# Ejemplo de Configuración de Prime Infrastructure Integration con ACS 4.2 TACACS

## Contenido



## Introducción

Este documento describe el ejemplo de configuración para Terminal Access Controller Access-Control System (TACACS+)

autenticación y autorización en la aplicación Cisco Prime Infrastructure (PI).

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Definir PI como cliente en Access Control Server (ACS)
- Defina la dirección IP y una clave secreta compartida idéntica en ACS e PI

### Componentes Utilizados

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

- ACS versión 4.2
- Prime Infrastructure versión 3.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

# Configurar

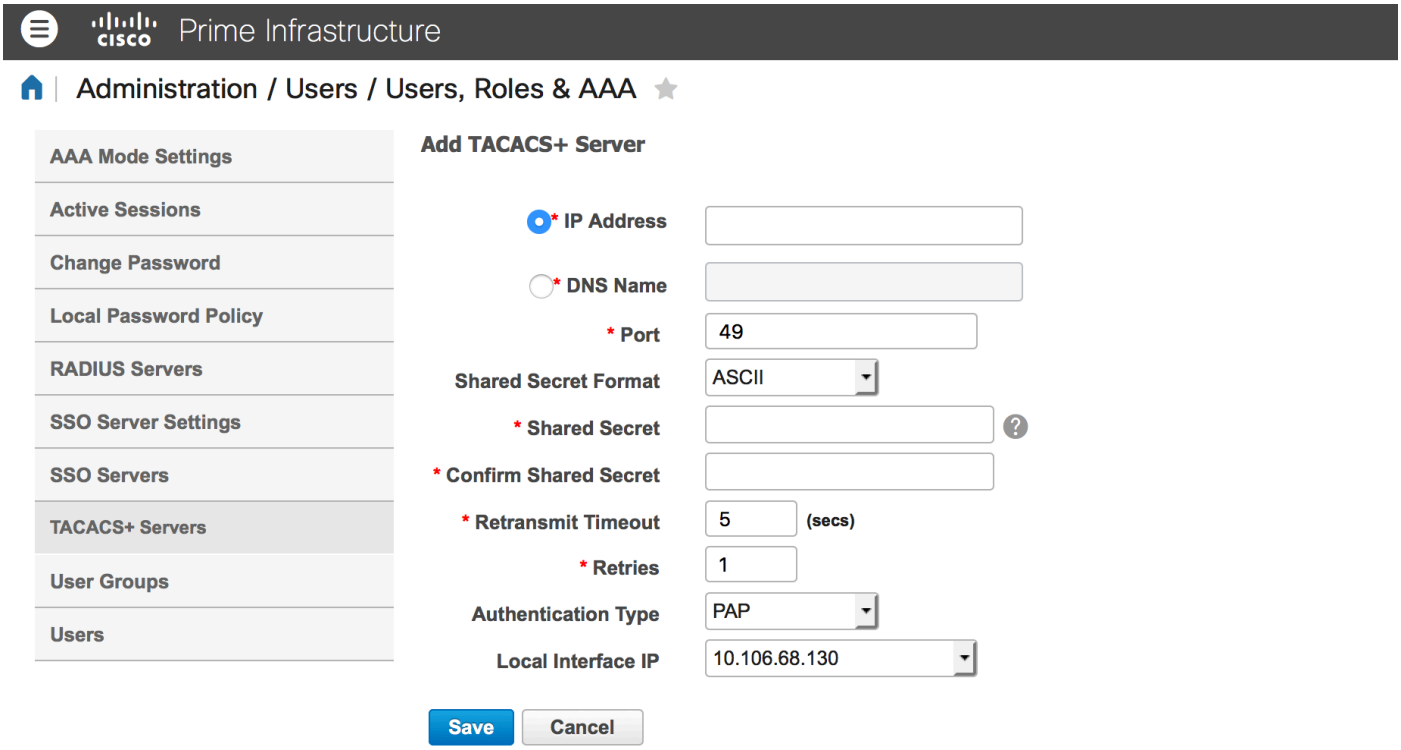
## Configuraciones

## Agregar ACS como servidor TACACS en PI

Complete estos pasos para agregar ACS como servidor TACACS:

Paso 1. Vaya a **Administración > Usuarios > Usuarios, funciones y AAA en PI**

Paso 2. En el menú de la barra lateral izquierda, seleccione **TACACS+ Servers** , en **Add TACACS+ servers** haga clic en **Go** y la página aparece como se muestra en la imagen:




Paso 3. Agregue la dirección IP del servidor ACS.

