NAC (CCA): Autenticación de la configuración en el Access Manager limpio (CAM) con el ACS

Contenido

Introducción

Este documento describe cómo configurar la autenticación en el Access Manager limpio (CAM) con el Cisco Secure Access Control Server (ACS). Para una configuración similar usando ACS 5.x y posterior, refiera al NAC (CCA): Configure la autenticación en el Access Manager limpio con ACS 5.x y posterior.

prerrequisitos

Requisitos

Esta configuración es aplicable a la versión 3.5 y posterior CAM.

Componentes Utilizados

La información en este documento se basa en la versión 4.1 CAM.

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.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

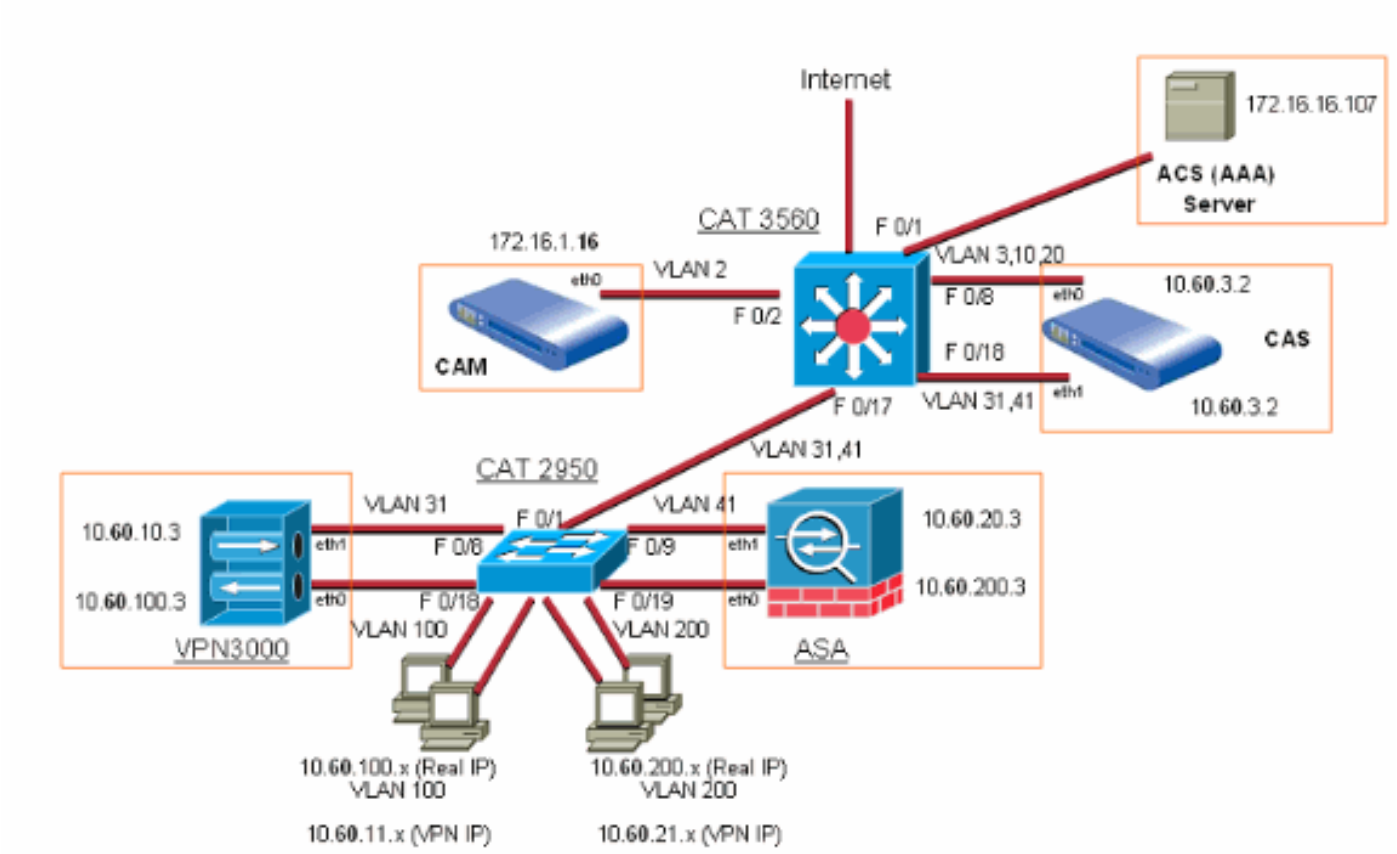
Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Utilice la herramienta Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

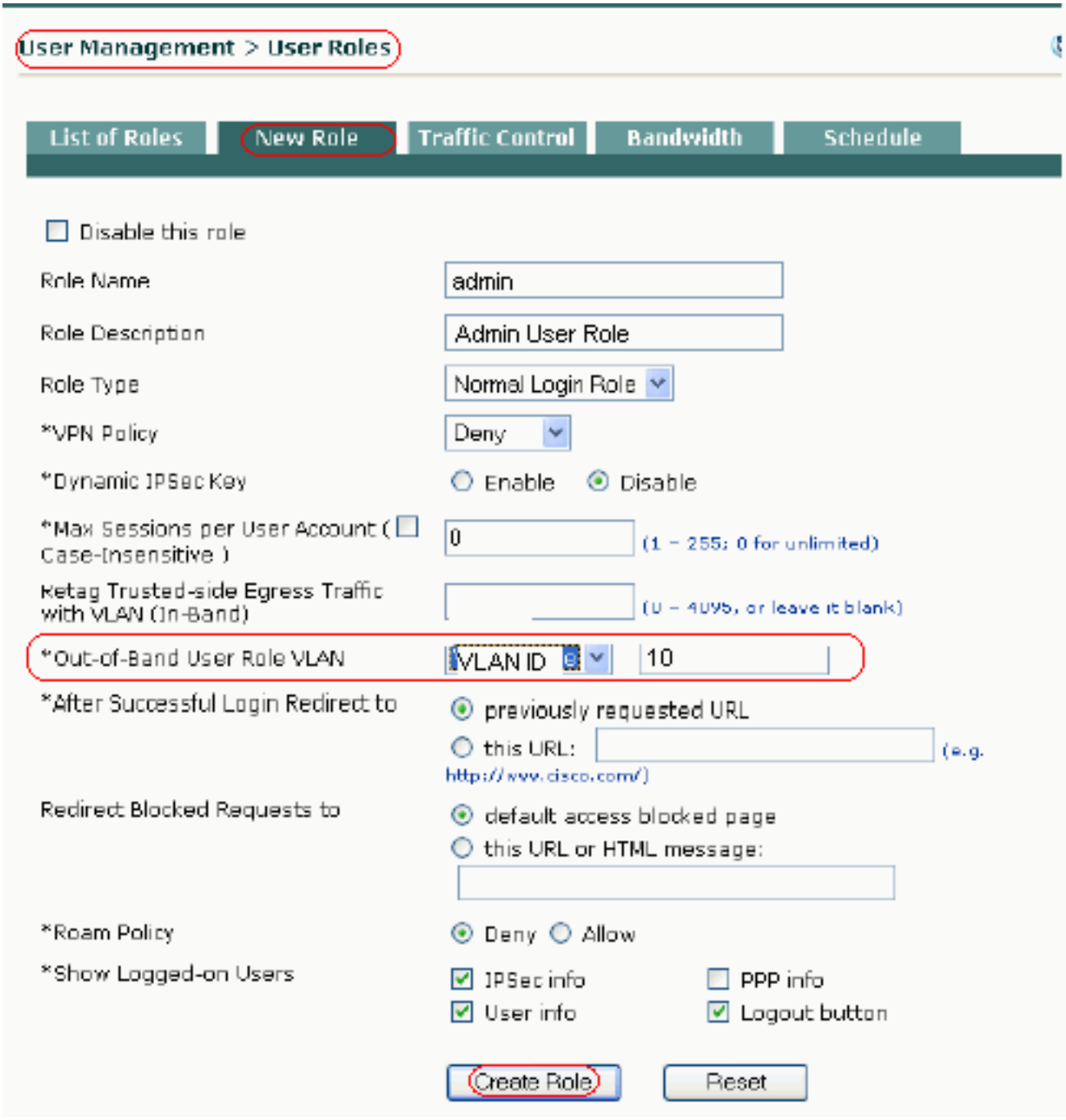
En este documento, se utiliza esta configuración de red:



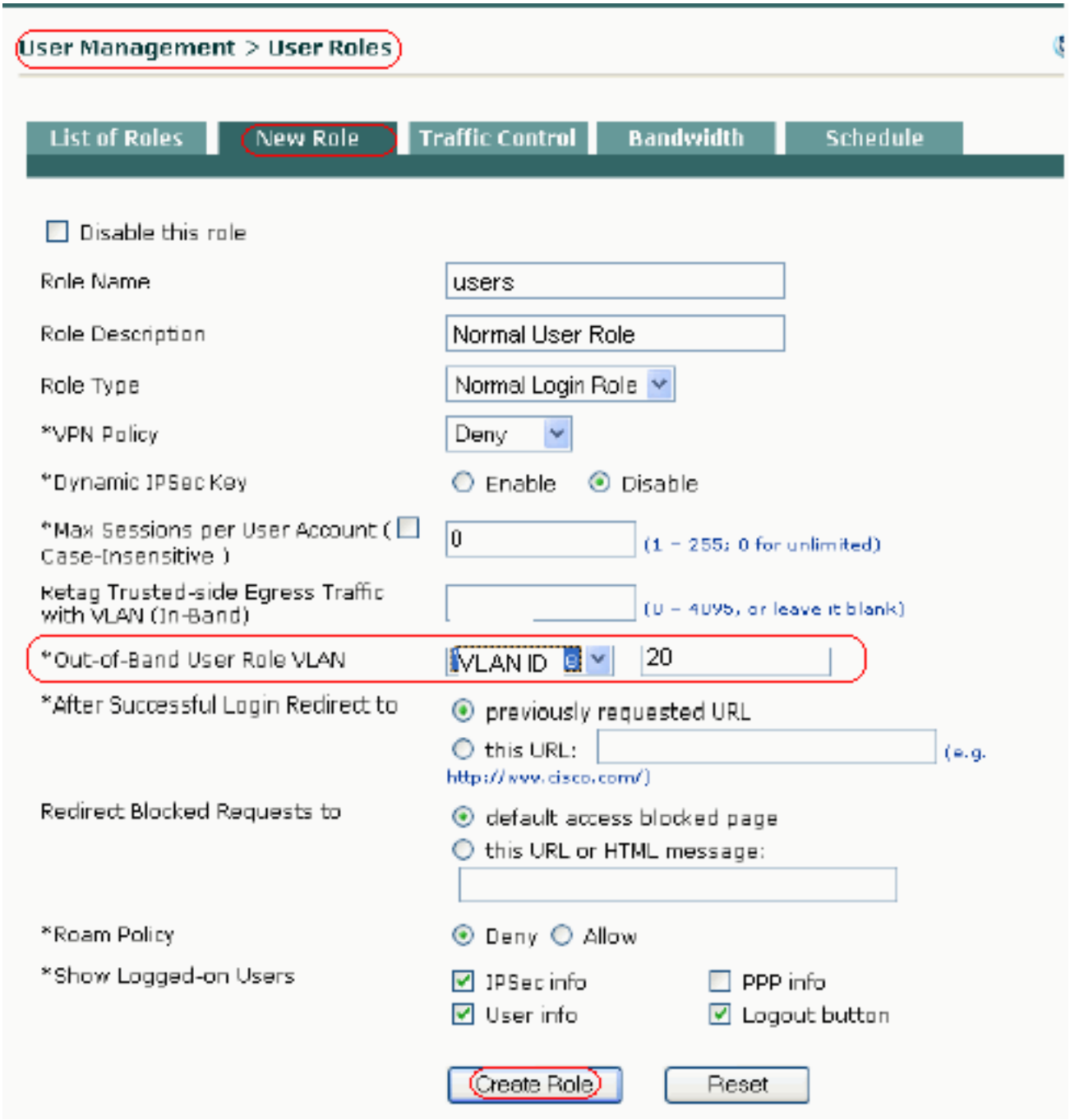
Pasos para configurar la autenticación encendido CCA con el ACS

Complete estos pasos:

1. **Agregue los nuevos papeles Cree un papel Admin**En el CAM, elija **User Management (Administración de usuario) > los rol del usuario > nuevo papel**.

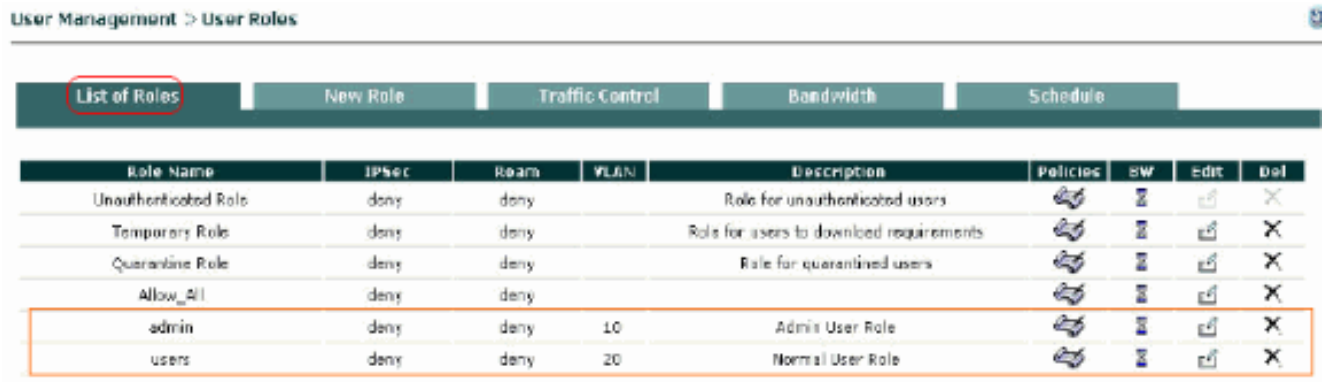


ngrese un nombre único, **admin**, para el papel en el campo de nombre del papel.Ingrese el **papel de Usuario administrador** como descripción opcional del papel.Elija el **papel normal del login** como el tipo del papel.Configure **(OOB) el** rol del usuario **fuera de banda del** VLA N con el VLA N apropiado. Por ejemplo, elija el VLAN ID y especifique el ID como 10.Cuando está acabado, el tecleo **crea el papel**. Para restablecer las propiedades predeterminadas en la forma, **restauración del** tecleo.El papel ahora aparece en la lista de lengueta de los papeles tal y como se muestra en de los VLA N de la etiqueta para la sección OOB Papel-basada de las asignaciones.**Cree un rol del usuario**En el CAM, elija **User Management (Administración de usuario) > los rol del usuario > nuevo papel**.

