Configuración de TACACS de autenticación externa de Catalyst Center con ISE

Contenido

Introducción

Este documento describe los pasos necesarios para integrar Cisco Identity Services Engine con Catalyst Center para habilitar la autenticación TACACS+.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Acceso de administrador a Cisco ISE y Cisco Catalyst Center.
- Comprensión básica de los conceptos de AAA (autenticación, autorización y contabilidad).
- Conocimientos prácticos del protocolo TACACS+.
- Conectividad de red entre Catalyst Center y el servidor ISE.

Componentes Utilizados

La información de este documento se basa en las siguientes versiones de hardware y software:

- Cisco Catalyst Center versión 2.3.7.x
- Cisco Identity Services Engine (ISE) versión 3.x (o posterior)
- Protocolo TACACS+ para la autenticación de usuarios externos

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.

Antecedentes

Esta integración permite a los usuarios externos iniciar sesión en Catalyst Center para el acceso administrativo y la gestión.

Configurar

Cisco Identity Services Engine (ISE)

Licencia y habilitación de los servicios TACACS+

Antes de comenzar con la configuración de TACACS+ en ISE, debe confirmar que se ha instalado la licencia correcta y que la función está activada.

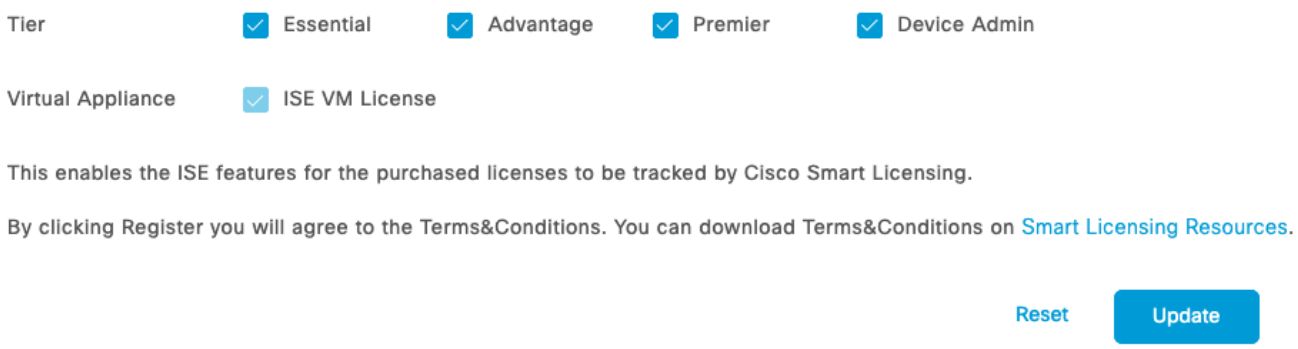
1. Verifique que tiene la licencia PID L-ISE-TACACS-ND= en el portal Cisco Smart Software Manager o Cisco License Central.

Habilite Device Administration en el portal de licencias de ISE.

- La licencia Device Admin (PID: L-ISE-TACACS-ND=) habilita los servicios TACACS+ en un nodo de servicios de políticas (PSN).
- Navegue hasta:

  Administration > System > Licensing

- Marque la casilla Device Admin en las opciones de nivel.



Administrador de dispositivos

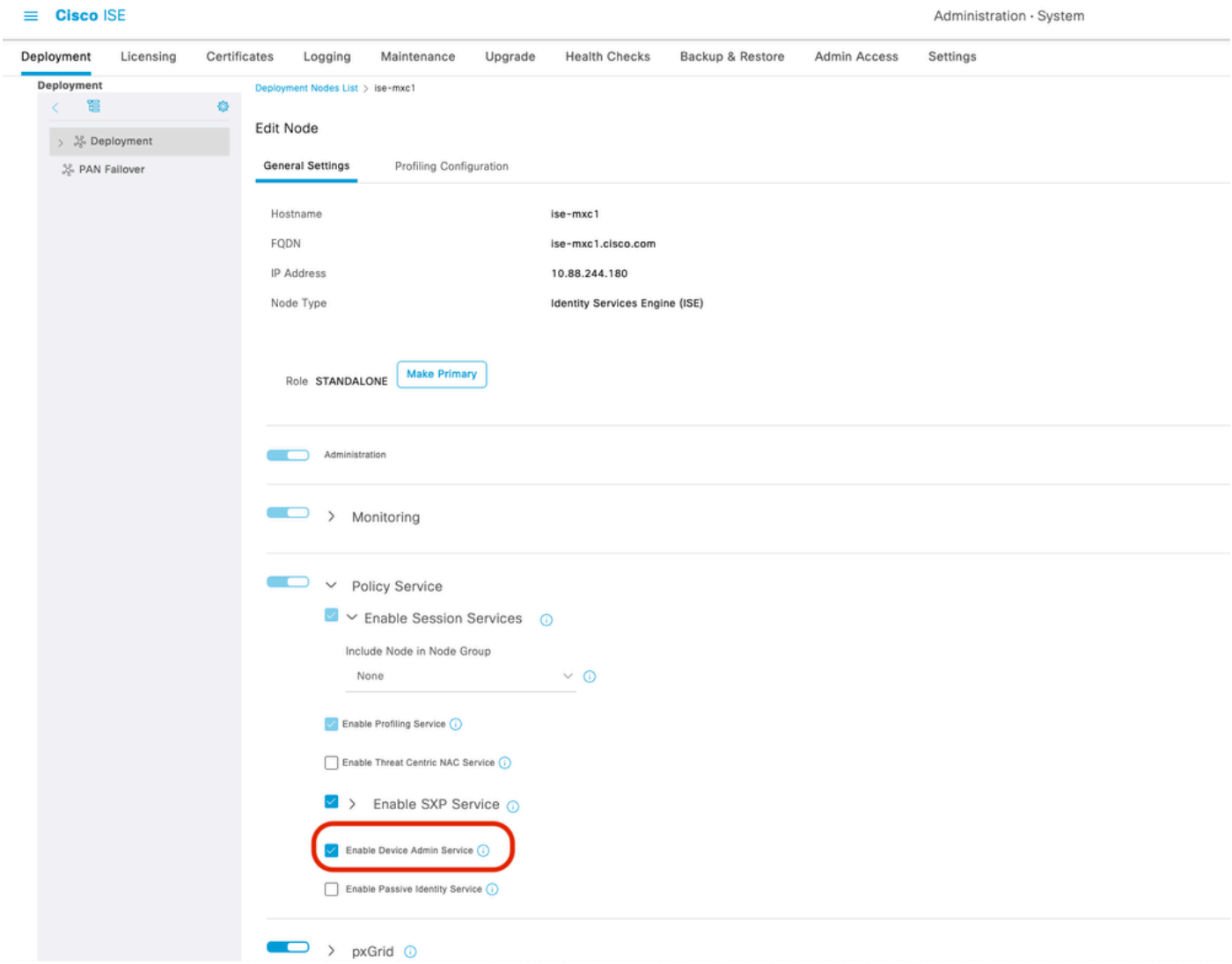
Licencia Device Admin

3. Habilite el Device Admin Service en el nodo ISE que ejecuta el servicio TACACS+.

- Navegue hasta:

  Administration > System > Deployment > Select the node

- Marque la opción Enable Device Admin Service.



