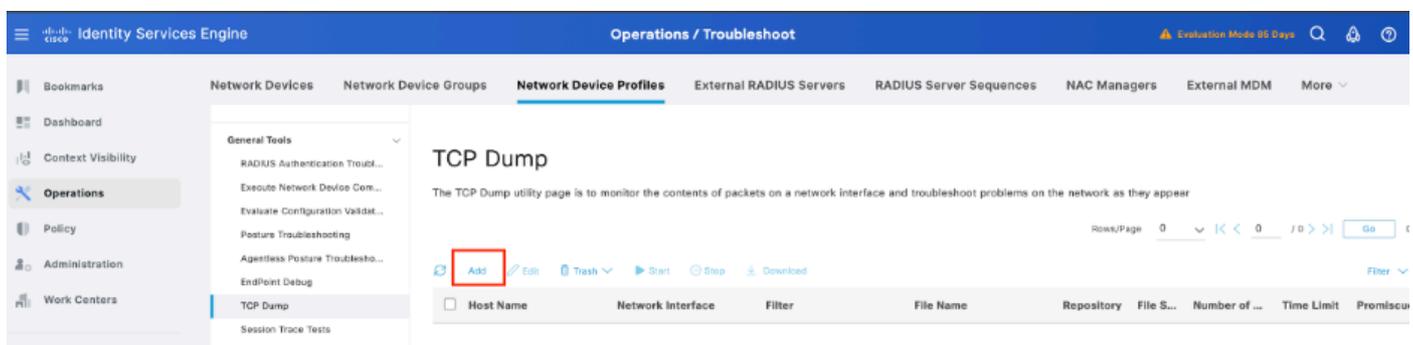
Dependiendo del motivo del fallo, puede ajustar la configuración o abordar la causa del fallo.



The screenshot shows the 'Live Logs' section of the Identity Services Engine. A table lists several authentication failures. The first row is highlighted with a red box around the 'Details' column, which contains a lock icon. The table columns include Logged Time, Status, Details, Identity, Type, Authentication Policy, Authorization Policy, Ise Node, Network Device, and Network Device ID.

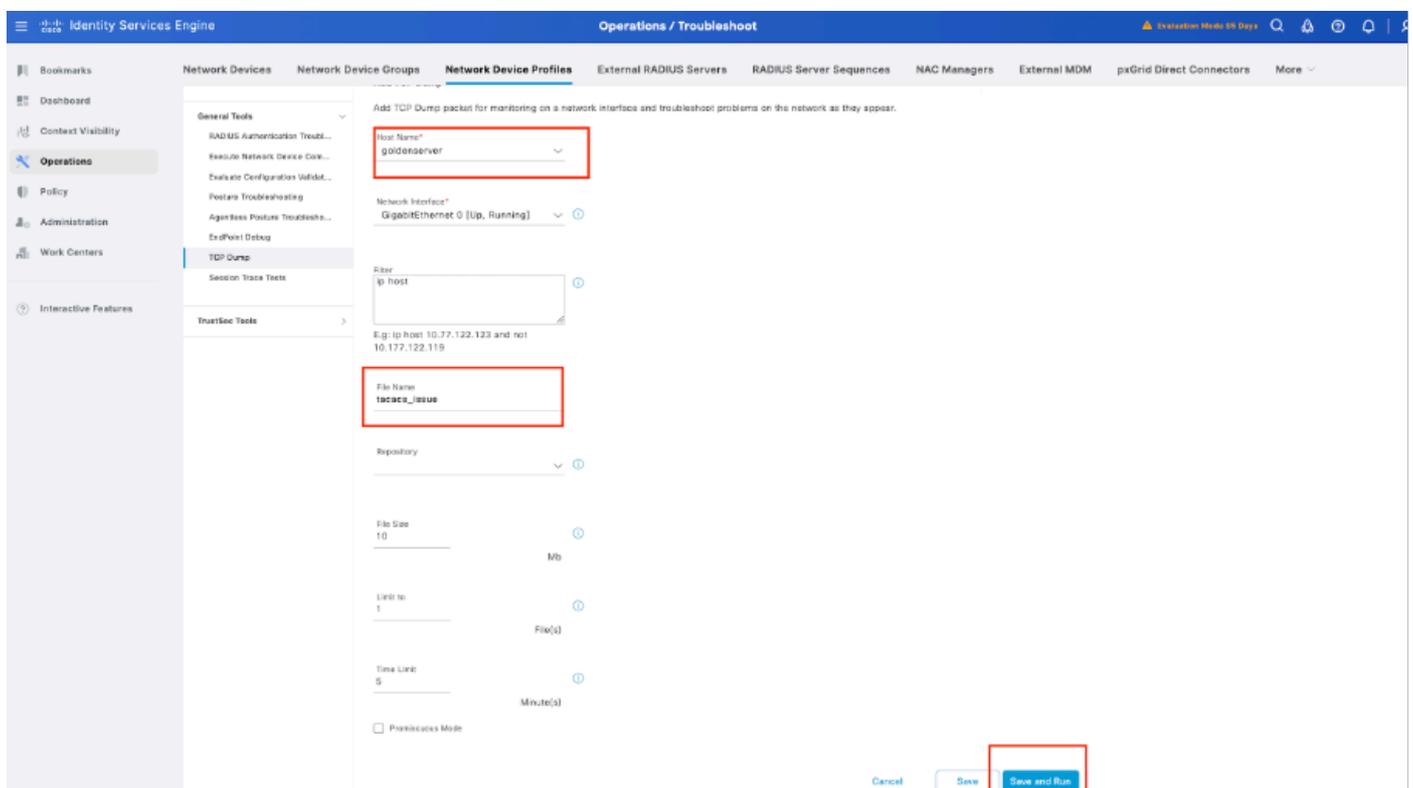
Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Device	Network Device ID
Mar 19, 2025 03:32:40.4...	Auth Fail	⛔	INVALID	Authentic...	Arista Switch Access >> Default	Authorization Policy	goldenserver	Arista_switch	
Mar 19, 2025 02:24:52.3...	Auth Fail	⛔	diviya	Authentic...	Arista Switch Access >> Default		goldenserver	Arista_switch	
Mar 19, 2025 02:24:34.4...	Auth Fail	⛔	INVALID	Authentic...	Arista Switch Access >> Default		goldenserver	Arista_switch	
Mar 19, 2025 02:22:0...	Auth Fail	⛔	INVALID	Authentic...	Arista Switch Access >> Default		goldenserver	Arista_switch	

