NAC: Ejemplo de Configuración de Integración LDAP con ACS

Contenido

Introducción

Este documento proporciona una configuración de ejemplo de los pasos para configurar Beacon y ACS para habilitar los dispositivos Cisco configurados para MAB para autenticar efectiva y eficientemente los dispositivos no compatibles con 802.1X en la red autenticada.

Cisco ha implementado una función llamada MAC Authentication Bypass (MAB) en sus switches, así como soporte requerido en ACS para alojar terminales en las redes habilitadas para 802.1X que no pueden autenticarse a través de 802.1X. Esta funcionalidad garantiza que los terminales que intentan conectarse a la red habilitada para 802.1X y que no están equipados con la funcionalidad 802.1X, por ejemplo, no tienen un suplicante 802.1X funcional, se puedan autenticar antes de la admisión, así como que se aplique una política de uso de red básica durante toda la conexión.

MAB permite configurar la red para admitir dispositivos identificados con el uso de su dirección MAC como la credencial principal cuando el dispositivo no participa en el protocolo 802.1X. Para que MAB se implemente y utilice de manera eficaz, el entorno debe tener un medio para identificar los dispositivos en el entorno que no son capaces de la autenticación 802.1X, y mantener una base de datos actualizada de estos dispositivos a lo largo del tiempo a medida que se producen movimientos, adiciones y cambios. Esta lista debe rellenarse y mantenerse en el servidor de autenticación (ACS) manualmente, o a través de algunos medios alternativos para

garantizar que los dispositivos que se autentican en MAC se completen y sean válidos en cualquier momento.

El generador de perfiles de terminales de baliza puede automatizar el proceso de identificación de terminales no autenticadores, aquellos que no poseen suplicantes 802.1X y el mantenimiento de la validez de estos terminales en redes de distinta escala en la funcionalidad de perfiles de terminales y supervisión del comportamiento. A través de una interfaz LDAP estándar, el sistema Beacon puede servir como una base de datos externa o directorio de los terminales que se autenticarán a través de MAB. Cuando se recibe una solicitud MAB de la infraestructura de borde, ACS puede consultar el sistema Beacon para determinar si un punto final determinado debe ser admitido o no en la red basándose en la información más actual sobre el punto final conocido por Beacon, para evitar la necesidad de configuración manual.

Consulte NAC: Ejemplo de Configuración de Integración LDAP con ACS 5.x y Posterior para obtener más información y una configuración similar usando ACS 5.x y posterior.

prerrequisitos

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.

- Switch Cisco 3750 que ejecuta 12.2(25)SEE2
- Cisco Secure Access Control Server para Windows 4.1

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.

Antecedentes

MAB es una funcionalidad esencial para el soporte dinámico de dispositivos como impresoras, teléfonos IP, equipos de fax y otros dispositivos no compatibles con 802.1X en el entorno posterior a la implementación de 802.1X. Sin una función MAB, los puertos de acceso a la red que proporcionan conectividad a terminales que no son compatibles con 802.1X deben aprovisionarse de forma estática para no intentar la autenticación 802.1X o mediante el uso de otras funciones que proporcionan opciones de políticas muy limitadas. Por razones obvias, esto no es necesariamente escalable en entornos de grandes empresas. Con MAB habilitado junto con 802.1X en todos los puertos de acceso, los terminales conocidos no compatibles con 802.1X se

pueden mover a cualquier lugar del entorno y, aun así, conectarse a la red de forma fiable (y segura). Debido a que los dispositivos admitidos en la red se están autenticando, se pueden aplicar diferentes políticas a diferentes dispositivos

Además, los terminales no compatibles con 802.1X que no se conocen en el entorno, como los portátiles que pertenecen a visitantes o contratistas, pueden tener acceso restringido a la red a través de MAB si lo desea.

Como sugiere el nombre, la opción de omisión de autenticación MAC utiliza la dirección MAC del terminal como la credencial principal. Con MAC Authentication Bypass habilitado en un puerto de acceso, si un punto final se conecta y no responde al desafío de autenticación 802.1X, el puerto vuelve al modo MAB. El switch que intenta el MAB de un punto final hace una solicitud RADIUS estándar al ACS con el MAC de la estación. Intenta conectarse a la red y solicita la autenticación del punto final desde ACS antes de la admisión del punto final a la red.

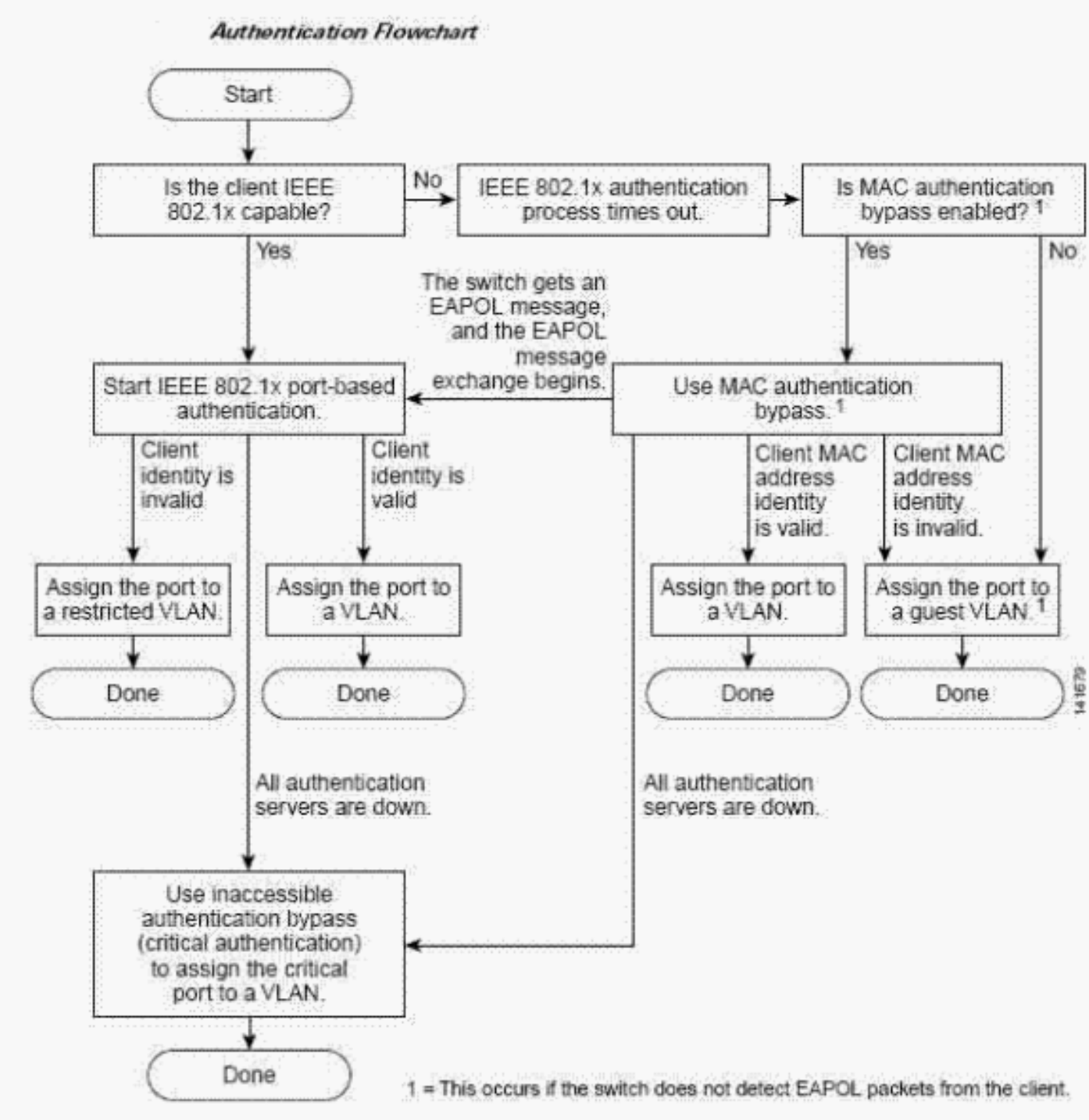
Configuración

Diagrama de diagrama de flujo

Este diagrama de flujo tomado de la documentación de Cisco Systems ilustra cómo se utiliza MAB junto con la autenticación 802.1X en la infraestructura del perímetro de Cisco a medida que los nuevos terminales intentan conectarse a la red.

Este documento utiliza este flujo de trabajo de diagrama de flujo:

Figura 1: Flujo de autenticación



ACS se puede configurar para utilizar su propia base de datos interna o un servidor LDAP externo para autenticar las solicitudes de los usuarios de direcciones MAC. El sistema de perfiles de punto final de baliza está completamente habilitado LDAP de forma predeterminada y puede ser utilizado por ACS para autenticar las solicitudes de usuario de direcciones MAC a través de la funcionalidad LDAP estándar. Debido a que Beacon automatiza tanto la detección como la definición de perfiles de todos los terminales en la red, ACS puede consultar la baliza a través de LDAP para determinar si el MAC debe ser admitido en la red, y en qué grupo se debe mapear el punto final. Esto automatiza y mejora significativamente la función de omisión de autenticación MAC, especialmente en entornos empresariales de gran tamaño.