Paso 4. Introduzca el secreto compartido TACACS+ configurado en el servidor ACS.

Paso 5. Vuelva a introducir el secreto compartido en el cuadro de **texto Confirmar secreto compartido**.

Paso 6. Deje el resto de los campos en su configuración predeterminada.

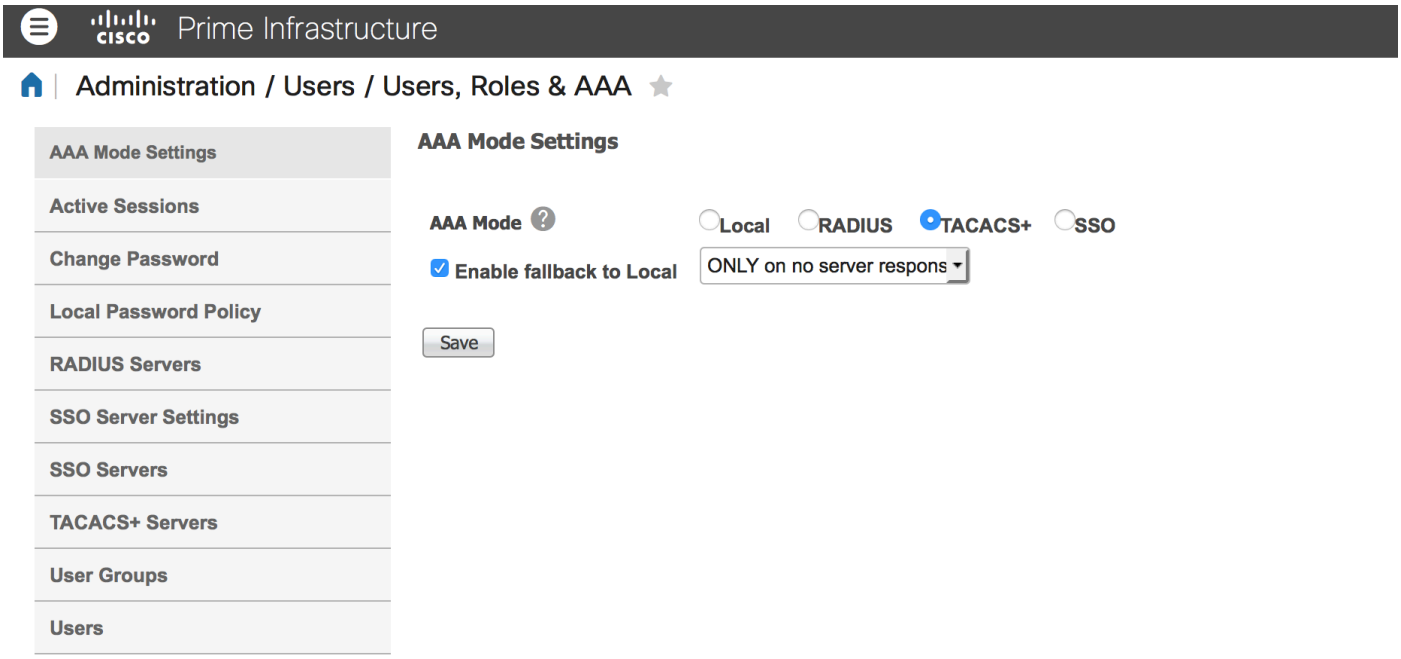
Paso 7. Haga clic en Submit (Enviar).

## Configuración del modo AAA en PI

Para elegir un modo de autenticación, autorización y contabilidad (AAA), realice estos pasos:

Paso 1. Vaya a **Administration > AAA**.

Paso 2. Elija **AAA Mode** en el menú de la barra lateral izquierda, puede ver la página como se muestra en la imagen:

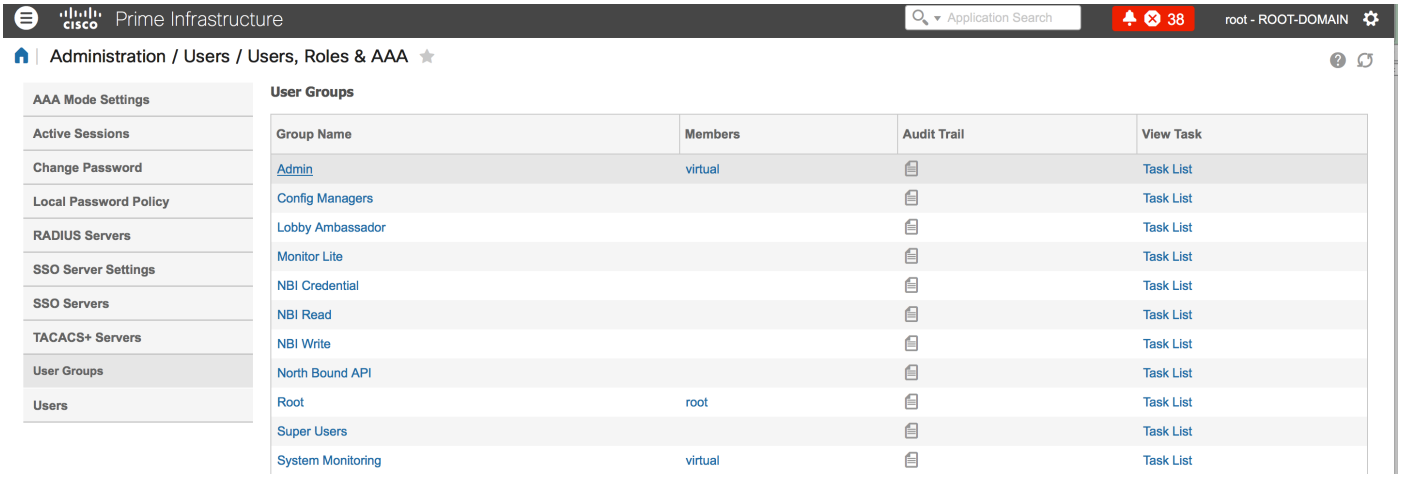



Paso 3. Seleccione **TACACS+**.

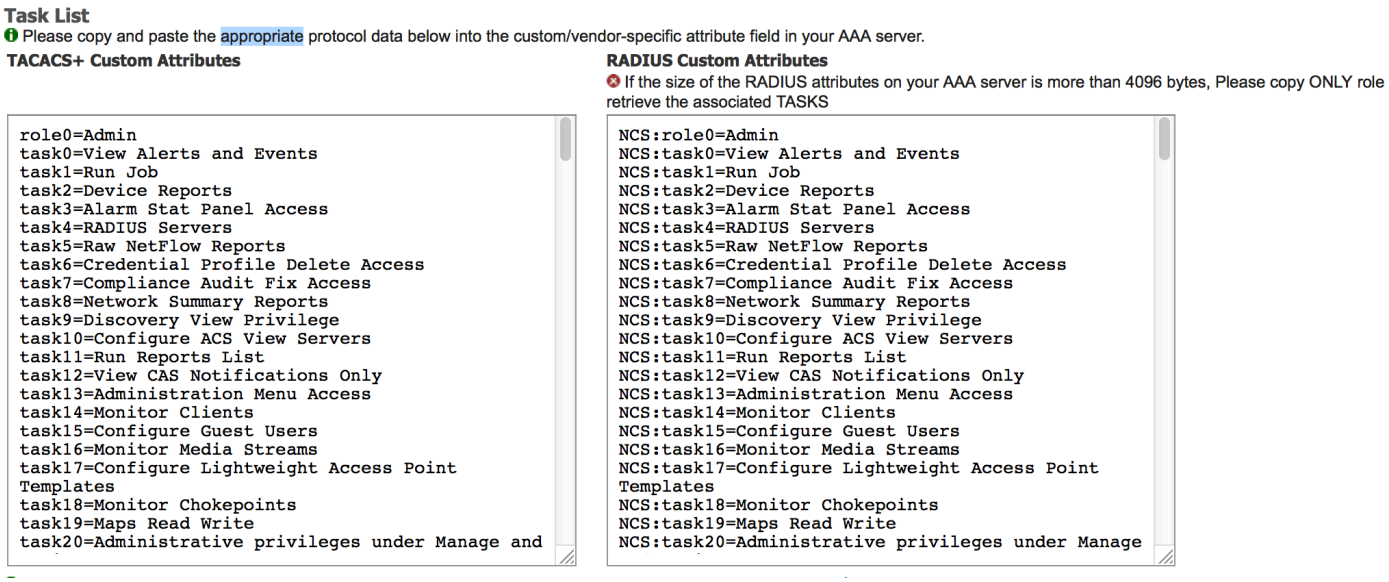
Paso 4. Marque la casilla **Enable Fallback to Local**, si desea que el administrador utilice la base de datos local cuando el servidor ACS no sea accesible. Esta es una configuración recomendada.

