

# Configuración del dominio de autenticación TACACS+ en UCS Manager con el servidor ISE

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configuración](#)

[Configuración de TACACS+ en ISE](#)

[Configuración de TACACS+ en ISE](#)

[Configurar los atributos y las reglas en ISE](#)

[Configuración de TACACS+ en UCSM](#)

[Crear funciones para usuarios](#)

[Crear un proveedor TACACS+](#)

[Crear un grupo de proveedores TACAC+](#)

[Crear un dominio de autenticación](#)

[Troubleshoot](#)

[Problemas comunes de TACACS+ en UCSM](#)

[Revisión de UCSM](#)

[Problemas comunes de TACAC en ISE](#)

[Revisión de ISE](#)

[Información Relacionada](#)

---

## Introducción

Este documento describe la configuración de la autenticación de Terminal Access Controller Access-Control System Plus (TACACS+) en Unified Compute System Manager (UCSM). TACACS+ es un protocolo de red que se utiliza para los servicios de autenticación, autorización y responsabilidad (AAA) , que proporciona un método centralizado para gestionar los dispositivos de acceso a la red (NAD) donde puede administrar y crear reglas a través de un servidor, en este caso práctico estamos utilizando Identity Services Engine (ISE).

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco UCS Manager (UCSM)
- Terminal Access Controller Access-Control System Plus (TACACS+)
- Identity Services Engine (ISE)

## Componentes Utilizados

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

- UCSM 4.2(3d)
- Cisco Identity Services Engine (ISE) versión 3.2

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.

## Configuración

### Configuración de TACACS+ en ISE

#### Configuración de TACACS+ en ISE

Paso 1. La primera tarea es revisar si ISE tiene las capacidades correctas para manejar las autenticaciones TACACS+ para lo cual necesita verificar si dentro del Policy Service Node (PSN) desea que tenga la función de Device Admin Service, navegue por el menú Administration > System > Deployment, seleccione el nodo donde ISE realiza TACACS+ y luego seleccione el botón edit.



The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes 'Cisco ISE', 'Evaluation Mode 90 Days', and various system management links like 'Deployment', 'Licensing', 'Certificates', 'Logging', 'Maintenance', 'Upgrade', 'Health Checks', 'Backup & Restore', 'Admin Access', and 'Settings'. The main content area is titled 'Deployment Nodes' and shows a table with one row for 'ise32'. The table columns are 'Hostname' (ise32), 'Persons' (Administration, Monitoring, Policy Service), 'Role(s)' (STANDALONE), 'Services' (SESSION, PROFILER), and 'Node Status' (green). Above the table, there are buttons for 'Edit', 'Register', 'Syncup', and 'Deregister', with the 'Edit' button being the one highlighted with a red box.

Paso 2. Desplácese hacia abajo hasta que vea la función correspondiente llamada Device Administration Service (observe que para habilitar esta función primero debe tener Policy Server Persona habilitado en el nodo y además tener licencias para TACACS+ disponibles en su implementación), seleccione esa casilla y luego guarde la configuración:

The screenshot shows the 'Deployment' tab in the Cisco ISE Administration interface. Under the 'Policy Service' section, the 'Enable Device Admin Service' checkbox is selected and highlighted with a red box. The 'Save' button at the bottom right is also highlighted with a red box.

Paso 3. Configure el Dispositivo de acceso a la red (NAD) que utiliza ISE como TACACS+ como servidor, navegue hasta el menú Administración > Recursos de red > Dispositivos de red y, a continuación, seleccione el botón +Agregar.

The screenshot shows the 'Network Devices' tab in the Cisco ISE Administration interface. The '+ Add' button in the toolbar is highlighted with a red box.

Paso 4. En esta sección configure :

- Un nombre para que UCSM sea el cliente TACACS+.
- Las direcciones IP que utiliza UCSM para enviar solicitudes a ISE.
- TACACS+ Shared Secret (Clave secreta compartida de TACACS+). Se trata de la contraseña que se debe utilizar para cifrar los paquetes entre UCSM e ISE.

Network Devices List > USCM

**Network Devices**

**Name**

**Description**

**IP Address**

**Device Profile**

**Model Name**

**Software Version**

**Network Device Group**

**Location**

**IPSEC**

**Device Type**

Shared Secret

Enable Single Connect Mode

Legacy Cisco Device



Nota: Para una configuración de clúster, agregue las direcciones IP del puerto de administración para ambas fabric interconectadas. Esta configuración garantiza que los usuarios remotos puedan seguir iniciando sesión si falla la primera fabric interconectada y el sistema conmuta por error a la segunda fabric interconectada. Todas las solicitudes de inicio de sesión se originan en estas direcciones IP, no en la dirección IP virtual que utiliza Cisco UCS Manager.

## Configurar los atributos y las reglas en ISE

Paso 1. Cree un perfil TACACS+, navegue hasta el menú Centros de trabajo > Administración de dispositivos > Elementos de política > Resultados > Perfiles TACACS y, a continuación, seleccione Agregar