Habilitar servicio de administración de dispositivos

Crear usuario administrador y agregar dispositivo de red

1. Cree el usuario administrador.

- Esta cuenta de usuario se utiliza para iniciar sesión en la interfaz de usuario de Catalyst Center a través de la autenticación de ISE.
- Navegue hasta:

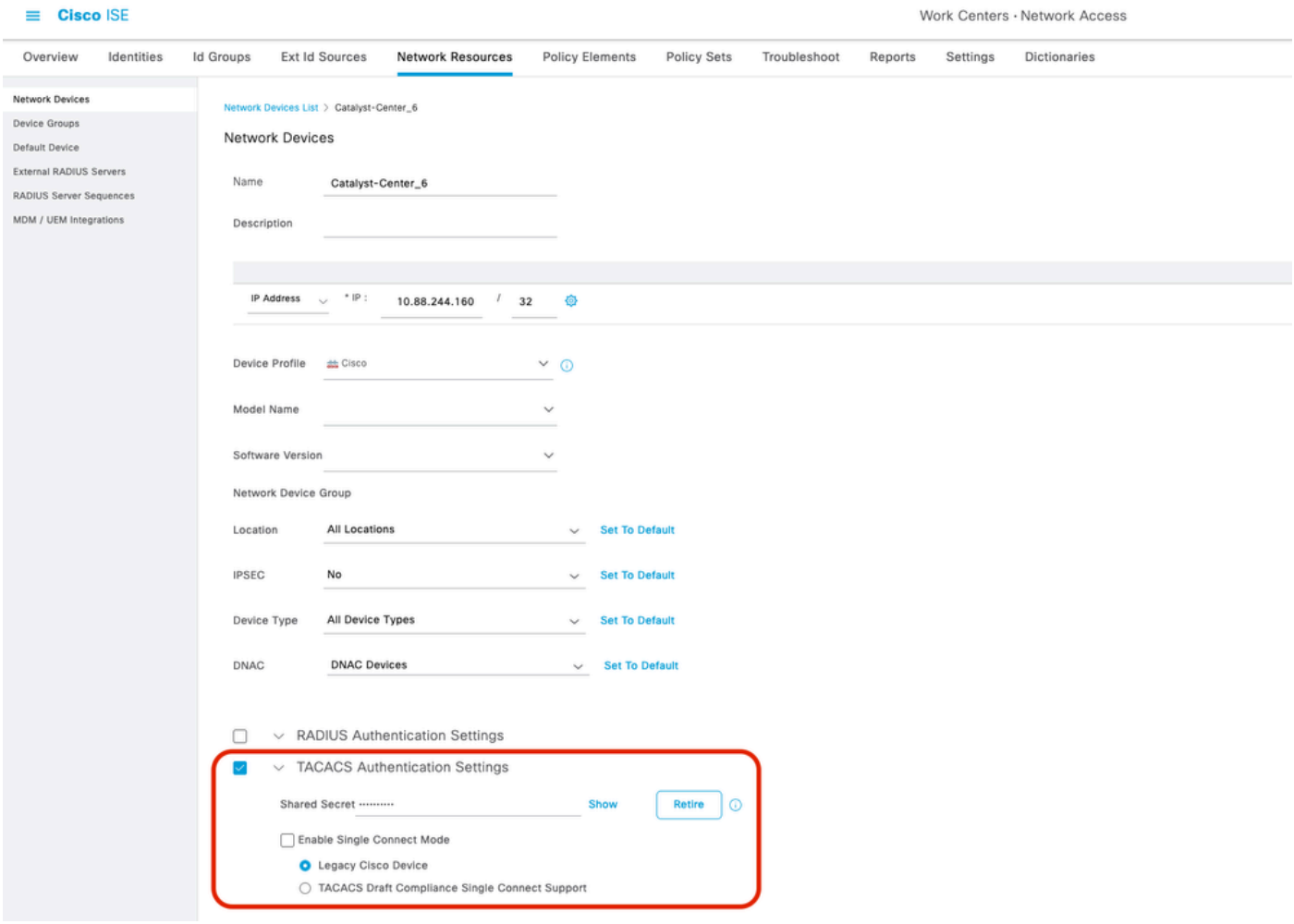
  Centros de trabajo > Acceso de red > Identidades > Usuario de acceso de red
- Agregue un nuevo usuario (por ejemplo, catc-user).
- Si el usuario ya existe, continúe con el siguiente paso.

2. Cree el dispositivo de red.

- Navegue hasta:

  Centros de trabajo > Acceso a la red > Identidades > Recurso de red

- Agregue la dirección IP de Catalyst Center o defina la subred donde se encuentra la dirección IP de Catalyst Center.
- Si el dispositivo ya existe, verifique que contenga los parámetros:
  - Los ajustes de autenticación de TACACS están habilitados.
  - El secreto compartido está configurado y es conocido (guarde este valor, ya que se requiere más adelante en el Centro de Catalyst).



Configuración de autenticación TACACS

Configurar perfil TACACS+

1. Cree un nuevo perfil TACACS+.

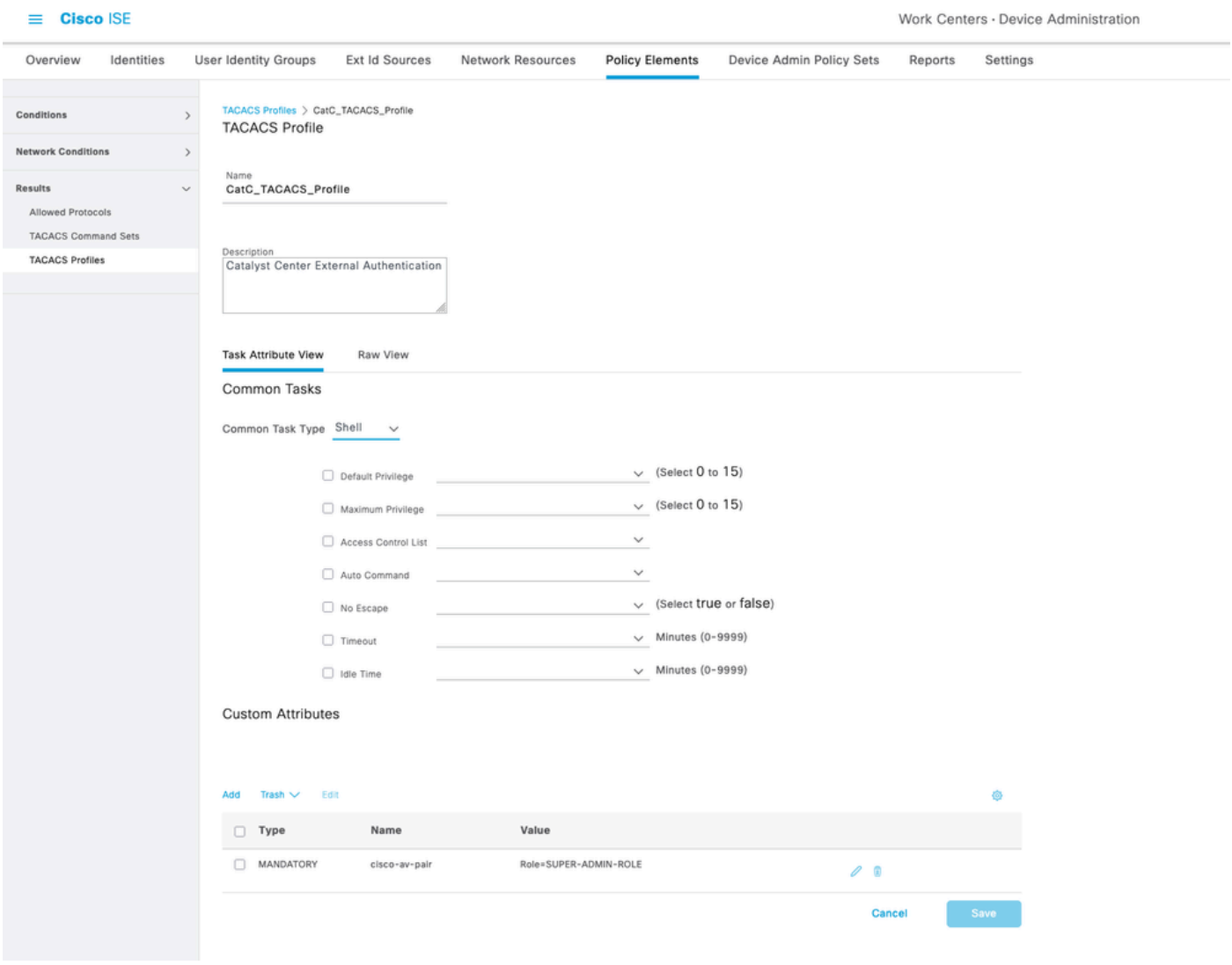
- Navegue hasta:

Centros de trabajo > Administración de dispositivos > Elementos de política > Resultados > Perfiles TACACS

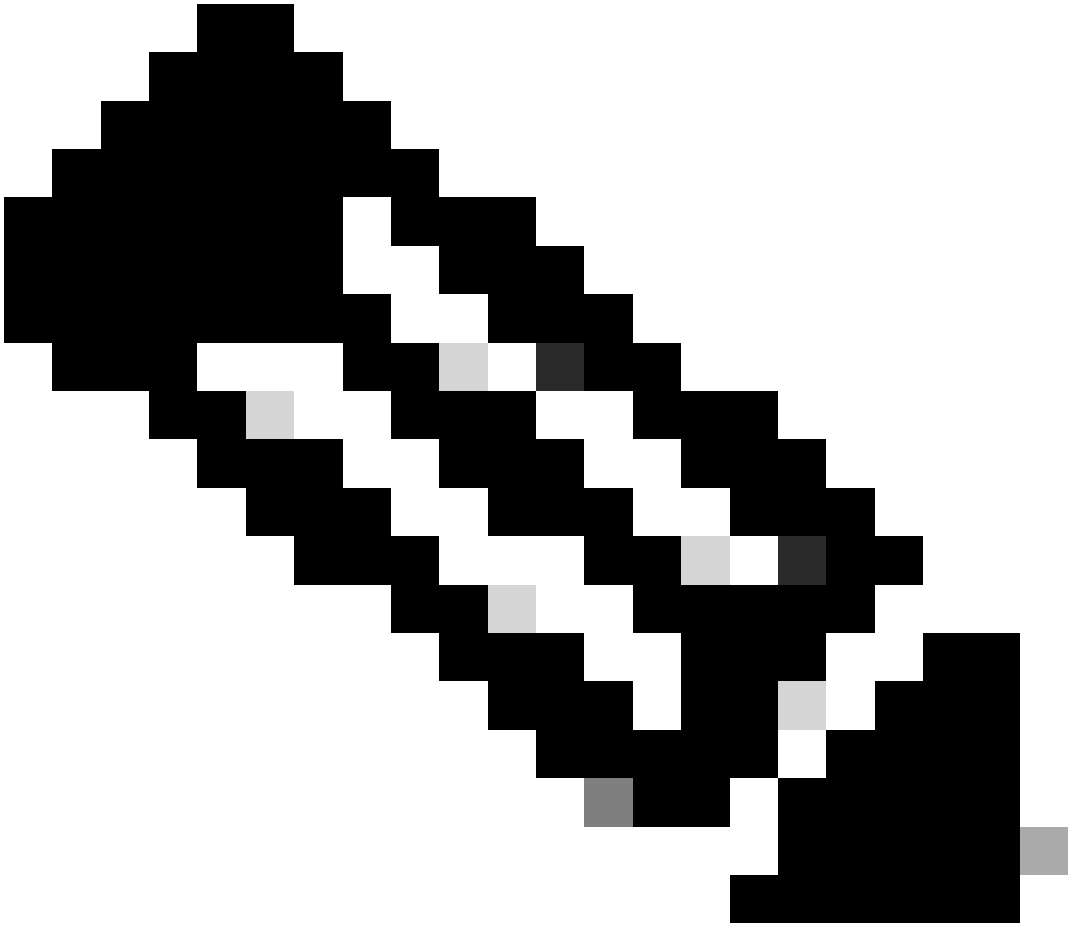
- Agregue un nombre de perfil.
- Agregue un atributo personalizado de la siguiente manera:

- Tipo: Obligatoria
- Nombre: cisco-av-pair
- Valor: Role=SUPER-ADMIN-ROLE

- Guarde el perfil.



Perfil de TACACS+



Nota: Cisco Catalyst Center admite servidores externos de autenticación, autorización y contabilidad (AAA) para el control de acceso. Si utiliza un servidor externo para la autenticación y autorización de usuarios externos, puede activar la autenticación externa en Cisco Catalyst Center. La configuración del atributo AAA predeterminado coincide con el atributo del perfil de usuario predeterminado.

El valor de atributo AAA predeterminado del protocolo TACACS es cisco-av-pair.

El valor de atributo AAA predeterminado del protocolo RADIUS es Cisco-AVPair.

El cambio solo es necesario si el servidor AAA tiene un atributo personalizado en el perfil de usuario. En el servidor AAA, el formato del valor del atributo AAA es Role=role1. En el servidor de Cisco Identity Services Engine (Cisco ISE), al configurar el perfil RADIUS o TACACS, el usuario puede seleccionar o introducir cisco av-pair como atributo AAA.

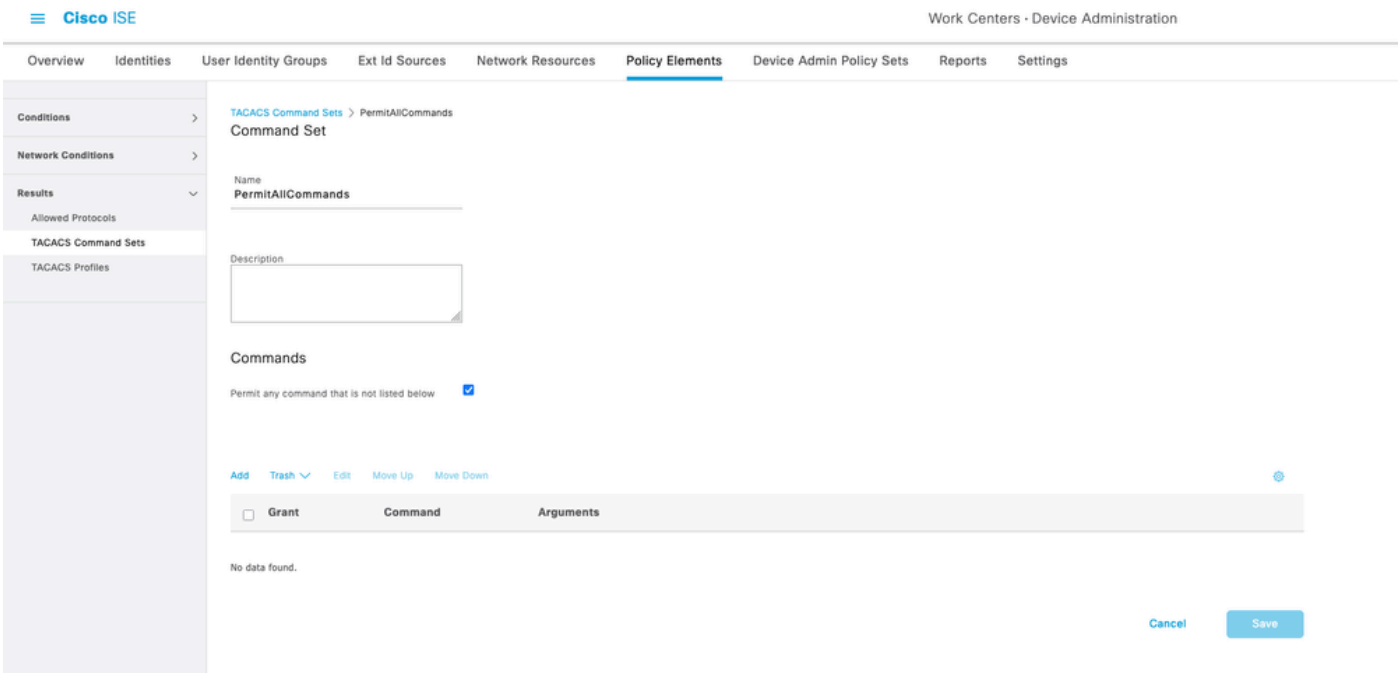
Por ejemplo, puede seleccionar y configurar manualmente el atributo AAA como cisco-av-pair=Role=SUPER-ADMIN-ROLE o Cisco-AVPair=Role=SUPER-ADMIN-ROLE.

