TACACS+ en una punta de acceso Aironet para la autenticación de inicio de sesión con el uso del ejemplo de la Configuración del GUI

Contenido

Introducción

Este documento explica cómo permitir a TACACS más los servicios (TACACS+) en una punta de acceso Aironet de Cisco (AP) para realizar la autenticación de inicio de sesión con el uso de un servidor TACACS+.

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento de cómo configurar los parámetros básicos en Aironet APs
- Conocimiento de cómo configurar un servidor TACACS+ como el Cisco Secure Access Control Server (ACS)
- Conocimiento de los conceptos TACACS+

Para la información sobre cómo los trabajos TACACS+, refieren *comprensión de la* sección *TACACS+ de* configurar los servidores RADIUS y TACACS+.

Componentes Utilizados

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

- Aironet Cisco Aironet 1240/1140 Series de los Puntos de acceso
- ACS que funciona con la versión de software 4.1
- ACS que funciona con la versión de software 5.2

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

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Configurar

Esta sección explica cómo configurar el Aironet AP y el servidor TACACS+ (ACS) para la autenticación de inicio de sesión TACACS+-based.

Este ejemplo de la configuración utiliza estos parámetros:

- Dirección IP del ACS — 172.16.1.1/255.255.0.0
- Dirección IP del AP — 172.16.1.30/255.255.0.0
- Clave secreta compartida que se utiliza en el AP y el ejemplo del servidor TACACS+

Éstas son las credenciales del usuario que este ejemplo configura en el ACS:

- Username — **User1**
- Palabra clave Cisco
- Grupo — **AdminUsers**

Usted necesita configurar las características TACACS+ para validar a los usuarios que intentan conectar con el AP a través de la interfaz Web o a través del comando line interface(cli). Para lograr esta configuración, usted debe realizar estas tareas:

1. Configure el servidor TACACS+ para la autenticación de inicio de sesión.
2. Configure el Aironet AP para autenticación de TACACS+.

Nota: Use la herramienta Command Lookup Tool (clientes registrados solamente) para encontrar más información sobre los comandos usados en este documento.

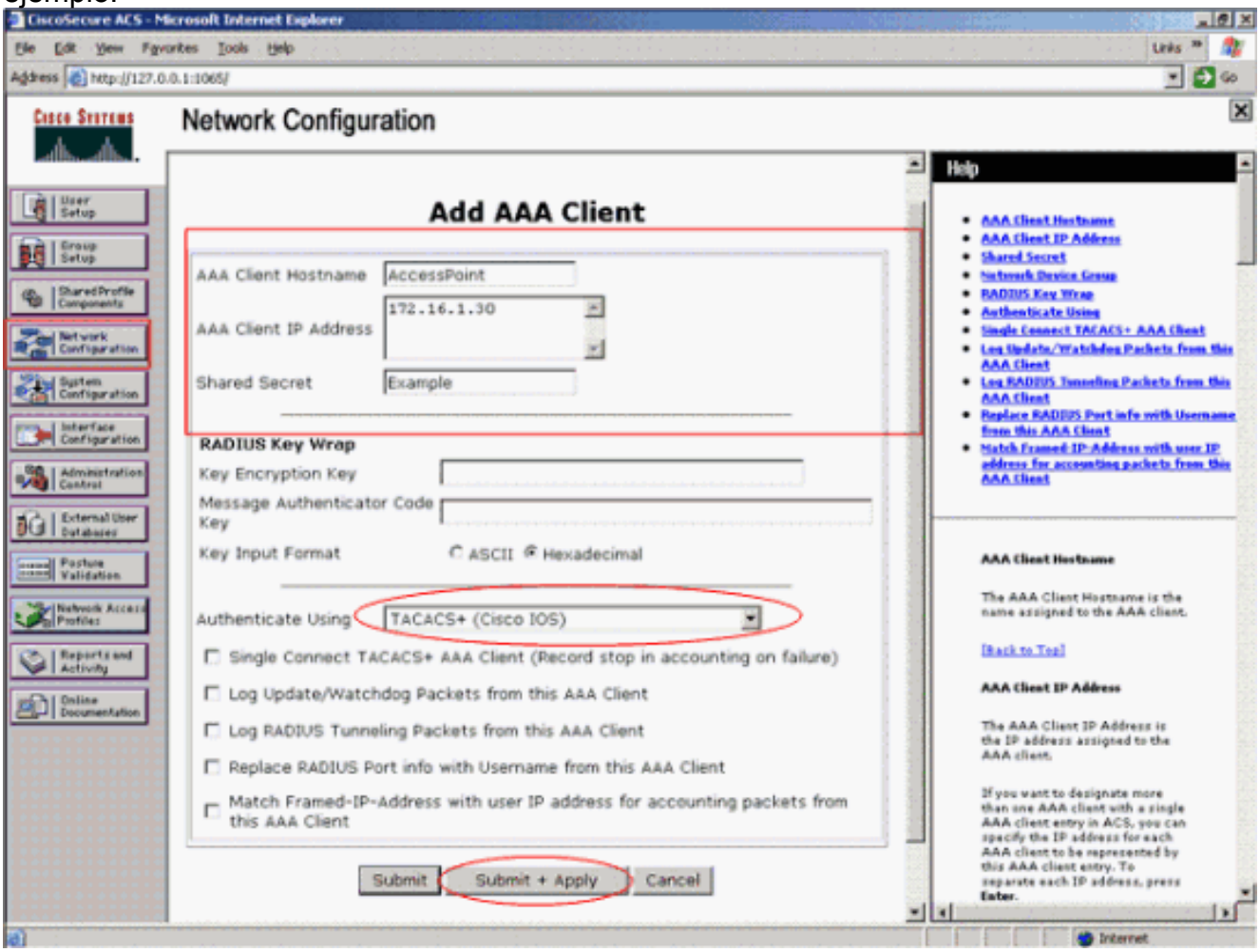
Diagrama de la red

En este documento, se utiliza esta configuración de red:

Configure el servidor TACACS+ para la autenticación de inicio de sesión - Usando ACS 4.1

El primer paso es poner una daemon TACACS+ para validar a los usuarios que intentan tener acceso al AP. Usted debe poner el ACS para autenticación de TACACS+ y crear una base de datos de usuarios. Usted puede utilizar cualquier servidor TACACS+. Este ejemplo utiliza el ACS como el servidor TACACS+. Complete estos pasos:

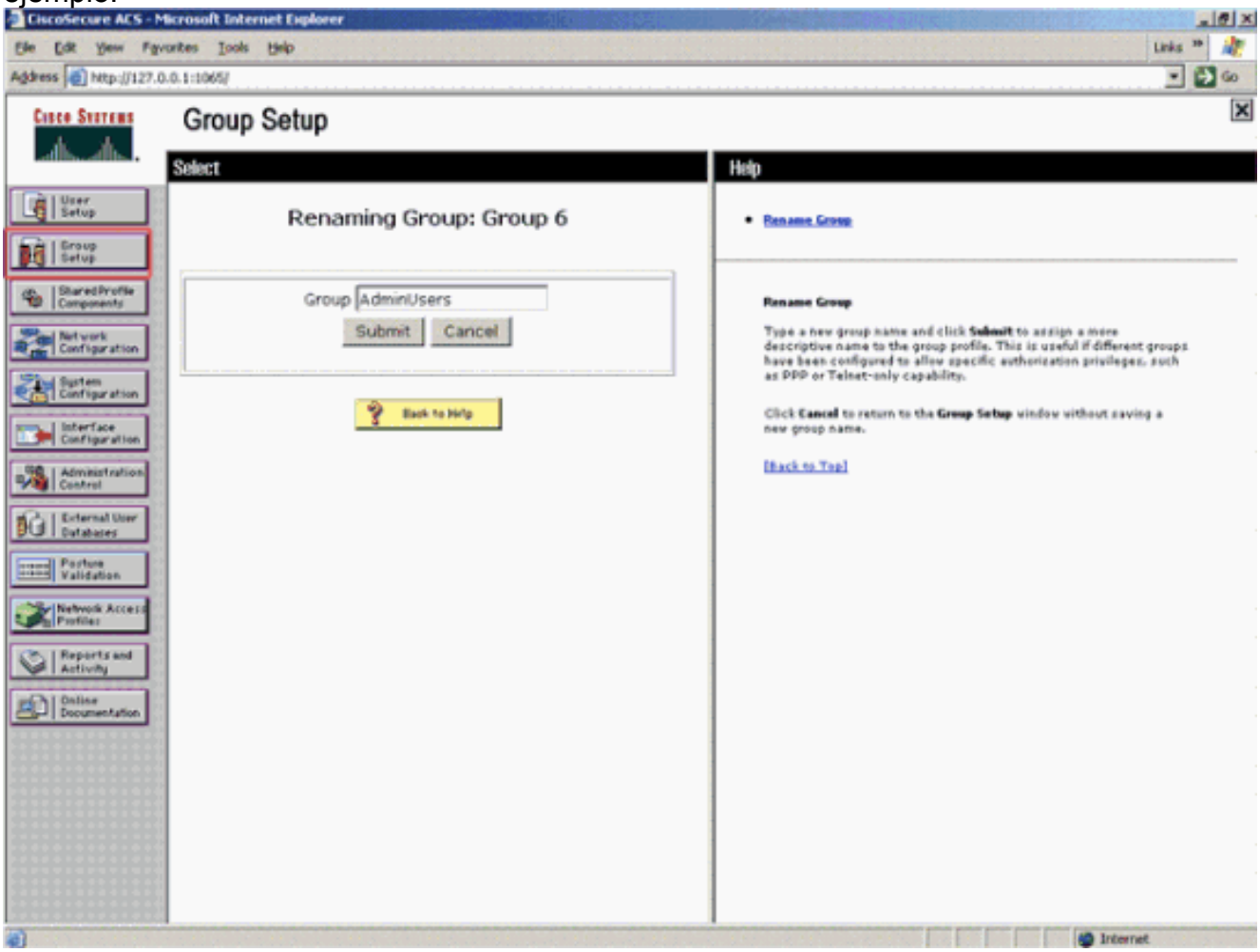
1. Complete estos pasos para agregar el AP como cliente del Authentication, Authorization, and Accounting (AAA):Del GUI ACS, haga clic la **configuración de red** cuadro.En los clientes AAA, haga clic en Add Entry (Agregar entrada).En la ventana del cliente AAA del agregar, ingrese el nombre de host AP, el IP address del AP, y una clave secreta compartida.Esta clave secreta compartida debe ser lo mismo que la clave secreta compartida que usted configura en el AP.De la autenticidad usando el menú desplegable, seleccione **TACACS+ (Cisco IOS)**.El tecleo **somete + reinicio** para salvar la configuración.Aquí tiene un ejemplo:



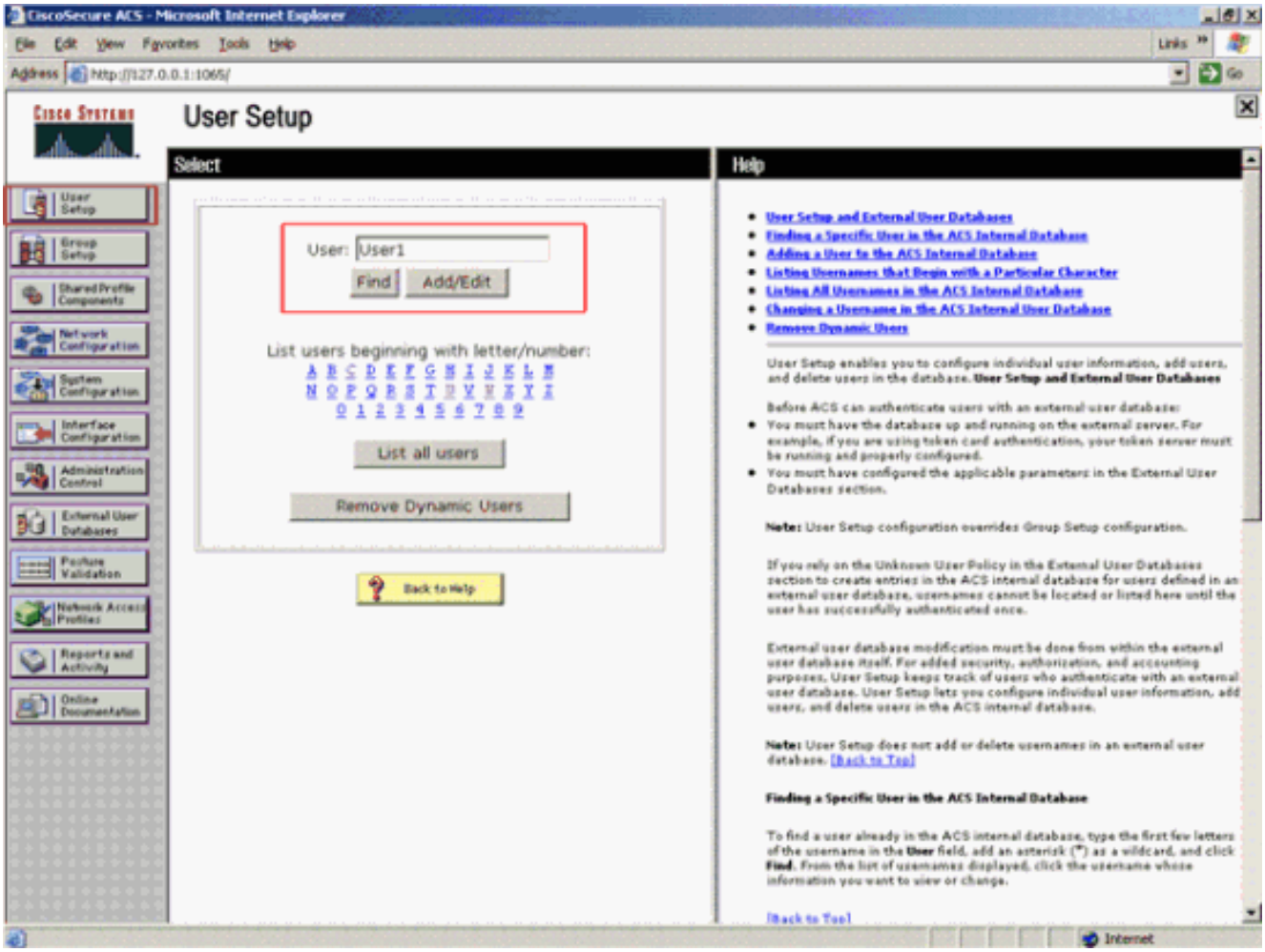
Este ejemplo utiliza:Nombre del host del cliente AAA el **AccessPoint**El direccionamiento

172.16.1.30/16 como la dirección IP del cliente AAA**El ejemplo de la** clave secreta compartida

2. Complete estos pasos para crear a un grupo que contenga a todos los usuarios administrativos (admin):Haga clic la **configuración de grupo del** menú a la izquierda.Una nueva ventana aparece.En la ventana de la configuración de grupo, seleccione a un grupo configurar del menú desplegable y el tecleo **retitula al grupo**.Este ejemplo selecciona el grupo 6 del menú desplegable y retitula el grupo AdminUsers.Haga clic en Submit (Enviar).Aquí tiene un ejemplo:

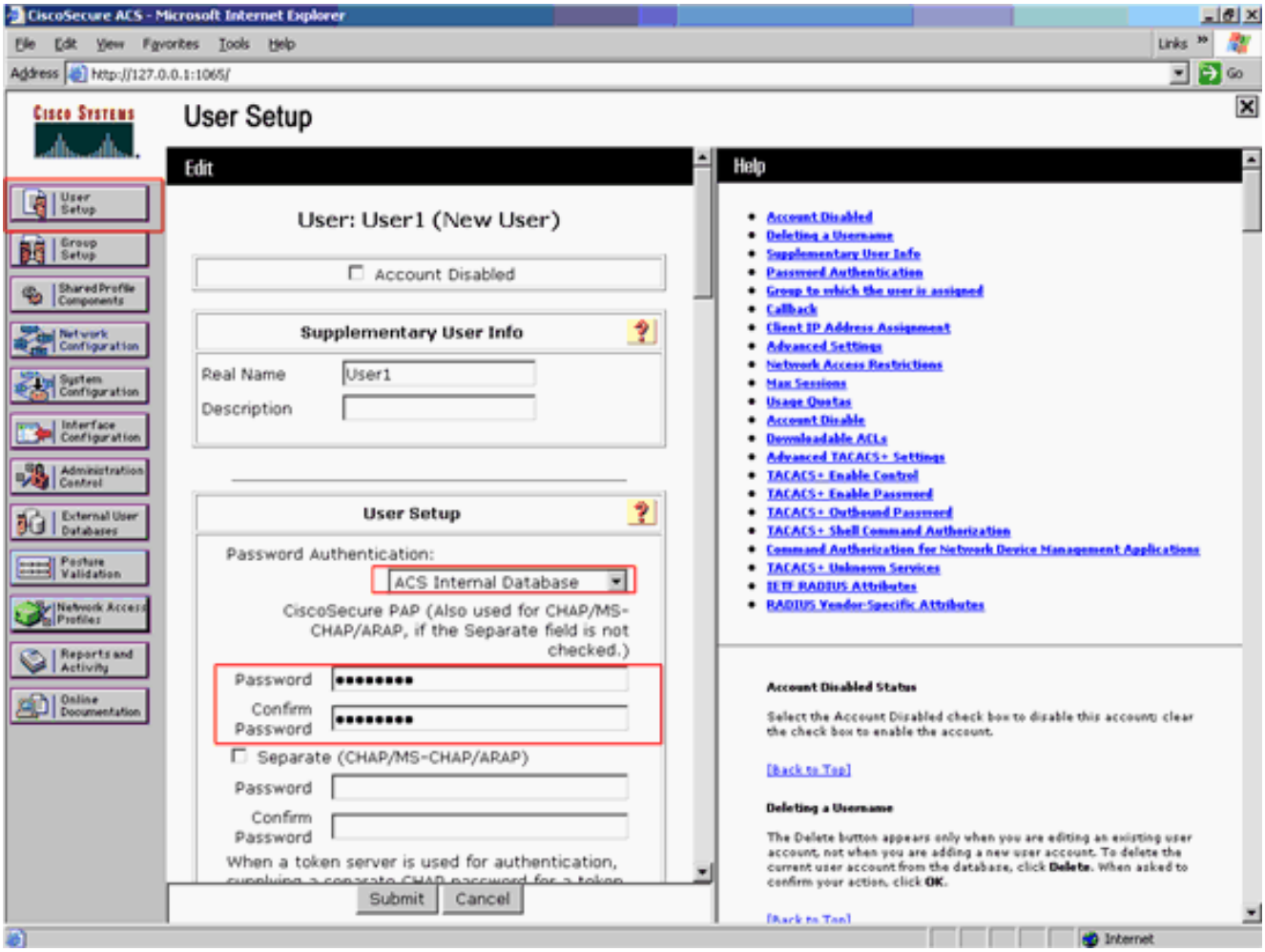


3. Complete estos pasos para agregar a los usuarios a la base de datos TACACS+:Haga clic la **configuración de usuario** cuadro.Para crear a un usuario nuevo, ingresar el username en el campo y el tecleo del usuario **agregue/corrija**.Aquí está un ejemplo, que crea **User1**:

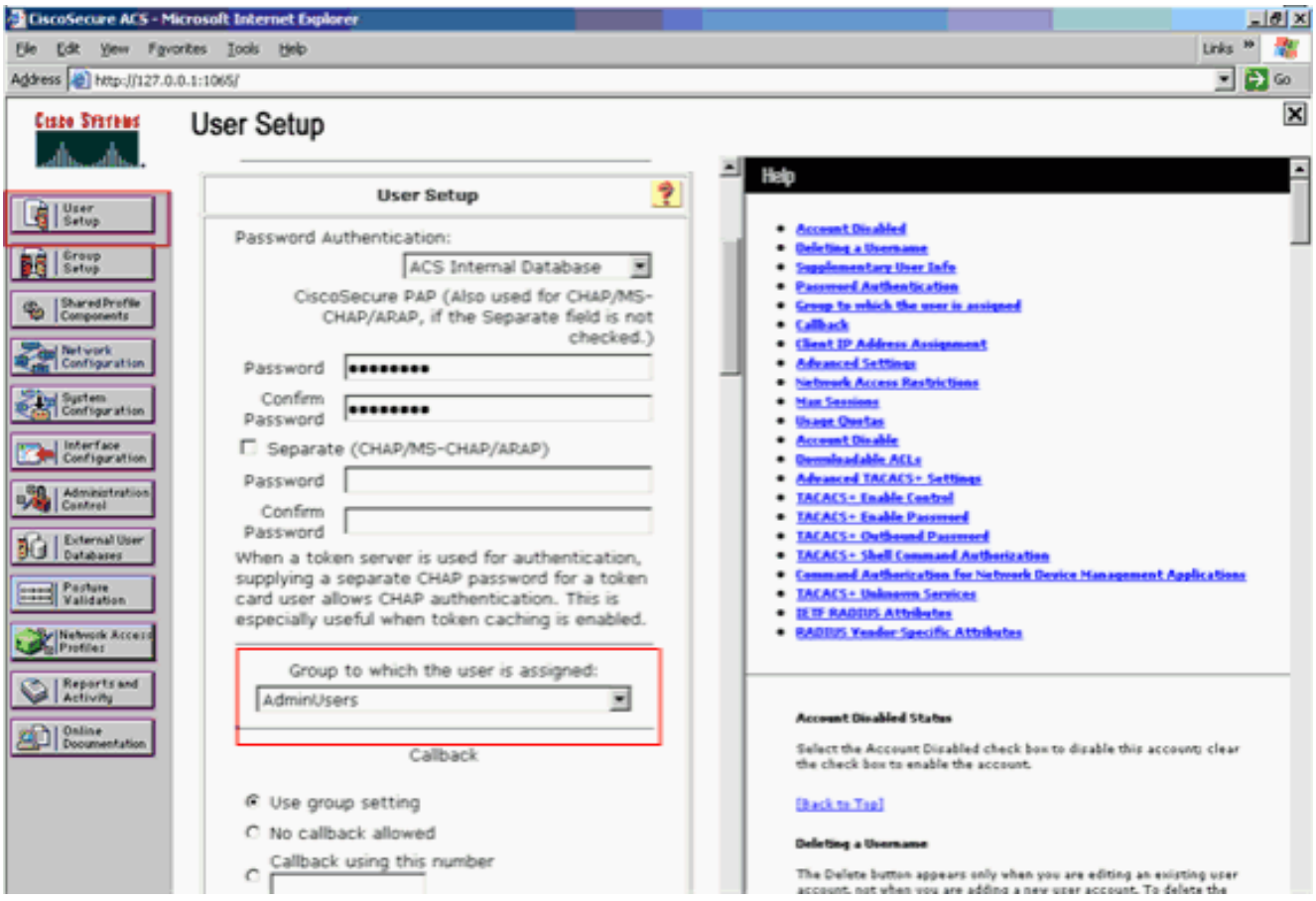


Después de que usted tecleo agregue/corrija, el agregar/corrija la ventana para este usuario aparece.

4. Ingrese las credenciales que son específicas a este usuario y el tecleo **somete** para salvar la configuración.Las credenciales que usted puede ingresar incluyen:Información sobre el usuario suplementariaConfiguración de usuarioEl grupo a quien asignan el usuarioAquí tiene un
ejemplo:

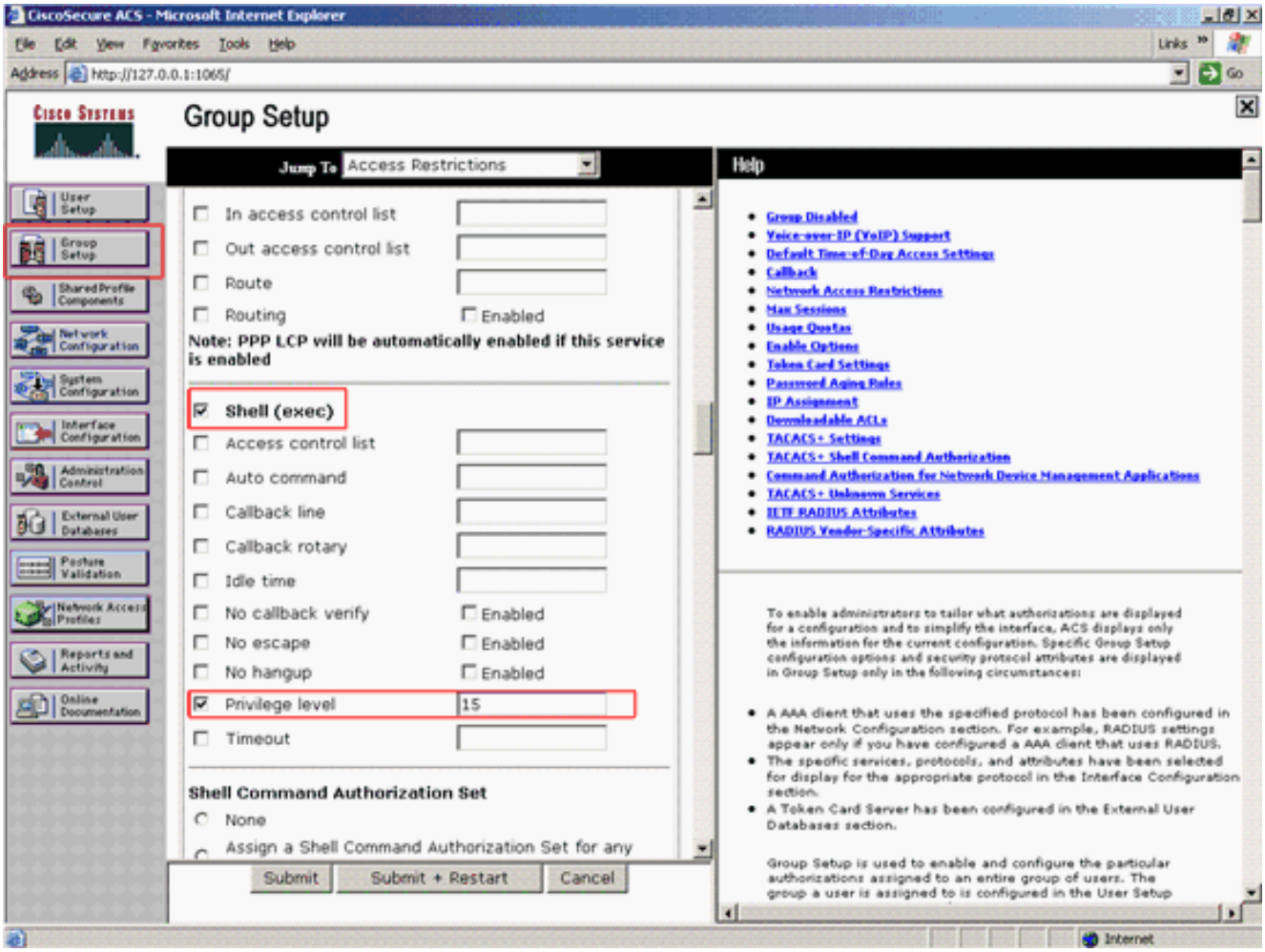


Usted puede ver que este ejemplo agrega al usuario User1 al grupo AdminUsers.



Nota: Si usted no crea a un grupo específico, asignan los usuarios al grupo predeterminado.

5. Complete estos pasos para definir el nivel de privilegio:Haga clic la **configuración de grupo** cuadro.Seleccione al grupo que usted asignó previamente a este usuario y el tecleo **corrige las configuraciones**.Este ejemplo utiliza el grupo AdminUsers.Bajo configuraciones TACACS+, controle la casilla de verificación del **shell (exec)** y controle la casilla de verificación del **nivel de privilegio** que tiene un valor de 15.El tecleo **somete + reinicio**.



Nota: El nivel de privilegio 15 se debe definir para el GUI y Telnet para ser accesible como nivel 15. Si no, por abandono, el usuario puede tener acceso solamente como nivel 1. Si el nivel de privilegio no se define y los intentos del usuario a ingresar activan el modo en el CLI (con el uso del telnet), el AP visualiza este mensaje de error:

```
AccessPoint>enable
% Error in authentication
```

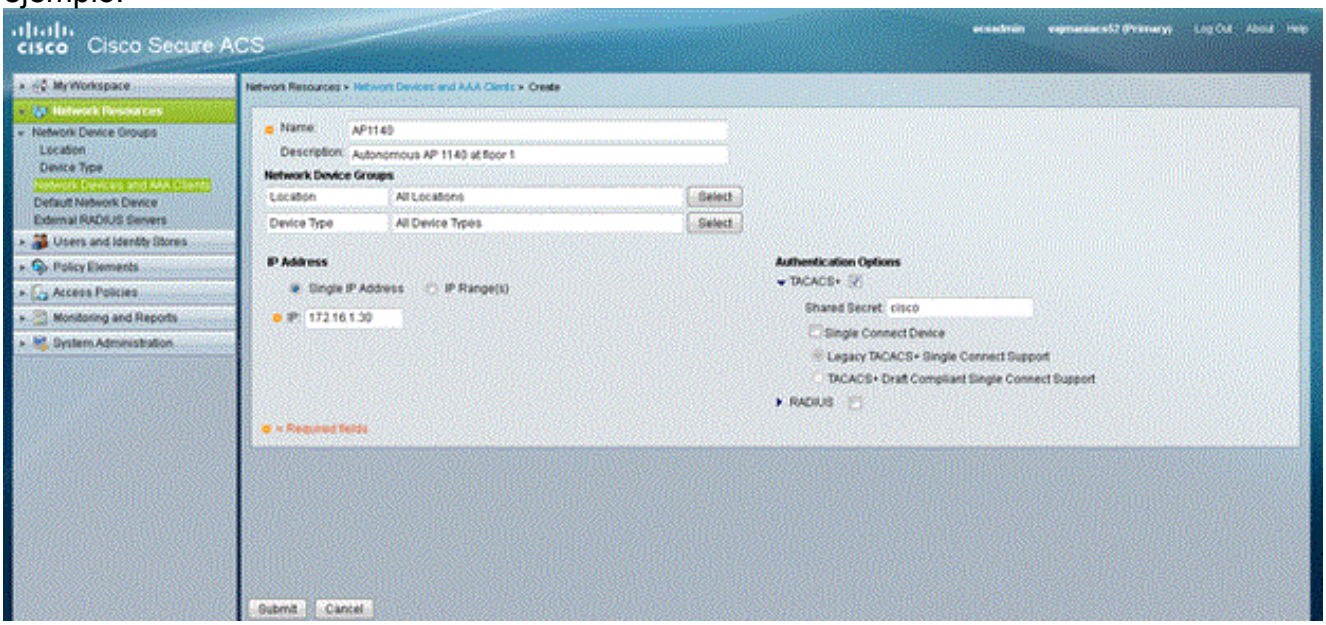
Relance los pasos 2 a 4 de este procedimiento si usted quiere agregar a más usuarios a la base de datos TACACS+. Después de que usted haya completado estos pasos, el servidor TACACS+ está listo para validar a los usuarios que intentan abrirse una sesión al AP. Ahora, usted debe configurar el AP para autenticación de TACACS+.