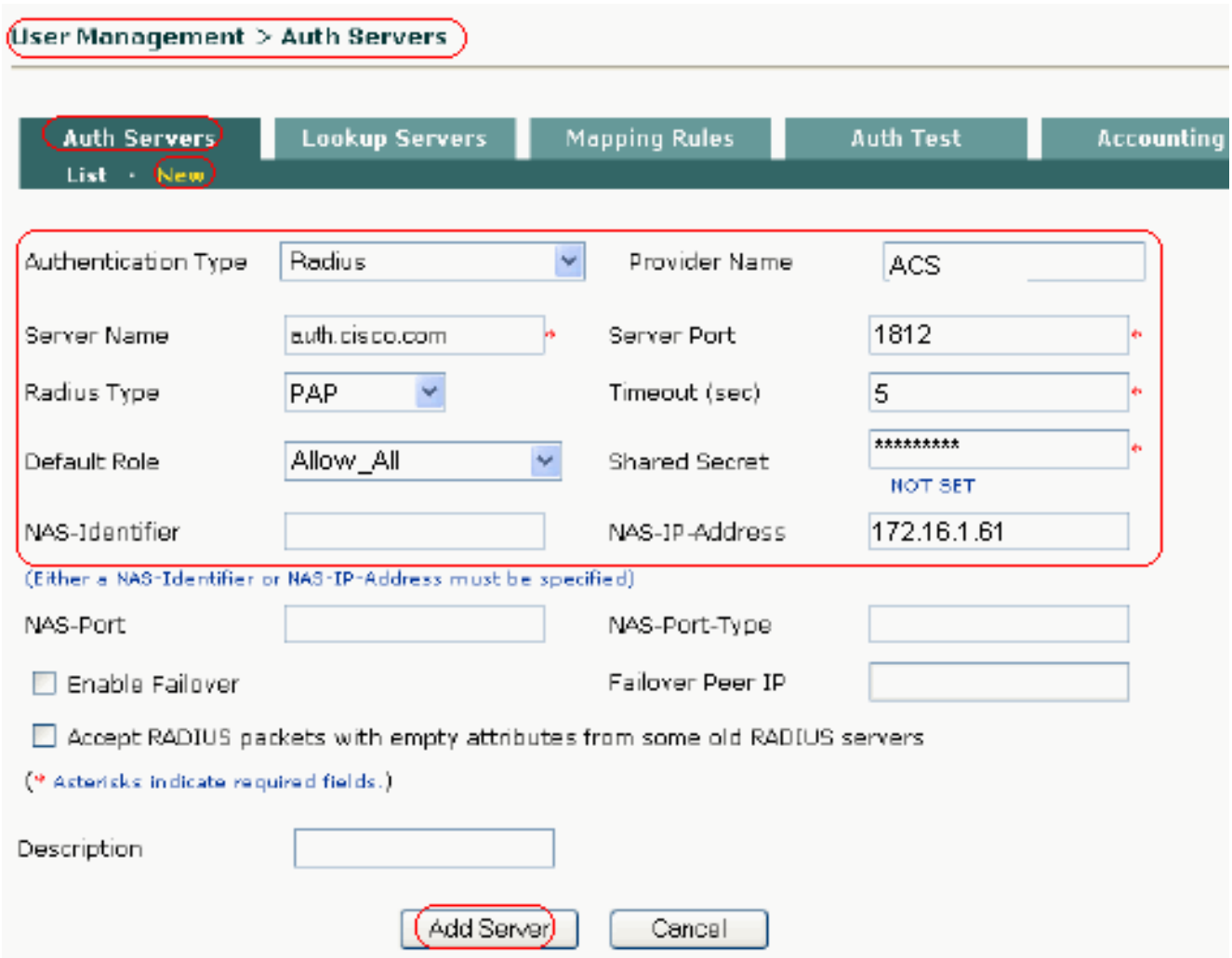


ngrese un nombre único, los **usuarios**, para el papel en el campo de nombre del papel.Ingrese el **papel de usuario normal** como descripción opcional del papel.Configure **(OOB) el** rol del usuario **fuera de banda del** VLA N con el VLA N apropiado. Por ejemplo, elija el VLAN ID y especifique el ID como 20.Cuando está acabado, el tecleo **crea el papel**. Para restablecer las propiedades predeterminadas en la forma, **restauración del** tecleo.El papel ahora aparece en la lista de lengueta de los papeles tal y como se muestra en de los VLA N de la etiqueta para la sección OOB Papel-basada de las asignaciones.

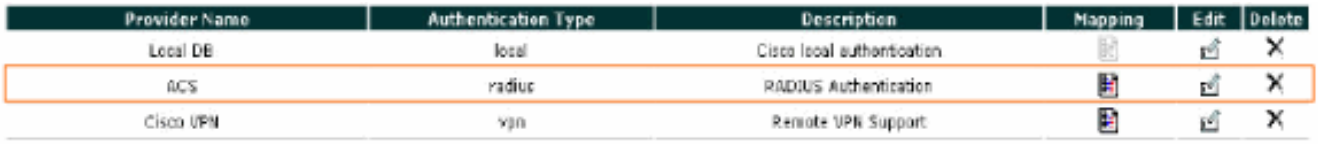
2. **VLA N de la etiqueta para las asignaciones OOB Papel-basadas**En el CAM, elija **User Management (Administración de usuario) > los rol del usuario > lista de papeles** para ver la lista de papeles hasta
ahora.



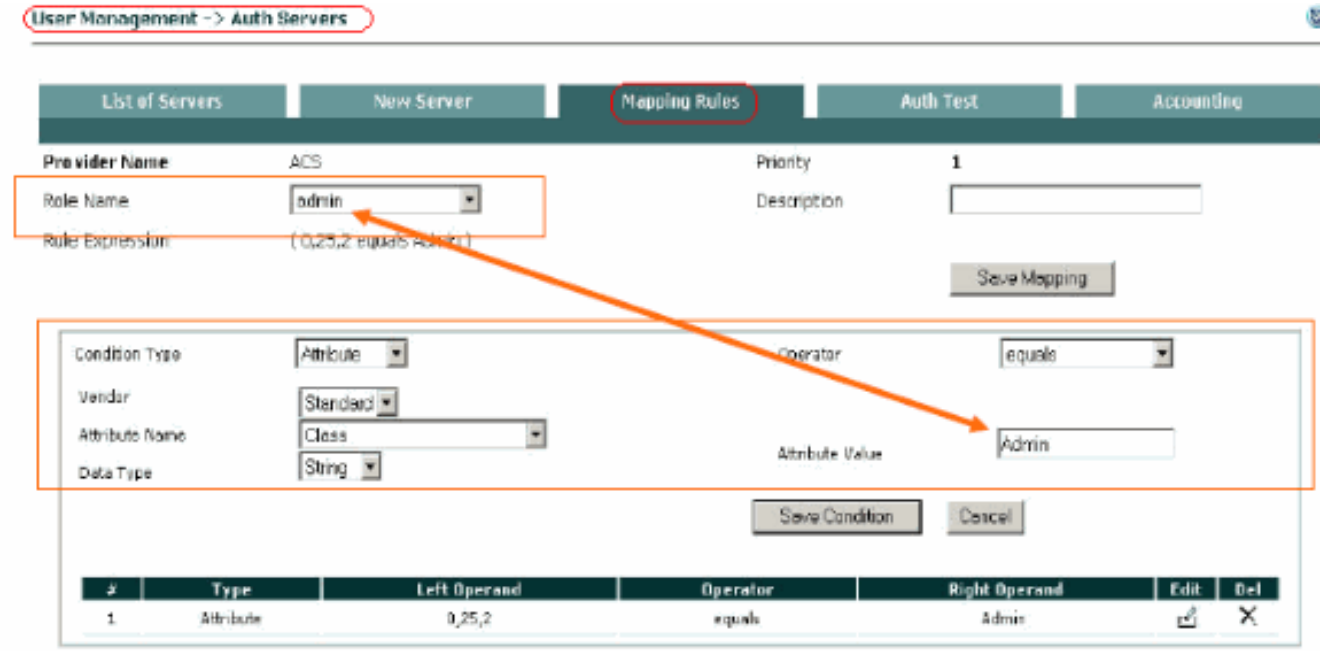
3. **Agregue al servidor de autenticación RADIUS (el ACS)**Elija **User Management (Administración de usuario) > los servidores de autenticación > nuevo**.