2. Cree un conjunto de comandos TACACS+.

- Navegue hasta:

Centros de trabajo > Administración de dispositivos > Elementos de política > Resultados > Conjuntos de comandos TACACS

- Agregue un nombre.
- Marque la opción Permit any command that is not listed below.
- Guarde el conjunto de comandos.



Conjuntos de comandos TACACS

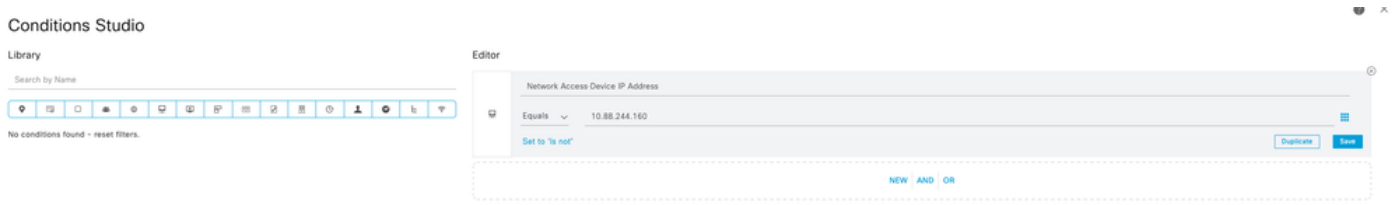
Configuración de políticas TACACS+

1. Cree un nuevo conjunto de políticas TACACS+.

- Navegue hasta:

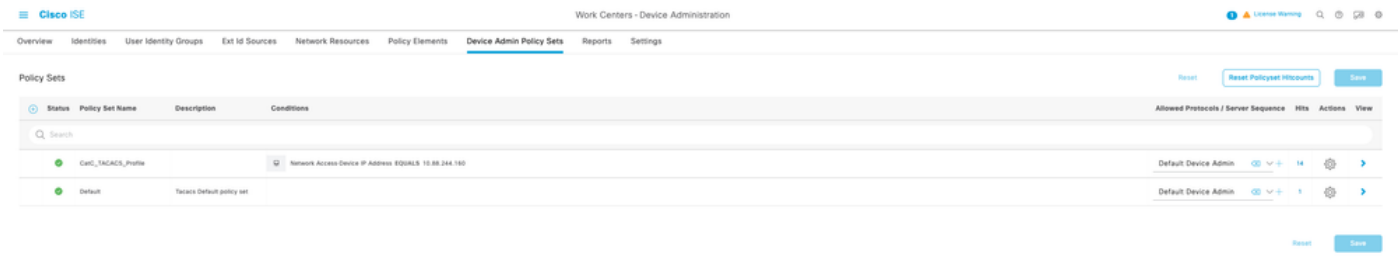
Centros de trabajo > Administración de dispositivos > Conjunto de políticas de administración de dispositivos

- Agregue un nombre para el conjunto de políticas.
- Configure la condición.
    - En este ejemplo, la condición coincide con la dirección IP de Catalyst Center.



Dirección IP de Catalyst Center

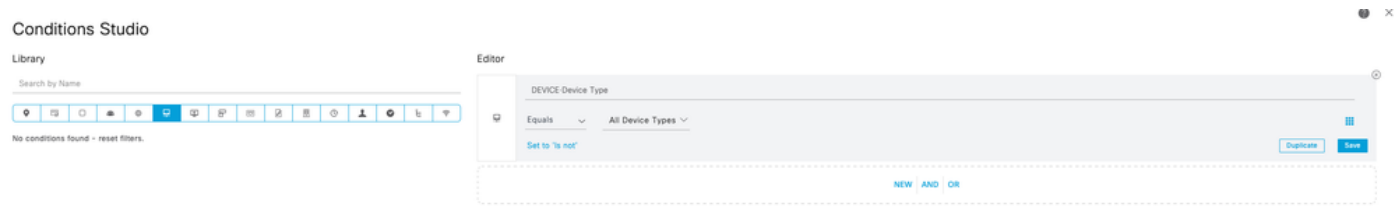
1.3 En Allowed Protocols / Server Sequence (Protocolos permitidos / Secuencia de servidor), seleccione Default Device Admin (Administrador de dispositivos predeterminado).



Seleccionar administrador de dispositivos predeterminado

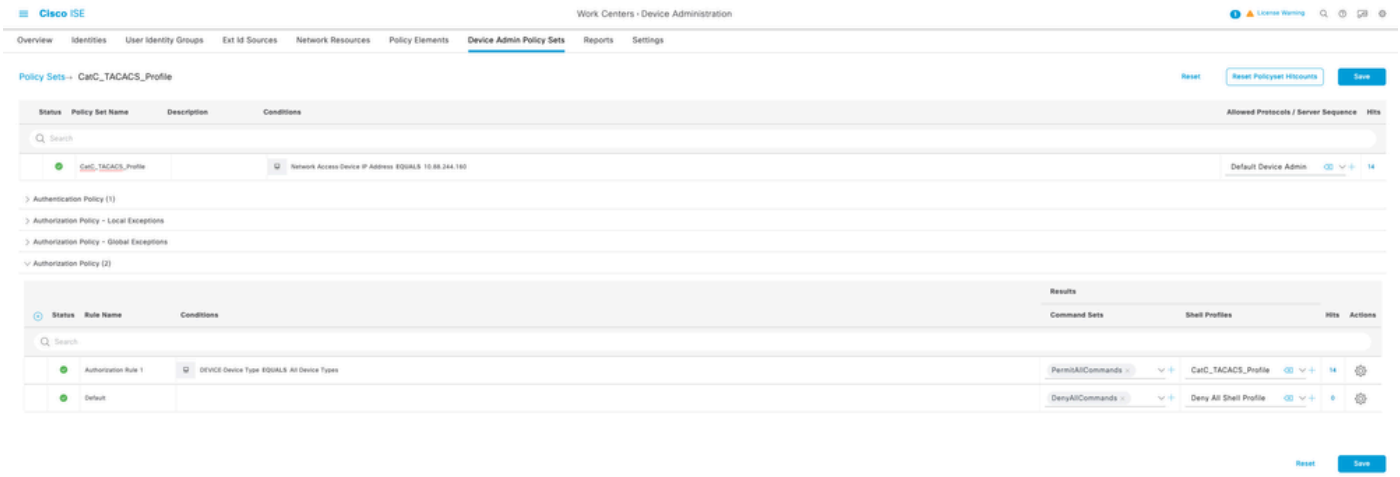
2. Configure el conjunto de políticas.