Configure el servidor TACACS+ para la autenticación de inicio de sesión - Usando ACS 5.2

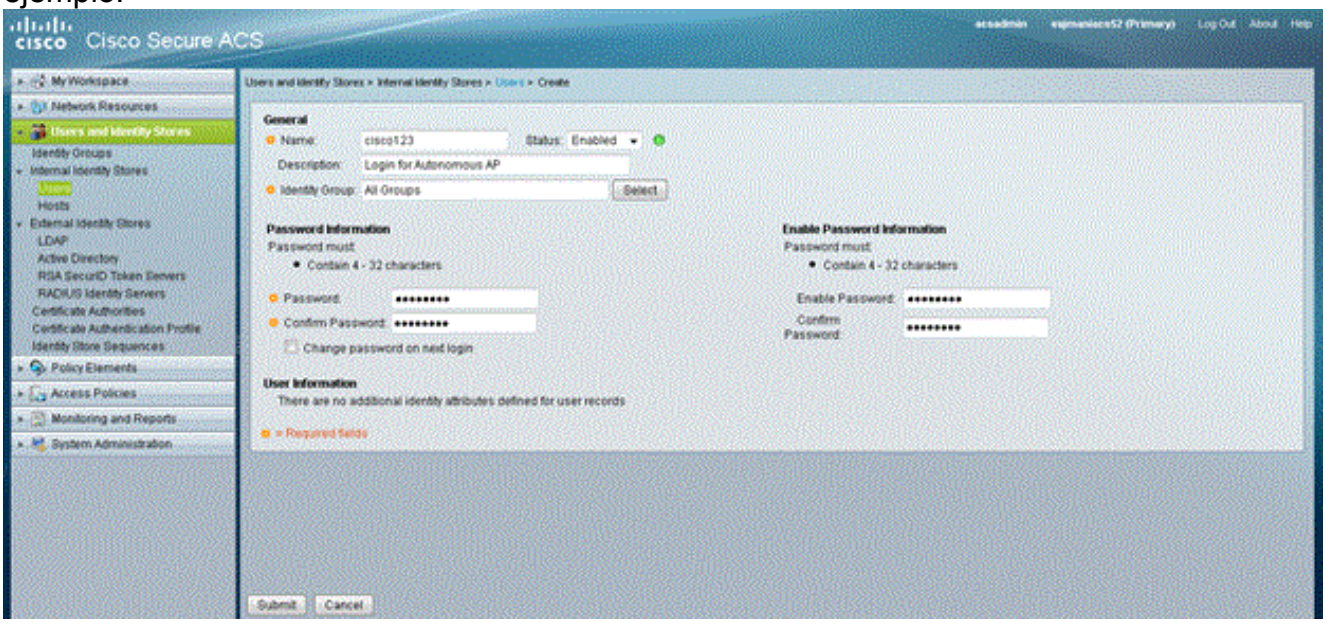
El primer paso es agregar el AP como cliente AAA en el ACS y crear una directiva TACACS para la clave.

1. Complete estos pasos para agregar el AP como cliente AAA:Del GUI ACS, haga clic a los

recursos de red, después haga clic los **dispositivos de red y a los clientes AAA**.Bajo dispositivos de red, el tecleo **crea**.Ingrese el hostname del AP en el **nombre**, y proporcione a una descripción sobre el AP.Seleccione la **ubicación** y el **tipo de dispositivo** si se definen estas categorías.Porque solamente se está configurando un solo AP, haga clic la **sola dirección IP**. Usted puede agregar el rango de los IP Addresses para los APs múltiples haciendo clic el **intervalo de direcciones IP**. Entonces, ingrese el IP address del AP.Bajo **opciones de autenticación**, controle el rectángulo **TACACS+** y ingrese el **secreto compartido**.Aquí tiene un
ejemplo:

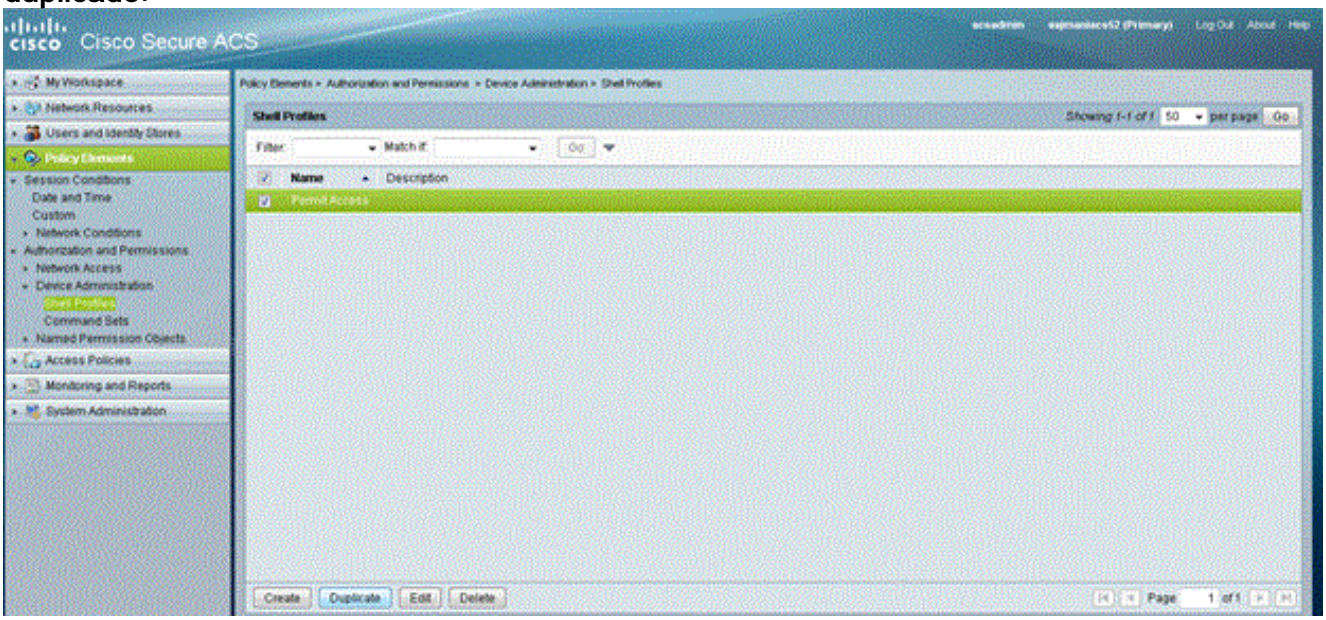


2. El siguiente paso es crear un nombre de usuario y contraseña de la clave:Haga clic los **usuarios y los almacenes de la identidad**, después haga clic a los **usuarios**.Haga clic en **Crear**.Dé el username bajo **nombre**, y proporcione a una descripción.Seleccione al **grupo de la identidad**, si lo hay.Ingrese la contraseña conforme al cuadro de texto de la **contraseña**, y éntrela de nuevo debajo **confirman la contraseña**.Usted puede modificar la contraseña de la activación ingresando una contraseña debajo **activa la contraseña**. Entre de nuevo para confirmar.Aquí tiene un
ejemplo:

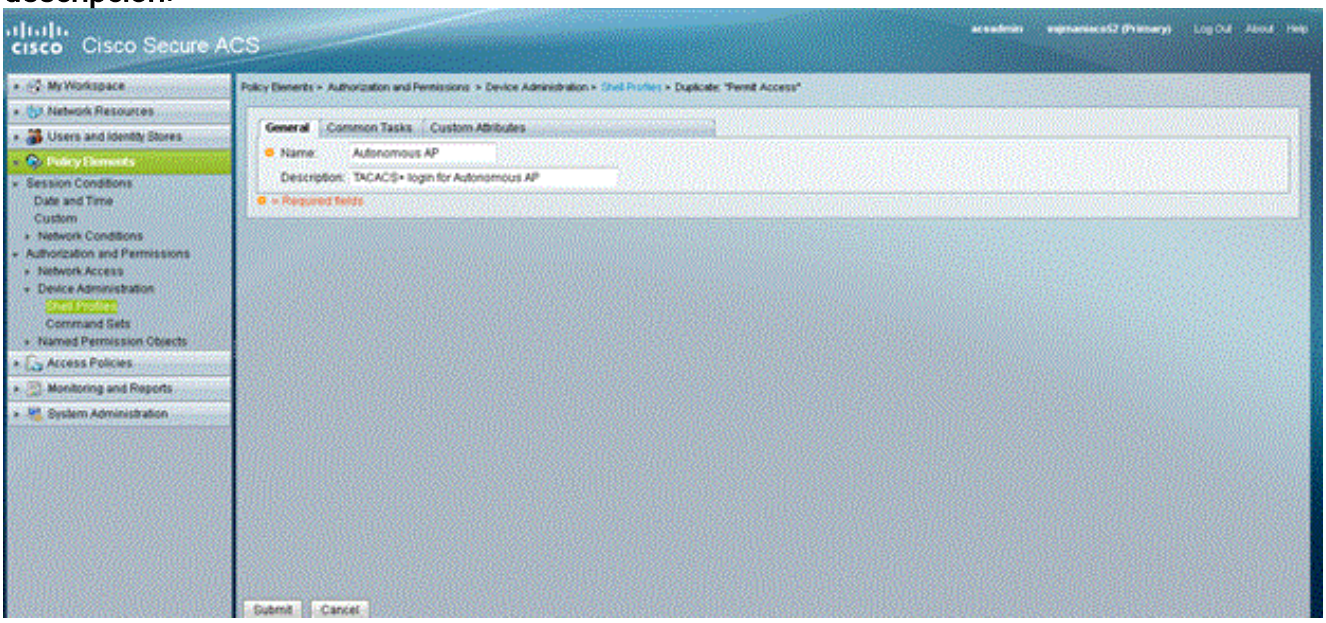


3. Complete estos pasos para definir el nivel de privilegio:Haga clic los **elementos de la directiva** > las **autorizaciones y los permisos** > los **perfiles de la administración** > del **shell del**