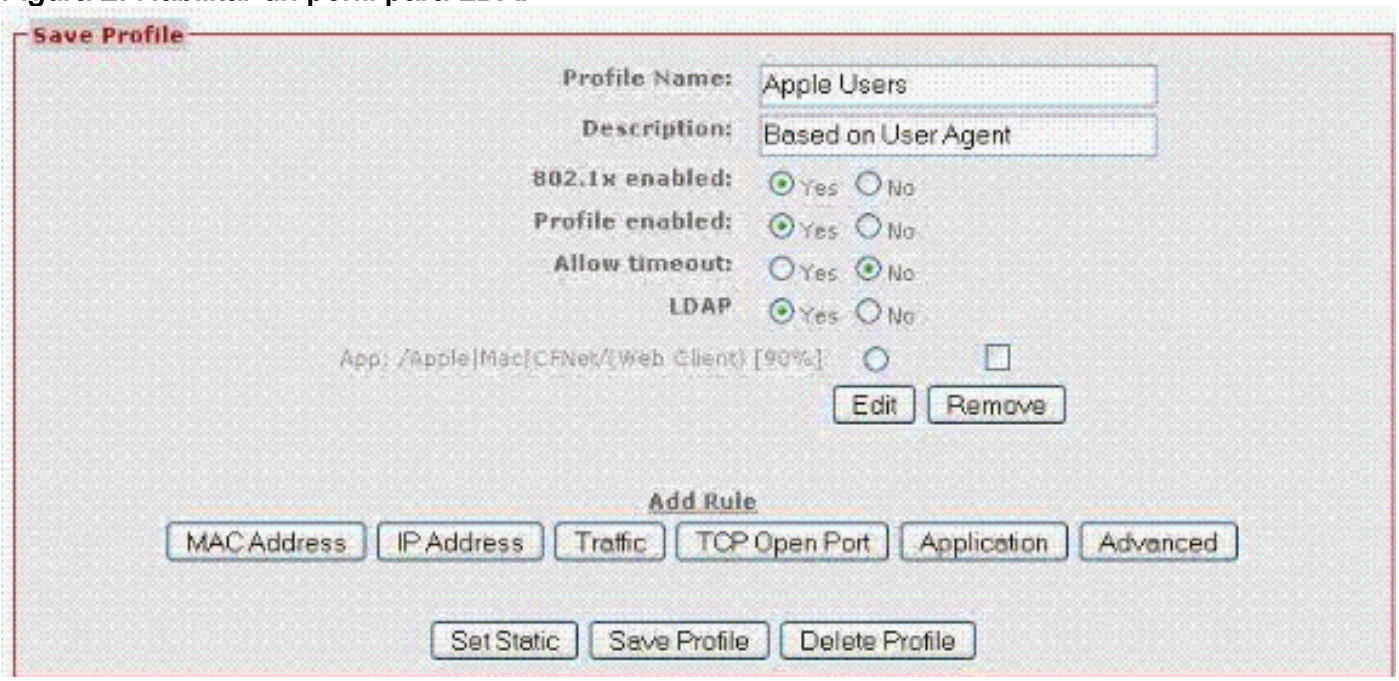
A través de la funcionalidad de Monitoreo de Comportamiento proporcionada por Beacon, los dispositivos que se observa que se comportan de manera inconsistente con los Profiles habilitados para MAB se pasan de 4 perfiles habilitados para LDAP y posteriormente fallan en el siguiente intento regular de reautenticación.

Configuración del sistema del generador de perfiles de punto final de baliza para MAB

La configuración del sistema Beacon para la integración con ACS a los fines de soporte MAB es sencilla, ya que la funcionalidad LDAP está habilitada de forma predeterminada. La tarea de configuración principal es identificar los perfiles que contienen los extremos que se desea autenticar a través de MAB en el entorno y luego habilitar esos perfiles para LDAP. Normalmente, los perfiles de baliza, que contienen dispositivos propiedad de la organización, deben tener acceso a la red cuando se ven en un puerto pero se sabe que no pueden autenticarse a través de 802.1X. Normalmente, estos son perfiles que contienen impresoras, teléfonos IP o UPS manejables como ejemplos comunes.

Si las impresoras profiladas por Beacon se colocaron en un perfil denominado *Impresoras*, y los teléfonos IP en un perfil denominado *Teléfonos IP*, por ejemplo, estos perfiles deben habilitarse para LDAP de modo que los terminales colocados en esos perfiles den como resultado una autenticación exitosa como Teléfono IP conocido e Impresoras en el entorno a través de MAB. Si habilita un perfil para LDAP, esto requiere que se seleccione el botón de opción LDAP en la configuración del perfil de terminal, como se muestra en este ejemplo:

Figura 2: Habilitar un perfil para LDAP



Cuando ACS proxies MAC authentication to Beacon through LDAP, la consulta consiste en dos subconsultas, las cuales deben devolver un resultado válido y no nulo. La primera consulta a Beacon es si se conoce o no el MAC para Beacon, por ejemplo, si se ha descubierto y agregado a la base de datos Beacon. Si Beacon aún no ha descubierto el terminal, éste se considera desconocido. La segunda consulta no es necesaria en el caso de los terminales que Beacon no ha detectado y que no están en su base de datos. Si se ha descubierto el punto final y se encuentra en la base de datos de baliza, la siguiente consulta es determinar el perfil actual del punto final. Si un punto final aún no ha sido definido o está actualmente en un perfil no habilitado 5 para LDAP, el resultado desconocido se devuelve a ACS y la autenticación del punto final por Beacon falla. Depende de cómo se configure ACS que esto puede dar como resultado la denegación de acceso a la red por completo, o que se le asigne una política apropiada para dispositivos desconocidos o invitados.

Solamente en el caso en que el MAC es un punto final que Beacon ha descubierto y colocado en

un Perfil habilitado para LDAP, la respuesta es que el punto final es conocido y Profilado por Beacon se devuelve al ACS. Lo que es más importante, para estos terminales, Beacon proporciona el nombre actual del perfil, que permite a ACS asignar los terminales conocidos a los grupos Cisco SecureAccess. Esto permite una determinación granular de la política, tan granular como una política independiente para cada perfil habilitado para LDAP de baliza, si lo desea.

Configuración ACS para MAB y utilización de Beacon como base de datos de usuario externa

La configuración de ACS para MAB y la utilización de Beacon como base de datos de usuario externa requieren tres pasos distintos. El orden ilustrado en este documento sigue un flujo de trabajo que es eficiente cuando realiza la configuración MAB en su totalidad y puede variar para los sistemas que han estado en funcionamiento con otros modos de autenticación ya configurados.

Configuración de Cisco SecureGroup(s)

Cuando intenta MAB para un punto final determinado que intenta conectarse a la red, ACS consulta a Beacon LDAP para determinar si Beacon ha descubierto el MAC, y en qué Profile Beacon ha colocado actualmente la dirección MAC como se describió anteriormente en el documento.

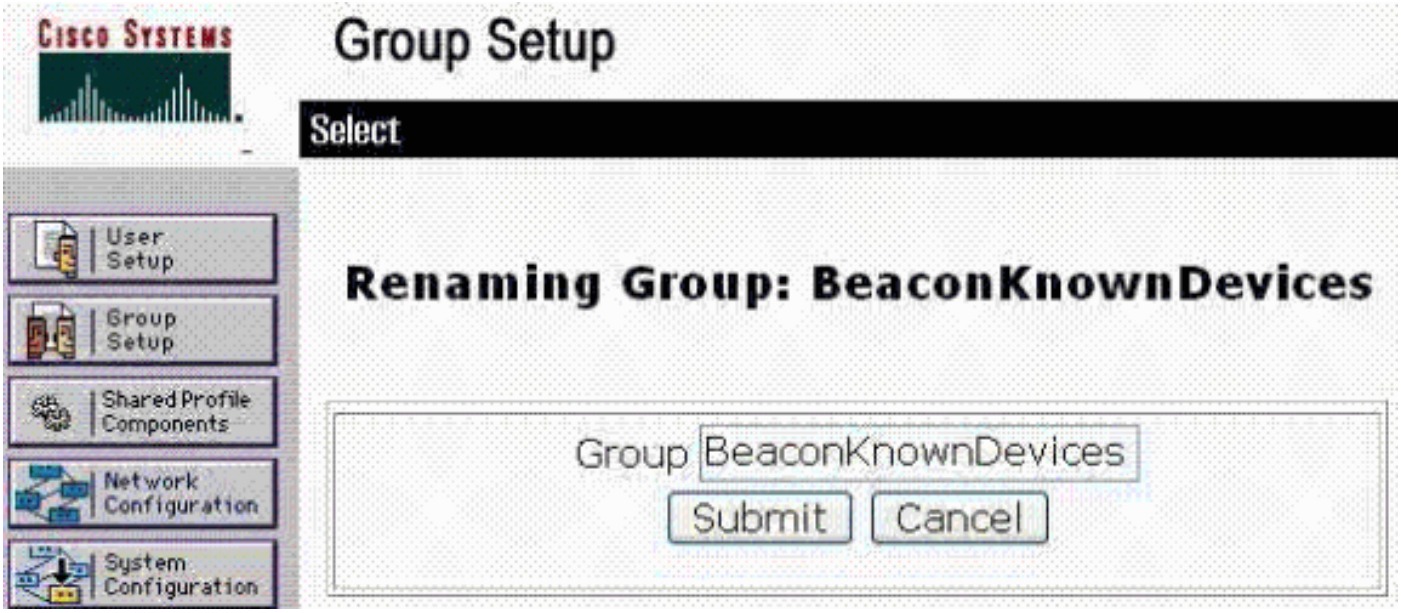
El mecanismo Cisco SecureGroup con ACS se puede utilizar para autenticar y aplicar políticas a los terminales que han sido descubiertos y perfilados por Beacon a través de MAB, así como a los errores de autenticación: aquellos dispositivos no conocidos o no actualmente Profilados por Beacon.

Por ejemplo, se puede agregar un grupo a la configuración ACS para terminales detectados y perfilados por Beacon y llamados *BeaconKnownDevices*, y otro grupo *BeaconUnknownDevices* para dispositivos que no son conocidos actualmente por Beacon. Beacon no ha descubierto el MAC, o no lo ha descrito en un perfil habilitado para LDAP. Como se muestra más adelante en este documento, los Grupos habilitan la aplicación de la política a los terminales cuando intentan unirse a la red.

Tenga en cuenta que en el ejemplo descrito en este documento, sólo se configuran dos grupos, BeaconKnown y BeaconUnknown. Sin embargo, es posible crear varios grupos seguros para los terminales detectados y perfilados por Beacon, hasta uno para cada perfil habilitado para LDAP en Beacon, cada uno con parámetros de política diferentes como asignación de VLAN. Además, el grupo de dispositivos BeaconUnkown se puede configurar para denegar todo acceso a los terminales que aún no se han descubierto o colocado en un perfil habilitado para LDAP por 6 baliza. Esto se logra si elige la casilla Grupo Desactivado en los parámetros de la ventana de configuración del grupo BeaconUnknownDevices.

La creación de grupo en ACS se inicia desde el botón Group Setup en la interfaz de usuario ACS. Elija uno de los Grupos disponibles y luego elija el botón **Cambiar nombre de grupo** para cambiar el nombre de grupo a dispositivos conocidosBeaconcomo se muestra en este ejemplo. Haga clic en **Enviar** para guardar el cambio.