- Haga clic en la flecha (>) de la derecha para expandir y configurar el conjunto de políticas.
- Agregue una nueva regla en Directiva de autorización.
- Configure la nueva regla de la siguiente manera:
  - Nombre: Introduzca un nombre de regla descriptivo.
  - Condición: En este ejemplo, la condición coincide con Todos los tipos de dispositivos.



Todos los tipos de dispositivos

- Conjunto de comandos: Seleccione el conjunto de comandos TACACS+creado anteriormente.
- Perfil de shell: Seleccione el perfil TACACS+ creado anteriormente.



Conjunto de comandos TACACS+

Cisco Catalyst Center

Configuración del servidor ISE/AAA

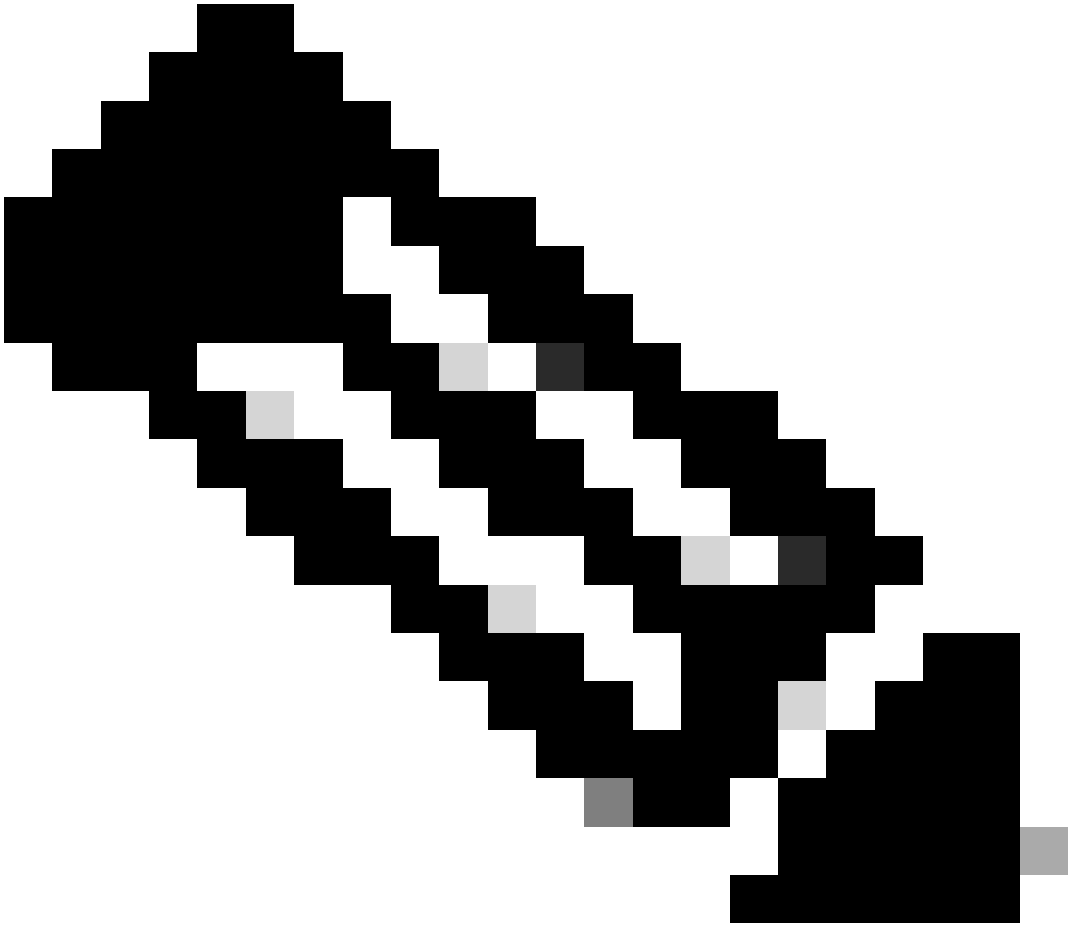
1. Inicie sesión en la interfaz web de Catalyst Center.

- Navegue hasta:

Main menu > System > Settings > External Services > Authentication and Policy Servers

2. Agregue un nuevo servidor. Puede seleccionar ISE o AAA.

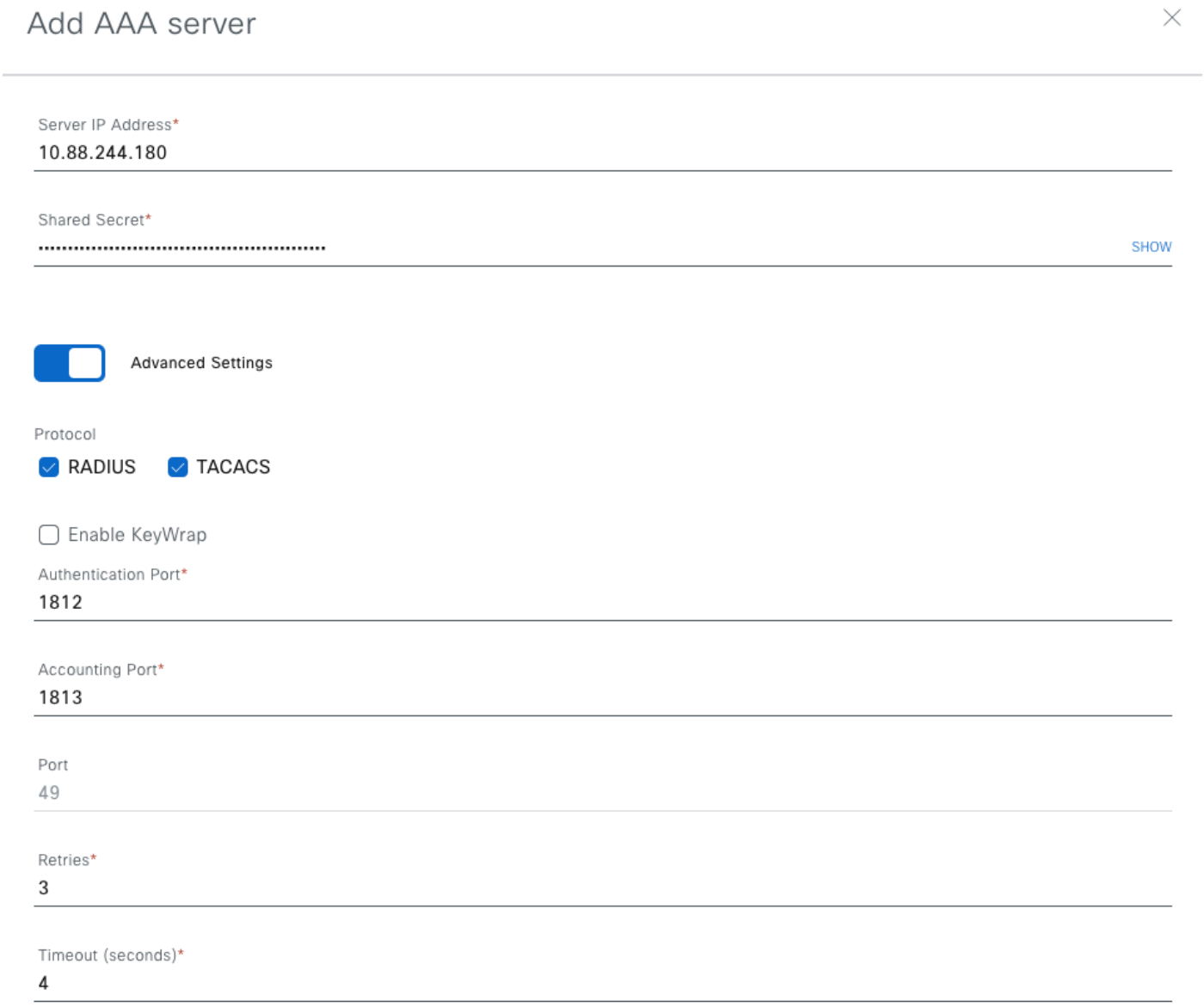
- Para esta demostración, se utiliza la opción de servidor AAA.