Work Centers - Device Administration

Policy Elements

**TACACS Profiles**

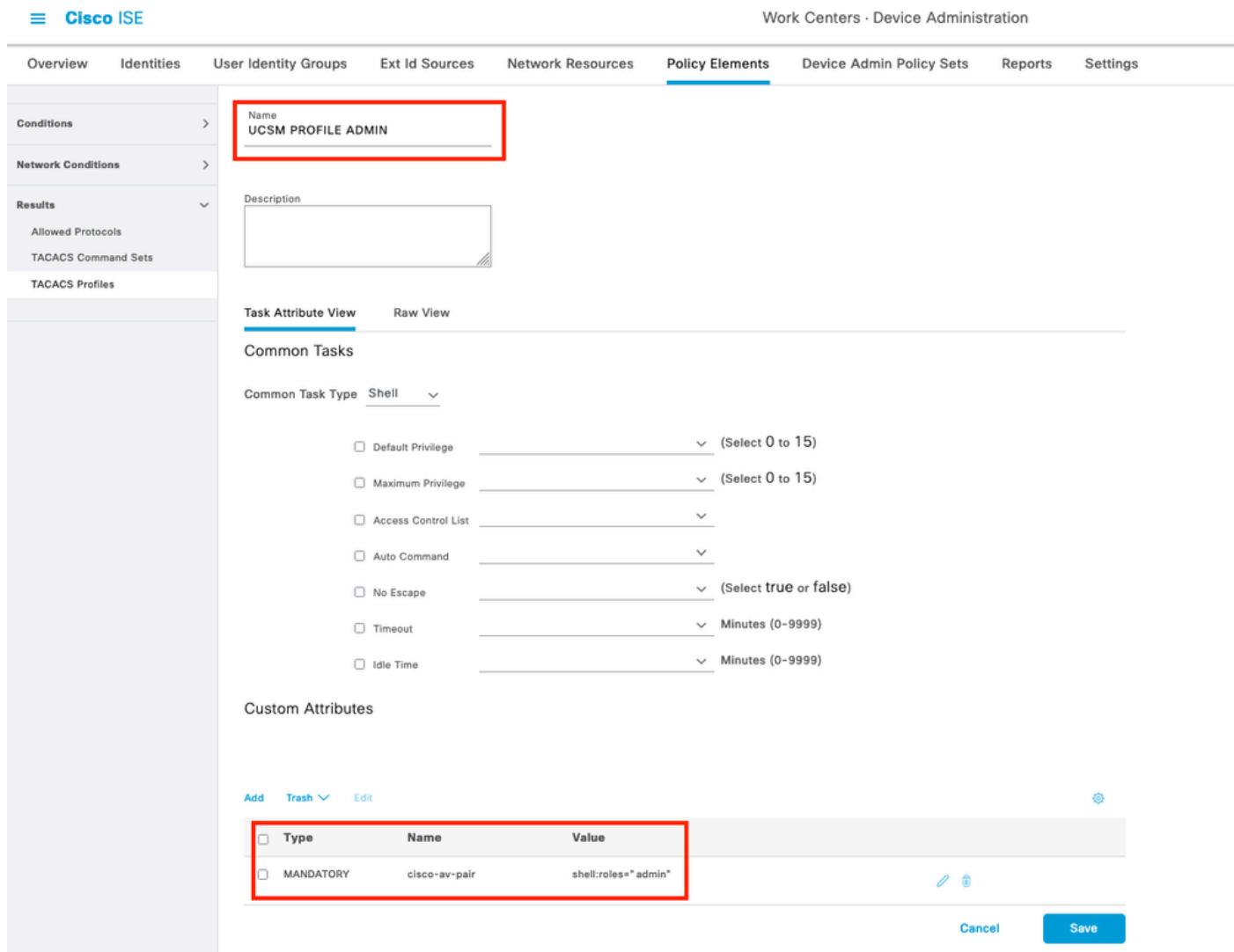
**Add**

<input type="checkbox"/> Name	Type	Description
<input type="checkbox"/> Default Shell Profile	Shell	Default Shell Profile

Rows/Page

Paso 2. En esta sección configure el perfil con un nombre y en la sección Atributos

personalizados, seleccione Agregar , luego cree un atributo de la característica OBLIGATORIO , denomínelo como cisco-av-pair y en el valor seleccione uno de los roles disponibles dentro de UCSM e ingrese que como un rol de shell, en este ejemplo está usando el rol admin y la entrada seleccionada debe ser shell:roles="admin", como se muestra aquí,



Work Centers - Device Administration

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

**Conditions** > **Name**  
UCSM PROFILE ADMIN

**Network Conditions** >

**Results** > **Description**

Allowed Protocols  
TACACS Command Sets  
TACACS Profiles

**Task Attribute View**    Raw View

**Common Tasks**

Common Task Type **Shell** ▾

Default Privilege ▾ (Select 0 to 15)  
 Maximum Privilege ▾ (Select 0 to 15)  
 Access Control List ▾  
 Auto Command ▾  
 No Escape ▾ (Select true or false)  
 Timeout ▾ Minutes (0-9999)  
 Idle Time ▾ Minutes (0-9999)

**Custom Attributes**

Add	Trash	Edit	Cancel	Save
<input type="checkbox"/>	Type	Name	Value	
<input type="checkbox"/>	MANDATORY	cisco-av-pair	shell:roles="admin"	

En el mismo menú, si selecciona la Vista sin procesar para el perfil TACACS, puede verificar la configuración correspondiente del atributo que se enviará a través de ISE.

Conditions > TACACS Profiles > UCSM PROFILE ADMIN

Network Conditions >

Results > Name: UCSM PROFILE ADMIN

Allowed Protocols

TACACS Command Sets

TACACS Profiles

Description

Task Attribute View **Raw View**

Profile Attributes

cisco-av-pair=shell:roles="admin"

Cancel Save



Nota: El nombre del par cisco-av es la cadena que proporciona el ID de atributo para el proveedor TACACS+.

Paso 3. Seleccione en la marca y guarde su configuración.

Paso 4. Crear un conjunto de políticas de administración de dispositivos para su UCSM, navegue por 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

Work Centers - Device Administration

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

Policy Sets

Status Policy Set Name Description Conditions

Search

Default Tacacs Default policy set

Allowed Protocols / Server Sequence Hits Actions View

Default Device Admin

Insert new row above

Reset Save

Paso 5. Asigne un nombre a este nuevo conjunto de políticas, agregue condiciones en función de las características de las autenticaciones TACACS+ que se están realizando desde el servidor UCSM y seleccione como Protocolos permitidos > Administrador de dispositivos predeterminado, guarde su configuración.

The screenshot shows the Cisco ISE Device Admin Policy Sets interface. At the top, there are tabs for Overview, Identities, User Identity Groups, Ext Id Sources, Network Resources, Policy Elements, Device Admin Policy Sets (which is selected), Reports, and Settings. Below the tabs, there is a search bar and a table for policy sets. The table has columns for Status, Policy Set Name, Description, and Conditions. One row is selected, showing 'USCM ACCESS' with the condition 'DEVICE Device Type EQUALS All Device Types'. To the right of the table, there are sections for 'Allowed Protocols / Server Sequence', 'Hits', 'Actions', and 'View'. At the bottom right, there are 'Reset', 'Save', and 'Reset Policyset Hitcounts' buttons.

Paso 6. Seleccione en la opción > view y seleccione en la sección Authentication Policy, el origen de identidad externo desde el que ISE consulta el nombre de usuario y las credenciales que se introducen en UCSM; en este ejemplo, las credenciales corresponden a los usuarios internos almacenados en ISE.

The screenshot shows the 'Authentication Policy' section of the Cisco ISE Device Admin Policy Sets interface. It includes a table for rules with columns for Status, Rule Name, Conditions, Use, Hits, and Actions. A new rule is being added, with the condition 'InternalUser IdentityGroup EQUALS User Identity Groups:Employee'. The 'Use' section shows 'Internal Users' selected, which is highlighted with a red box. At the bottom right, there are 'Reset', 'Save', and 'Reset Policyset Hitcounts' buttons.

Paso 7. Desplácese hacia abajo hasta la sección denominada Authorization Policy hasta la política Default, seleccione el icono de engranaje y luego inserte una regla.

Paso 8. Asigne un nombre a la nueva regla de autorización, agregue condiciones relativas al usuario que ya se han autenticado como pertenencia a un grupo y, en la sección Perfiles de shell, agregue el perfil TACACS que configuró anteriormente y guarde la configuración.

The screenshot shows the Authorization Policy interface. It includes a table for rules with columns for Status, Rule Name, Conditions, and Actions. A new rule is being added, with the condition 'InternalUser IdentityGroup EQUALS User Identity Groups:Employee'. The 'Actions' section shows 'UCSM PROFILE ADMIN' selected. At the bottom right, there are 'Reset', 'Save', and 'Reset Policyset Hitcounts' buttons. The 'Save' button is highlighted with a red box.

## Configuración de TACACS+ en UCSM

Inicie sesión **Cisco UCS Manager** en la GUI con un usuario con privilegios de administrador.