Figura 3: Editar grupo CiscoSecure

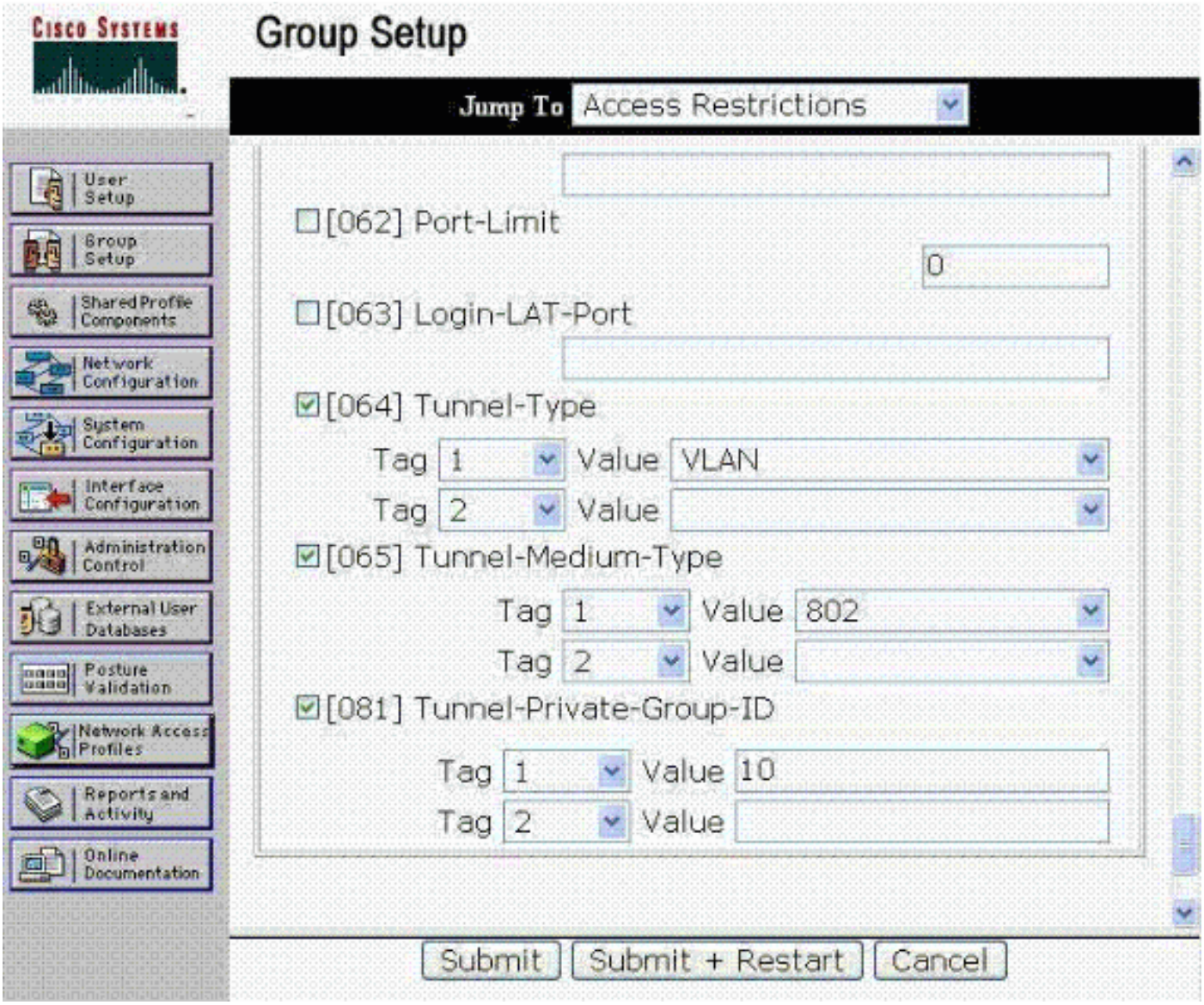


Elija **Edit Settings** para editar la configuración del Grupo. Edite los parámetros del grupo BeaconKnownDevices como desee. A efectos del ejemplo de este documento, los parámetros de grupo que se cambian incluyen sólo los atributos de radio IETF, que se encuentran en la parte inferior de la página.

Específicamente, usted designará que los dispositivos autenticados a este grupo, las direcciones MAC que Beacon ha Profilado a los Perfiles seleccionados para MAB y habilitados para LDAP, tienen parámetros de política devueltos al switch de autenticación que habilita la admisión de los puntos finales a la red en la VLAN adecuada. Para hacer esto, los atributos RADIUS 064 Tunnel-Type, 065 Tunnel-Medium-Type y 081 Tunnel-Private-Group-ID se configuran para que los terminales se coloquen en la VLAN deseada, como se muestra en la Figura 4.

Asegúrese de que las casillas de verificación situadas junto a cada atributo RADIUS estén marcadas.

Figura 4: Atributos de VLAN de grupo

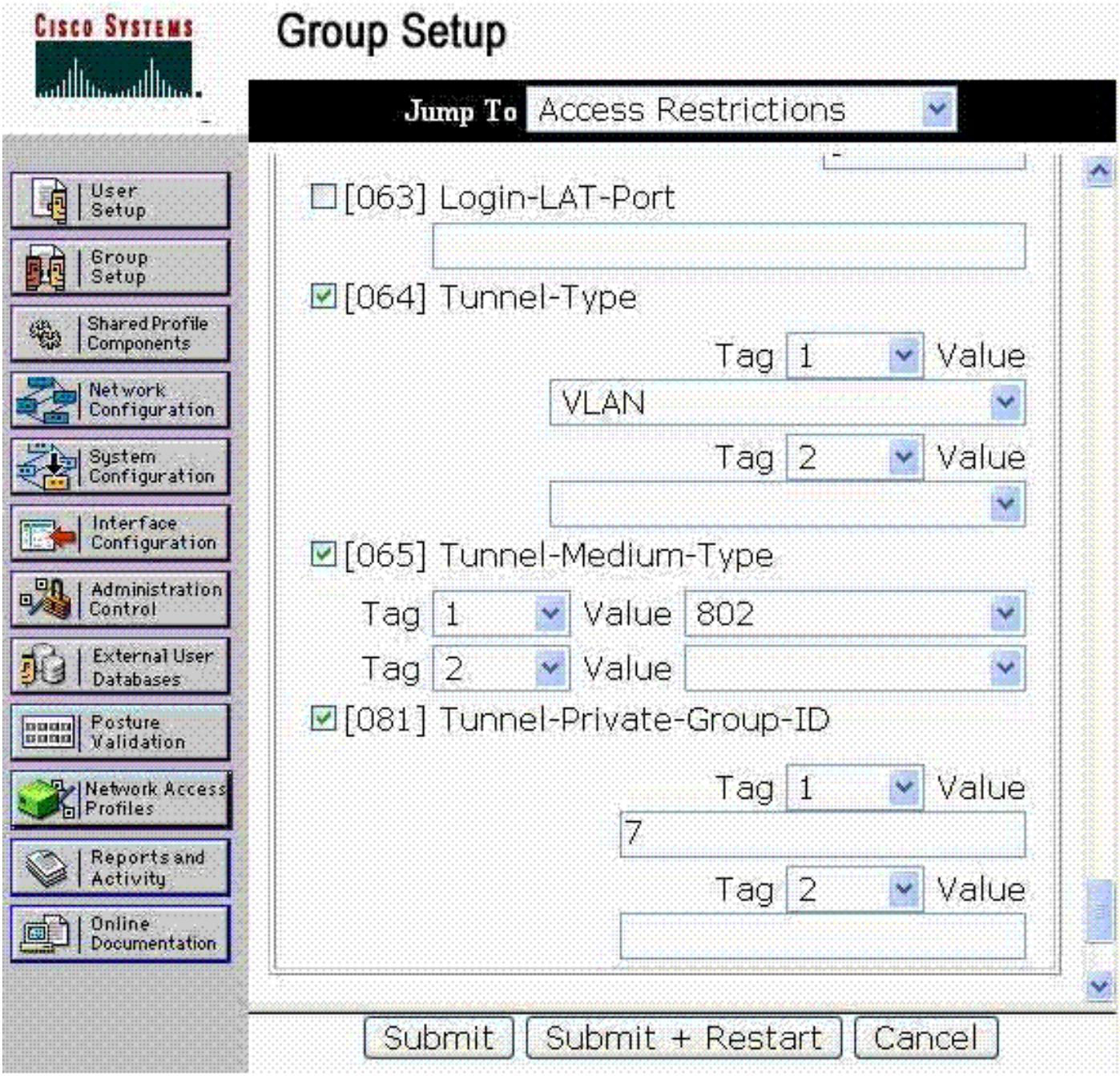


En el ejemplo que se muestra, los terminales autenticados correctamente por Beacon y posteriormente asignados al grupo ACS BeaconKnownDevices se colocan en la VLAN 10, la VLAN autorizada en la configuración de red de ejemplo, durante la conexión a la red y autenticados correctamente en MAB por ACS con el uso de Beacon como base de datos de usuario externa.

De manera similar, se crea el grupo BeaconUnknownDevices para dispositivos que Beacon no conoce actualmente, como se muestra. Una vez más, si estos dispositivos no deberían tener acceso a la red, simplemente marque la casilla de verificación **Grupo Desactivado** en la parte superior del formulario. Los terminales que no han sido detectados por Beacon o que no están actualmente Profilados por Beacon en un perfil habilitado para LDAP fallan MAB y no son admitidos en la red.

Esta figura muestra la alternativa al uso de la casilla Grupo Desactivado. En este caso, los terminales que Beacon no puede autenticar se asignan a un grupo que está habilitado, pero que tiene una política diferente a la de los terminales conocidos. Consulte la Figura 5.

Figura 5: Parámetros de VLAN para BeaconUnknownDevices



Tenga en cuenta que para los dispositivos desconocidos en este ejemplo, se admiten a la red pero se relegan a una VLAN de invitado o restringida, VLAN 7. En la red de ejemplo, VLAN 7 es la VLAN de invitado, que permite a los terminales sólo acceso a Internet y prohíbe el acceso a los recursos internos.