## Recuperar atributos de rol de usuario de PI

Paso 1. Vaya a **Administration > AAA > User Groups**. Este ejemplo muestra la autenticación del administrador. Busque el **nombre del grupo de administradores** en la lista y haga clic en la **opción Lista de tareas** de la derecha, como se muestra en la imagen:



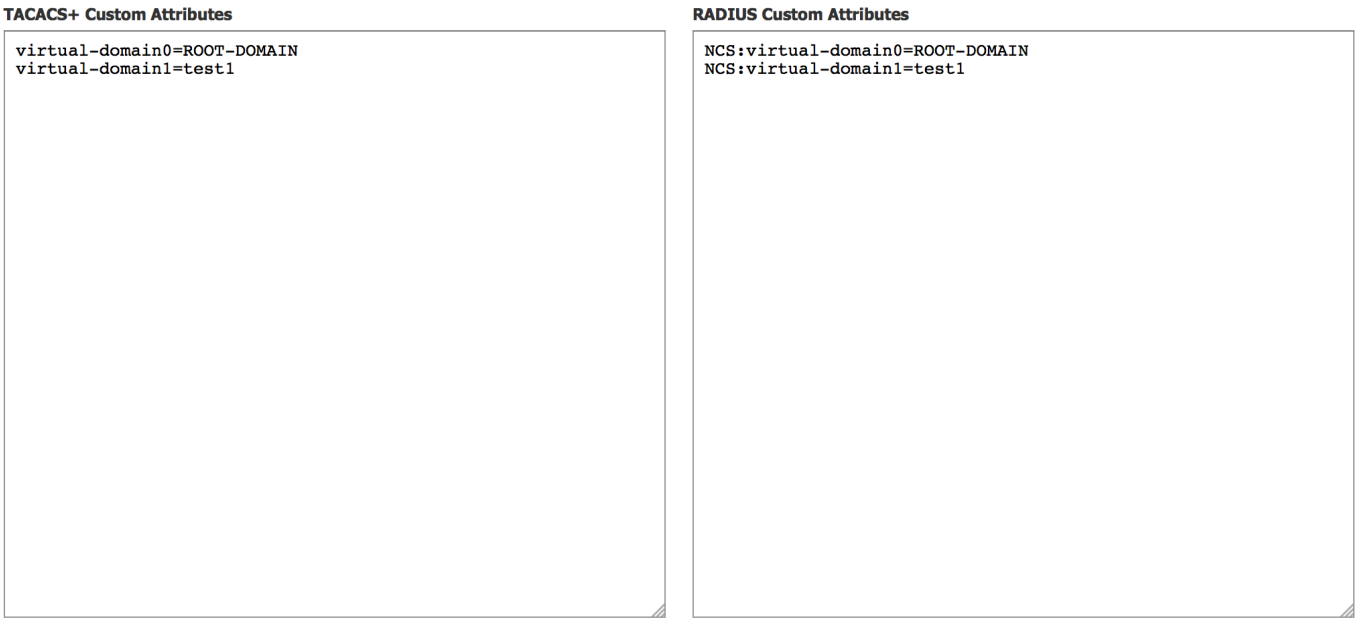

Una vez que haga clic en la opción **Lista de tareas**, aparecerá la ventana, como se muestra en la imagen:




Paso 2. Copie estos atributos y guárdelos en un archivo de bloc de notas.

Paso 3. Es posible que deba agregar atributos de dominio virtual personalizados en el servidor ACS. Los atributos de dominio virtual personalizados están disponibles en la parte inferior de la misma página de lista de tareas.


Paso 4. Haga clic en la opción **Click here** para obtener la página del atributo del dominio virtual, y puede ver la página, como se muestra en la imagen:




## Configuración de ACS 4.2

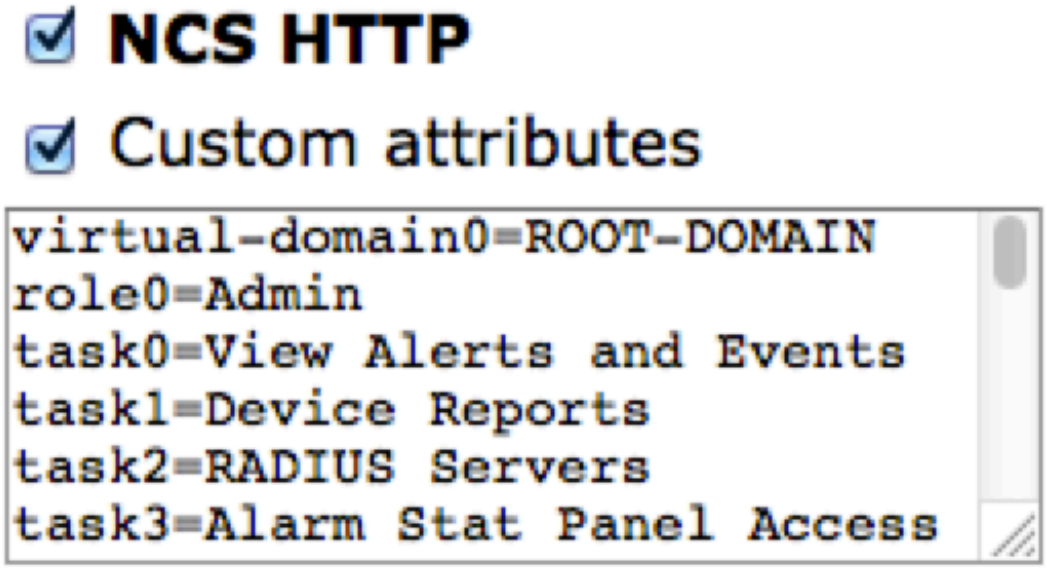
Paso 1. Inicie sesión en la **GUI de ACS Admin** y navegue hasta la **configuración de la interfaz** > la página **TACACS+**.

Paso 2. Cree un nuevo servicio para prime. Este ejemplo muestra un nombre de servicio configurado con el nombre **NCS**, como se muestra en la imagen:

**New Services**

| | | Service | Protocol |
|---|---|---|---|
| ☑ | ☐ | ciscowlc | common |
| ☑ | ☐ | Wireless-WCS | HTTP |
| ☑ | ☐ | NCS | HTTP |
| ☐ | ☐ | | |
| ☐ | ☐ | | |

Paso 3. Agregue todos los atributos del bloc de notas creado en el paso 2 a la configuración de usuario o grupo. Asegúrese de agregar atributos de dominio virtual.




Paso 4. Click OK.

## Verificación

Inicie sesión en prime con el nuevo nombre de usuario que creó y confirme que tiene la función **Admin**.

## Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

Revise usermgmt.log desde la CLI de la raíz principal disponible en el directorio **/opt/CSCOlumos/logs**. Verifique si hay algún mensaje de error.

```
2016-05-12 15:24:18,517 [http-bio-443-exec-10] DEBUG usermgmt - [        [TacacsLoginModule]
user entered username: 138527]
2016-05-12 15:24:18,517 [http-bio-443-exec-10] DEBUG usermgmt - [        [TacacsLoginModule]
Primary server=172.18.70.243:49]
2016-05-12 15:24:18,517 [http-bio-443-exec-10] DEBUG usermgmt - Thread Id : [835], Entering
Method : [login], Class : [com.cisco.xmp.jaas.tacacs.TacacsLoginClient].
2016-05-12 15:24:18,517 [http-bio-443-exec-10] DEBUG usermgmt - Thread Id : [835], Entering
Method : [login], Class : [com.cisco.xmp.jaas.tacacs.SecondaryTacacsLoginClient].
2016-05-12 15:24:18,518 [http-bio-443-exec-10] INFO  usermgmt - [Tacacs:connectTacacs()] :
[prepare to ping TACACS+ server (> 0):/172.18.70.243 (-1)].
2016-05-12 15:24:18,619 [http-bio-443-exec-10] INFO  usermgmt - [Tacacs:connectTacacs()] :
[Tacacs: Num of ACS is  3].
2016-05-12 15:24:18,619 [http-bio-443-exec-10] INFO  usermgmt - [Tacacs:connectTacacs()] :
[Tacacs:activeACSIndex is  0].
2016-05-12 15:24:18,619 [http-bio-443-exec-10] INFO  usermgmt - [Tacacs:connectTacacs()] :
[Tacacs: Unable to connect to Server 2: /172.18.70.243 Reason: Connection refused].
2016-05-12 15:24:18,619 [http-bio-443-exec-10] DEBUG usermgmt - [        [Thu May 12 15:24:18
EST 2016] [TacacsLoginModule] exception in client.login( primaryServer, primaryPort,seconda..:
com.cisco.xmp.jaas.XmpAuthenticationServerException: Server Not Reachable: Connection refused]
```

Este ejemplo muestra un ejemplo de mensaje de error, que podría deberse a varias razones, como la conexión rechazada por un firewall, o cualquier dispositivo intermedio, etc.