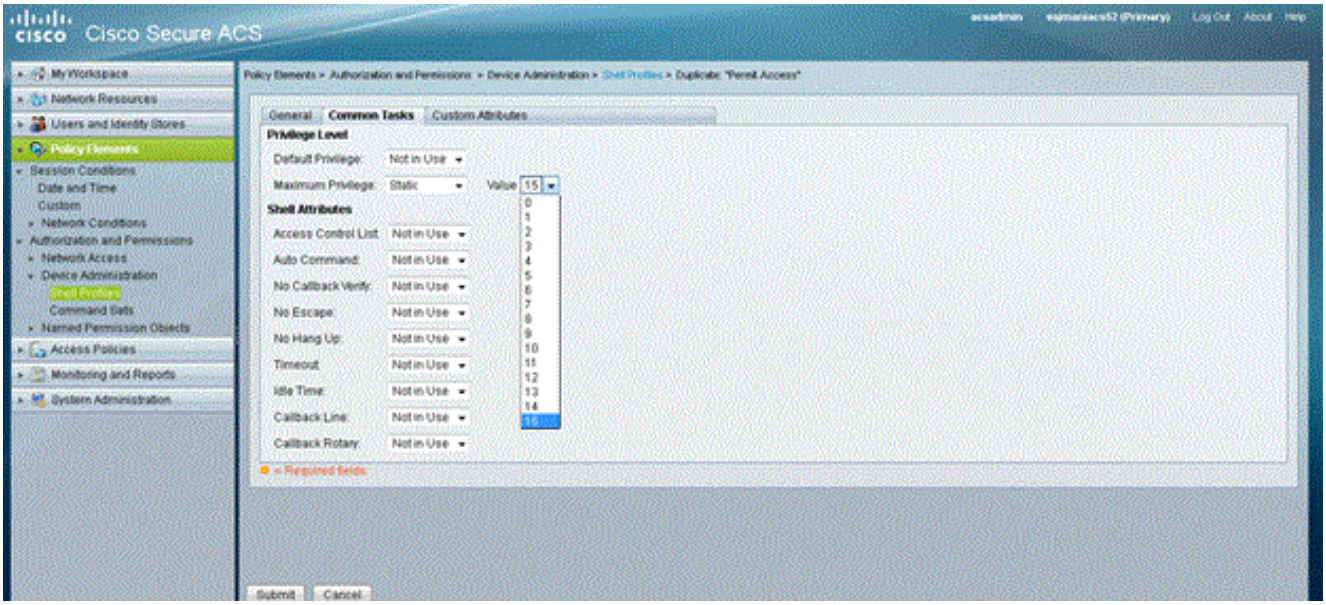
dispositivo.Controle el cuadro de **verificación de acceso del permiso** y haga clic el **duplicado**.



Ingrese el **nombre** y la **descripción**.

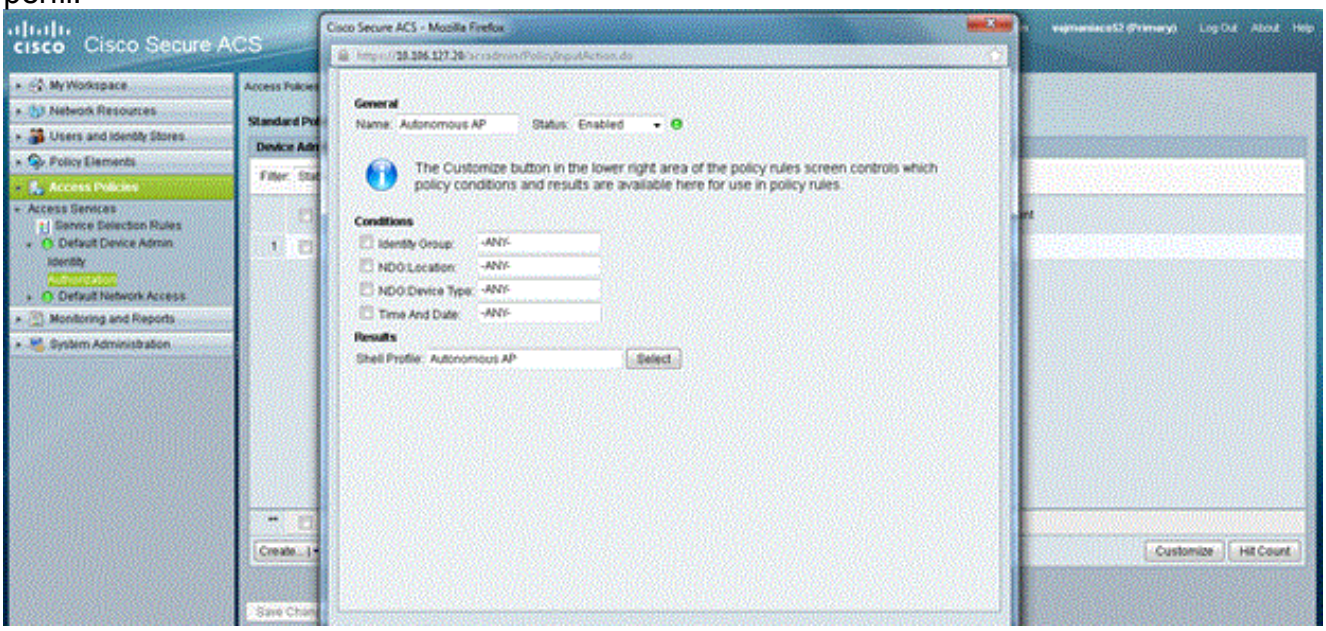


Seleccione la tabulación común de las tareas y elija **15** para el privilegio máximo.

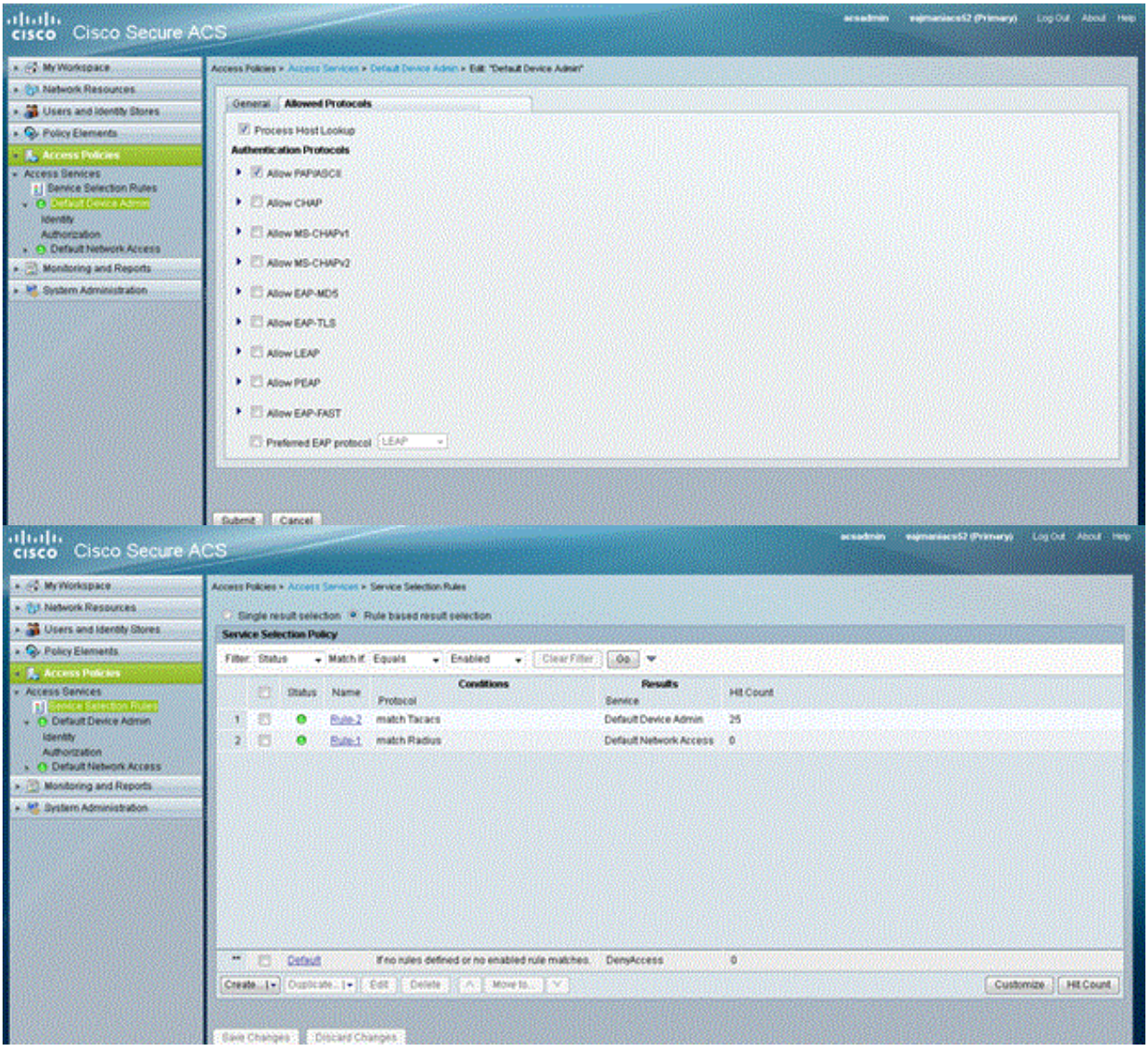


Haga clic en Submit (Enviar).

4. Complete estos pasos para crear una directiva de la autorización:Haga clic las **políticas de acceso** > los **servicios del acceso** > el **dispositivo del valor por defecto Admin** > **autorización**.El tecleo **crea** para crear una nueva directiva de la autorización.Un nuevo hace estallar para arriba aparece crear las reglas para la directiva de la autorización.Seleccione el **grupo de la identidad**, la **ubicación** etc. para el username específico y al cliente AAA (AP), si ninguno.Haga clic **seleccionan** para que el perfil del shell elija el AP autónomo creado perfil.



Una vez que se hace esto, haga clic los **cambios de la salvaguardia**.Haga clic el **dispositivo Admin del valor por defecto**, después haga clic los **protocolos permitidos**.El control **permite PAP/ASCII**, después hace clic **somete**.**Las reglas de selección del servicio del** tecleo para asegurarse de allí son una regla que corresponde con TACACS y que señala para omitir el dispositivo
Admin.