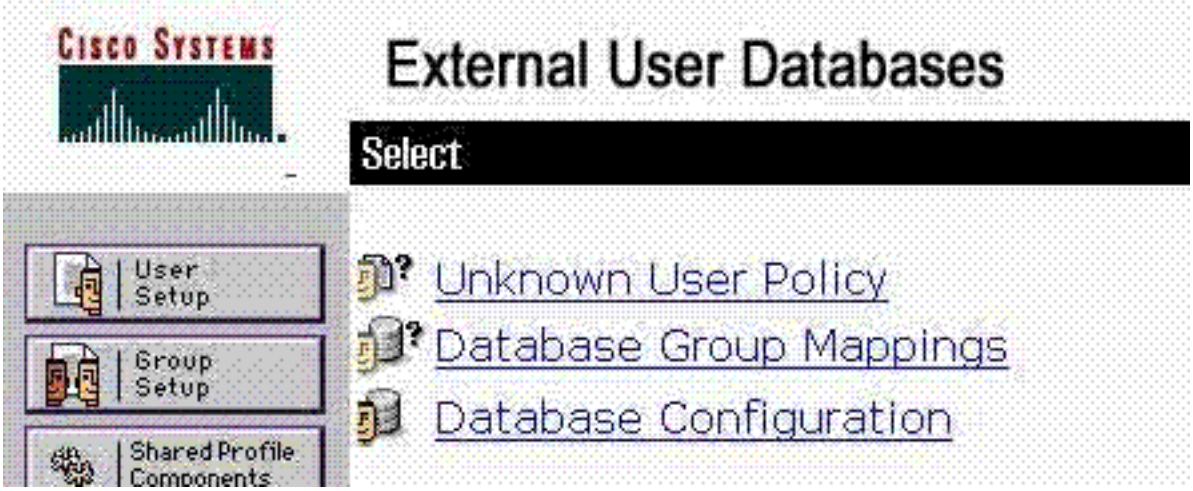
Cuando el ACS solicita la autenticación desde el Beacon de un MAC de un punto final que aún no ha sido descubierto o descrito por Beacon, el ACS coloca el MAC en este grupo y devuelve el resultado al switch de autenticación habilitado para el MAB.

Configuración de Base de Datos de Usuario Externa ACS

ACS se debe configurar para proxy las solicitudes MAB de los switches de acceso a Beacon vía LDAP. Esto requiere que la configuración ACS incluya el sistema Beacon como base de datos de usuario externa LDAP genérica. Los pasos descritos en esta sección ilustran cómo agregar el sistema de perfiles de punto final de baliza 9 como una base de datos de usuarios externos que ACS consultará cuando reciba solicitudes MAB. Elija **Base de datos de usuario externa** en el panel de navegación global para activar la ventana Base de datos de usuario externa que se

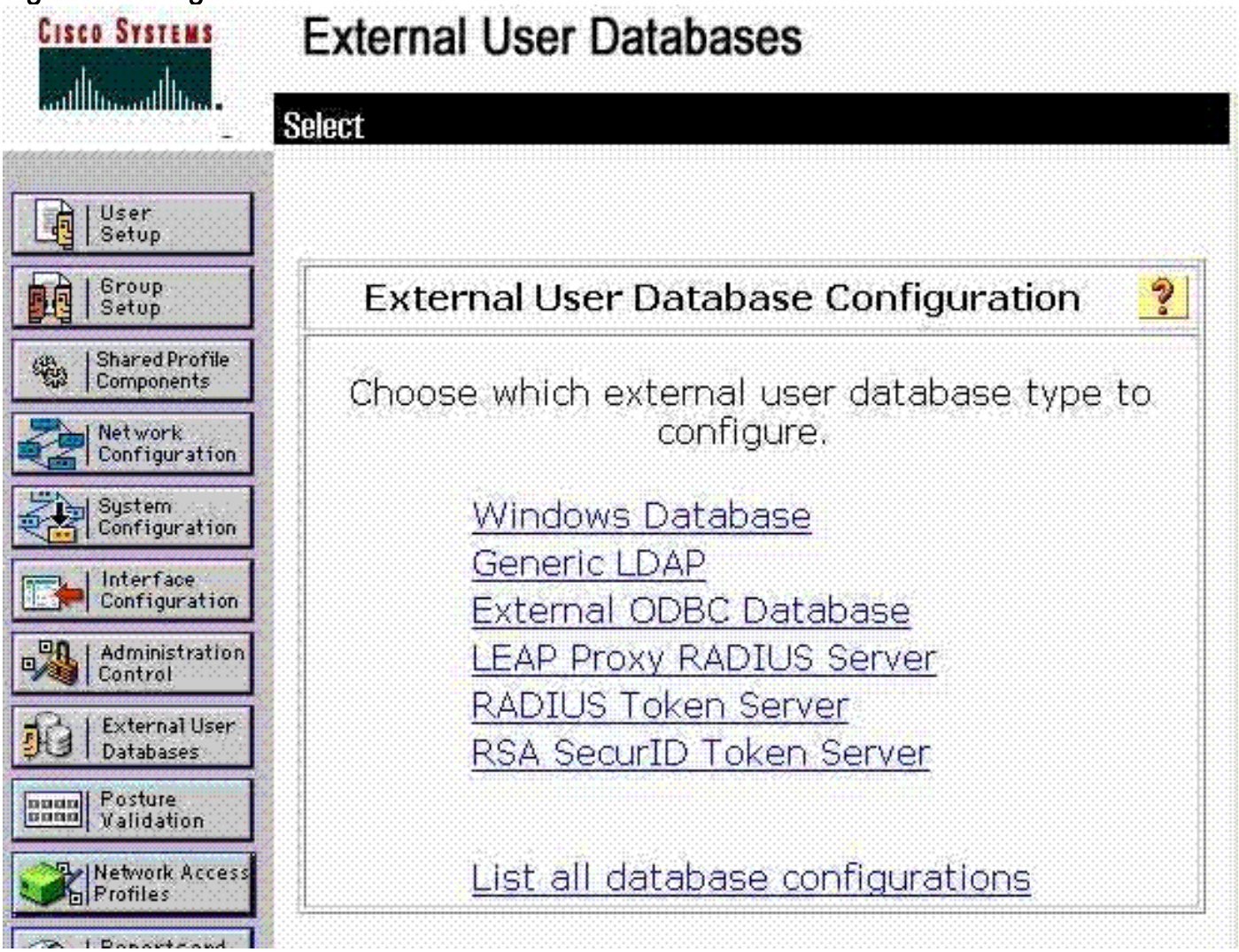
muestra en la Figura 6.

Figura 6: Pantalla principal de configuración de la base de datos externa



La primera tarea en la configuración de Beacon como base de datos de usuario externa es agregar el sistema Beacon como base de datos de usuario externo LDAP genérico. Elija **Database Configuration** para que aparezca la ventana ilustrada en la Figura 7.

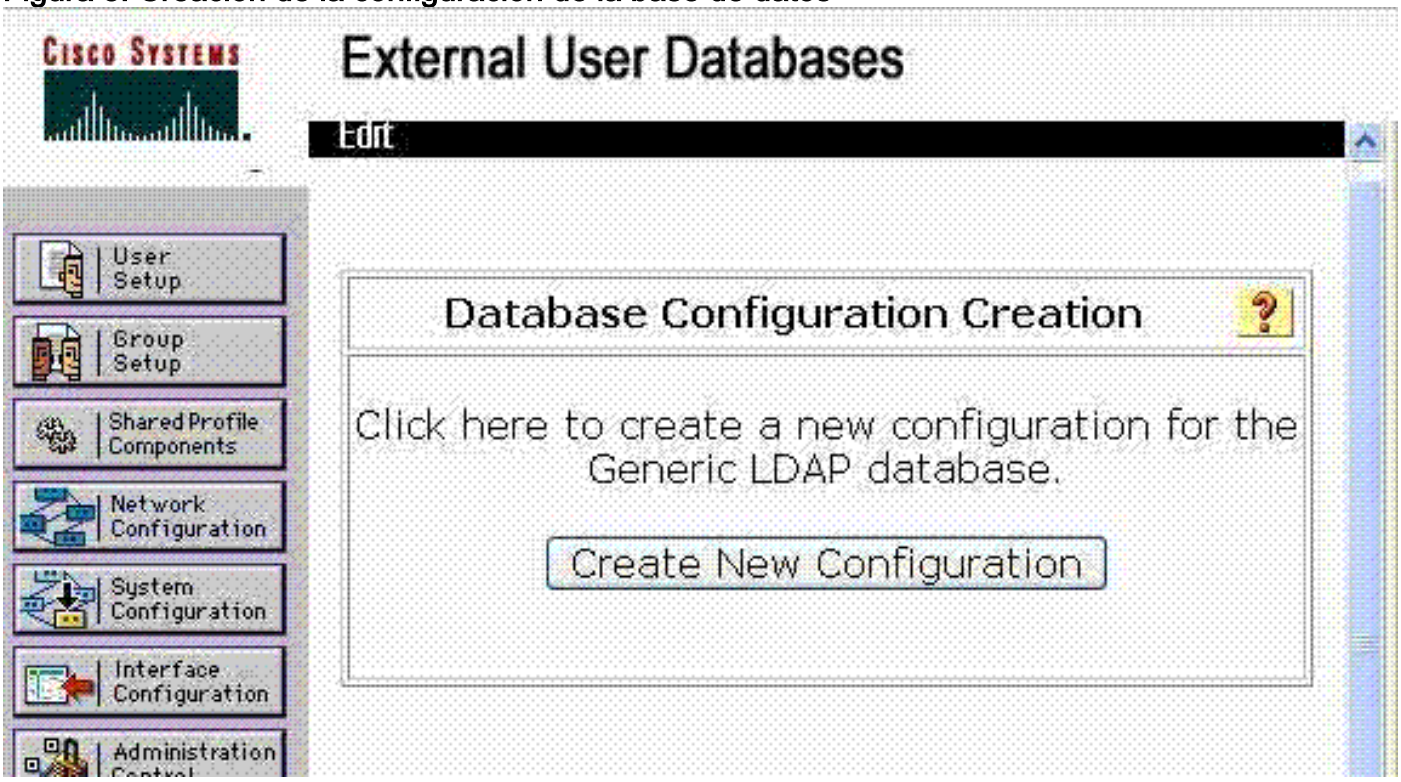
Figura 7: Configuración de Base de Datos de Usuario Externa ACS



Elija **Generic LDAP** para abrir el formulario utilizado para agregar el sistema de perfiles de punto final de baliza como base de datos de usuario externo en la configuración ACS. Esta ventana aparece para habilitar la creación de una nueva configuración de base de datos de usuario