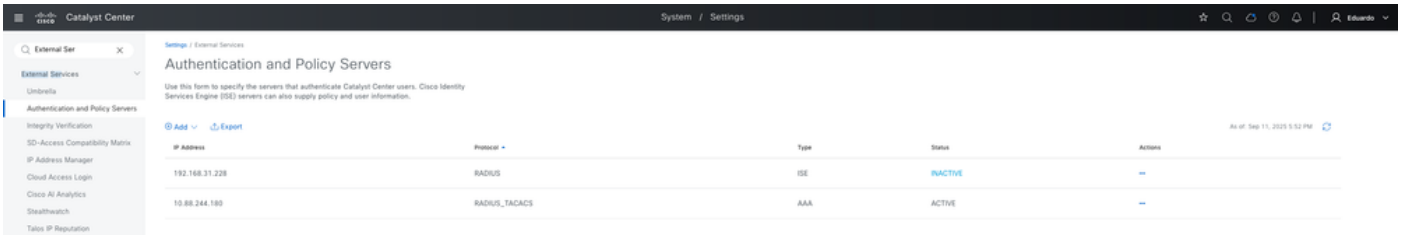
Nota: Un clúster de Catalyst Center solo puede tener configurado un clúster de ISE.

3. Configure estas opciones y, a continuación, guarde:

- Introduzca la dirección IP del servidor AAA.
- Agregue el secreto compartido (el mismo secreto configurado en el recurso de red de Cisco ISE).
- Cambie Advanced Settings a On.
- Marque la opción TACACS.



Servidores de autenticación y políticas



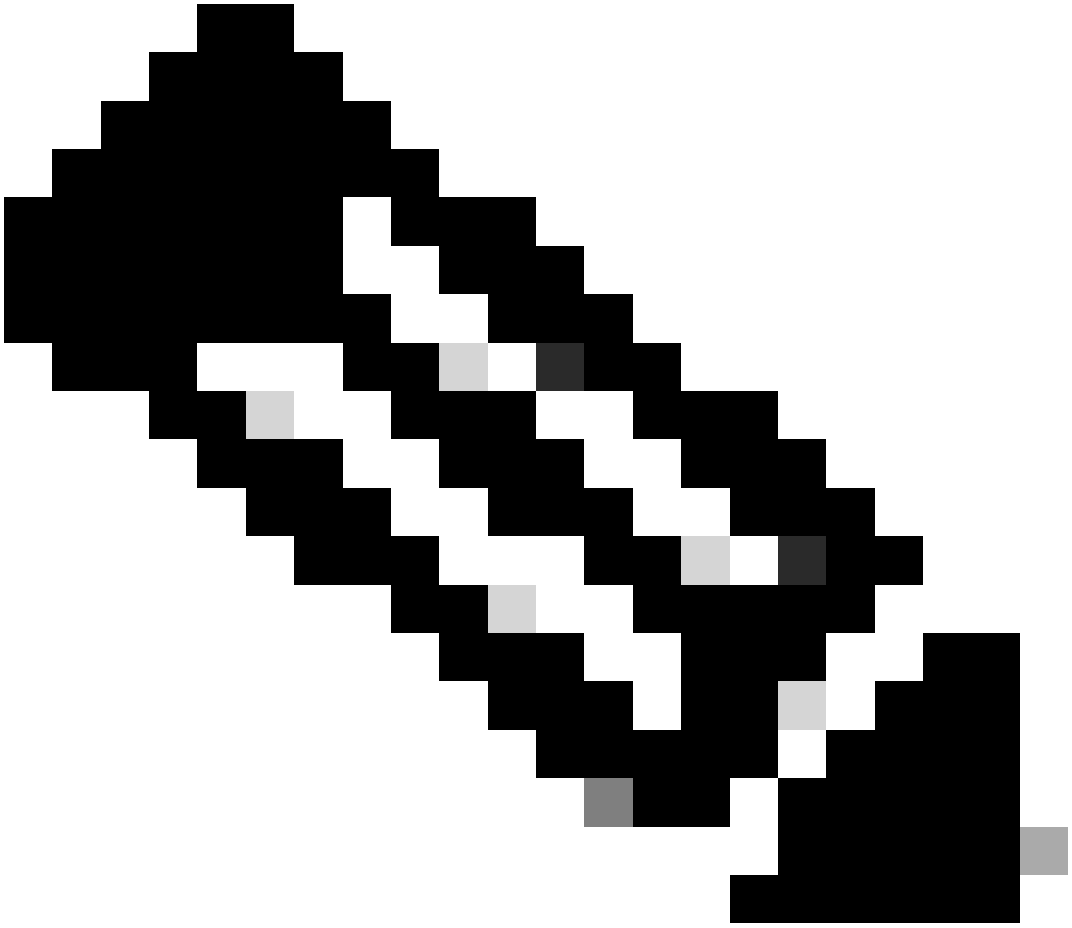
Configuración avanzada

Habilite y configure la autenticación externa.