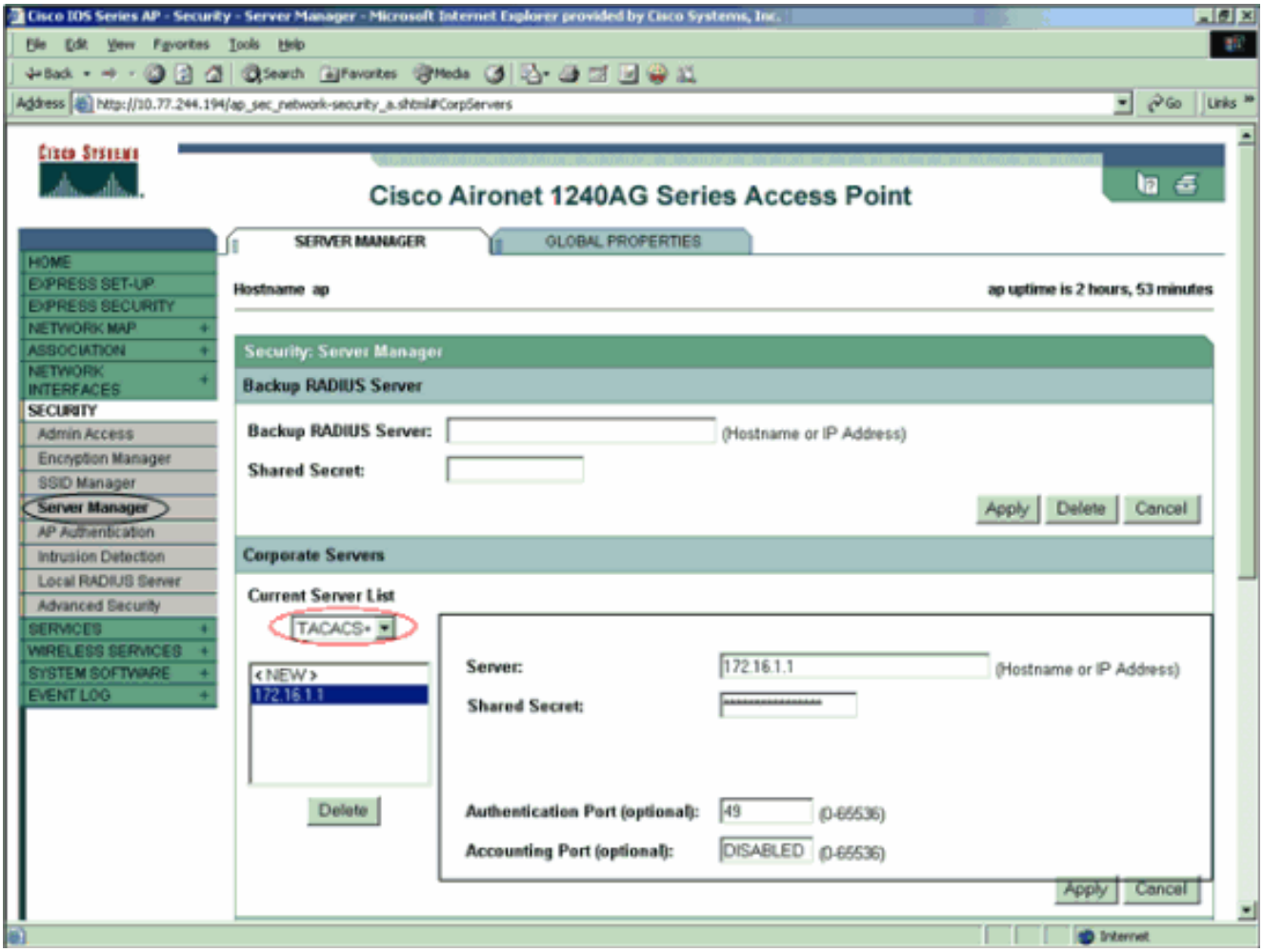


Configure el Aironet AP para autenticación de TACACS+

Usted puede utilizar el CLI o el GUI para activar las características TACACS+ en el Aironet AP. Esta sección explica cómo configurar el AP para la autenticación de inicio de sesión TACACS+ con el uso del GUI.

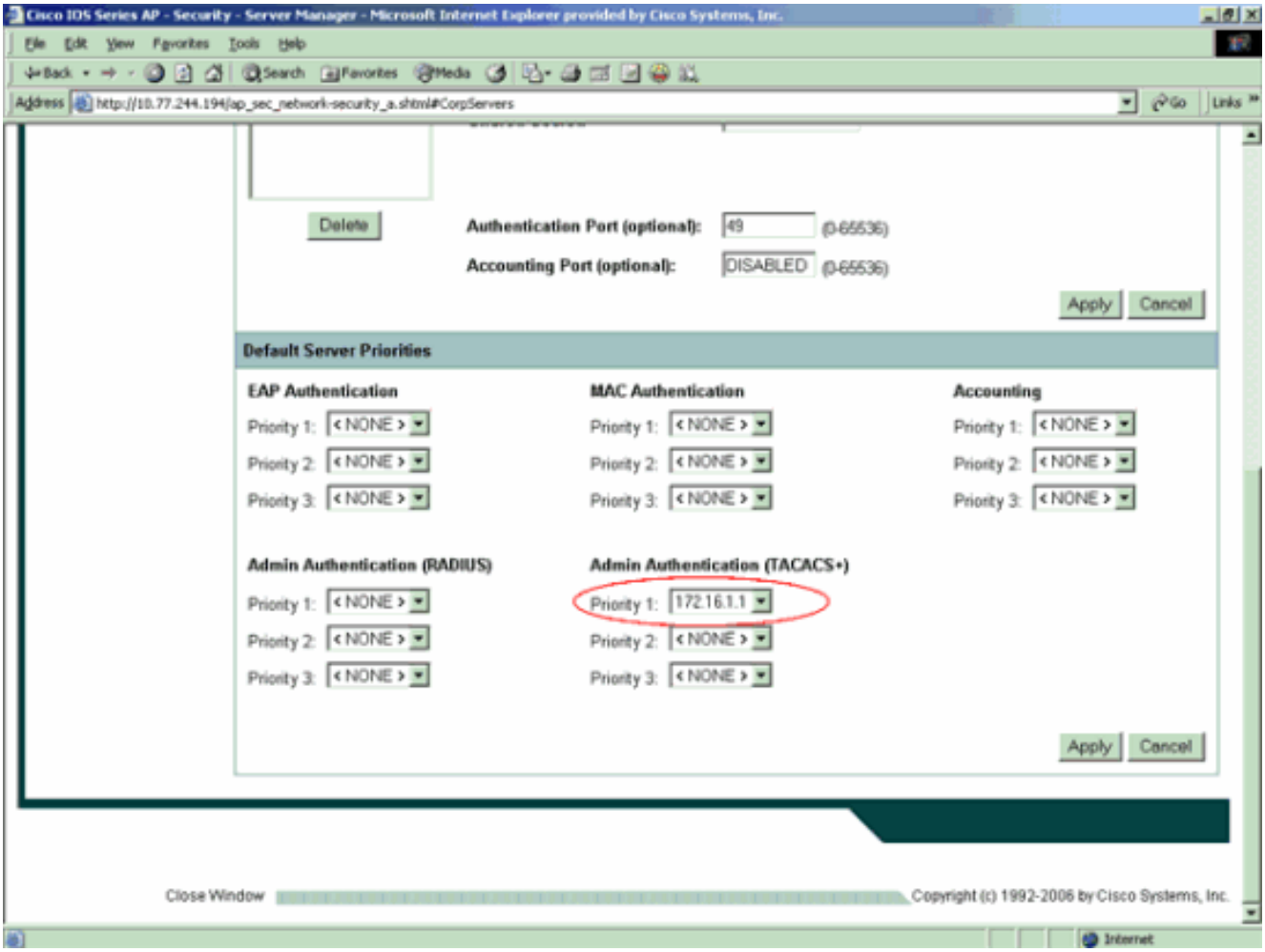
Complete estos pasos para configurar TACACS+ en el AP con el uso del GUI:

1. Complete estos pasos para definir los parámetros del servidor TACACS+:Del GUI AP, elija la **Seguridad > al administrador de servidor**.La Seguridad: La ventana de administrador de servidor aparece.En el área de los servidores corporativos, seleccione **TACACS+ del** menú desplegable de la lista del servidor actual.En esta misma área, ingrese el IP address, el secreto compartido, y el número del puerto de autenticación del servidor TACACS+.Haga clic en Apply (Aplicar).Aquí tiene un
ejemplo:

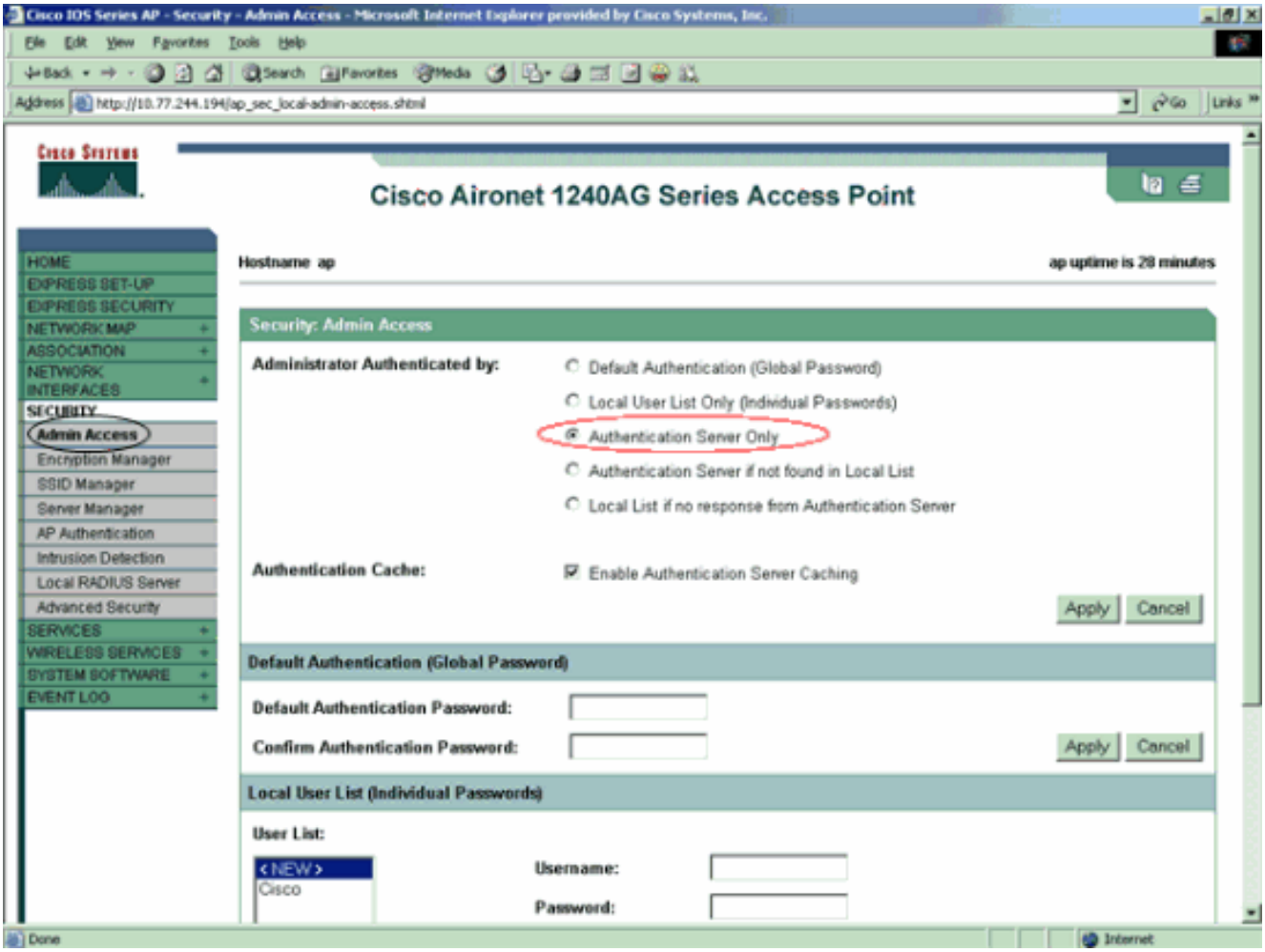


Nota: Por abandono, TACACS+ utiliza el puerto 49 TCP.**Nota:** La clave secreta compartida que usted configura en el ACS y el AP debe hacer juego.

2. Elija las **prioridades > la autenticación Admin (TACACS+) del servidor del valor por defecto**, seleccione del menú desplegable de la prioridad 1 la dirección IP del servidor TACACS+ que usted ha configurado, y el tecleo **se aplica**.Aquí tiene un ejemplo:



3. Elija la **Seguridad > el acceso Admin** y, porque el administrador autenticado por: , elija el **servidor de la autenticación solamente** y el tecleo **se aplica**.Esta selección se asegura de que un servidor de la autenticación autentiquen a los usuarios que intentan abrirse una sesión al AP.Aquí tiene un
ejemplo:



Ésta es la configuración CLI por el ejemplo de la configuración:

AccessPoint

```
AccessPoint#show running-config

Current configuration : 2535 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname AccessPoint
!
!
ip subnet-zero
!
!
aaa new-model
!--- Enable AAA. ! ! aaa group server radius rad_eap !
aaa group server radius rad_mac ! aaa group server
radius rad_acct ! aaa group server radius rad_admin
cache expiry 1 cache authorization profile admin_cache
cache authentication profile admin_cache ! aaa group
server tacacs+ tac_admin
!--- Configure the server group tac_admin. server
172.16.1.1
!--- Add the TACACS+ server 172.16.1.1 to the server
group. cache expiry 1
```

```
!--- Set the expiration time for the local cache as 24
hours. cache authorization profile admin_cache
 cache authentication profile admin_cache
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa authentication login default group tac_admin
!--- Define the AAA login authentication method list to
use the TACACS+ server. aaa authentication login
eap_methods group rad_eap aaa authentication login
mac_methods local aaa authorization exec default group
tac_admin
!--- Use TACACS+ for privileged EXEC access
authorization !--- if authentication was performed with
use of TACACS+. aaa accounting network acct_methods
start-stop group rad_acct aaa cache profile admin_cache
all ! aaa session-id common ! ! username Cisco password
7 00271A150754 ! bridge irb ! ! interface Dot11Radio0 no
ip address no ip route-cache shutdown speed basic-1.0
basic-2.0 basic-5.5 basic-11.0 station-role root bridge-
group 1 bridge-group 1 subscriber-loop-control bridge-
group 1 block-unknown-source no bridge-group 1 source-
learning no bridge-group 1 unicast-flooding bridge-group
1 spanning-disabled ! interface Dot11Radio1 no ip
address no ip route-cache shutdown speed station-role
root bridge-group 1 bridge-group 1 subscriber-loop-
control bridge-group 1 block-unknown-source no bridge-
group 1 source-learning no bridge-group 1 unicast-
flooding bridge-group 1 spanning-disabled ! interface
FastEthernet0 no ip address no ip route-cache duplex
auto speed auto bridge-group 1 no bridge-group 1 source-
learning bridge-group 1 spanning-disabled ! interface
BVI1 ip address 172.16.1.30 255.255.0.0 no ip route-
cache ! ip http server ip http authentication aaa
!--- Specify the authentication method of HTTP users as
AAA. no ip http secure-server ip http help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/he
lp/ea ip radius source-interface BVI1 ! tacacs-server
host 172.16.1.1 port 49 key 7 13200F13061C082F tacacs-
server directed-request radius-server attribute 32
include-in-access-req format %h radius-server vsa send
accounting ! control-plane ! bridge 1 route ip ! ! !
line con 0 transport preferred all transport output all
line vty 0 4 transport preferred all transport input all
transport output all line vty 5 15 transport preferred
all transport input all transport output all ! end
```

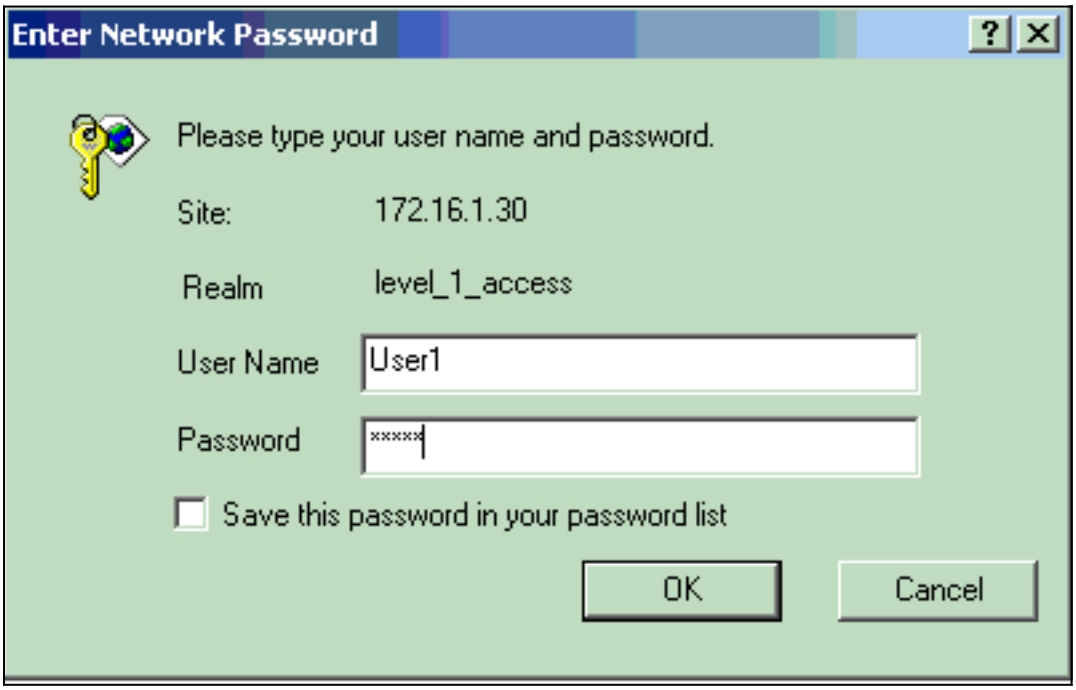
Nota: Usted debe tener Cisco IOS Software Release 12.3(7)JA o Posterior para que todos los comandos en esta configuración de trabajar correctamente. Una versión de software anterior del Cisco IOS no pudo tener todos estos comandos disponibles.

Verificación

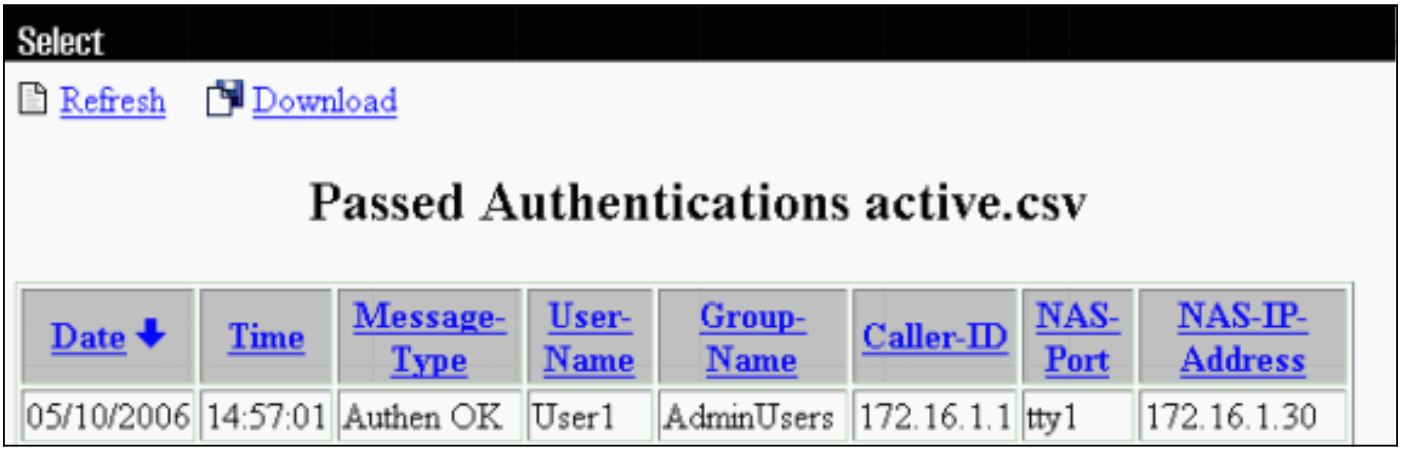
Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice el OIT para ver un análisis de la **salida del comando show**.

Para verificar la configuración, intente abrirse una sesión al AP con el uso del GUI o del CLI. Cuando usted intenta tener acceso al AP, el AP le incita para un nombre de usuario y contraseña.