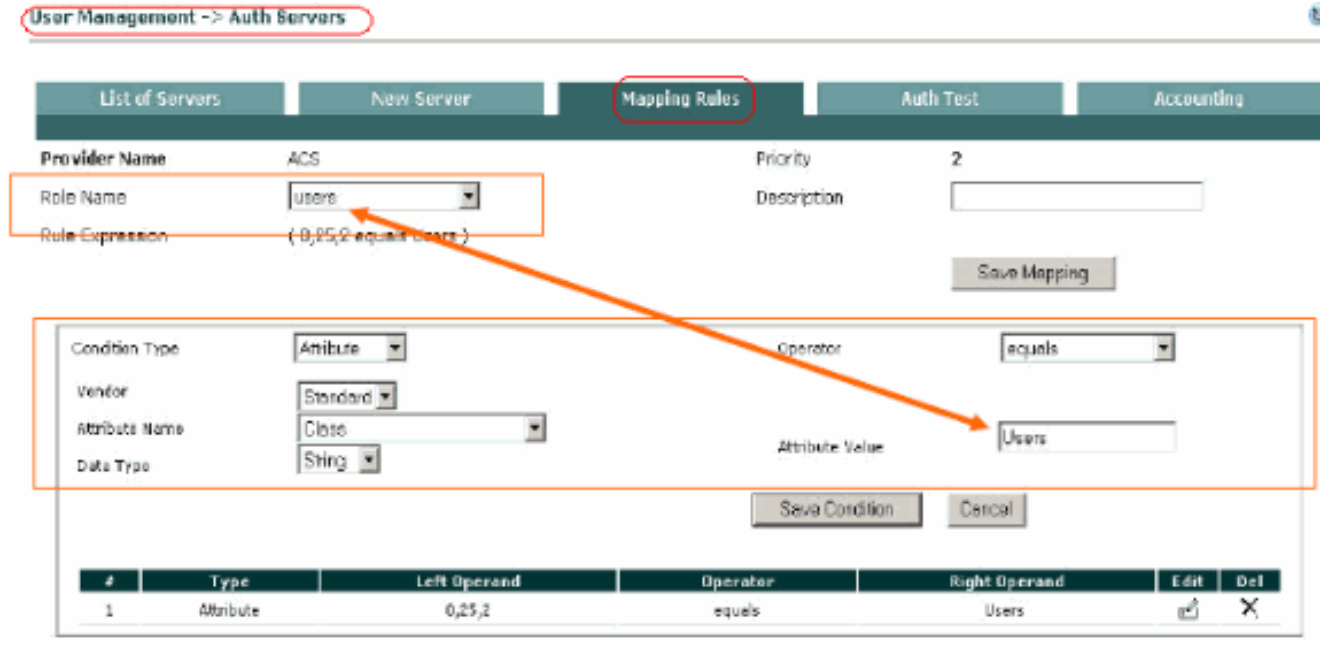
Del menú desplegable del tipo de autenticación, elija el **radio**.Ingrese el nombre del proveedor como **ACS**.Ingrese Nombre del servidor como **auth.cisco.com**.**Puerto de servidor** — El número del puerto **1812** en el cual el servidor de RADIUS está escuchando.**Tipo del radio** — El método de autenticación de RADIUS. Los métodos aceptados incluyen EAPMD5, el PAP, la GRIETA, el MSCHAP y el MSCHAP2.Se utiliza el **papel predeterminado** si asocia al ACS no se define ni se fija correctamente, o si el atributo de RADIUS no se define ni se fija correctamente en el ACS.**Secreto compartido** — El límite del secreto compartido RADIUS a la dirección IP del cliente especificado.**Nas-ip-address** — Este valor que se enviará con todos los paquetes de la autenticación de RADIUS.El tecleo **agrega el servidor**.



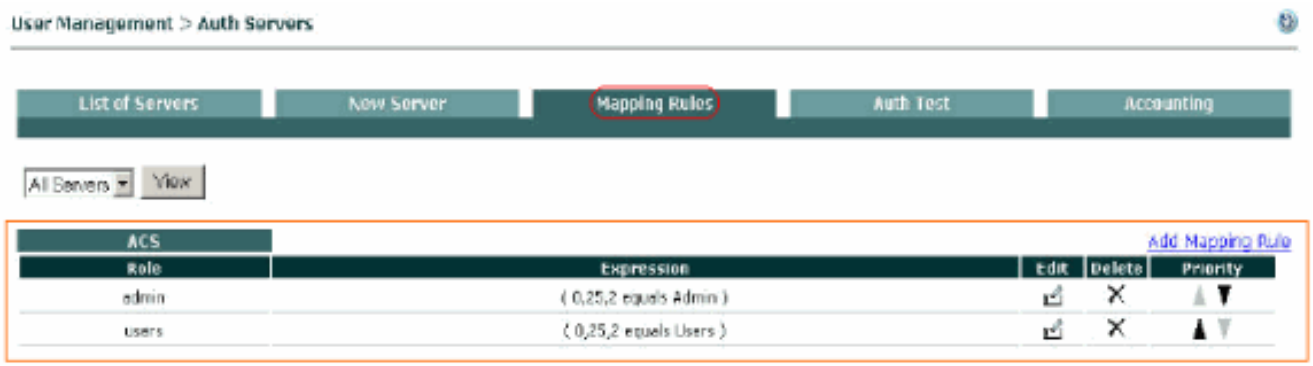
4. **Usuarios de ACS del mapa CCA a los rol del usuario**Elija **User Management (Administración de usuario) > los servidores de autenticación > las reglas de la asignación > Add que asocian el link** para asociar al Usuario administrador en el ACS CCA al papel de Usuario administrador.



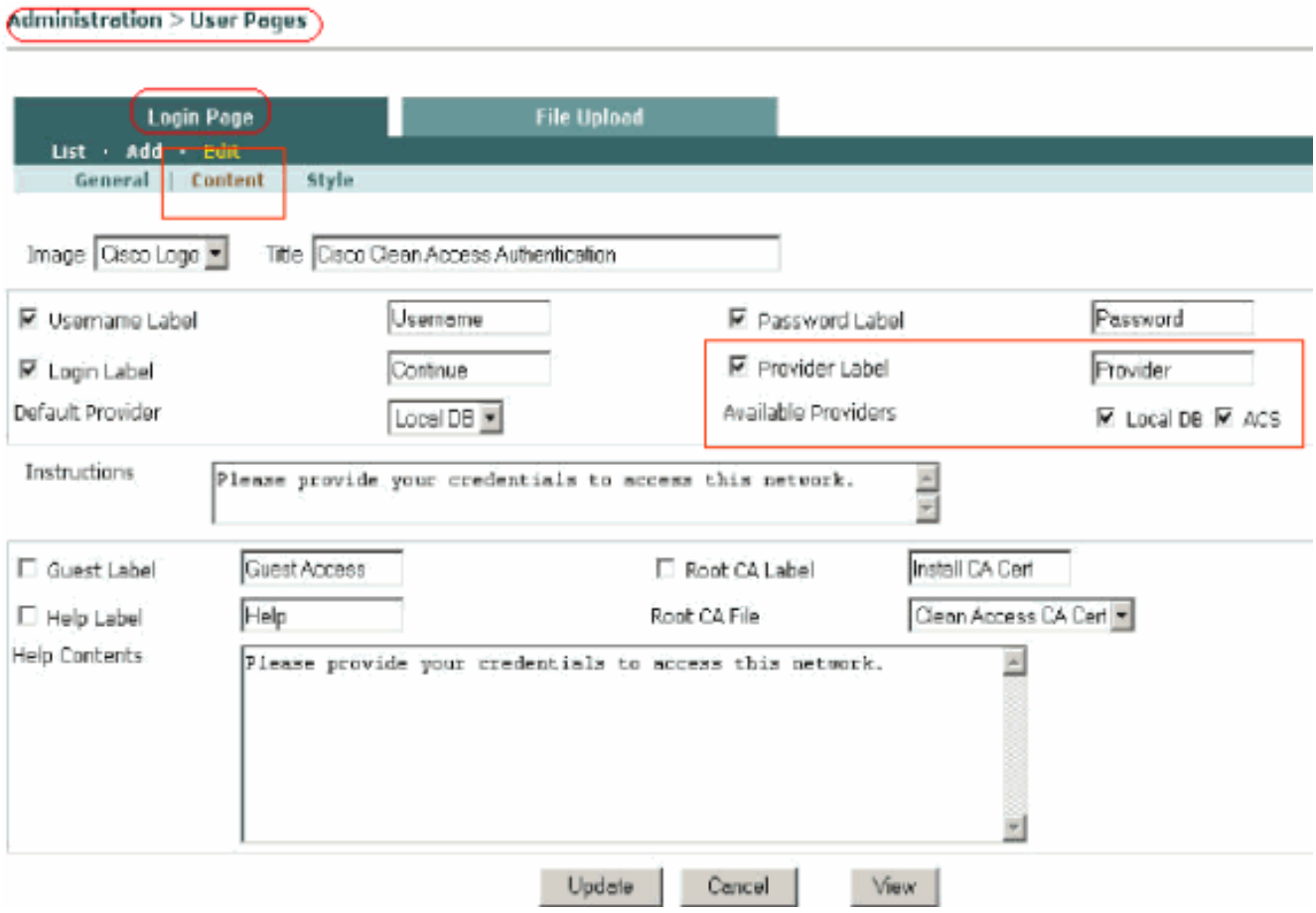
Elija **User Management (Administración de usuario) > los servidores de autenticación > las reglas de la asignación > Add que asocian el link** para asociar al usuario normal en el ACS CCA al rol del
usuario.