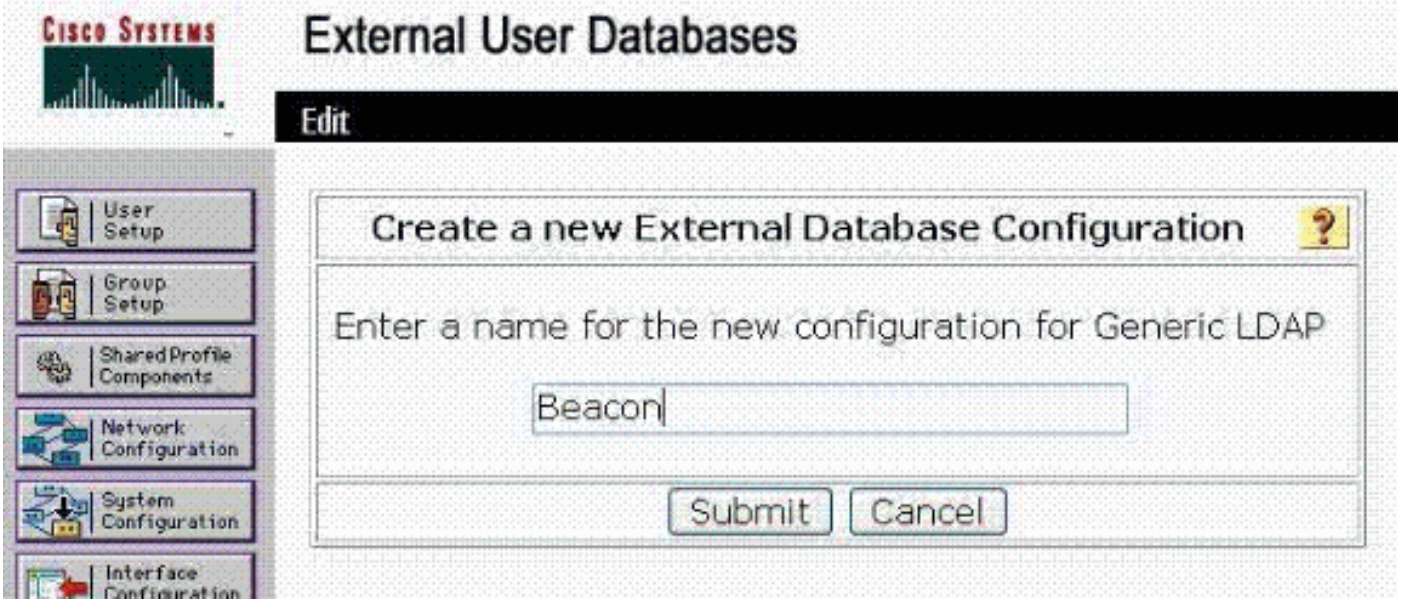
externa del tipo LDAP genérico.

Figura 8: Creación de la configuración de la base de datos



Elija el botón **Crear nueva configuración** para crear la base de datos LDAP genérica para Beacon. Esta ventana aparece y permite asignar el nombre a la nueva base de datos externa.

Figura 9: Base de datos de usuario externa de baliza de nombre

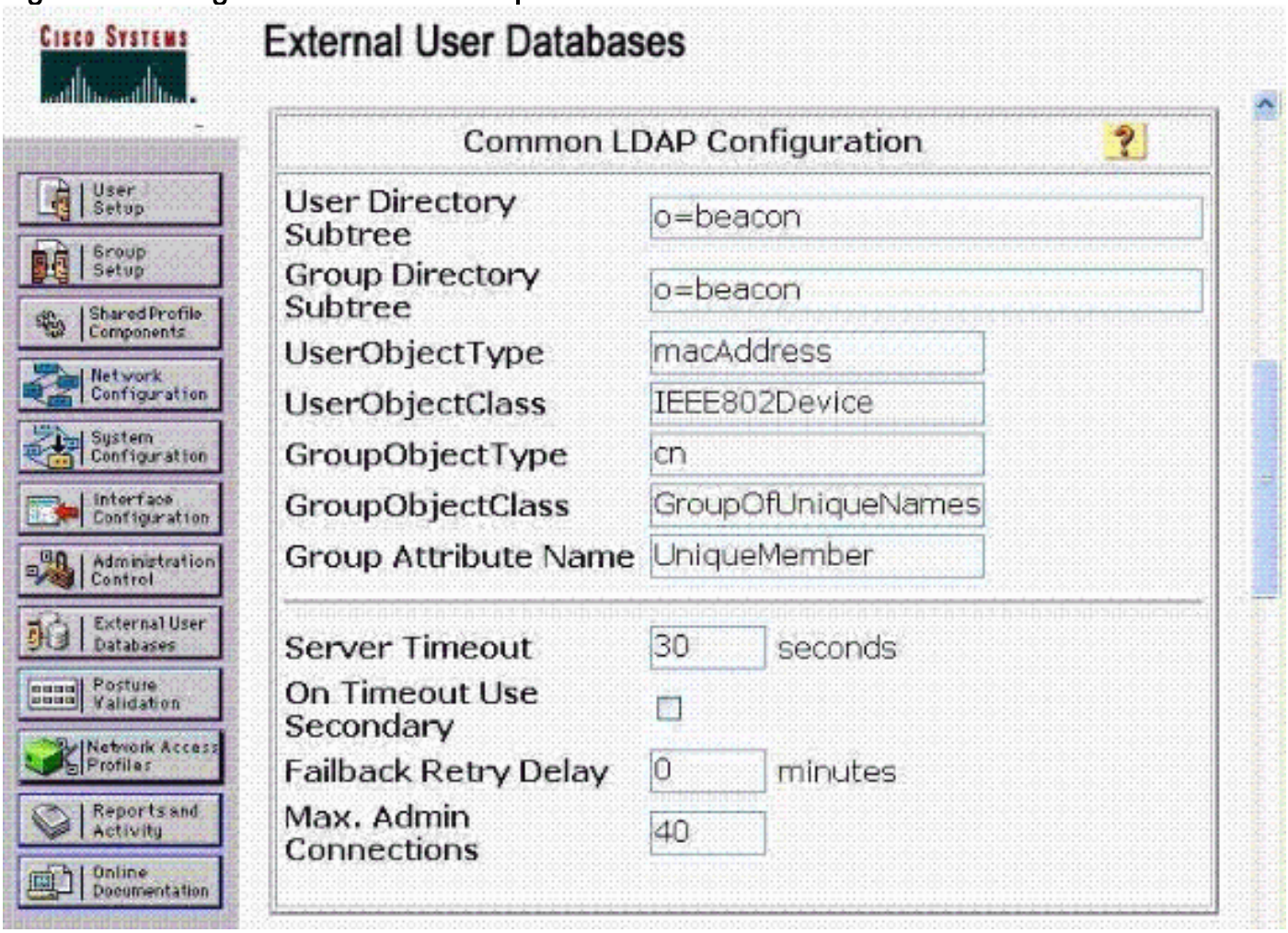


Ingrese un nombre para la base de datos externa LDAP genérica de baliza que permite diferenciarla fácilmente de otras bases de datos externas en la configuración. Elija **Submit** para pasar a la entrada de los parámetros LDAP requeridos que habilitan la comunicación entre 11 ACS y Beacon para el propósito de la autenticación de las direcciones MAC con el uso de la información de la base de datos Beacon.

La Figura 10 ilustra los parámetros de configuración común de LDAP que deben ingresarse para la base de datos de usuario externo LDAP genérico de baliza que se agrega a la configuración

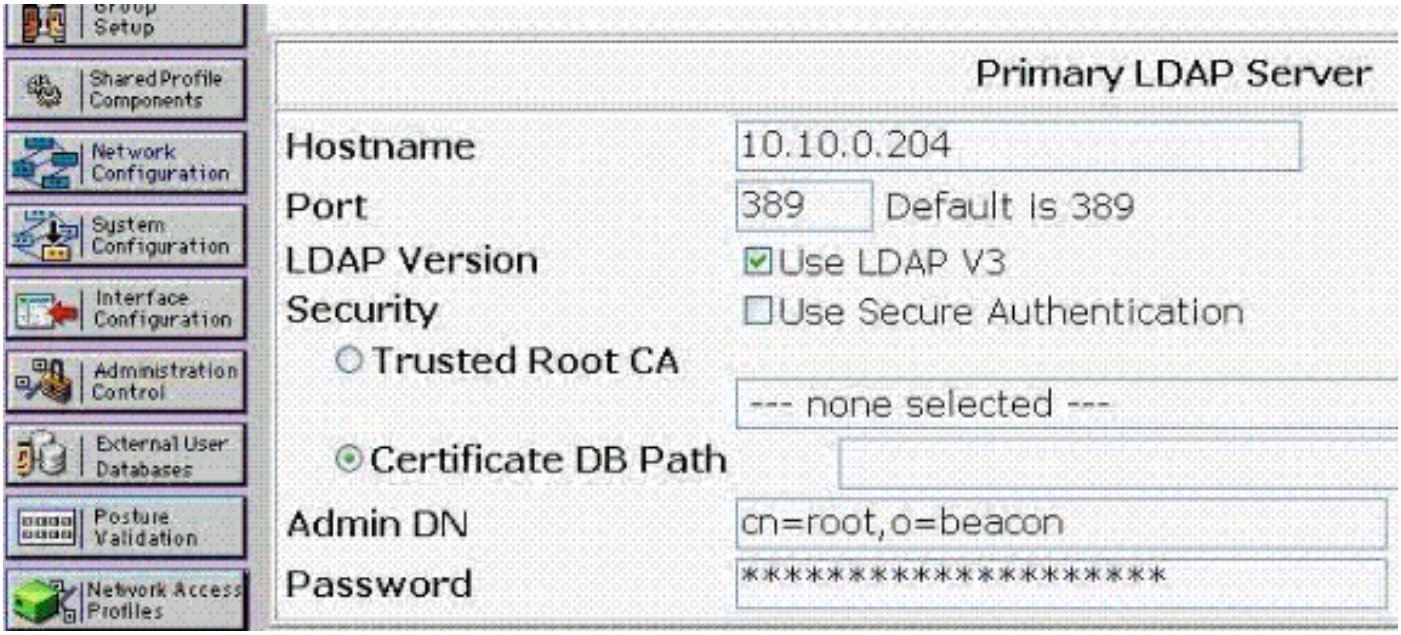
ACS. Tenga en cuenta que estos parámetros proporcionan al ACS la información que necesita para consultar la baliza a través de LDAP. Estos parámetros deben ingresarse exactamente como se muestra en esta figura para facilitar la comunicación entre el ACS y el generador de perfiles de punto final de baliza.

Figura 10: Configuración LDAP común para baliza



Nota: Utilice la **baliza GBS** de contraseña para la contraseña de enlace LDAP. La contraseña se introduce en la parte inferior del formulario que se muestra en la figura 11.