Paso 3. En caso de que no vea ningún livelog, proceda a realizar una captura de paquetes. Vaya al menú Operaciones > Troubleshooting > Herramientas de diagnóstico > Herramientas generales > TCP Dump , seleccione Add:



The screenshot shows the 'TCP Dump' configuration page in the Identity Services Engine. The 'Add' button is highlighted with a red box. Below the button is a table with columns: Host Name, Network Interface, Filter, File Name, Repository, File Size, Number of Files, Time Limit, and Promiscuous Mode.

Host Name	Network Interface	Filter	File Name	Repository	File Size	Number of Files	Time Limit	Promiscuous Mode
-----------	-------------------	--------	-----------	------------	-----------	-----------------	------------	------------------



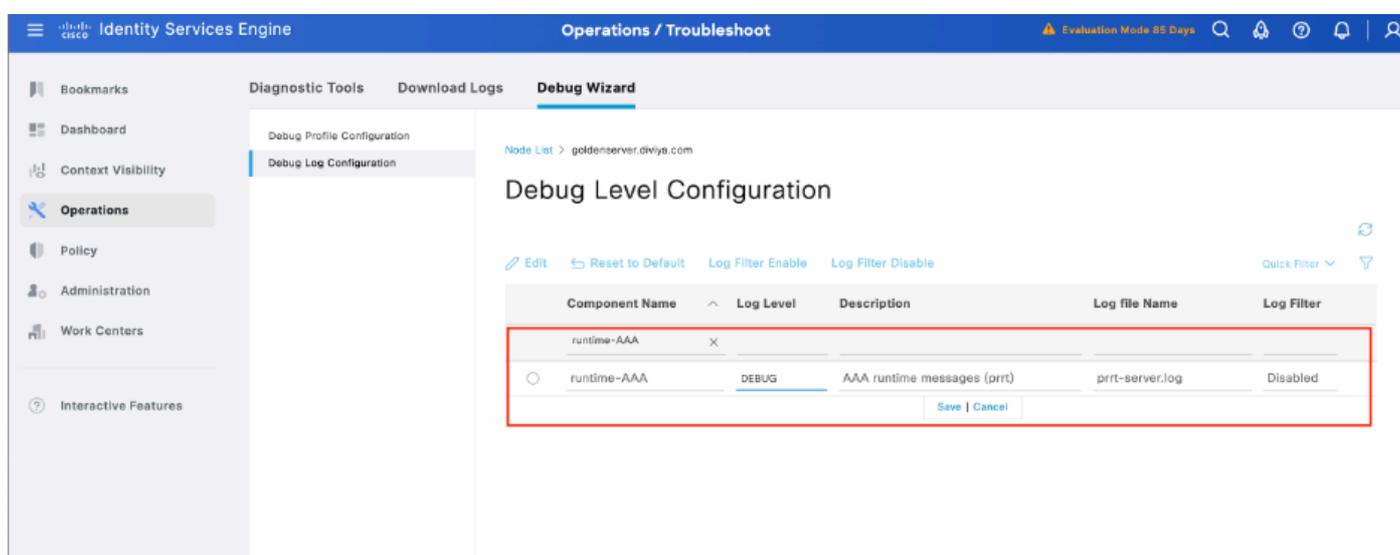
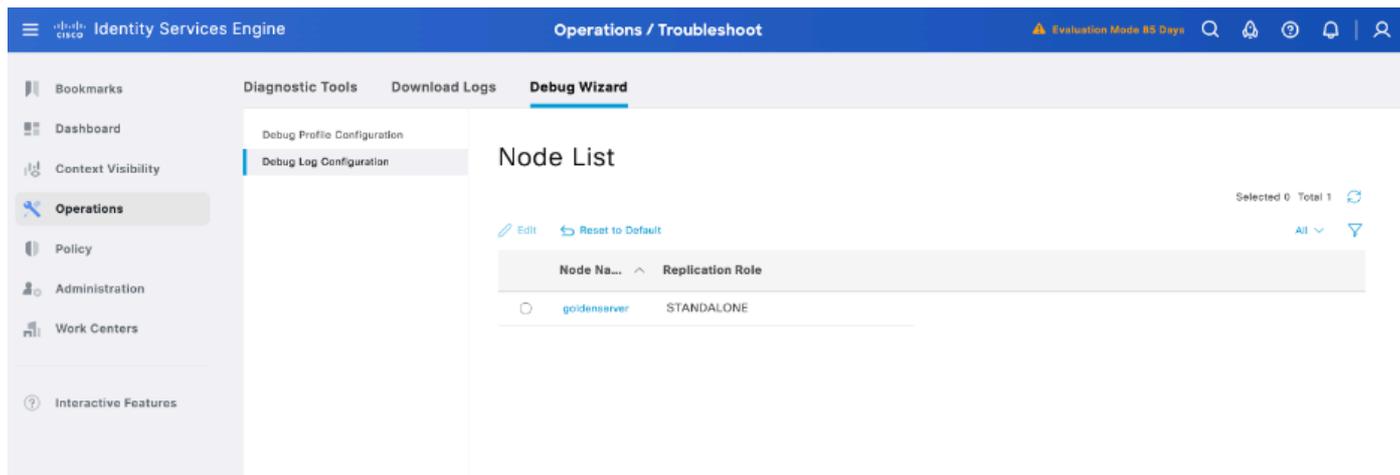
The screenshot shows the 'Add TCP Dump packet' configuration form. The 'Host Name' dropdown is set to 'goldenserver', the 'Network Interface' is 'GigabitEthernet 0 (Up, Running)', and the 'File Name' is 'tacacs_issue'. The 'Save and Run' button is highlighted with a red box.

Host Name: goldenserver
Network Interface: GigabitEthernet 0 (Up, Running)
Filter: ip host
File Name: tacacs_issue
Repository: [Dropdown]
File Size: 10 Mb
Limit to: 1 File(s)
Time Limit: 5 Minute(s)
Promiscuous Mode: [Unchecked]

Buttons: Cancel, Save, Save and Run

Paso 4. Habilite el componente Runtime-AAA en debug dentro de PSN desde donde se realiza la autenticación en Operaciones > Troubleshooting > Debug Wizard > Debug log configuration,

seleccione PSN node, luego seleccione el botón Edit:



Identifique el componente runtime-AAA, establezca su nivel de registro en debug, reproduzca el problema y analice los registros para una investigación adicional.