Aquí está el rol del usuario del resumen de la asignación:

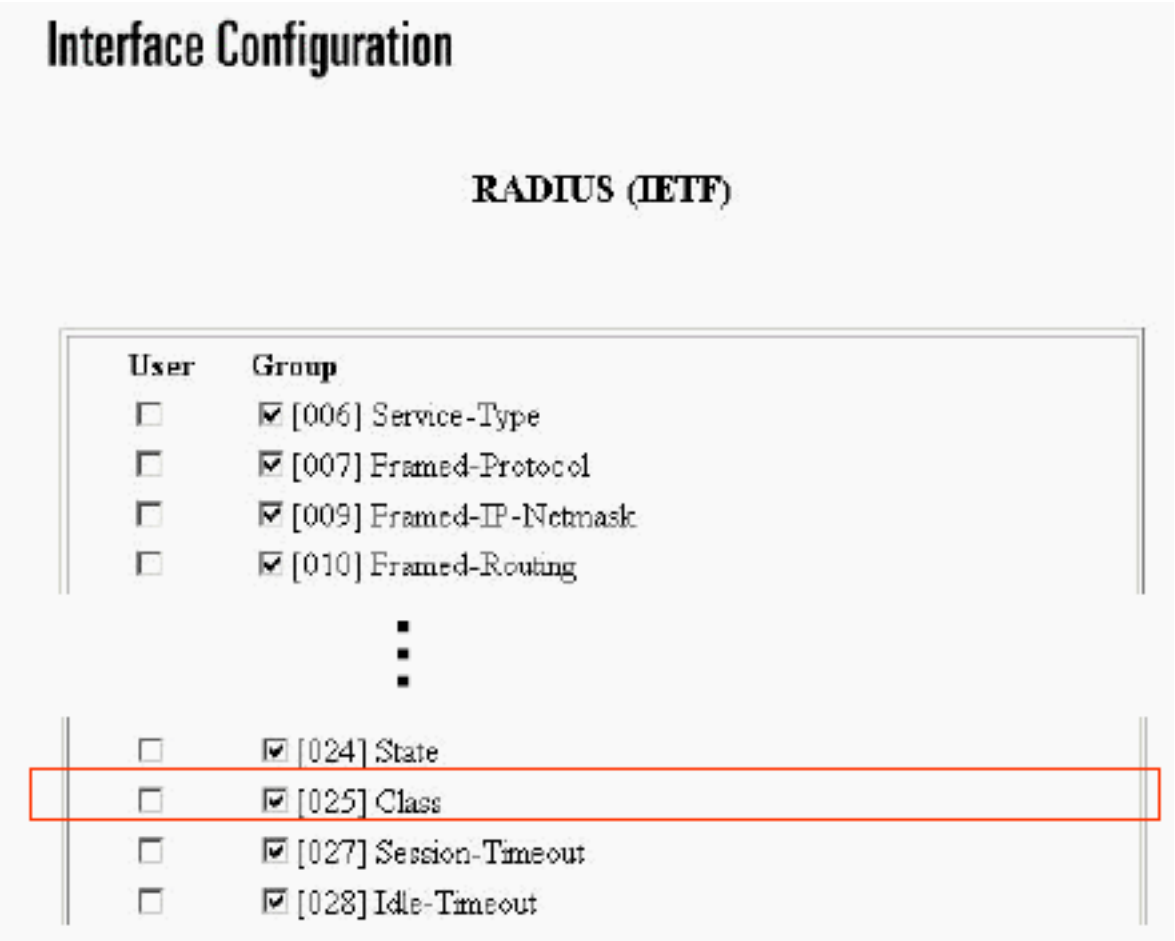


5. **Proveedores alternos del permiso en la página del usuario**Elija la **administración > las páginas del usuario > la página de registro > Add > contenido** para habilitar los proveedores alternos en la página del ingreso del usuario al sistema.