Cuando usted proporciona a los credenciales de usuario, el AP adelante las credenciales al servidor TACACS+. El servidor TACACS+ valida las credenciales en base de la información que está disponible en su base de datos y proporciona al acceso al AP sobre la autenticación satisfactoria. Usted puede elegir los **informes y la actividad > autenticación pasajera** en el ACS y utilizar el informe pasajero de la autenticación para controlar para saber si hay autenticación satisfactoria para este usuario. Aquí tiene un ejemplo:



Usted puede también utilizar el **comando show tacacs** para verificar la configuración correcta del servidor TACACS+. Aquí tiene un ejemplo:

```
AccessPoint#show tacacs

Tacacs+ Server            : 172.16.1.1/49
              Socket opens:        348
             Socket closes:        348
             Socket aborts:          0
             Socket errors:          0
          Socket Timeouts:           0
   Failed Connect Attempts:          0
        Total Packets Sent:        525
```

```
        Total Packets Recv:       525
```

Verificación para ACS 5.2

Usted puede verificar las tentativas falladas/pasajeras para las credenciales de la clave del ACS 5.2:

1. **Supervisión del** tecleo **e informes > espectador de la supervisión y del informe del lanzamiento**.Un nuevo hace estallar abre con el panel.
2. **Autenticaciones-TACACS-hoy del** tecleo. Esto muestra los detalles de las tentativas falladas/pasajeras.

Troubleshooting

Usted puede utilizar estos comandos debug en el AP para resolver problemas su configuración:

Nota: Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

- **ponga a punto los eventos de los tacacs** — Este comando visualiza la Secuencia de eventos que sucede durante la autenticación de TACACS. Aquí está un ejemplo de la salida de este comando:

```
*Mar  1 00:51:21.113: TPLUS: Queuing AAA Authentication request 0 for
processing
*Mar  1 00:51:21.113: TPLUS: processing authentication start request id 0
*Mar  1 00:51:21.113: TPLUS: Authentication start packet created for 0(User1)
*Mar  1 00:51:21.114: TPLUS: Using server 172.16.1.1
*Mar  1 00:51:21.115: TPLUS(00000000)/0/NB_WAIT/C6DC40: Started 5 sec timeout
*Mar  1 00:51:21.116: TPLUS(00000000)/0/NB_WAIT: socket event 2
*Mar  1 00:51:21.116: TPLUS(00000000)/0/NB_WAIT: wrote entire 25 bytes request
*Mar  1 00:51:21.116: TPLUS(00000000)/0/READ: socket event 1
*Mar  1 00:51:21.117: TPLUS(00000000)/0/READ: Would block while reading
*Mar  1 00:51:21.120: TPLUS(00000000)/0/READ: socket event 1
*Mar  1 00:51:21.120: TPLUS(00000000)/0/READ: read entire 12 header bytes (expect
16 bytes data)
*Mar  1 00:51:21.120: TPLUS(00000000)/0/READ: socket event 1
*Mar  1 00:51:21.120: TPLUS(00000000)/0/READ: read entire 28 bytes response
*Mar  1 00:51:21.121: TPLUS(00000000)/0/C6DC40: Processing the reply packet
*Mar  1 00:51:21.121: TPLUS: Received authen response status GET_PASSWORD (8)
*Mar  1 00:51:21.121: TPLUS: Queuing AAA Authentication request 0 for processing
*Mar  1 00:51:21.121: TPLUS: processing authentication continue request id 0
*Mar  1 00:51:21.122: TPLUS: Authentication continue packet generated for 0
*Mar  1 00:51:21.122: TPLUS(00000000)/0/WRITE/C6DC40: Started 5 sec timeout
*Mar  1 00:51:21.122: TPLUS(00000000)/0/WRITE: wrote entire 22 bytes request
*Mar  1 00:51:21.178: TPLUS(00000000)/0/READ: socket event 1
*Mar  1 00:51:21.178: TPLUS(00000000)/0/READ: read entire 12 header bytes (expect
6 bytes data)
*Mar  1 00:51:21.178: TPLUS(00000000)/0/READ: socket event 1
*Mar  1 00:51:21.178: TPLUS(00000000)/0/READ: read entire 18 bytes response
*Mar  1 00:51:21.179: TPLUS(00000000)/0/C6DC40: Processing the reply packet
*Mar  1 00:51:21.179: TPLUS: Received authen response status PASS (2)
```

- **autenticación de la depuración ip http** — Utilice este comando de resolver problemas los problemas de autenticación HTTP. El comando visualiza el método de autenticación que el router intentó y los mensajes de estado autenticación-específicos.
- **autenticación aaa de la depuración** — Este comando visualiza la información sobre el AAA

autenticación de TACACS+.

Si el usuario ingresa un username que no exista en el servidor TACACS+, la autenticación falla. Aquí está la salida del **comando debug tacacs authentication** para una autenticación fallada:

```
*Mar  1 00:07:26.624: TPLUS: Queuing AAA Authentication request 0 for processing
*Mar  1 00:07:26.624: TPLUS: processing authentication start request id 0
*Mar  1 00:07:26.624: TPLUS: Authentication start packet created for 0(User3)
*Mar  1 00:07:26.624: TPLUS: Using server 172.16.1.1
*Mar  1 00:07:26.625: TPLUS(00000000)/0/NB_WAIT/A88784: Started 5 sec timeout
*Mar  1 00:07:26.626: TPLUS(00000000)/0/NB_WAIT: socket event 2
*Mar  1 00:07:26.626: TPLUS(00000000)/0/NB_WAIT: wrote entire 25 bytes request
*Mar  1 00:07:26.627: TPLUS(00000000)/0/READ: socket event 1
*Mar  1 00:07:26.627: TPLUS(00000000)/0/READ: Would block while reading
*Mar  1 00:07:26.631: TPLUS(00000000)/0/READ: socket event 1
*Mar  1 00:07:26.632: TPLUS(00000000)/0/READ: read entire 12 header bytes (expect 16
bytes data)
*Mar  1 00:07:26.632: TPLUS(00000000)/0/READ: socket event 1
*Mar  1 00:07:26.632: TPLUS(00000000)/0/READ: read entire 28 bytes response
*Mar  1 00:07:26.632: TPLUS(00000000)/0/A88784: Processing the reply packet
*Mar  1 00:07:26.632: TPLUS: Received authen response status GET_PASSWORD (8)
*Mar  1 00:07:26.632: TPLUS: Queuing AAA Authentication request 0 for processing
*Mar  1 00:07:26.633: TPLUS: processing authentication continue request id 0
*Mar  1 00:07:26.633: TPLUS: Authentication continue packet generated for 0
*Mar  1 00:07:26.634: TPLUS(00000000)/0/WRITE/A88784: Started 5 sec timeout
*Mar  1 00:07:26.634: TPLUS(00000000)/0/WRITE: wrote entire 22 bytes request
*Mar  1 00:07:26.688: TPLUS(00000000)/0/READ: socket event 1
*Mar  1 00:07:26.688: TPLUS(00000000)/0/READ: read entire 12 header bytes (expect 6
bytes data)
*Mar  1 00:07:26.689: TPLUS(00000000)/0/READ: socket event 1
*Mar  1 00:07:26.689: TPLUS(00000000)/0/READ: read entire 18 bytes response
*Mar  1 00:07:26.689: TPLUS(00000000)/0/A88784: Processing the reply packet
*Mar  1 00:07:26.689: TPLUS: Received authen response status FAIL (3)
```

Usted puede elegir los **informes y la actividad > no pudo la autenticación** para considerar el intento de autenticación fallado en el ACS. Aquí tiene un ejemplo:

Date ⬇	Time	Message-Type	User-Name	Group-Name	Caller-ID	Authen-Failure-Code	Author-Failure-Code	Author-Data	NAS-Port
05/17/2006	19:40:14	Authen failed	User3	..	..	CS user unknown	..	..	..

Si usted utiliza una versión de software del Cisco IOS en el AP que es anterior que el Cisco IOS Software Release 12.3(7)JA, usted puede golpear un bug cada vez que usted intente abrir una sesión al AP con el uso del HTTP. El ID de bug de Cisco es CSCeb52431 (clientes registrados solamente).

La puesta en práctica del software del Cisco IOS HTTP/AAA requiere la autenticación independiente de cada uno conexión separada HTTP. El GUI inalámbrico del software del Cisco IOS implica la referencia de muchas docenas de archivos distintos dentro de una sola página web (por ejemplo Javascript y GIF). Tan si usted carga una sola página en el GUI inalámbrico del software del Cisco IOS, las docenas y las docenas de autenticación/de peticiones separadas de la autorización puede golpear el servidor AAA.

Para la autenticación HTTP, el uso RADIUS o la autenticación local. Todavía sujetan al servidor de RADIUS a las peticiones de la autenticación múltiple. Pero el RADIUS es más escalable que

TACACS+, y así que es probable proporcionar a un impacto del rendimiento menos-adverso.

Si usted debe utilizar TACACS+ y usted tiene Cisco ACS, utilice la palabra clave de la **sola conexión** con el **comando tacacs-server**. El uso de esta palabra clave con el comando ahorra el ACS la mayor parte de la conexión TCP puesta/los gastos indirectos del desmontaje y es probable reducir la carga en el servidor hasta cierto punto.

Para los Cisco IOS Software Release 12.3(7) JA y después el AP, el software incluye un arreglo. El resto de esta sección describe el arreglo.

Utilice la característica del caché de la autenticación AAA para ocultar la información esa las devoluciones del servidor TACACS+. La característica del caché y del perfil de la autenticación permite que el AP oculte la autenticación/las respuestas de autorización para un usuario de modo que las peticiones de la autenticación subsiguiente/de la autorización no necesiten ser enviadas al servidor AAA. Para activar esta característica con el CLI, utilice estos comandos:

```
cache expiry
cache authorization profile
cache authentication profile
aaa cache profile
```

Para más información sobre esta característica y los comandos, refiera a *configurar la* sección del *caché y del perfil de la autenticación de* administrar el Punto de acceso.

Para activar esta característica en el GUI, elegir la **Seguridad > el acceso Admin** y controlar el **servidor de la autenticación del permiso que oculta la** casilla de verificación. Porque este documento utiliza el Cisco IOS Software Release 12.3(7)JA, el documento utiliza el arreglo, pues las configuraciones ilustran.

Información Relacionada

- Configurar los servidores RADIUS y TACACS+
- Aviso de problemas El Punto de acceso IOS bombardea el servidor TACACS+ con las peticiones
- Autenticación EAP con el servidor de RADIUS
- Soporte de Productos de Red Inalámbrica
- Soporte Técnico y Documentación - Cisco Systems