

Integración del ACS versión 5.x con el ejemplo de configuración WAAS

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Configuración ACS](#)

[Configuración en el WAAS](#)

[Verificación](#)

[Troubleshooting](#)

Introducción

Este documento describe cómo configurar la integración del Wide Area Application Services de Cisco (WAAS) con la versión 5.x del Access Control Server de Cisco (ACS). Cuando están configurados por los pasos en este documento, los usuarios pueden autenticar a WAAS con las credenciales TACACS+ vía el ACS.

Prerequisites

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

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

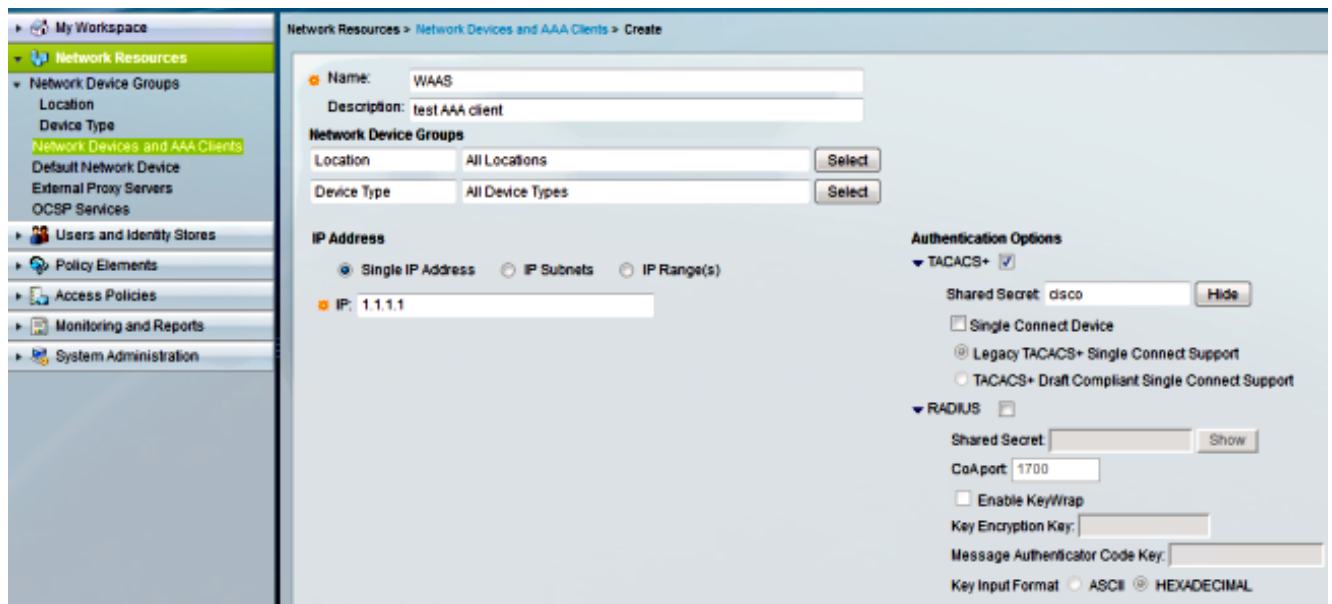
- Versión 5.x del Cisco Secure ACS
- Cisco WAAS

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 la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configurar