Crear funciones para usuarios

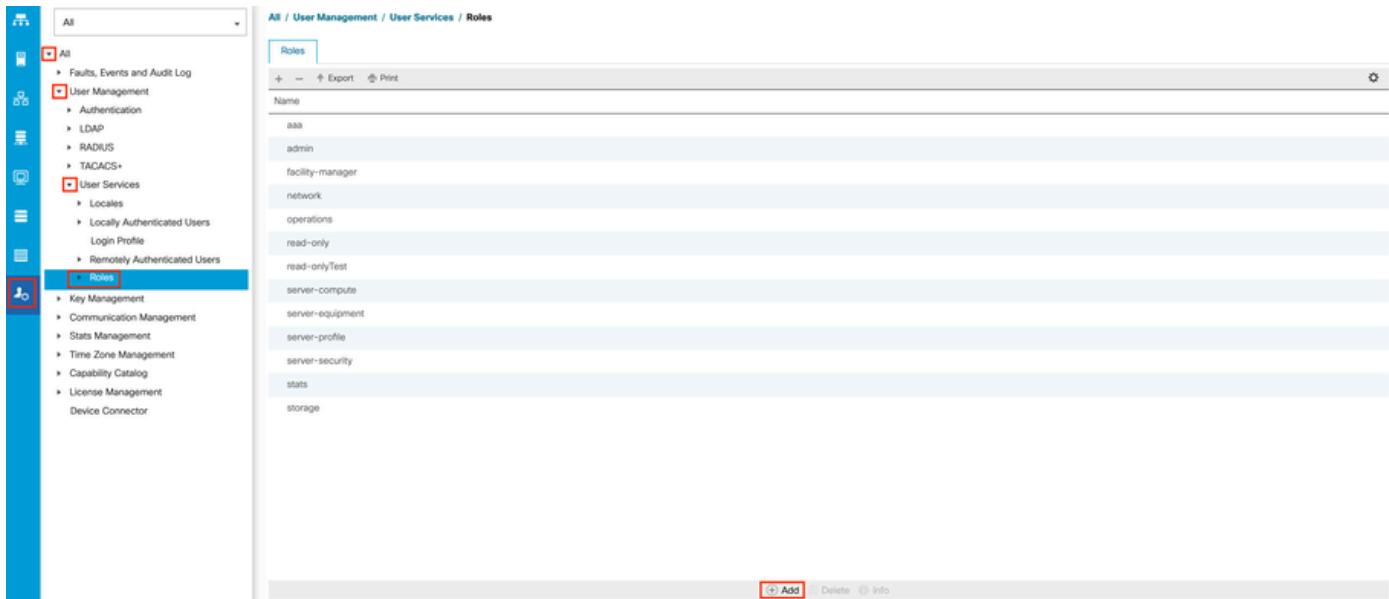
Paso 1. En el panel de navegación, seleccione la ficha Admin.

Paso 2. En la pestaña Admin, expanda All > User Management >User Services > Roles.

Paso 3. En el panel, seleccione General la ficha.

Paso 4. Seleccione Agregar para roles personalizados. Este ejemplo utiliza Roles predeterminados.

Paso 5. Verifique las coincidencias del rol de nombre con el nombre configurado previamente en el perfil TACACS.



The screenshot shows the 'User Management' section of a web-based management interface. On the left, a navigation tree is expanded to show 'User Management' and 'TACACS+'. Under 'TACACS+', 'User Services' is expanded, and 'Roles' is selected. The main panel displays a list of roles with the following names: aaa, admin, facility-manager, network, operations, read-only, read-onlyTest, server-compute, server-equipment, server-profile, server-security, stats, and storage. A red box highlights the 'Roles' link in the navigation tree. A red box also highlights the 'Add' button at the bottom of the role list.

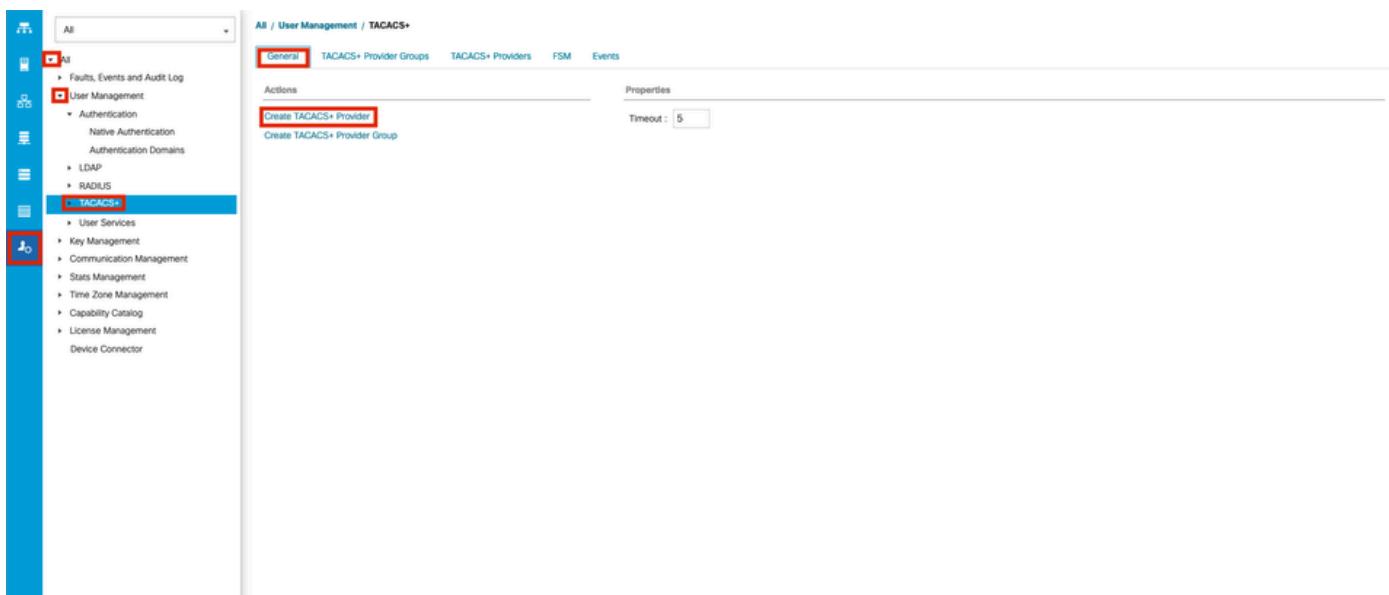
Crear un proveedor TACACS+

Paso 1. En el panel de navegación, seleccione la ficha Admin.

Paso 2. En la pestaña Admin, expanda All > User Management > TACACS+.

Paso 3. En el panel, seleccione la pestaña que desee.

Paso 4. En el área Actions, seleccione **Create TACACS+ Provider**.