1. Acceda a la página Autenticación Externa:

   Menú principal > Sistema > Usuario y rol > Autenticación externa

2. Agregue el atributo AAA cisco-av-pair y haga clic en Update para guardar los cambios.



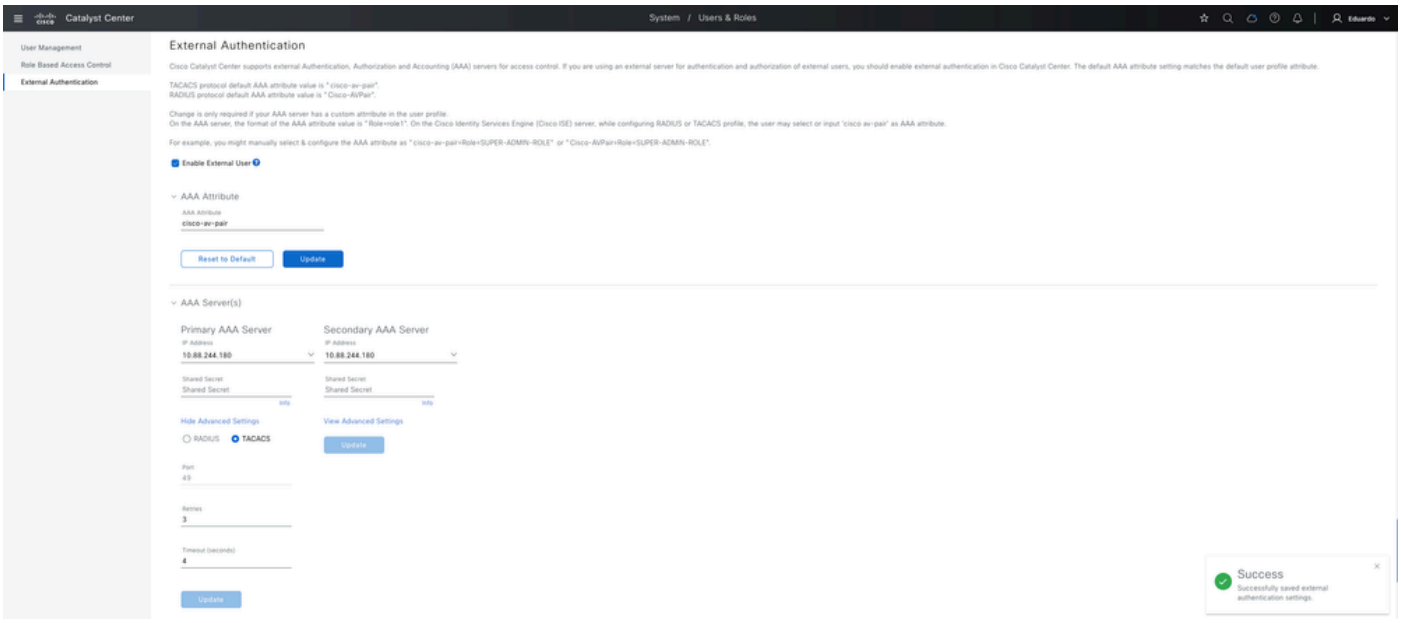
Nota: Este paso no es obligatorio ya que el atributo predeterminado para TACACS+ ya es cisco-av-pair, pero se considera una práctica recomendada configurarlo explícitamente.

3. En Primary AAA Server, seleccione el servidor AAA configurado anteriormente.

- Haga clic en View Advanced Settings para mostrar opciones adicionales.
- Seleccione la opción TACACS+.
- Introduzca el secreto compartido configurado en el recurso de red de Cisco ISE.
- Haga clic en Update para guardar los cambios.

4. Active la casilla de verificación Usuario externo.

- Esta acción guarda automáticamente la configuración.



Autenticación externa

Verificación

1. Abra una nueva sesión del navegador o utilice Incognito Mode e inicie sesión en la página web de Catalyst Center con la cuenta de usuario configurada en Cisco ISE.

2. En Catalyst Center, confirme que el inicio de sesión se haya realizado correctamente.

Inicio de sesión Configuración de TACACS de autenticación externa de Catalyst Center con ISE

3. En Cisco ISE, valide los registros:

   Operations > TACACS > Live Logs

- Estado de autenticación: Pass
- Estado de autorización: Pass

Registros en directo

4. En Detalles de autorización, compárelo con el siguiente resultado:

    - Texto del mensaje: Device-Administration: Autorización de sesión correcta
    - Todos los atributos de respuesta: cisco-av-pair=Role=SUPER-ADMIN-ROLE

Authorization Details

Generated Time	2025-09-12 00:12:20.801 +0:00
Logged Time	2025-09-12 00:12:20.801
Epoch Time (sec)	1757635940
ISE Node	ise-mxc1
Message Text	Device-Administration: Session Authorization succeeded
Failure Reason	
Resolution	
Root Cause	
Username	catc-user
Network Device Name	Catalyst-Center_6
Network Device IP	10.88.244.160
Network Device Groups	IPSEC#Is IPSEC Device#No,DNAC#DNAC Devices,Location#All Locations,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	console
Remote Address	10.189.17.203

Authorization Attributes

All Request Attribues	
All Response Attribues	cisco-av-pair=Role=SUPER-ADMIN-ROLE

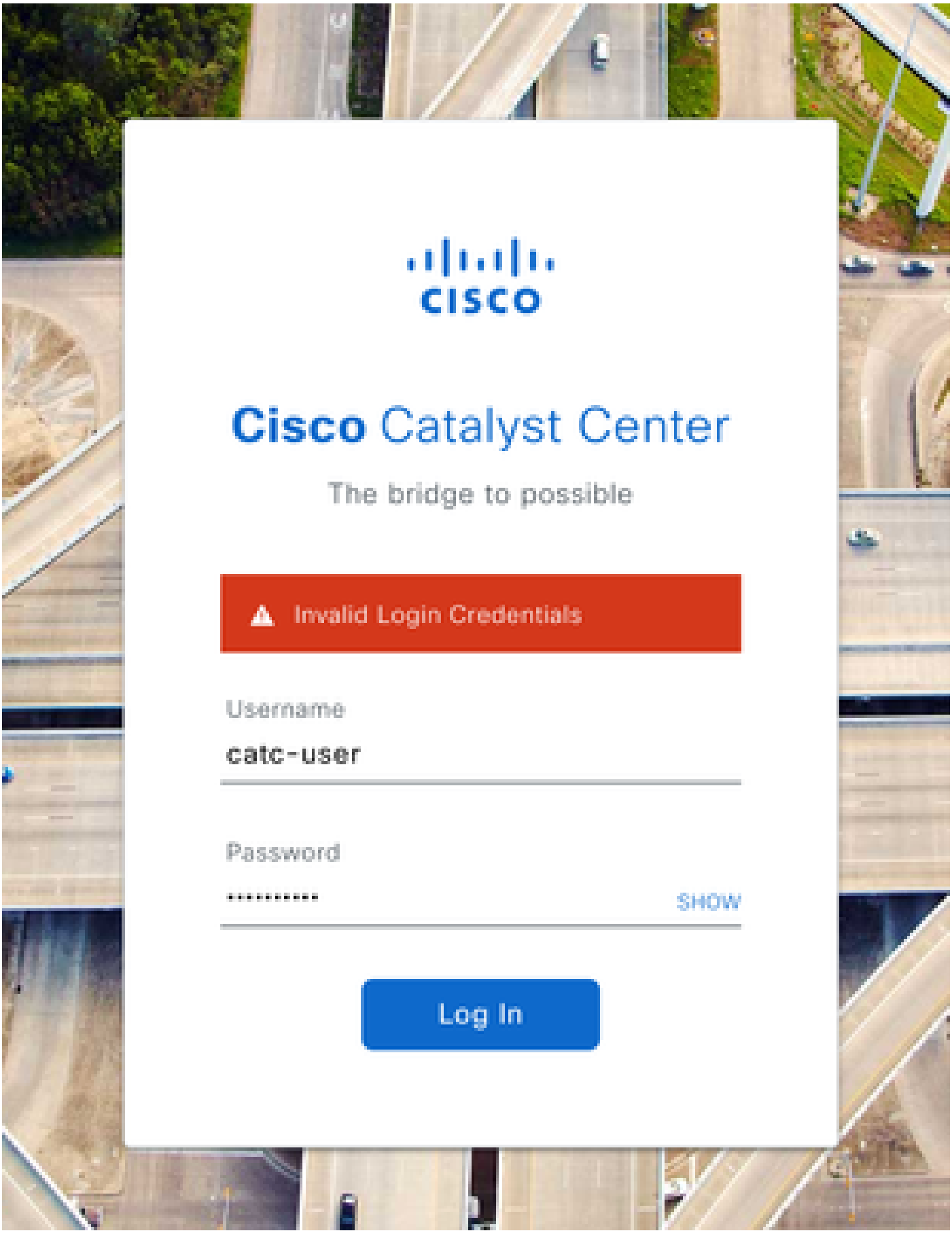
cisco-av-pair=Role=SUPER-ADMIN-ROLE

Troubleshoot

A continuación se indican algunos problemas comunes que puede encontrar durante la integración y cómo identificarlos:

1. Error de configuración de atributos

Síntoma en Catalyst Center: credenciales de inicio de sesión no válidas



Error de configuración de atributos

- Síntoma en Cisco ISE (registros TACACS):

- Autenticación: Pass
- Autorización: Pass

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Device...	Network Device...	Device Type	Location	Device Port	Failure Reason	Remote Address	Matched Comm...	Shell Profile
Sep 12, 2025 12:12:20.801...	✓		catc-user	Authorization		CatC_TACACS_Profile >> Authoriz...	ise-mac1	Catalyst-Center_6	10.88.244.160	Device Type#All D...	Location#All Locati...	console		10.189.17.203		CatC_TACACS_Pr...
Sep 12, 2025 12:12:20.788...	✓		catc-user	Authentication	CatC_TACACS_Profile >> Default		ise-mac1	Catalyst-Center_6	10.88.244.160	Device Type#All D...	Location#All Locati...	console		10.189.17.203		

Error de configuración de atributos

- Posibles Causas:
  - Existe un espacio en el valor del atributo.