Resolución de problemas

Problema 1

La autenticación TACACS+ entre Cisco ISE y el switch Arista (o cualquier dispositivo de red) falla con el mensaje de error:

"13036 El perfil de shell seleccionado es DenyAccess"

Overview		Steps	
Request Type	Authentication	13013	Received TACACS+ Authentication START Request
Status	Fail	15049	Evaluating Policy Group (🕒 Step latency=1ms)
Session Key	goldenserver/541265148/80	15008	Evaluating Service Selection Policy (🕒 Step latency=0ms)
Message Text	Failed-Attempt: Authentication failed	15048	Queried PIP - DEVICE.Device Type (🕒 Step latency=2ms)
Username	diviya	15041	Evaluating Identity Policy (🕒 Step latency=3ms)
Authentication Policy	Arista SW_TACACS >> Arista SW_TACACS Auth	15048	Queried PIP - Network Access.Protocol (🕒 Step latency=2ms)
Selected Authorization Profile	Deny All Shell Profile	15013	Selected Identity Source - Internal Users (🕒 Step latency=2ms)
		24210	Looking up User in Internal Users IDStore (🕒 Step latency=0ms)
		24212	Found User in Internal Users IDStore (🕒 Step latency=37ms)
		13045	TACACS+ will use the password prompt from global TACACS+ configuration (🕒 Step latency=0ms)
		13015	Returned TACACS+ Authentication Reply (🕒 Step latency=0ms)
		13014	Received TACACS+ Authentication CONTINUE Request (🕒 Step latency=68ms)
		15041	Evaluating Identity Policy (🕒 Step latency=0ms)
		15013	Selected Identity Source - Internal Users (🕒 Step latency=4ms)
		24210	Looking up User in Internal Users IDStore (🕒 Step latency=0ms)
		24212	Found User in Internal Users IDStore (🕒 Step latency=7ms)
		22037	Authentication Passed (🕒 Step latency=0ms)
		15036	Evaluating Authorization Policy (🕒 Step latency=0ms)
		15048	Queried PIP - Network Access.UserName (🕒 Step latency=4ms)