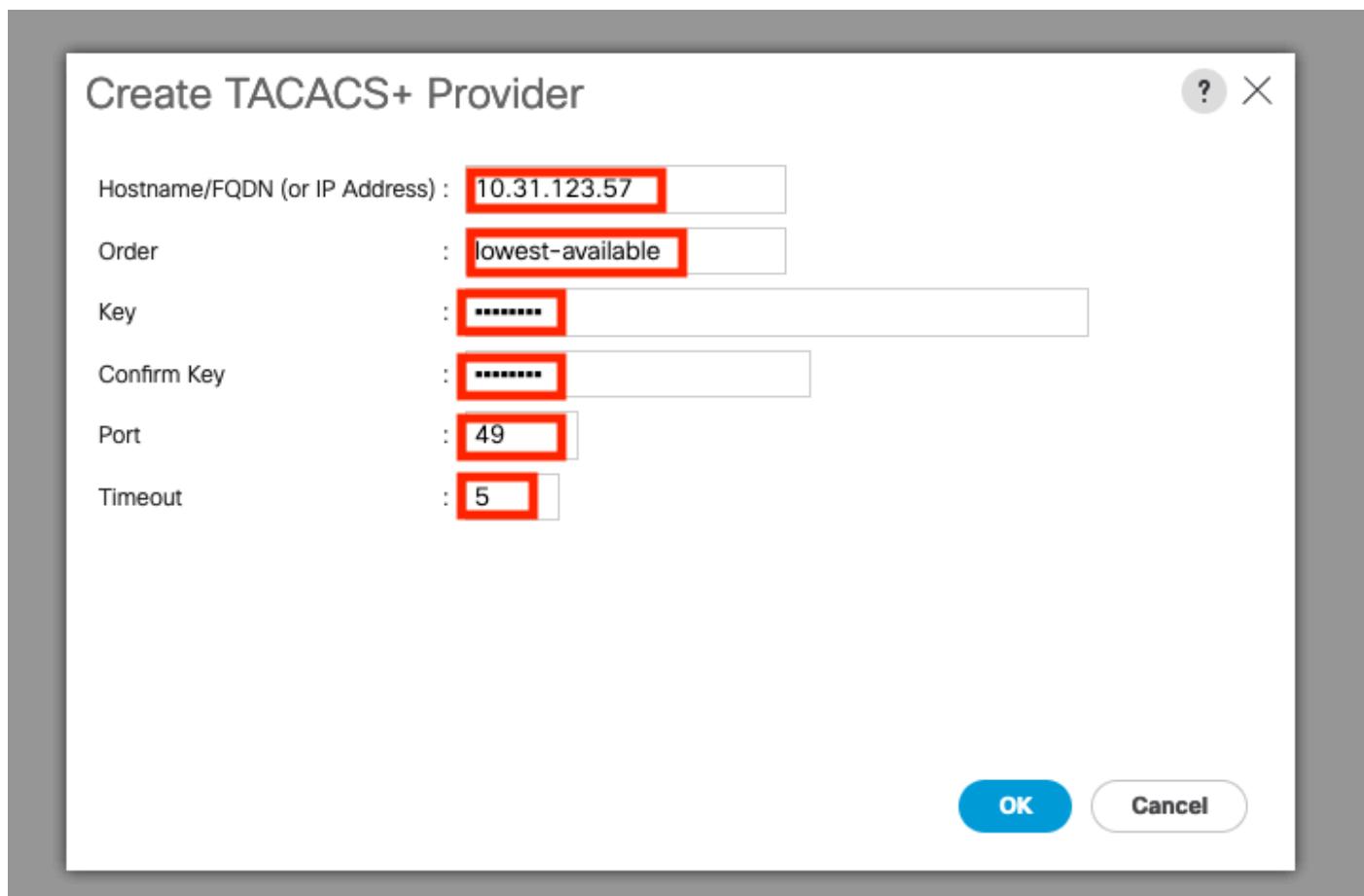
The screenshot shows the 'TACACS+' configuration interface. The left navigation tree is expanded to show 'TACACS+', which is selected with a red box. The main panel has tabs for 'General', 'TACACS+ Provider Groups', 'TACACS+ Providers', 'FSM', and 'Events'. The 'General' tab is selected. Under 'Actions', there is a red box around the 'Create TACACS+ Provider' link. On the right, there is a 'Properties' section with a 'Timeout' field set to '5'. A red box highlights the 'Create TACACS+ Provider' link.

Paso 5. En el asistente **Create TACACS+ Provider**, introduzca la información correspondiente.

- En el campo Hostname, escriba la dirección IP o el nombre de host del servidor TACACS+.
- En el campo Pedido, el orden en el que Cisco UCS utiliza este proveedor para autenticar a los usuarios.

Introduzca un número entero entre 1 y 16, o bien introduzca el número más bajo disponible o 0 (cero) si desea que Cisco UCS asigne el siguiente pedido disponible en función de los otros proveedores definidos en esta instancia de Cisco UCS.

- En el campo Key, la clave de cifrado SSL para la base de datos.
- En el campo Confirm Key, la clave de cifrado SSL se repite con fines de confirmación.
- En el campo Puerto, el puerto a través del cual Cisco UCS se comunica con la base de datos TACACS+ (puerto predeterminado 49).
- En el campo Tiempo de espera, el tiempo en segundos que el sistema emplea para intentar contactar con la base de datos TACACS+ antes de que se agote el tiempo de espera.



Paso 6. Seleccione Aceptar.



Nota: Si utiliza un nombre de host en lugar de una dirección IP, debe configurar un servidor DNS en Cisco UCS Manager.

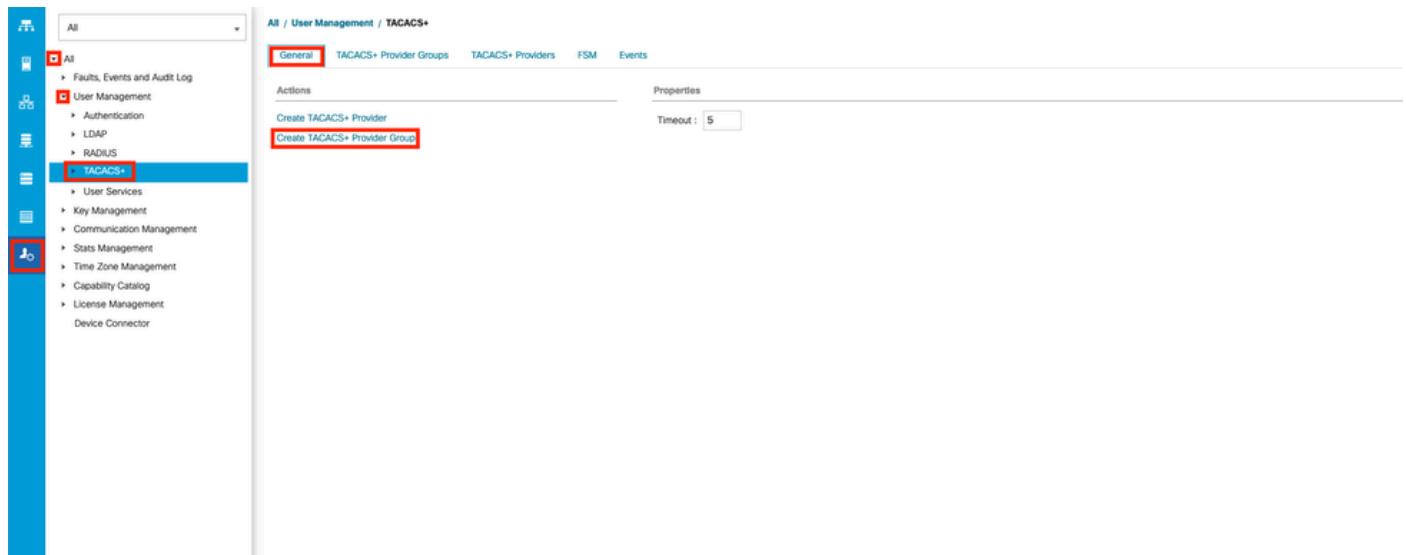
## Crear un grupo de proveedores TACAC+

Paso 1. En **Navigation** el panel, seleccione la **Admin** ficha.