Figura 11: Parámetros del servidor de baliza

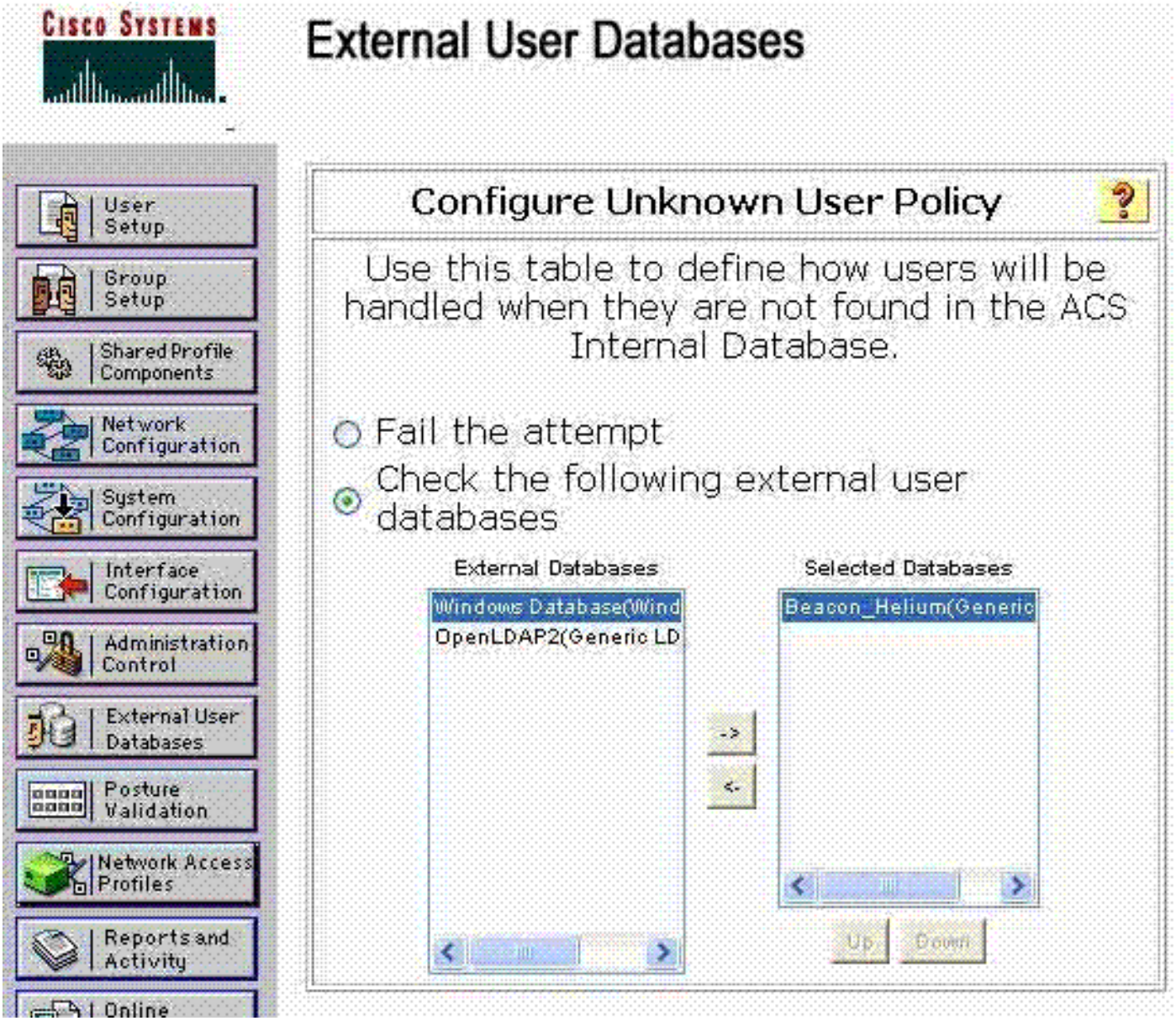


La segunda tarea de configuración asociada a la configuración de Beacon como base de datos de usuario externa es la configuración de la política de usuario desconocida. La política de usuario desconocido le indica a ACS que consulte la base de datos de baliza cada vez que recibe una solicitud de autenticación para un usuario, que es una dirección MAC en el caso de MAB, para la que no tiene información en su propia base de datos.

Tenga en cuenta que en una implementación típica de ACS, puede haber bases de datos de usuarios externos configuradas y ya se pueden configurar para consultar esas bases de datos cuando se envían credenciales de usuario desconocidas. La base de datos de usuarios externos de Beacon se debe agregar a la lista para consultarla cuando los switches solicitan MAB de direcciones MAC individuales.

Estas cifras describen el flujo de trabajo para la configuración de la política de usuario desconocida y la adición de Beacon como base de datos de usuario externa que se debe consultar. Para, elija el enlace **Directiva de usuario desconocida** en la página principal Base de datos de usuario externa, como se muestra en la Figura 6, para iniciar el flujo de trabajo.

Figura 12: Configurar política de usuario desconocida

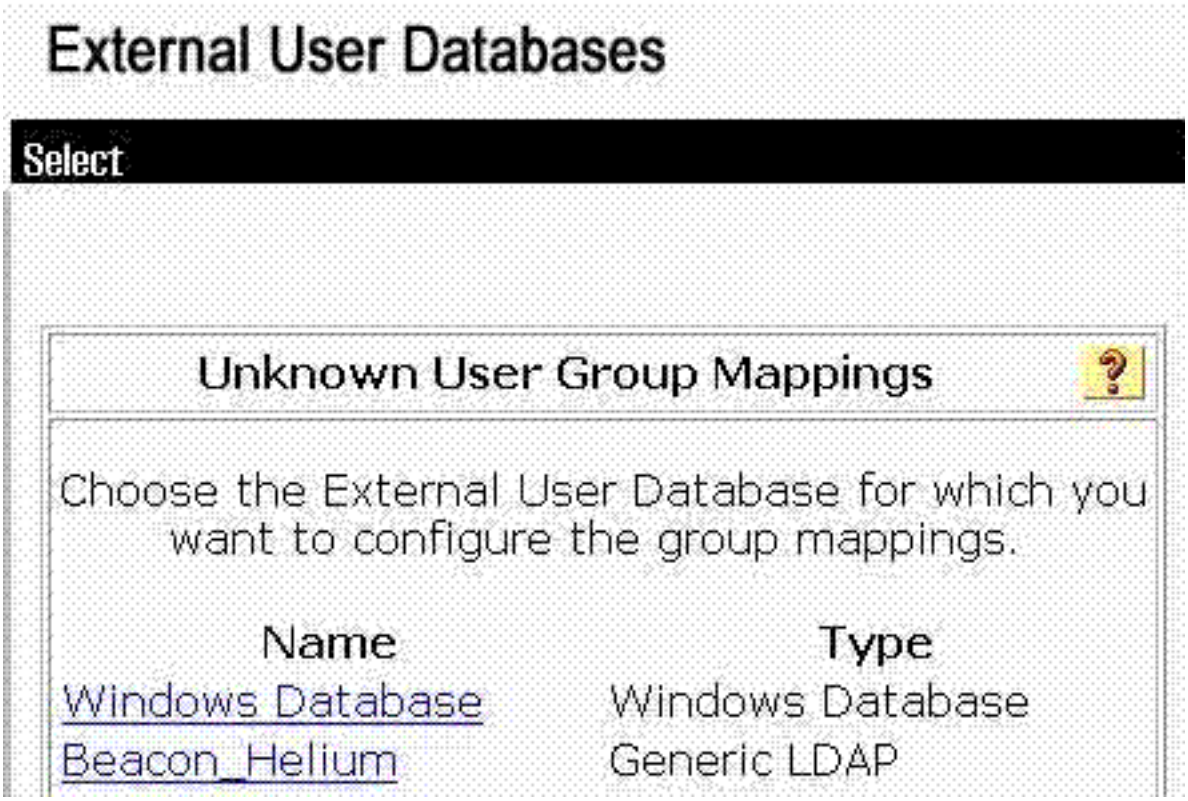


Elija la base de datos LDAP genérica de baliza agregada a la configuración ACS en el último paso de la lista de bases de datos externas a la izquierda (Beacon_Helium) en el ejemplo. Utilice **->** para desplazarse a las bases de datos seleccionadas. Asegúrese de elegir el botón de opción **Verificar las siguientes bases de datos de usuario externas**. Esto asegura que cuando los switches envían direcciones MAC para la autenticación a ACS, ACS consulta a Beacon para determinar si el punto final se conoce y tiene el perfil actual, si lo hubiera.

La tarea de configuración final para agregar Beacon como base de datos de usuarios externa es la finalización de Asignaciones de Grupos de Bases de Datos. Básicamente, esta asignación une los grupos de CiscoSecure creados, por ejemplo, BeaconKnownDevices y BeaconUnknownDevices, a consultas LDAP exitosas y fallidas realizadas a Beacon para que cada MAB intentado por los switches dé como resultado la asignación del terminal a un grupo CiscoSecure por ACS. Esto permite al ACS responder al switch independientemente de si el punto final debe ser admitido en la red y, si se admite, cuál debe ser la política como los atributos de VLAN.

Elija **Asignaciones de Grupo de Base de Datos** en la página principal de Bases de Datos de Usuario Externas como se muestra en la Figura 6 para configurar las asignaciones.