Configuración ACS

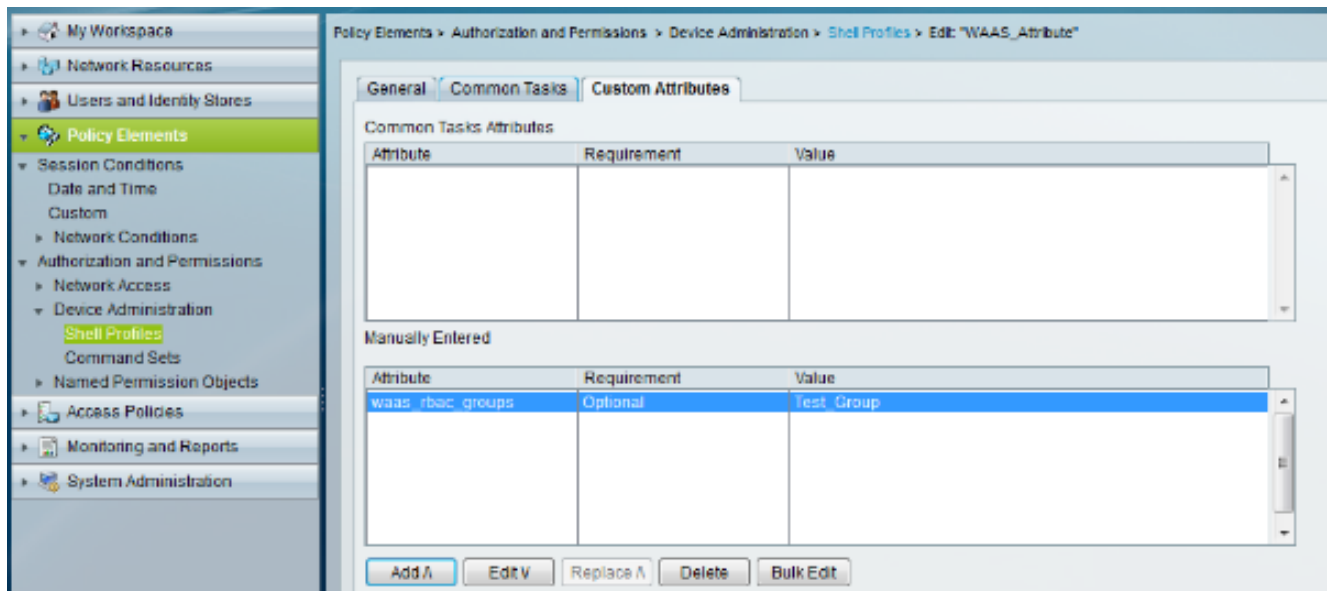
1. Para definir a un cliente AAA en el ACS versión 5.x, navegue a los **recursos de red > a los dispositivos de red y a los clientes AAA**. Configure al cliente AAA con un nombre descriptivo, una sola dirección IP, y una clave secreta compartida para el TACACS+.



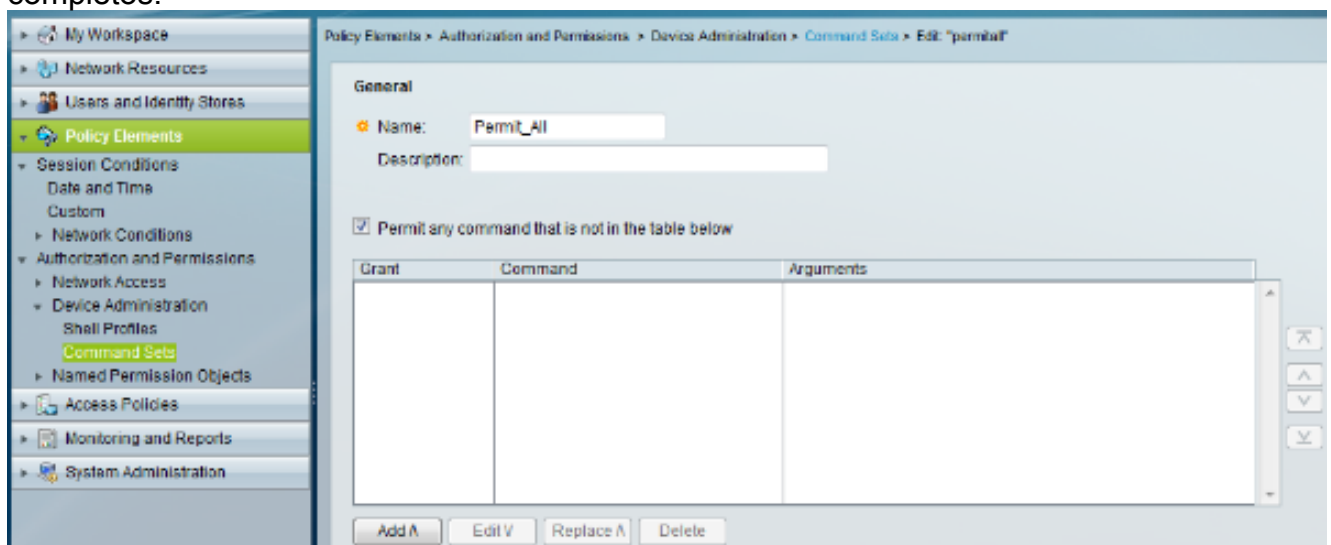
The screenshot shows the 'Create' page for a new AAA client in the ACS 5.x interface. The left sidebar contains a navigation menu with 'Network Resources' expanded. The main content area is titled 'Network Resources > Network Devices and AAA Clients > Create'. The form includes the following fields and options:

- Name:** WAAS
- Description:** test AAA client
- Network Device Groups:**
 - Location:** All Locations (with a 'Select' button)
 - Device Type:** All Device Types (with a 'Select' button)
- IP Address:**
 - Radio buttons for **Single IP Address** (selected), **IP Subnets**, and **IP Range(s)**.
 - IP:** 1.1.1.1
- Authentication Options:**
 - TACACS+:** Checked. Includes a **Shared Secret** field with the value 'disco' and a 'Hide' button.
 - Single Connect Device
 - Legacy TACACS+ Single Connect Support
 - TACACS+ Draft Compliant Single Connect Support
 - RADIUS:** Unchecked. Includes a **Shared Secret** field with a 'Show' button, a **CoAport** field with the value '1700', Enable KeyWrap, a **Key Encryption Key** field, a **Message Authenticator Code Key** field, and a **Key Input Format** section with ASCII and HEXADECIMAL.

2. Para definir un perfil del shell, navegue a los **elementos de la directiva > a la autorización y a los permisos > Device Administration (Administración del dispositivo) > los perfiles del shell**. En este ejemplo, un nuevo perfil del shell llamado **WAAS_Attribute** se configura. Este atributo personalizado se envía al WAAS, que permite que deduzca qué grupo de usuarios es el Grupo del administrador. Configure estos atributos personalizados:
El atributo es waas_rbac_groups. El requisito es opcional de modo que no perturbe ningún otro dispositivo. El valor es el nombre del grupo que debe ser asignado el acceso administrativo (grupo de prueba).