Paso 2. En **Admin** la ficha, expanda **All > User Management > TACACS+**.

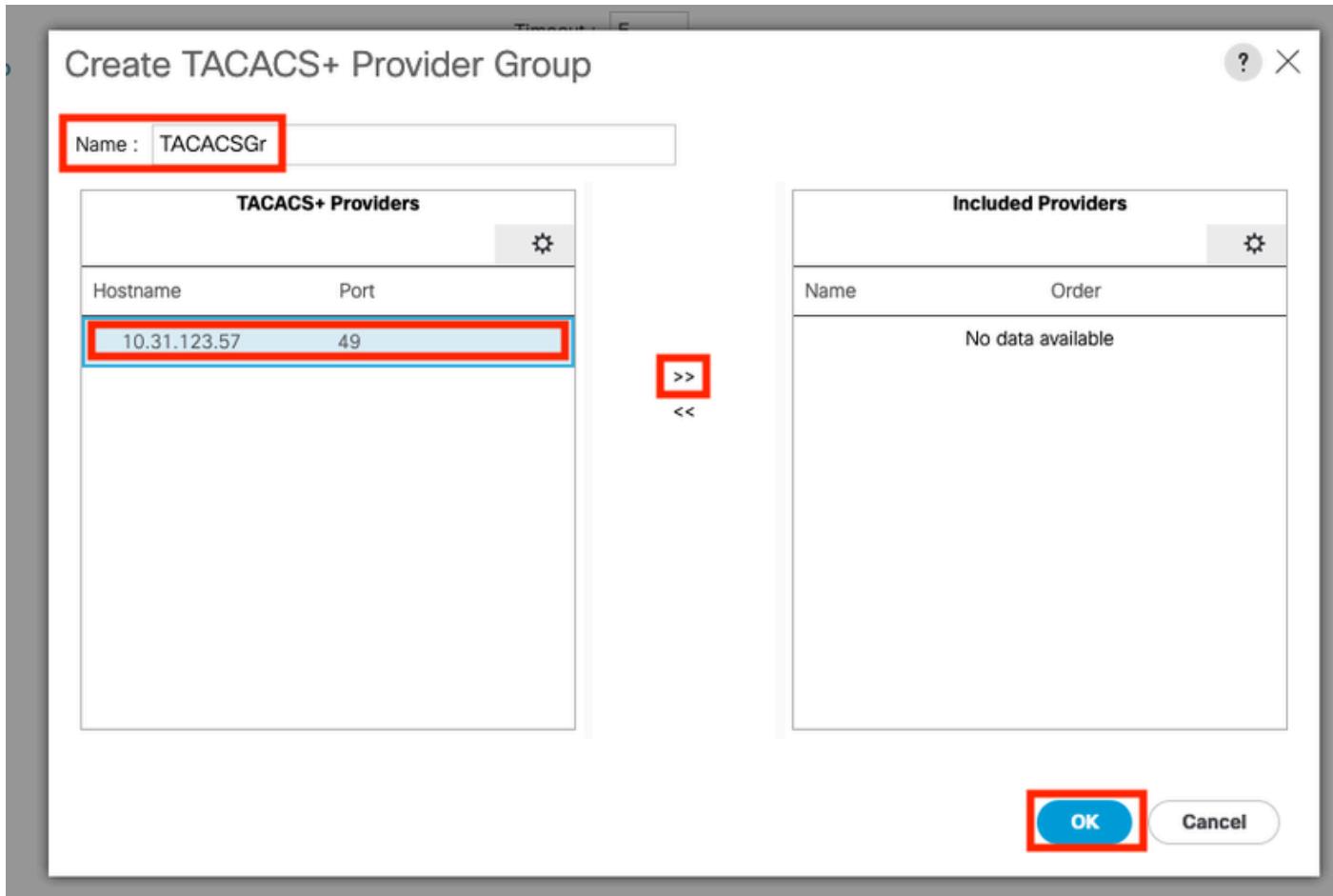
Paso 3. En **Work** el panel, seleccione la **General** pestaña.

Paso 4. En **Actions** el área, Create TACACS+ Provider seleccione **Grupo**.



Paso 5. En el cuadro de diálogo Crear grupo de proveedores de TACACS+, ingrese la información solicitada.

- En el campo Nombre, introduzca un nombre único para el grupo.
- En la tabla Proveedores TACACS+, elija los proveedores que se incluirán en el grupo.
- Seleccione el botón **>>** para agregar los proveedores a la tabla Proveedores incluidos.



Paso 6. Seleccione Aceptar.

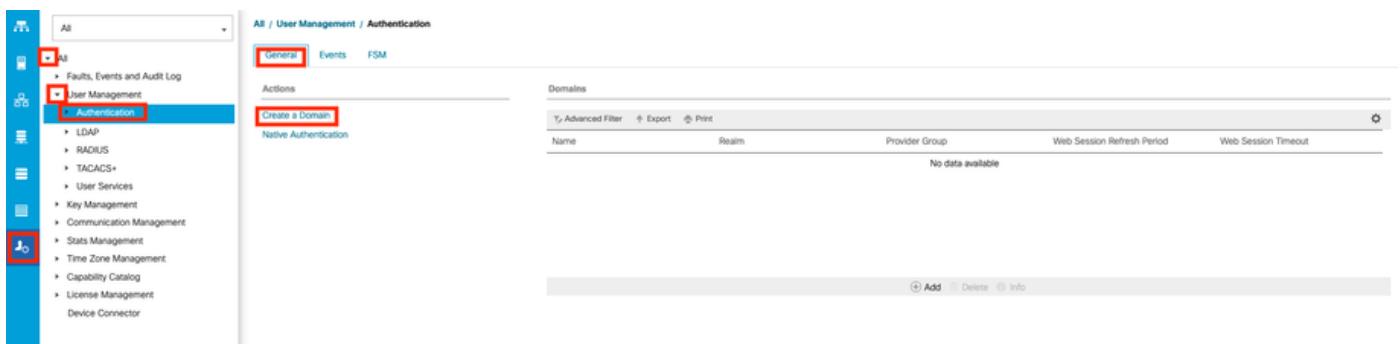
Crear un dominio de autenticación

Paso 1. En el **Navigation** panel, seleccione la **Admin** pestaña.

Paso 2. En la **Admin** ficha, expanda **All > User Management > Authentication**

Paso 3. En **Worklet** panel, seleccione la **General** pestaña.