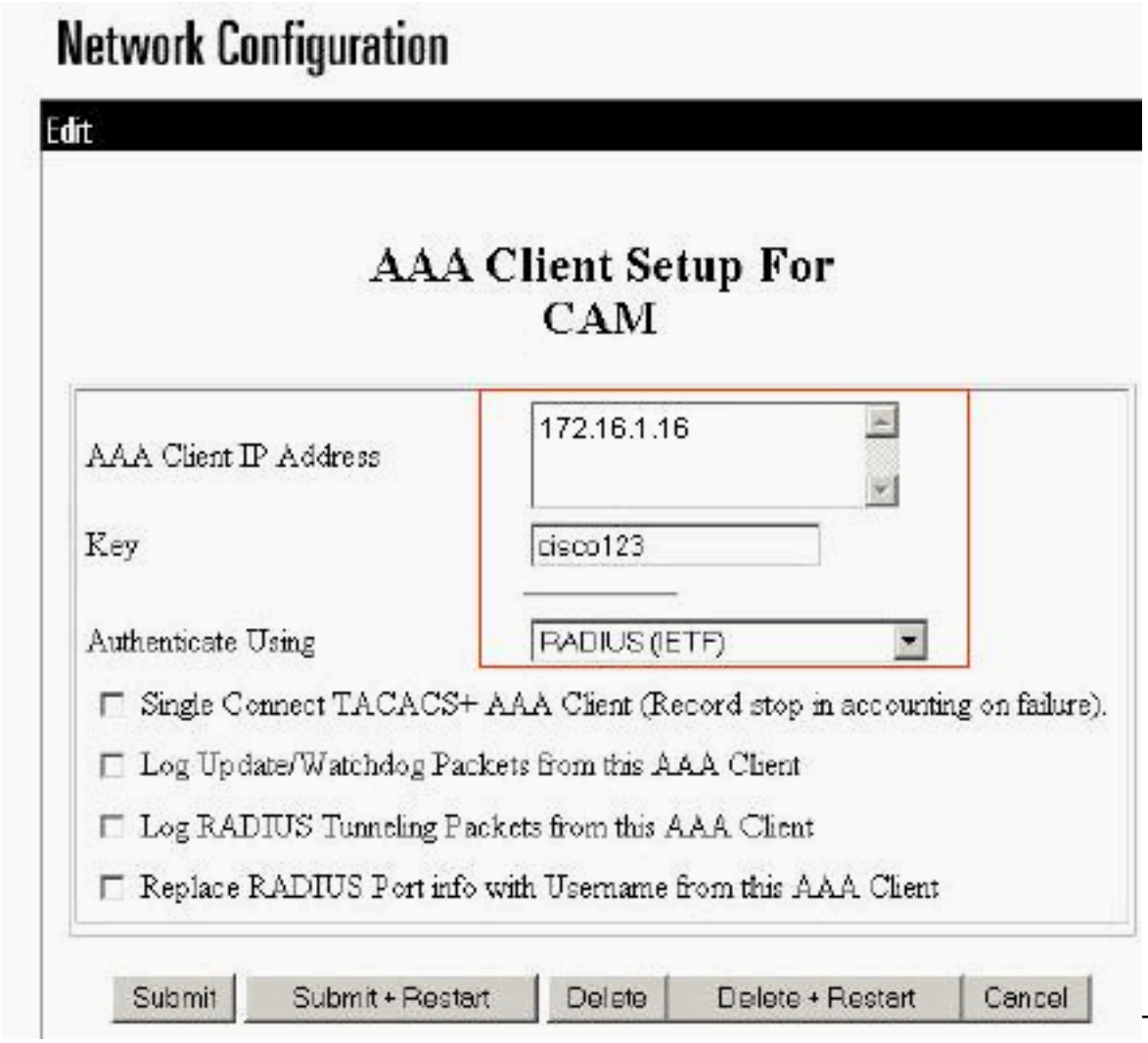
Configuración de ACS

1. Elija la **configuración de la interfaz** para aseegurarse que el atributo de clase [025] RADIUS (IETF) está



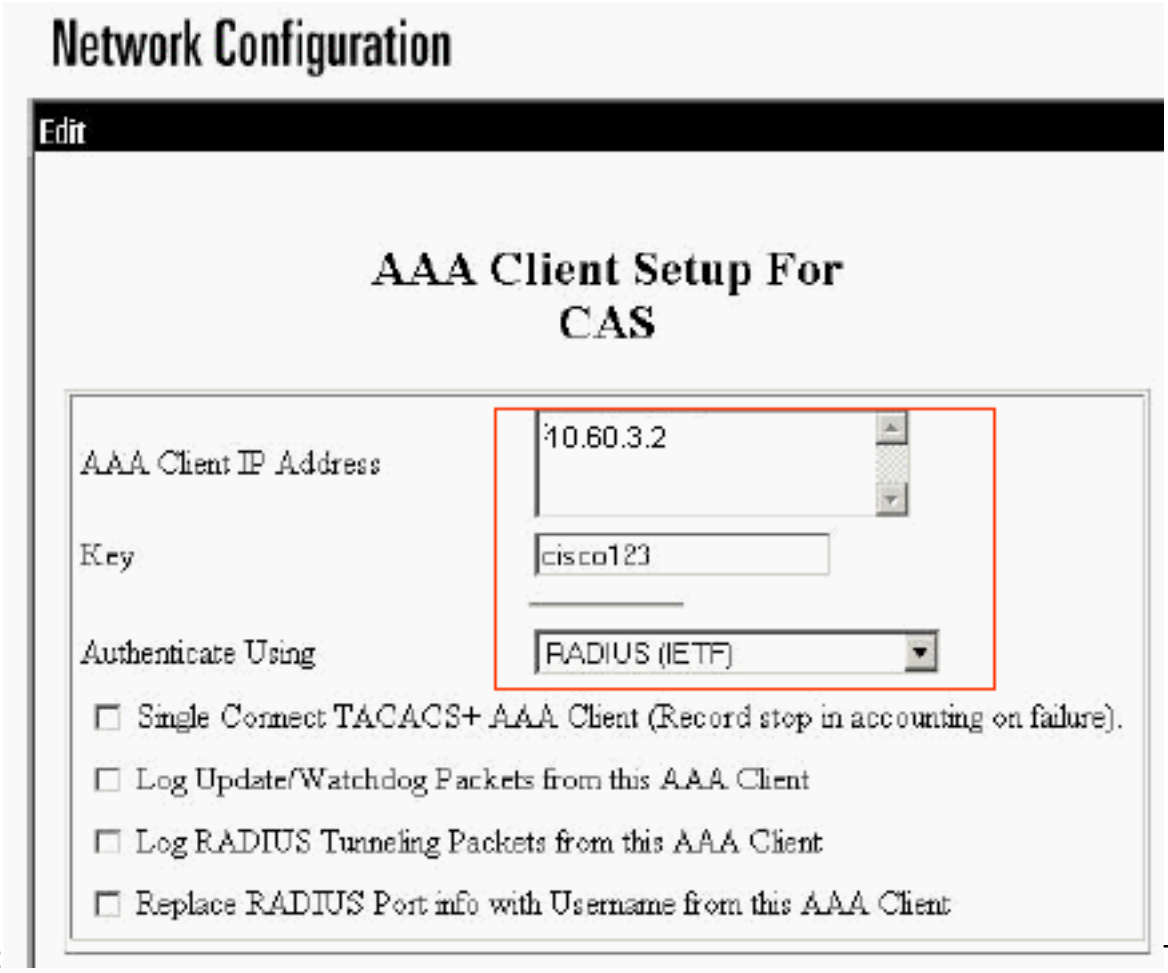
habilitado.

2. **Agregue al cliente RADIUS al servidor ACS**Elija la **configuración de red** para agregar al cliente AAA CAM como se

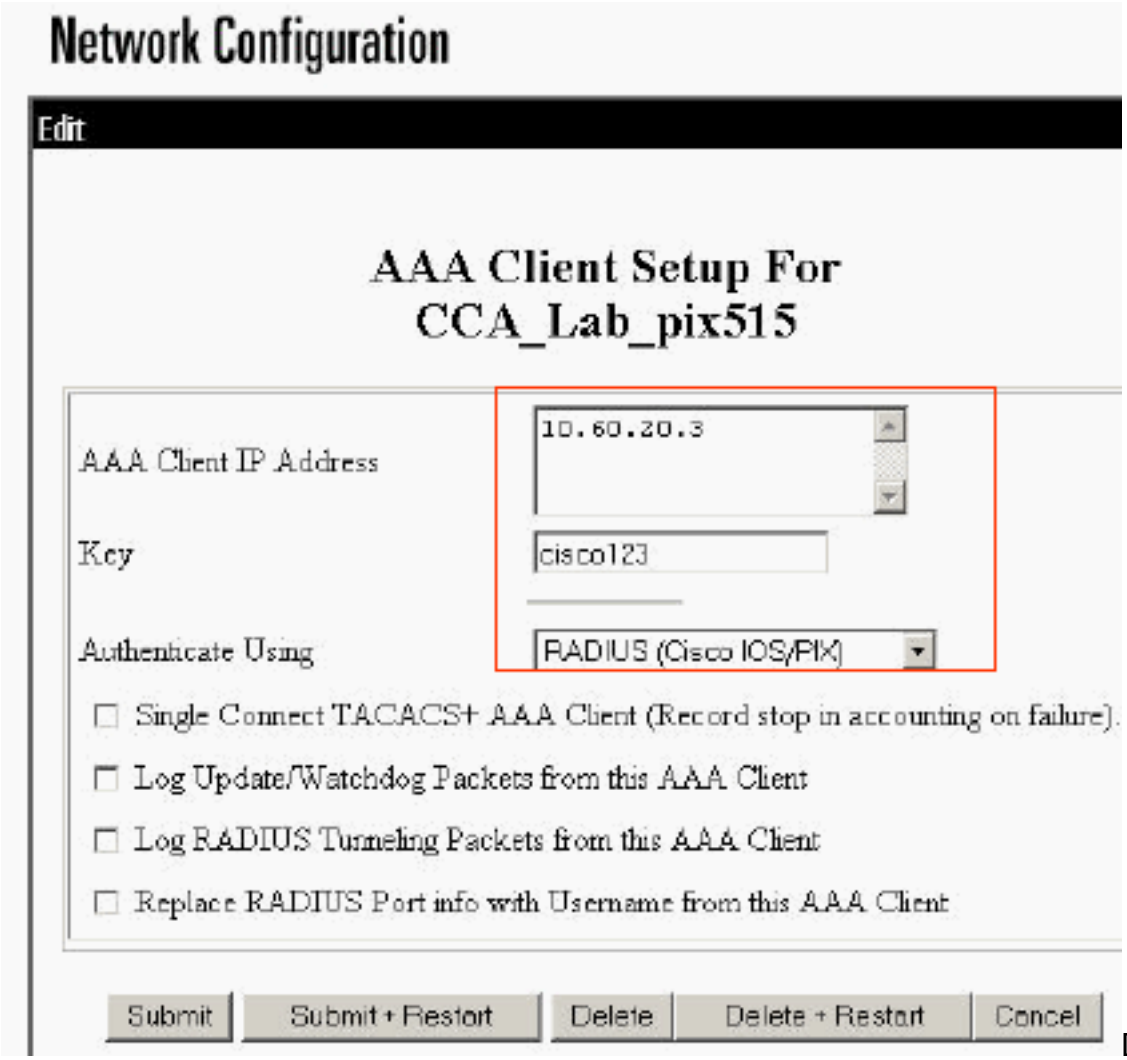


muestra: T

ecleo **Submit + Restart**.**Nota:** Aseegurese que la clave RADIUS hace juego con el cliente AAA y utiliza RADIUS (IETF).Elija la **configuración de red** para agregar al cliente AAA CAS como se