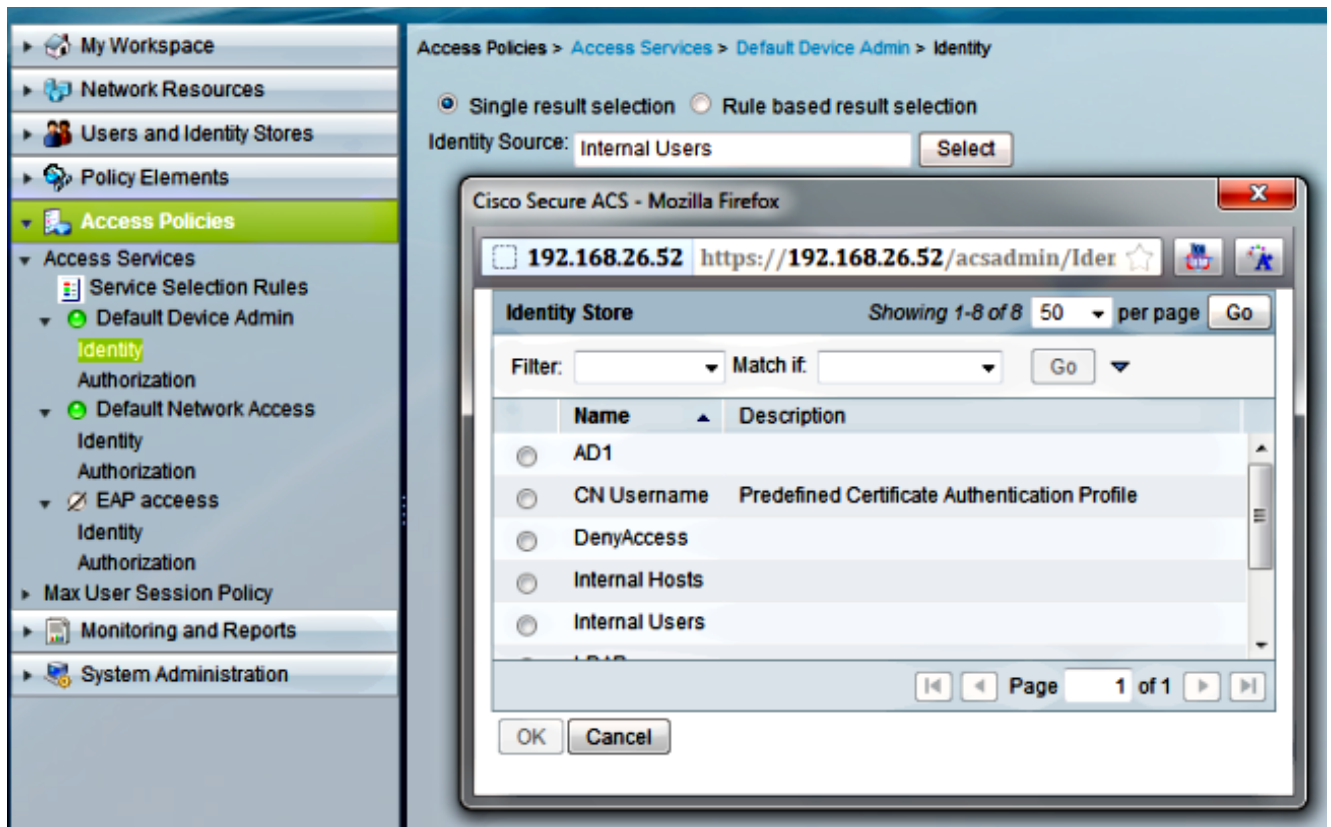


3. Para definir un comando set de permitir los comandos all, navegue a los **elementos de la directiva > a la autorización y a los permisos > Device Administration (Administración del dispositivo) > los comandos establece**.
 Edite el comando set de **Permit_All**. Si usted marca el comando **permit any** que no está en la **tabla debajo de** casilla de verificación, conceden el usuario los privilegios completos.