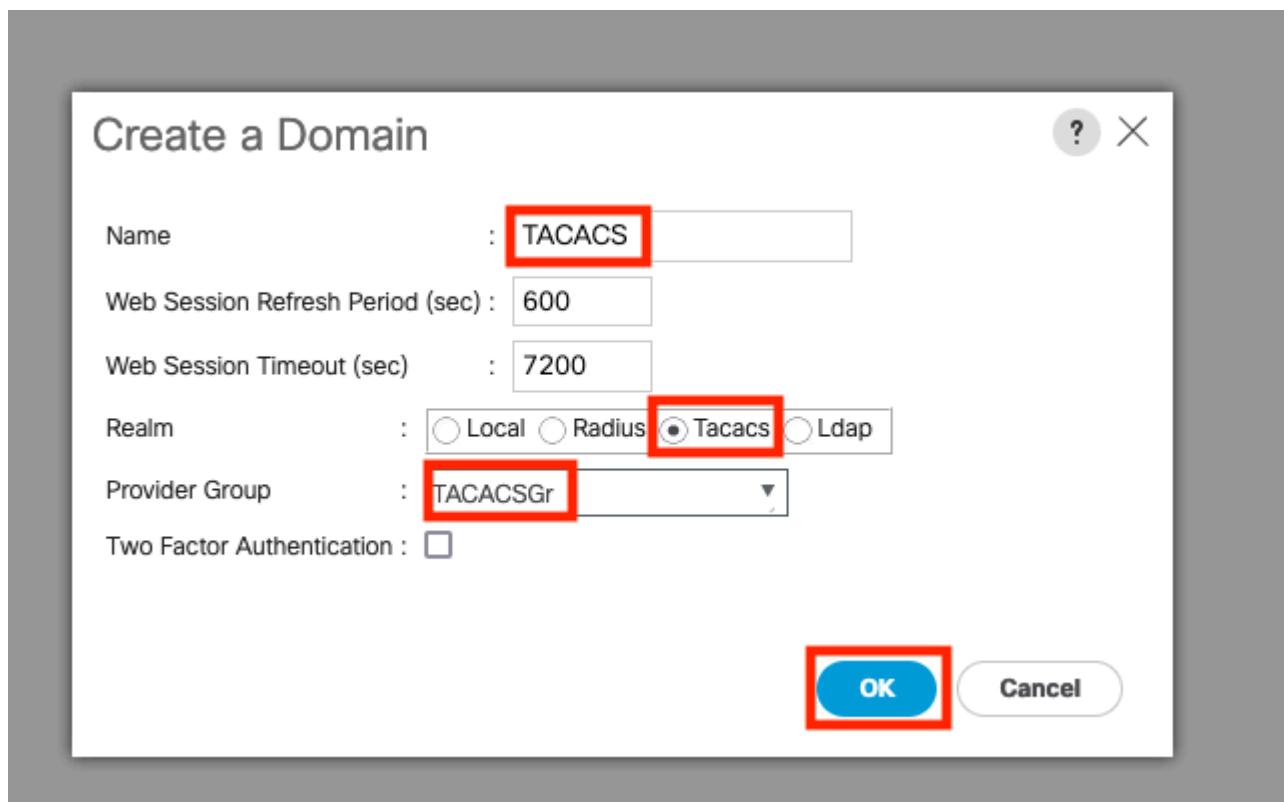
Paso 4. En **Actions** el área, seleccione **Create a Domain**.



Paso 5. En el cuadro de diálogo Crear dominio, ingrese la información solicitada.

- En el campo Nombre, introduzca un nombre único para el dominio.
- En el rango, seleccione la opción Tacacs.

- En la lista desplegable Grupo de Proveedores, seleccione el grupo de proveedores TACACS+ creado anteriormente y seleccione Aceptar



## Troubleshoot

### Problemas comunes de TACACS+ en UCSM

- Clave incorrecta o caracteres no válidos.
- Puerto Incorrecto.
- No hay comunicación con nuestro proveedor debido a una regla de firewall o proxy.
- FSM no es el 100%.

Verifique la configuración de UCSM TACACS+:

Debe asegurarse de que UCSM haya implementado la configuración. Para comprobar que el estado de la máquina de estado finito (FSM) aparece como 100% completado.

Verifique la configuración desde la línea de comandos de UCSM

```
<#root>
UCS-A#
scope security

UCS-A /security #
scope tacacs
```

```
UCS-A /security/tacacs #
```

```
show configuration
```

```
[UCS-AS-MXC-P25-02-A# scope security
[UCS-AS-MXC-P25-02-A /security # scope tacacs
[UCS-AS-MXC-P25-02-A /security/tacacs # show configuration
  scope tacacs
    enter auth-server-group TACACSGR
      enter server-ref 10.31.123.57
        set order 1
      exit
    exit
    enter server 10.31.123.57
      set order 1
      set port 49
      set timeout 5
  !
  set key
exit
  set timeout 5
exit
```

```
<#root>
```

```
UCS-A /security/tacacs #
```

```
show fsm status
```

```
[UCS-AS-MXC-P25-02-A /security/tacacs # show fsm status
```

```
FSM 1:
```

```
  Status: Nop
  Previous Status: Update Ep Success
  Timestamp: 2023-06-24T20:54:05.021
  Try: 0
  Progress (%): 100
  Current Task:
```

Verifique la configuración de Tacacs desde el NXOS:

```
<#root>
```

```
UCS-A#
```

```
connect nxos
```

```
UCS-A(nx-os)#
```

```
show tacacs-server
```

```
UCS-A(nx-os)#
```

```
show tacacs-server groups
```

```
[UCS-AS-MXC-P25-02-A# connect nxos
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2023, Cisco and/or its affiliates.
All rights reserved.

The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their own
licenses, such as open source. This software is provided "as is," and unless
otherwise stated, there is no warranty, express or implied, including but not
limited to warranties of merchantability and fitness for a particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.

A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.

[UCS-AS-MXC-P25-02-A(nx-os)# show tacacs-server
timeout value:5
deadtime value:0
source interface:any available
Global Test Username:test
Global Test Password:*****
total number of servers:1

following TACACS+ servers are configured:
  10.31.123.57:
    available on port:49
    TACACS+ shared secret:*****
    timeout:5

[UCS-AS-MXC-P25-02-A(nx-os)# show tacacs-server groups
total number of groups:2

following TACACS+ server groups are configured:
  group tacacs:
    server 10.31.123.57 on port 49
    deadtime is 0
    vrf is management
  group TACACSGr:
    server 10.31.123.57 on port 49
    deadtime is 0
    vrf is management
```

Para probar la autenticación de NX-OS, utilice el `test aaa` comando (solo disponible en NX-OS).