Ejemplo:

Authorization Details

Generated Time	2025-09-12 00:12:20.801 +0:00
Logged Time	2025-09-12 00:12:20.801
Epoch Time (sec)	1757635940
ISE Node	ise-mxc1
Message Text	Device-Administration: Session Authorization succeeded
Failure Reason	
Resolution	
Root Cause	
Username	catc-user
Network Device Name	Catalyst-Center_6
Network Device IP	10.88.244.160
Network Device Groups	IPSEC#Is IPSEC Device#No,DNAC#DNAC Devices,Location#All Locations,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	console
Remote Address	10.189.17.203

Authorization Attributes

All Request Attribues	
All Response Attribues	cisco-av-pair=Role=SUPER-ADMIN-ROLE

Error de configuración de atributos

- El atributo está configurado incorrectamente, falta la palabra clave Role=.

  Ejemplo:

Authorization Details

Generated Time	2025-09-12 00:12:20.801 +0:00
Logged Time	2025-09-12 00:12:20.801
Epoch Time (sec)	1757635940
ISE Node	ise-mxc1
Message Text	Device-Administration: Session Authorization succeeded
Failure Reason	
Resolution	
Root Cause	
Username	catc-user
Network Device Name	Catalyst-Center_6
Network Device IP	10.88.244.160
Network Device Groups	IPSEC#Is IPSEC Device#No,DNAC#DNAC Devices,Location#All Locations,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	console
Remote Address	10.189.17.203

Authorization Attributes

All Request Attribues	
All Response Attribues	cisco-av-pair=Role=SUPER-ADMIN-ROLE

Error de configuración de atributos

2. Discordancia secreta compartida

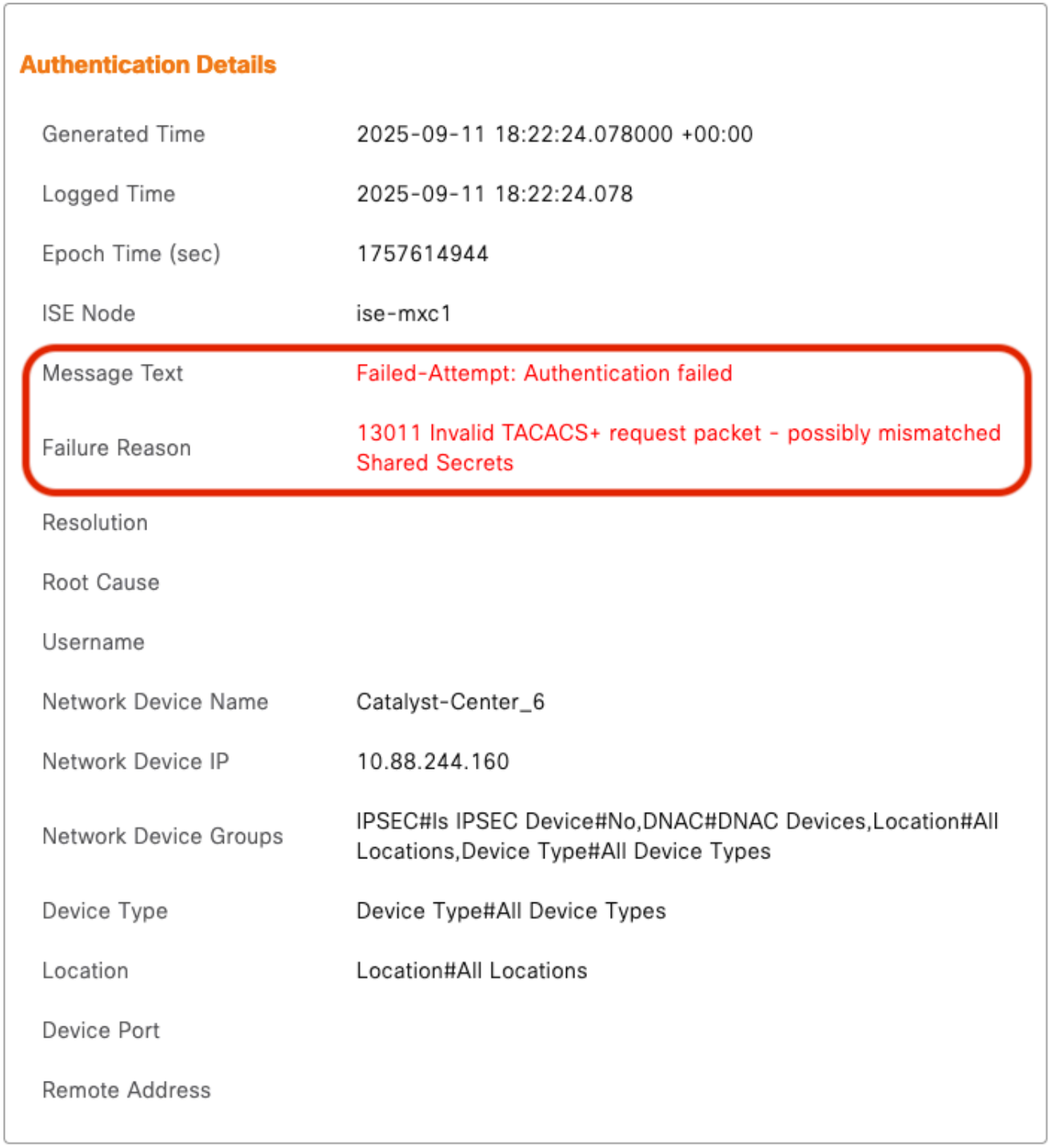
- Síntoma: Los paquetes de autenticación fallan entre Catalyst Center y Cisco ISE.

- Posible causa: El secreto compartido configurado en el recurso de red de ISE no coincide con el configurado en la página Catalyst Center > Autenticación externa.

Cómo verificar:

- Compruebe la configuración de recursos de red en ISE.
- Compare el secreto compartido con la configuración de Catalyst Center > External Authentication.

Ejemplo:



Authentication Details

Generated Time	2025-09-11 18:22:24.078000 +00:00
Logged Time	2025-09-11 18:22:24.078
Epoch Time (sec)	1757614944
ISE Node	ise-mxc1
Message Text	Failed-Attempt: Authentication failed
Failure Reason	13011 Invalid TACACS+ request packet - possibly mismatched Shared Secrets
Resolution	
Root Cause	
Username	
Network Device Name	Catalyst-Center_6
Network Device IP	10.88.244.160
Network Device Groups	IPSEC#Is IPSEC Device#No,DNAC#DNAC Devices,Location#All Locations,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	
Remote Address	

Discordancia de secreto compartido

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).