Figura 13: Asignaciones de grupos de base de datos

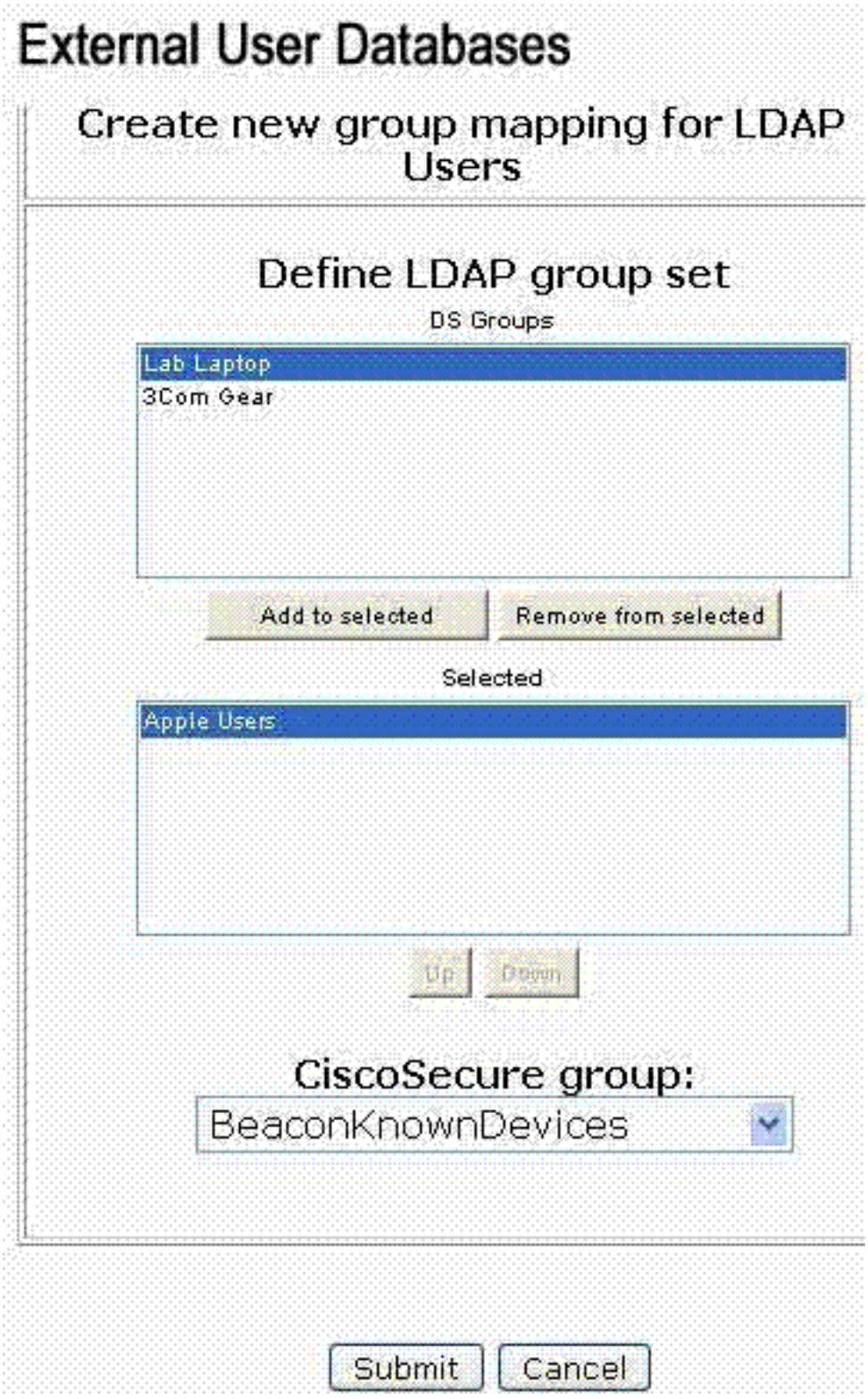


Cuando se elige la base de datos de usuarios externos de baliza creada anteriormente en esta sección con la selección del enlace, Beacon_Helium en el ejemplo anterior, se muestra la ventana ilustrada en la figura 14. Tenga en cuenta que todos los perfiles de baliza habilitados para LDAP dentro de la configuración del sistema de baliza, como se describe en la primera sección de estas instrucciones de configuración, se rellenan en los grupos de DS que están disponibles para la selección para crear mapeos dentro de ACS. Si los nombres del perfil de baliza habilitados para LDAP no se muestran en la interfaz ACS, esto indica un problema con la configuración de ACS LDAP. Consulte las instrucciones sobre la baliza de configuración como base de datos de usuario externa descritas anteriormente en esta sección, en particular los parámetros LDAP.

Tenga en cuenta que esta es la interfaz que permite la asignación de perfiles individuales habilitados para LDAP en Beacon con los grupos CiscoSecure configurados dentro de ACS. La interfaz permite la asignación de cada perfil habilitado para LDAP de baliza individual a un único grupo de CiscoSecure. En este ejemplo, sólo se creó un único grupo para dispositivos conocidos en perfiles de baliza habilitados para LDAP: BeaconKnownDevices. Sin embargo, se pueden crear varios grupos, cada uno con sus propios parámetros de política para manejar las autenticaciones exitosas de manera diferente según el perfil de baliza actual del dispositivo.

Por ejemplo, se puede crear un grupo CiscoSecure para BeaconKnownIPPhones, que devolvió los atributos de VLAN que asignan puntos finales en el perfil del teléfono IP en Beacon a la VLAN del teléfono cuando se une a la red y se autentica a través de MAB.

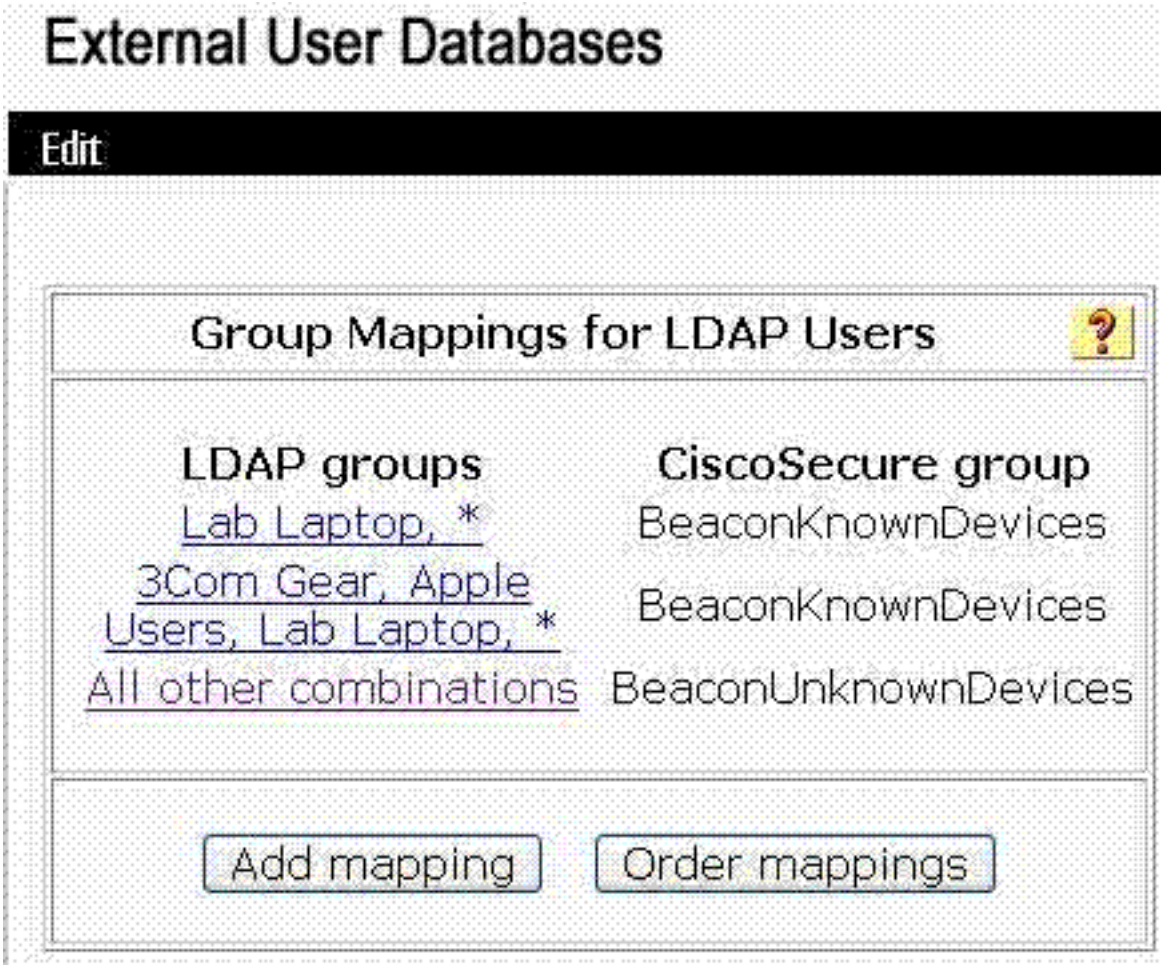
Figura 14: Asignación de perfil a grupo



Elija un grupo DS (perfil de baliza con LDAP habilitado) y asigne puntos finales en ese perfil al grupo CiscoSecure deseado en el menú desplegable. En el ejemplo anterior, las direcciones MAC que se encuentran actualmente en el perfil de usuarios de Apple en Beacon se autentican a través de MAB, colocadas en BeaconKnownDevices que da lugar a una autenticación y ubicación exitosas en la VLAN de usuario cuando se une a la red.

Al seleccionar enviar, aparece la lista de Asignaciones de grupo actuales en ACS cuando se autentican usuarios desconocidos en la base de datos de usuarios externos de Beacon.

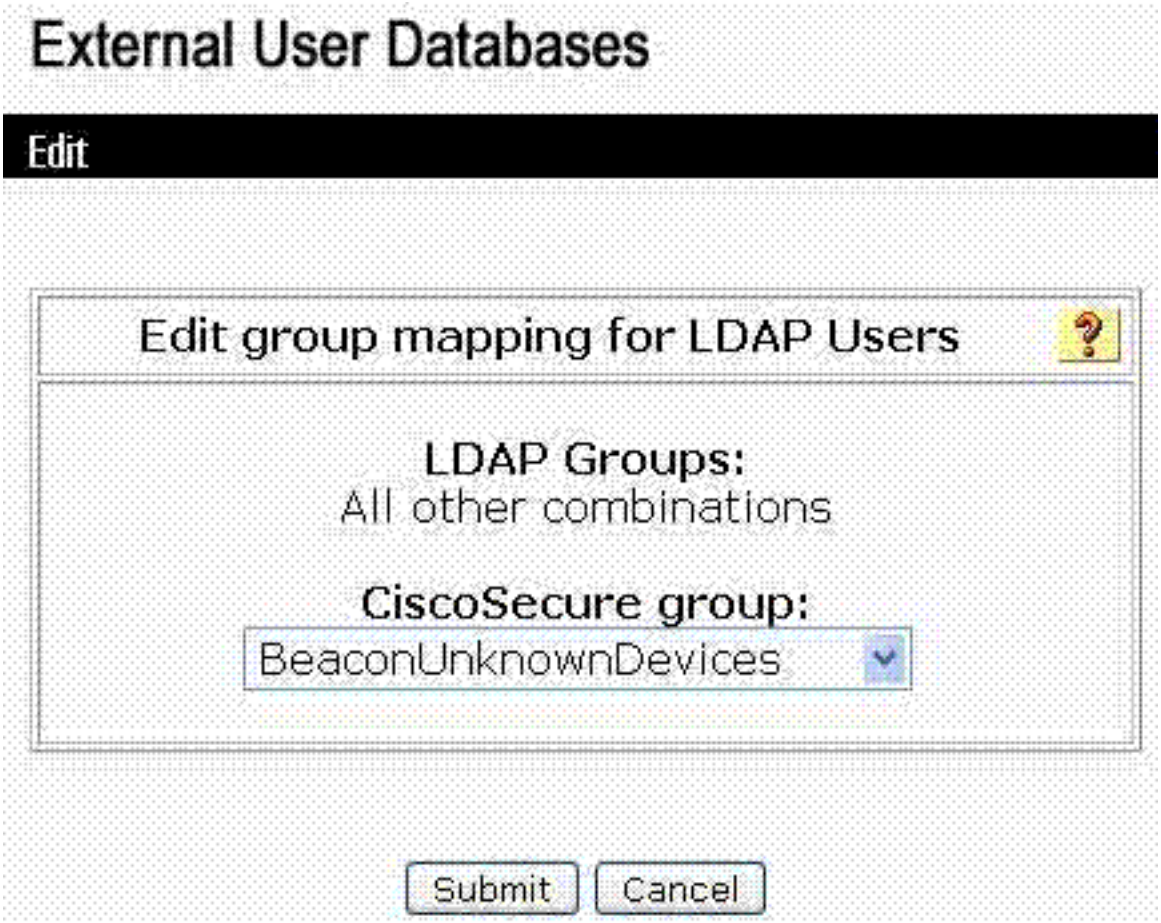
Figura 15: Asignaciones de grupo de lista