Valide la configuración de su servidor:

<#root>

```
UCS-A(nx-os)#  
test aaa server tacacs+  
<TACACS+-server-IP-address or FQDN> <username> <password>
```

```
[UCS-AS-MXC-P25-02-A# connect nxos  
Cisco Nexus Operating System (NX-OS) Software  
TAC support: http://www.cisco.com/tac  
Copyright (C) 2002-2023, Cisco and/or its affiliates.  
All rights reserved.  
The copyrights to certain works contained in this software are  
owned by other third parties and used and distributed under their own  
licenses, such as open source. This software is provided "as is," and unless  
otherwise stated, there is no warranty, express or implied, including but not  
limited to warranties of merchantability and fitness for a particular purpose.  
Certain components of this software are licensed under  
the GNU General Public License (GPL) version 2.0 or  
GNU General Public License (GPL) version 3.0 or the GNU  
Lesser General Public License (LGPL) Version 2.1 or  
Lesser General Public License (LGPL) Version 2.0.  
A copy of each such license is available at  
http://www.opensource.org/licenses/gpl-2.0.php and  
http://opensource.org/licenses/gpl-3.0.html and  
http://www.opensource.org/licenses/lgpl-2.1.php and  
http://www.gnu.org/licenses/old-licenses/library.txt.  
[UCS-AS-MXC-P25-02-A(nx-os)# test aaa server tacacs+ 10.31.123.57 operator Cisc0123
```

## Revisión de UCSM

### Verificación de disponibilidad

```
<#root>  
UCS-A#  
connect local-mgmt  
UCS-A(local-mgmt)#  
ping  
<TACACS+-server-IP-address or FQDN>
```

```
[UCS-AS-MXC-P25-02-A# connect local-mgmt
pCisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php

[UCS-AS-MXC-P25-02-A(local-mgmt)# ping 10.31.123.57
PING 10.31.123.57 (10.31.123.57) from 10.31.123.8 : 56(84) bytes of data.
64 bytes from 10.31.123.57: icmp_seq=1 ttl=64 time=0.347 ms
64 bytes from 10.31.123.57: icmp_seq=2 ttl=64 time=0.309 ms
```

## Verificación de puertos

```
<#root>

UCS-A#
connect local-mgmt

UCS-A(local-mgmt)#
telnet
<TACACS+-server-IP-address or FQDN> <Port>
```

```
[UCS-AS-MXC-P25-02-A# connect local-mgmt
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php

[UCS-AS-MXC-P25-02-A(local-mgmt)# telnet 10.31.123.57 49
Trying 10.31.123.57...
Connected to 10.31.123.57.
Escape character is '^]'.
```

El método más efectivo para ver errores es habilitar la depuración de NXOS, con esta salida puede ver los grupos, la conexión y el mensaje de error que causa la mala comunicación.

- Abra una sesión SSH en UCSM e inicie sesión con cualquier usuario con privilegios con permisos de administrador (preferiblemente un usuario local), cambie al contexto de la CLI de NX-OS e inicie el monitor de terminal.

```
<#root>

UCS-A#

connect nxos

UCS-A(nx-os)#

terminal monitor
```

- Habilite los indicadores de depuración y verifique el resultado de la sesión SSH en el archivo de registro.

```
<#root>

UCS-A(nx-os)#

debug aaa all

UCS-A(nx-os)#

debug aaa aaa-request

UCS-A(nx-os)#

debug tacacs+ aaa-request

UCS-A(nx-os)#

debug tacacs+ aaa-request-lowlevel

UCS-A(nx-os)#

debug tacacs+ all
```

```
[UCS-AS-MXC-P25-02-A# connect nxos
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2023, Cisco and/or its affiliates.
All rights reserved.

The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their own
licenses, such as open source. This software is provided "as is," and unless
otherwise stated, there is no warranty, express or implied, including but not
limited to warranties of merchantability and fitness for a particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.

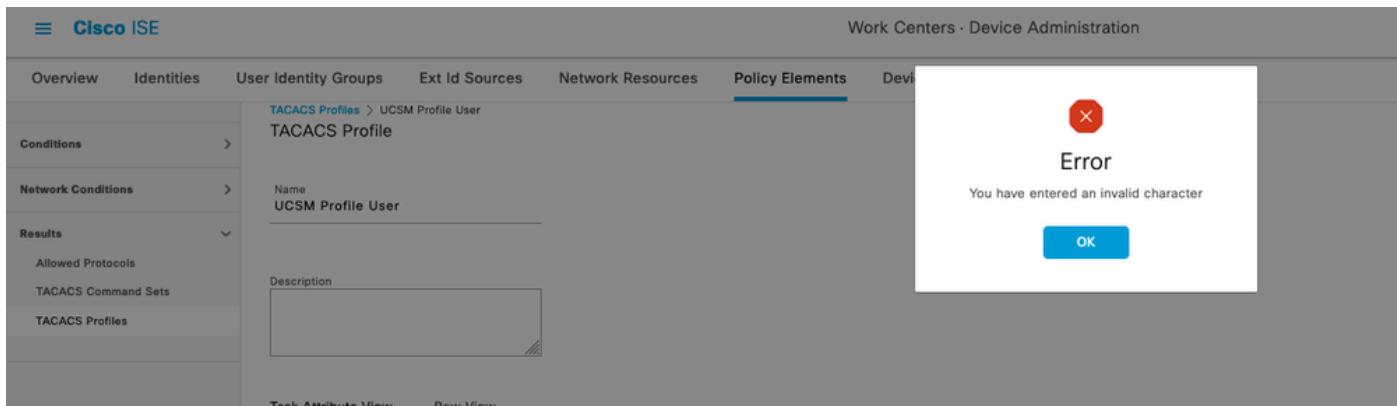
[UCS-AS-MXC-P25-02-A(nx-os)# terminal monitor
[UCS-AS-MXC-P25-02-A(nx-os)# debug tacacs+ all
2023 Jun 26 04:42:22.104286 tacacs: event_loop(): calling process_rd_fd_set
2023 Jun 26 04:42:22.104311 tacacs: process_rd_fd_set: calling callback for fd 6
2023 Jun 26 04:42:22.104341 tacacs: fsrv didnt consume 182 opcode
2023 Jun 26 04:42:22.104994 tacacs: mts_message_handler: sdwrap_process_msg
2023 Jun 26 04:42:22.105011 tacacs: process_rd_fd_set: callback returned for fd 6
[UCS-AS-MXC-P25-02-A(nx-os)# debug aaa all]
```

- Ahora abra una nueva sesión GUI o CLI e intente iniciar sesión como usuario remoto (TACACS+).
- Una vez que haya recibido un mensaje de error de inicio de sesión, desactive los debugs que cierran la sesión o con este comando.

```
UCS-A(nx-os)# undebug all
```

## Problemas comunes de TACAC en ISE

- En ISE, este comportamiento se muestra al intentar configurar un perfil tacacs en los atributos necesarios para que UCSM asigne los roles correspondientes a admin o a cualquier otro rol. Seleccione en el botón save (guardar) y verá este comportamiento:



Este error se debe al siguiente bug <https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwc91917> ,

por favor asegúrese de que tiene donde se ha solucionado este defecto.