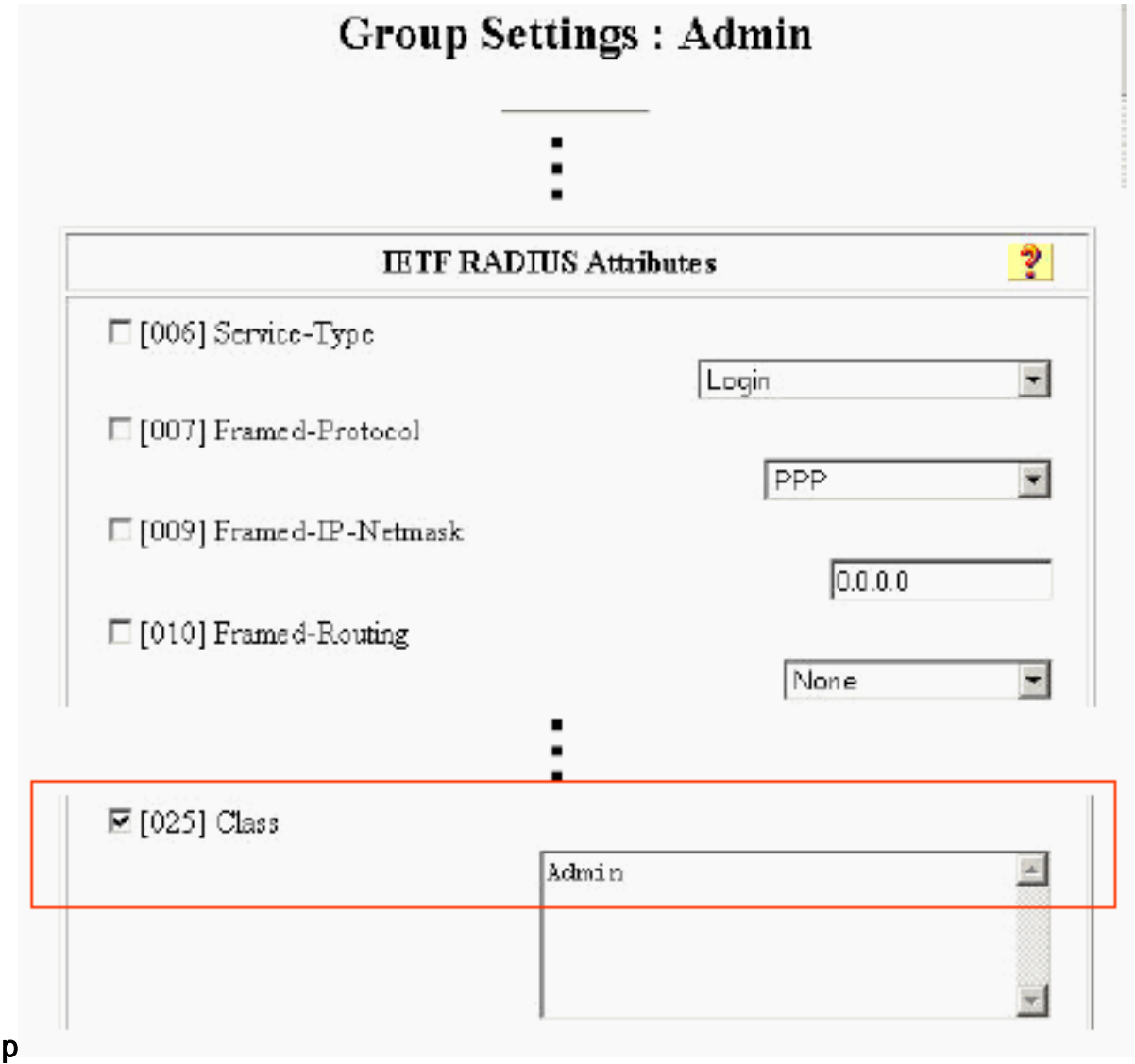


muestra: T ecleo **Submit + Restart**.**Nota:** Para las estadísticas del gateway de VPN RADIUS, CCA la directiva debe permitir que los paquetes de las estadísticas RADIUS (UDP 1646/1813) de la dirección IP de CAS pasen el unauthenticated a la dirección IP del servidor ACS.Elija la **configuración de red** para agregar al cliente AAA ASA como se

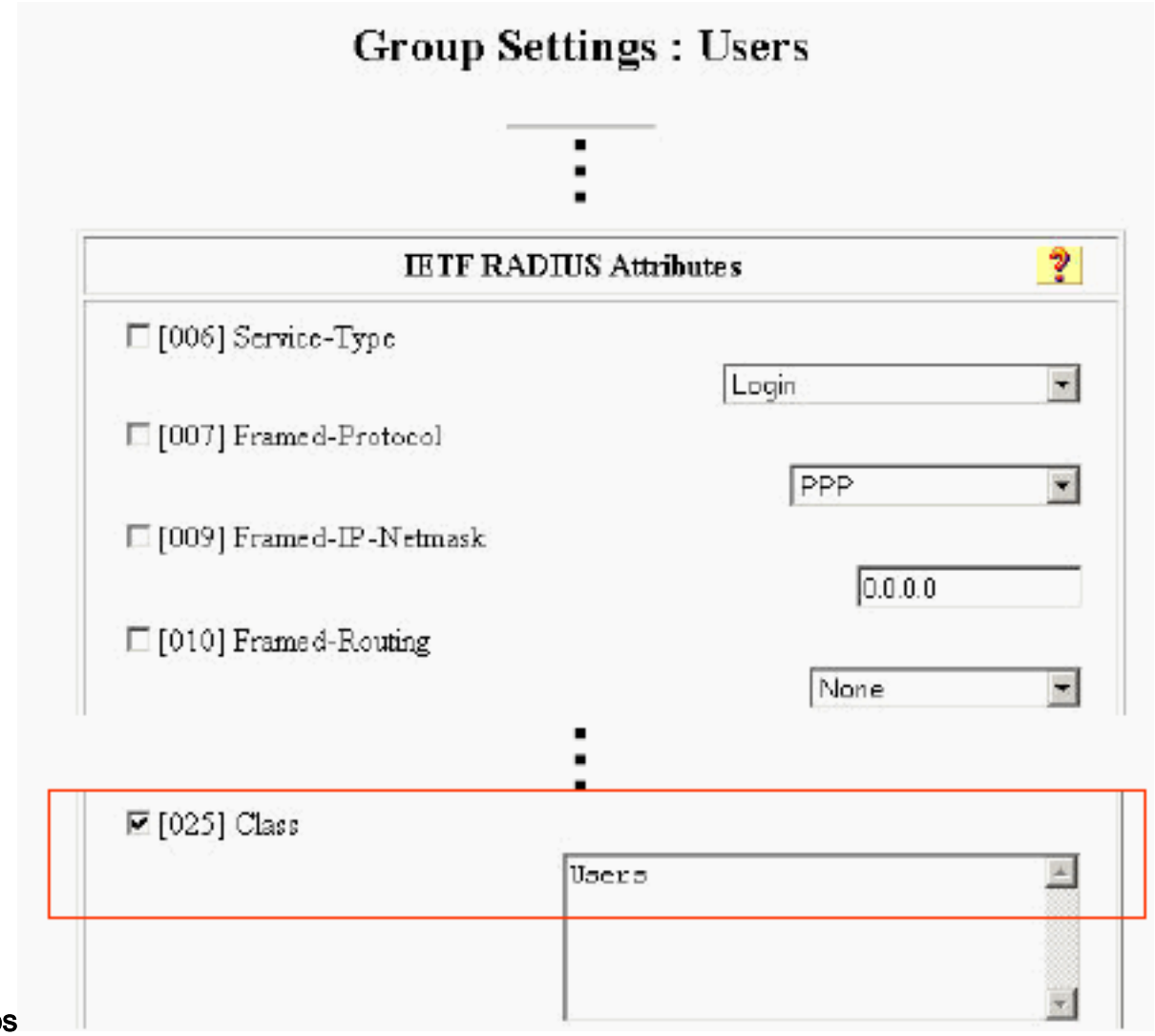


muestra: Direc cionamiento izquierdo de la interfaz del PIX/ASA del usuario (típicamente interfaz interior)Fije el tipo a RADIUS (Cisco IOS/PIX).