Authentication Details	
Generated Time	2025-07-27 16:06:30.094000 +05:30
Logged Time	2025-07-27 16:06:30.094
Epoch Time (sec)	1753612590
ISE Node	goldenserver
Message Text	Failed-Attempt: Authentication failed
Failure Reason	13036 Selected Shell Profile is DenyAccess
Resolution	Check whether the Device Administration Authorization Policy rules are correct
Root Cause	Selected Shell Profile fails for this request
Username	diviya

El error "13036 Selected Shell Profile is DenyAccess" en Cisco ISE normalmente significa que durante un intento de administración de un dispositivo TACACS+, la política de autorización coincidió con un perfil de shell establecido en DenyAccess. Esto no suele ser el resultado de un perfil de shell mal configurado, sino que indica que ninguna de las reglas de autorización configuradas coincidió con los atributos de usuario entrante (como la pertenencia a grupos, el tipo de dispositivo o la ubicación). Como resultado, ISE recurre a una regla predeterminada o a una regla de denegación explícita, lo que provoca la denegación del acceso.

Posibles Causas

- Revise las reglas de la política de autorización en ISE. Confirme que el usuario o dispositivo coincide con la regla correcta que asigna el perfil de shell deseado, como una que permite el acceso adecuado.
- Asegúrese de que la asignación de grupos de usuarios internos o AD sea correcta y de que las condiciones de la directiva, como la pertenencia a grupos de usuarios, el tipo de dispositivo y el protocolo, se especifiquen correctamente.
- Utilice los registros en directo de ISE y los detalles del intento fallido para ver exactamente qué regla coincide y por qué.

Problema 2

La autenticación TACACS+ entre Cisco ISE y el switch Arista (o cualquier dispositivo de red) falla con el mensaje de error:

"13017 paquetes TACACS+ recibidos desde un dispositivo de red o cliente AAA desconocido"

The screenshot displays the Cisco ISE interface with a blue header. It is divided into two main sections: 'Overview' and 'Authentication Details'. The 'Overview' section shows a failed authentication attempt with a status of 'Fail' and a message text of 'Failed-Attempt: TACACS+ Request dropped'. The 'Authentication Details' section provides a timestamp of 2025-07-27 17:50:17.705, identifies the ISE node as 'goldenserver', and lists the failure reason as '13017 Received TACACS+ packet from unknown Network Device or AAA Client'. A 'Steps' section on the right shows a single step with the same failure reason.

Overview	
Request Type	Authentication
Status	Fail
Session Key	
Message Text	Failed-Attempt: TACACS+ Request dropped
Username	
Authentication Policy	
Selected Authorization Profile	

Authentication Details	
Generated Time	2025-07-27 17:50:17.705000 +05:30
Logged Time	2025-07-27 17:50:17.705
Epoch Time (sec)	1753618817
ISE Node	goldenserver
Message Text	Failed-Attempt: TACACS+ Request dropped
Failure Reason	13017 Received TACACS+ packet from unknown Network Device or AAA Client
Resolution	
Root Cause	
Username	

Steps	
13017	Received TACACS+ packet from unknown Network Device or AAA Client

Posibles Causas

- El motivo más común es que la dirección IP del switch no se agrega como dispositivo de red en ISE (en Administración > Recursos de red > Dispositivos de red).
- Asegúrese de que la dirección IP o el rango coincidan exactamente con la IP de origen que está utilizando el switch Arista para enviar paquetes TACACS+.
- Si el switch utiliza una interfaz de gestión, verifique que su IP exacta (no solo una subred/rango) se agregue en ISE.

Solución

- Vaya a Administración > Recursos de red > Dispositivos de red en la GUI de ISE.
- Verifique si la dirección IP de origen exacta en el switch de Arista está utilizando para la comunicación TACACS+ (generalmente la IP de la interfaz de administración).
- Especifique el secreto compartido (debe coincidir con el establecido en el conmutador Arista).

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).