## Revisión de ISE

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

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

<#root>

```
ise32/admin#  
show ports | include 49  
  
tcp: 169.254.4.1:49, 169.254.2.1:49, 169.254.4.1:49, 10.31.123.57:49
```

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 ,

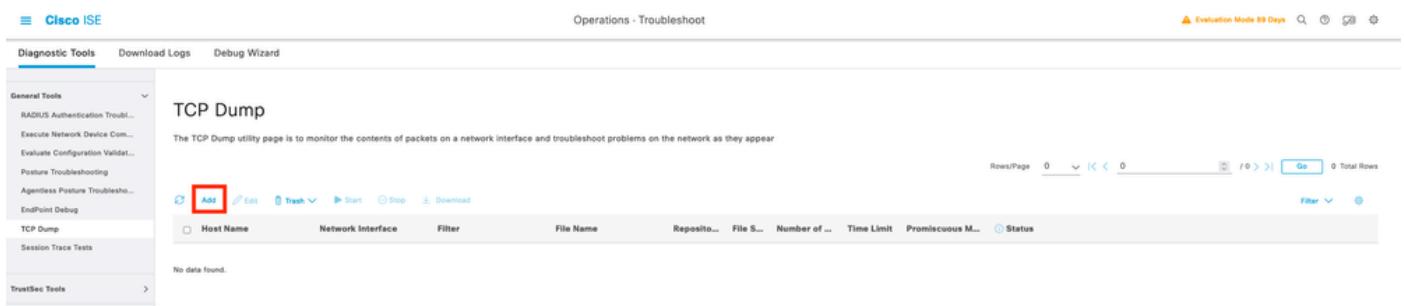
Dependiendo del motivo del fallo, puede ajustar la configuración o abordar la causa del fallo.



The screenshot shows the Cisco ISE Operations - TACACS Live Logs page. The table displays the following data:

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Device N...	Network Devic...	Device Type	Location	Device P...	Failure Reason	Remote Address
Jun 25, 2023 12:30:16...	●	○	INVALID	Authentic...	Default >> Default		ise32	UCSM	10.31.123.8	Device Type>All ...	Location>All Loc...		22056 Subject not found in the ap...	10.99.183.4
Jun 25, 2023 12:20:38.7...	●	○		Authentic...			ise32		10.31.123.9			13017 Received TACACS+ packet f...		
Jun 25, 2023 12:20:02.2...	●	○		Authentic...			ise32		10.31.123.9			13017 Received TACACS+ packet f...		

Paso 3. En caso de que no vea ningún livelog, proceda a tomar una captura de paquetes navegue hasta el menú Operaciones > Troubleshooting > Herramientas de diagnóstico > Herramientas generales > TCP Dump , seleccione on add



The screenshot shows the Cisco ISE Operations - Troubleshoot page. The TCP Dump section is highlighted. The table shows the following data:

Host Name	Network Interface	Filter	File Name	Repository...	File S...	Number of ...	Time Limit	Promiscuous M...	Status
No data found.									

Seleccione el nodo de Servicio de políticas desde el que UCSM envía la autenticación y, a continuación, en los filtros, proceda a introducir ip host X.X.X.X correspondiente a la IP de UCSM

desde la que se envía la autenticación, asigne un nombre a la captura y desplácese hacia abajo para guardarla, ejecute la captura e inicie sesión desde UCSM .

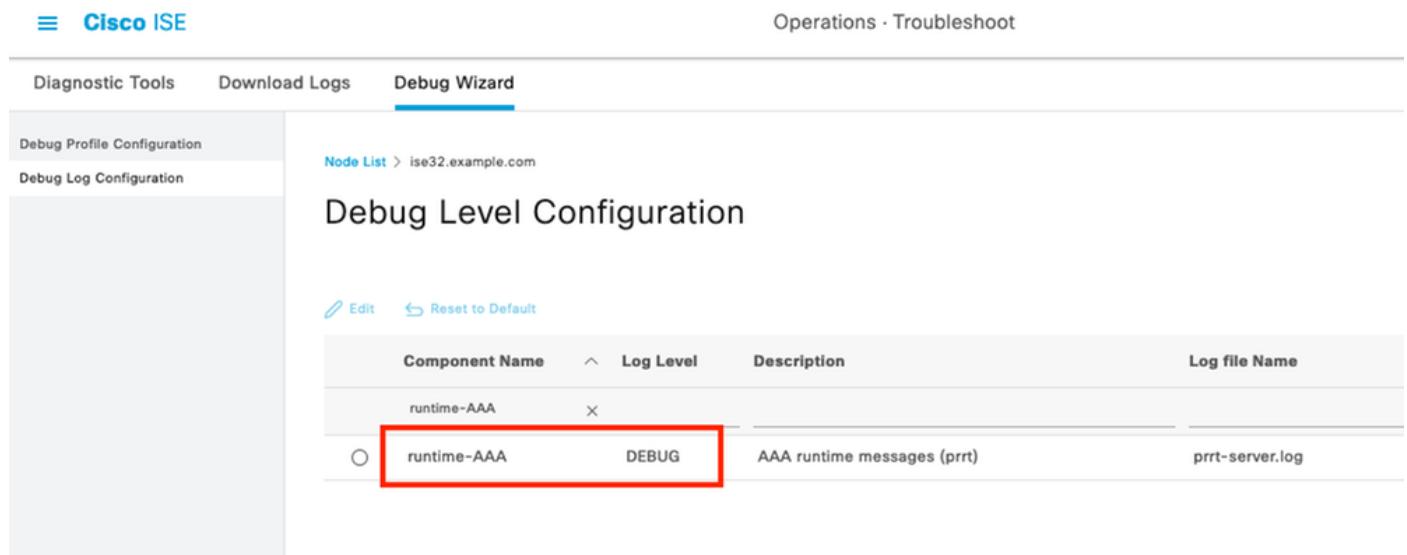
The screenshot shows the Cisco ISE Diagnostic Tools interface for TCP Dump. The 'Host Name\*' field is set to 'ise32'. The 'Network Interface\*' field is set to 'GigabitEthernet 0 [Up, Running]'. The 'Filter' field contains 'ip host 10.31.123.7'. The 'File Name' field is set to 'tacccap'. The 'Save and Run' button is highlighted with a red box.

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 el nodo PSN , luego seleccione next en edit button .

The screenshot shows the Cisco ISE Diagnostic Tools interface for the Debug Wizard - Node List. The 'Node Name' is set to 'ise32' and the 'Replication Role' is 'STANDALONE'. The 'Edit' button is highlighted with a red box.

Busque el componente runtime-AAA y cambie su nivel a debug para luego reproducir el problema

otra vez, y proceda a analizar los registros .



The screenshot shows the Cisco ISE Debug Wizard interface. The top navigation bar includes 'Cisco ISE', 'Operations · Troubleshoot', 'Diagnostic Tools', 'Download Logs', and 'Debug Wizard' (which is underlined, indicating it is the active tab). A sidebar on the left lists 'Debug Profile Configuration' and 'Debug Log Configuration'. The main content area is titled 'Debug Level Configuration' and contains a table with the following data:

Component Name	Log Level	Description	Log file Name
runtime-AAA	DEBUG	AAA runtime messages (prrt)	prrt-server.log

Two buttons are visible above the table: 'Edit' and 'Reset to Default'. The 'runtime-AAA' row is highlighted with a red box.



Nota: Para obtener más información, consulte el vídeo en el canal de Cisco Youtube How to Enable Debugs on ISE 3.x Versions <https://www.youtube.com/watch?v=E3USz8B76c8>

## Información Relacionada

[Guía de administración de Cisco UCS Manager](#)

[Guía de configuración de Cisco UCS CIMC TACACS+](#)

## 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).