3. **Agregue a los grupos de /Configure en el servidor ACSCree el admin**

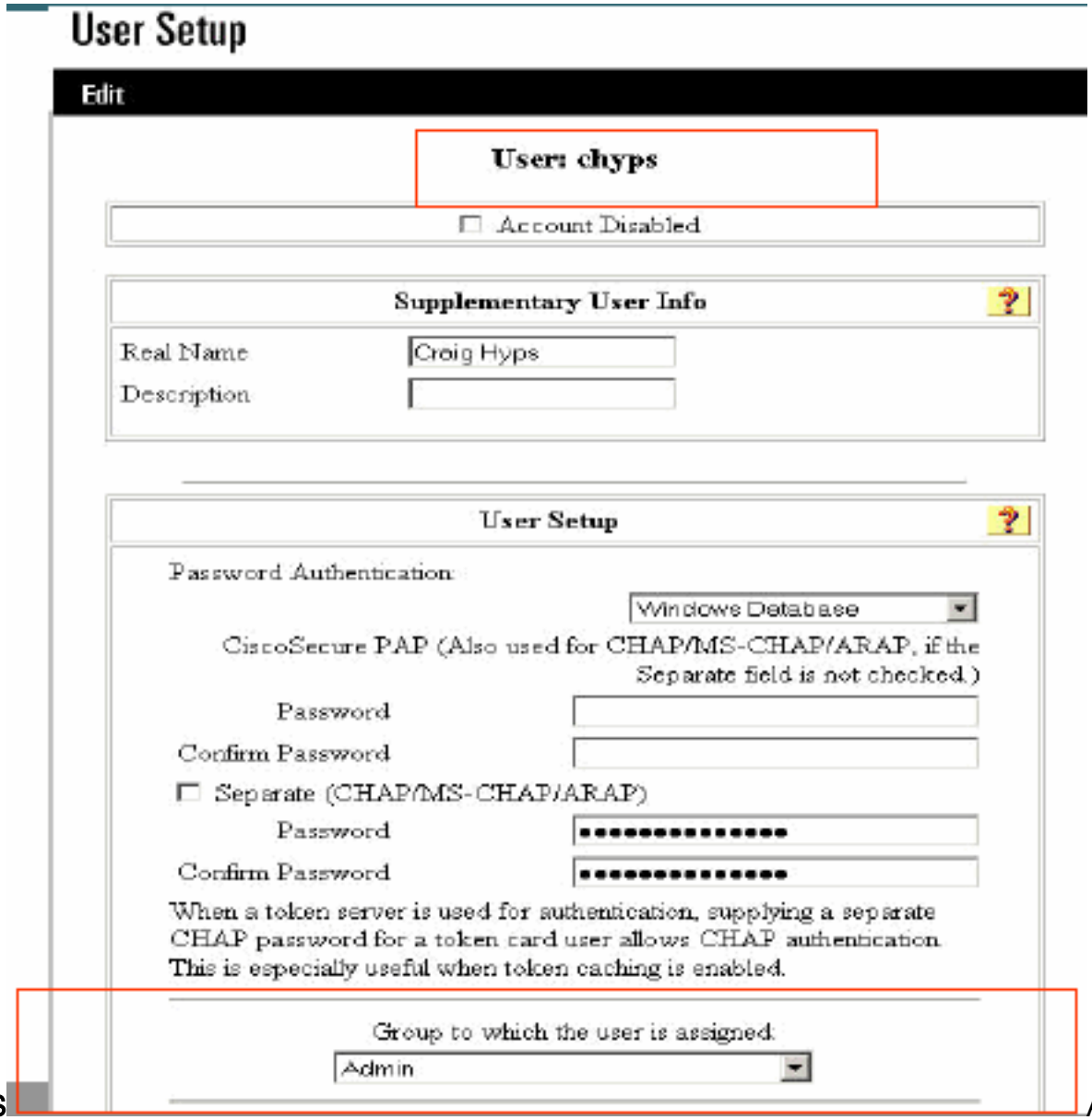


group Fije el atributo de clase [025] del IETF RADIUS para apropiarse del valor de grupo.El valor debe hacer juego eso configurada en asociar de CAS.**Cree al grupo de**



usuarios

Agregue/grupo de la configuración para que cada rol del usuario limpio del acceso sea asociado.**Agregue/los usuarios de la configuración en el servidor**

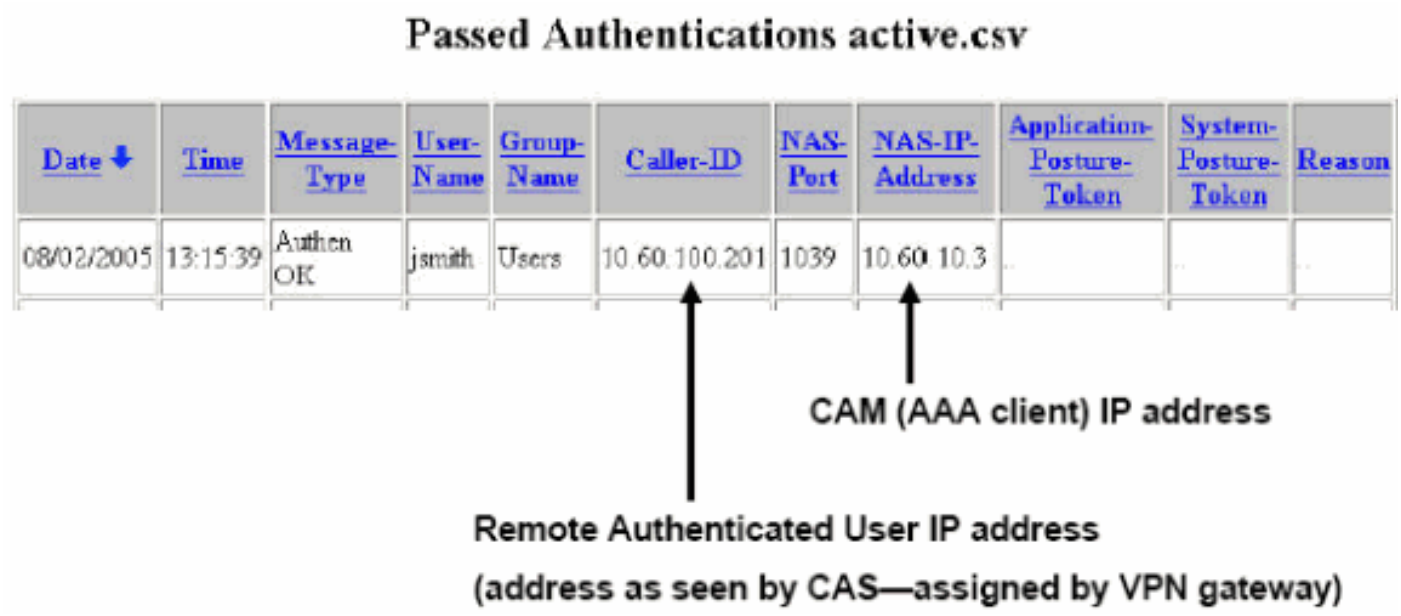


ACS Agregue/usuario de ACS de la configuración para que cada usuario limpio del acceso sea autenticado por el ACS.Fije la membresía del grupo ACS.El ACS también soporta la autenticación de representación a otros servidores externos.

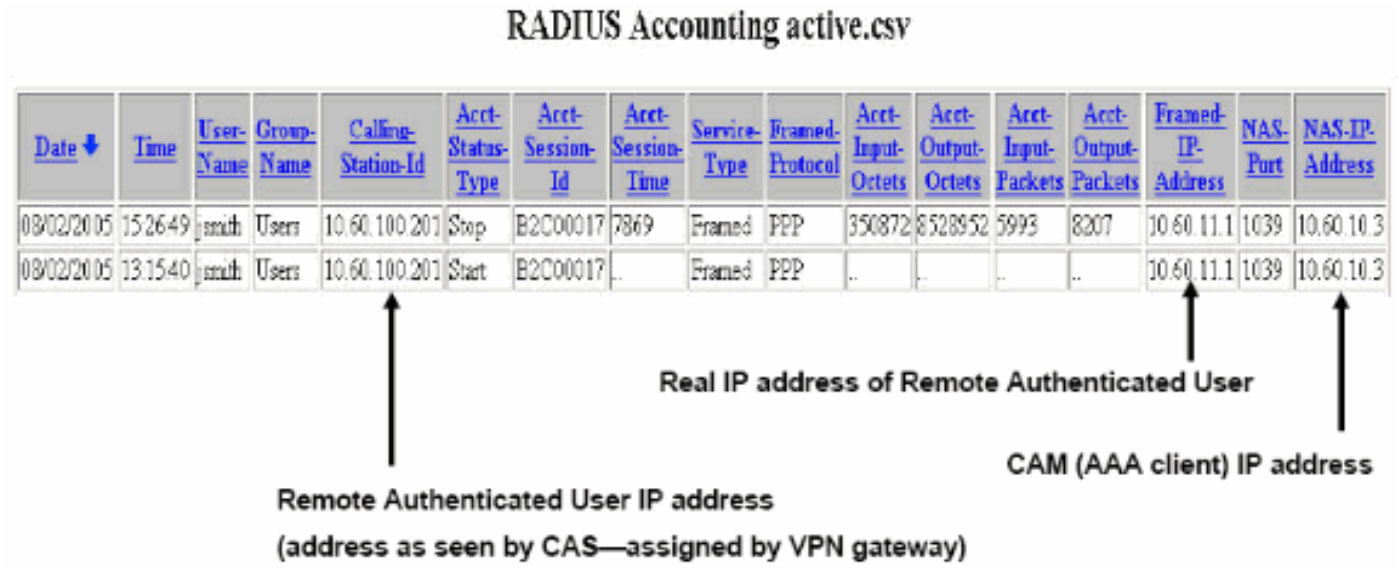
Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

En la sección de la supervisión ACS, usted puede ver la información sobre las autenticaciones pasajeras como se muestra:



Semejantemente, usted puede ver el tiro de pantalla para las estadísticas RADIUS:



Troubleshooting

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

Información Relacionada

- Página de soporte del dispositivo NAC de Cisco
- Soporte Técnico y Documentación - Cisco Systems