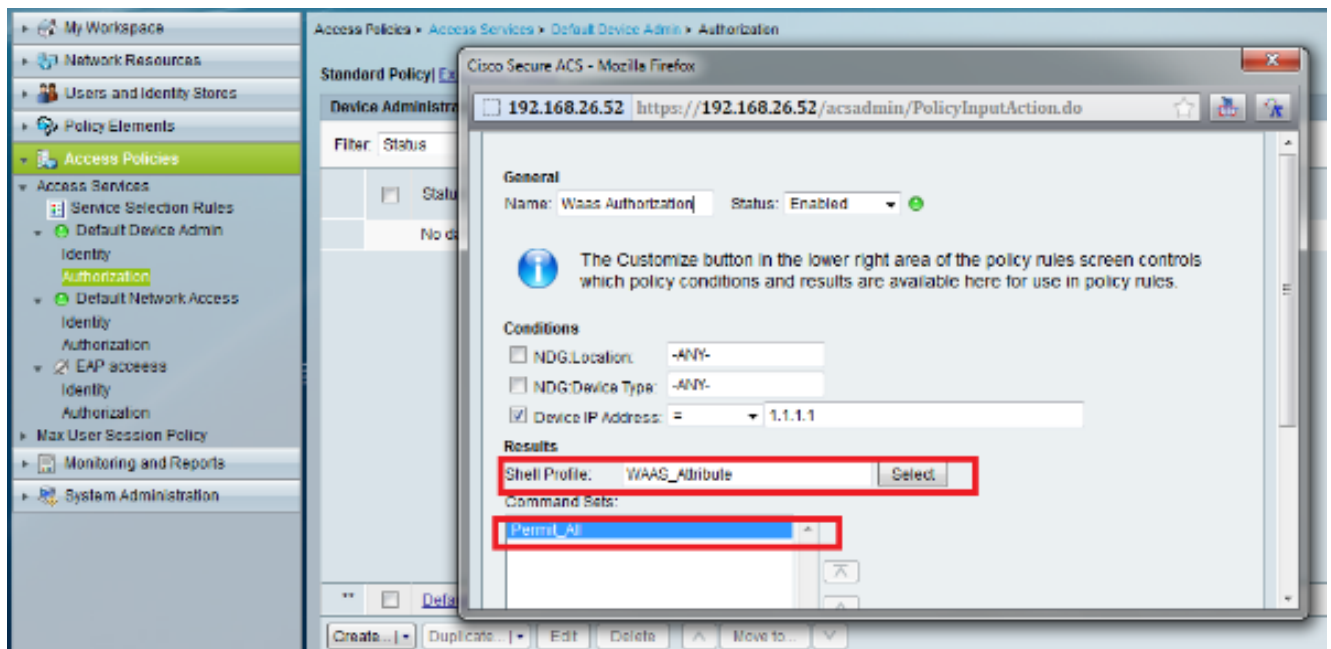


Note: Puesto que este ejemplo utiliza el TACACS, el servicio predeterminado seleccionado es el **dispositivo predeterminado admin**.

4. Para señalar la identidad a la fuente correcta de la identidad, navegue a las **políticas de acceso > a los servicios del acceso > al dispositivo del valor por defecto Admin > identidad**. Si el usuario existe en la base de datos ACS local, seleccione a los **usuarios internos**. Si el usuario existe en el Active Directory, seleccione el almacén configurado de la identidad (**AD1** en este ejemplo).



- Para crear una regla de la autorización, navegue a los servicios de los >Access de las políticas de acceso > al dispositivo del valor por defecto Admin > autorización. Cree una nueva directiva de la autorización llamada **autorización WAAS**. Esto marca para saber si hay peticiones de WAAS. En este ejemplo, el IP del dispositivo se utiliza como condición. Sin embargo, esto se puede cambiar basó en los requisitos del despliegue. Aplique el perfil y a los comandos establece del shell configurados en los pasos 2 y 3 en esta sección.



Configuración en el WAAS

- Para definir un servidor TACACS+, navegue a los dispositivos >> Security (Seguridad) del administrador del sistema del name> <Central> de la configuración >AAA > TACACS+. Configure la dirección IP y la clave previamente compartida del servidor ACS.

Devices > pi-wavecm01 > Configure > Security > AAA > TACACS+

TACACS+ Server Settings for Central Manager, [redacted] Print Apply Defaults Remove Settings

TACACS+ Server Settings

Use ASCII Password Authentication:

Time to Wait: (seconds) (1-20)

Number of Retransmits: (1-3)

Security Word:

Primary Server: Primary Server Port:

Secondary Server: Secondary Server Port:

Tertiary Server: Tertiary Server Port:

* To use TACACS+ for Login or Configuration Authentication, please go to the Authentication Methods page.

2. Para modificar los métodos de autenticación y autorización, navegue a los **dispositivos >> Security (Seguridad) del administrador del sistema del name <Central >** de la configuración **>AAA > los métodos de autenticación**. En este tiro de pantalla, el método de inicio de sesión primario se configura para el **local** con el secundario configurado para el **TACACS+**.

Devices > pi-wavecm01 > Configure > Security > AAA > Authentication Methods

Authentication and Authorization Methods for Central Manager, pi-wave... Print Apply Defaults Remove Settings

Authentication and Authorization Methods

Failover to next available authentication method:

Authentication Login Methods: It is highly recommended to set the auther

Primary Login Method:

Secondary Login Method:

Tertiary Login Method:

Quaternary Login Method:

Authorization Methods:

Primary Configuration Method:


Secondary Configuration Method:

Tertiary Configuration Method:

Quaternary Configuration Method:

3. Navegue **para dirigirse > Admin >AAA > los grupos de usuarios** para agregar el nombre del grupo que hace juego el **valor de atributo personalizado** (véase el paso 2 en la sección de la configuración ACS) en WAAS.

Home > Admin > AAA > User Groups

Creating New User Group 

User Group Information

Name:




Comments

Note: * - Required Field

4. Asigne las derechas de este admin-nivel del grupo (Test_Group) en el **hogar > el Admin > AAA >** lengüeta de la **Administración del papel de los grupos de usuarios**. El papel admin en el administrador central se preconfigura.



Home > Admin > AAA > User Groups

External User Group Management **Role Management** Domain Management

 Refresh Table  Assign all Roles  Remove all Roles

Roles

Filter: Name Match if: like

Role	
  admin	Admin role

Verificación

Intente iniciar sesión a WAAS con las credenciales TACACS+. Si todo se configura correctamente, le conceden el acceso.

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.