Tenga en cuenta que las asignaciones realizadas explícitamente con el procedimiento descrito anteriormente se enumeran en esta vista. Los grupos DS (perfiles habilitados para LDAP de baliza) no se asignan explícitamente a un grupo, que incluye los puntos finales que Beacon aún no ha detectado o colocado en un perfil habilitado para LDAP caen en el colector Todas las demás combinaciones. Básicamente, esto permite a los terminales sobre los que Beacon no puede proporcionar información en un grupo de CiscoSecure, por ejemplo, BeaconUnknownDevices. Como se ha descrito anteriormente, este grupo se puede inhabilitar por completo, lo que resulta en una falla de MAB, o como en el ejemplo anterior, se puede diseñar para proporcionar solamente conectividad limitada a los terminales no conocidos por Beacon.

A todas las demás combinaciones se les puede asignar un CiscoSecure Group (BeaconUnkownDevices) si hace clic en el enlace **Todas las demás combinaciones** para obtener esta ventana:

Figura 16: Asignación de un grupo a todas las demás combinaciones

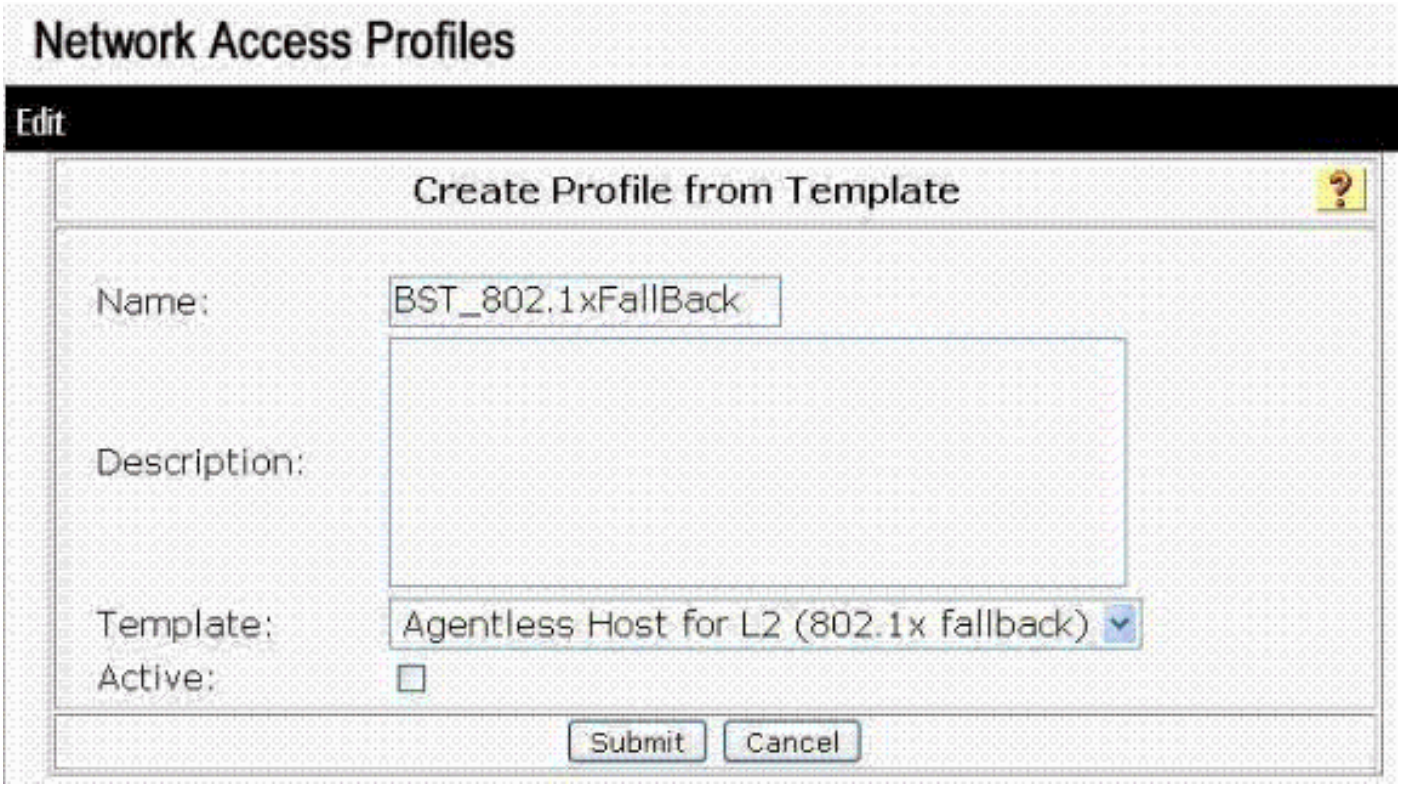


Configuración del perfil de acceso a la red

El último paso necesario en la configuración ACS para que MAB utilice el sistema de perfiles de punto final de baliza como proxy es la configuración de un perfil de acceso de red para la reserva 802.1X. Complete estos pasos descritos para configurar el perfil de acceso de red requerido para completar la configuración ACS de manera que MAB se configure y funcione según la configuración completada previamente.

El perfil de acceso a la red que se agregará es un perfil de plantilla. Elija los **perfiles de acceso a la red** de la página de navegación global. Luego elija **Add Template Profile** para mostrar este formulario ilustrado.

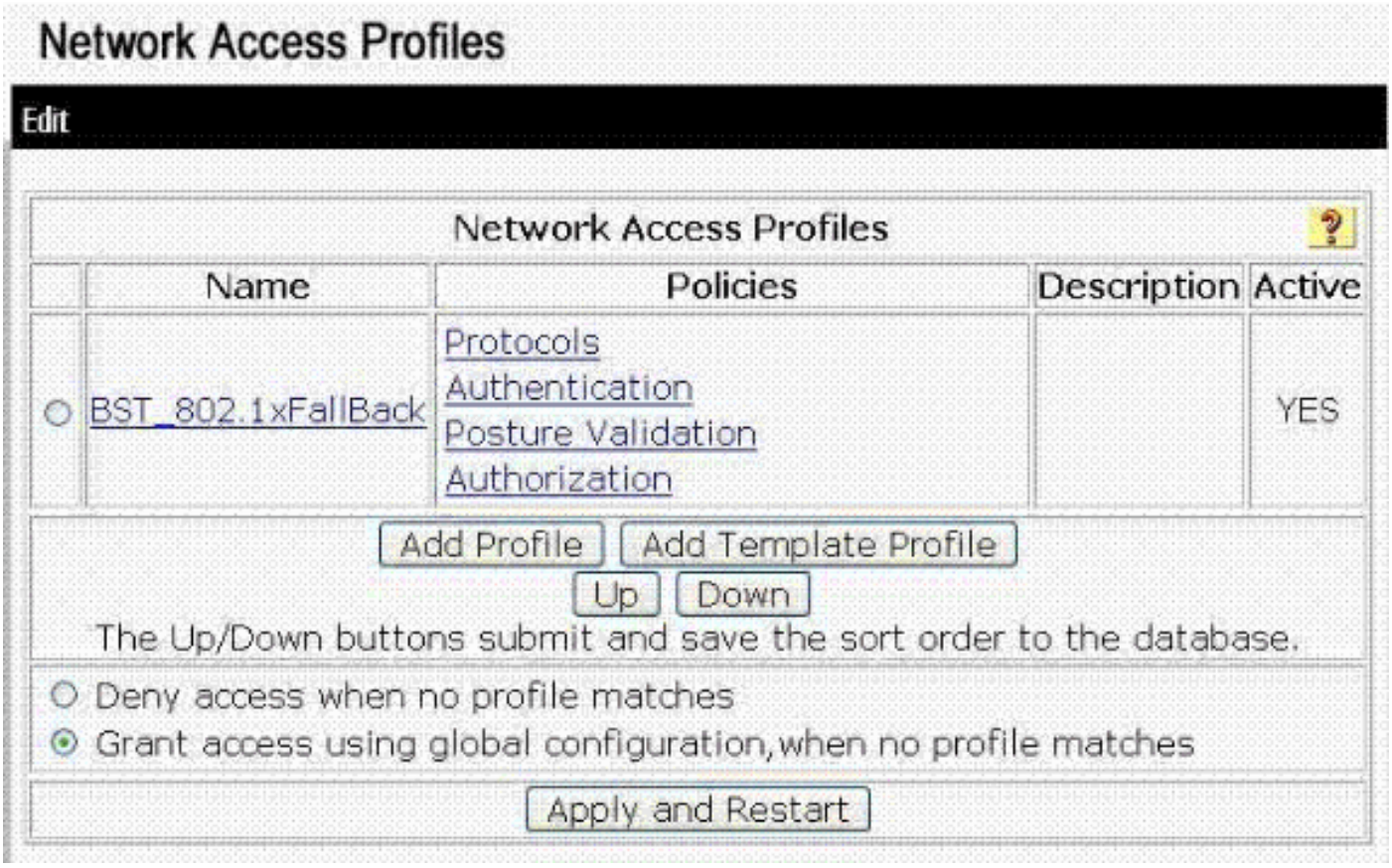
Figura 17: Agregar un perfil de acceso de red de plantilla



Asigne un nombre al perfil de acceso a la red para poder distinguirlo de otros y, si lo desea, agregue una descripción. La plantilla para este perfil se selecciona en la lista desplegable. Asegúrese de que **Host sin agente para L2 (reserva 802.1x)** esté seleccionado y marque la casilla de verificación **Activo**. Haga clic en el botón **Submit** cuando termine para guardar el perfil de acceso a la red.

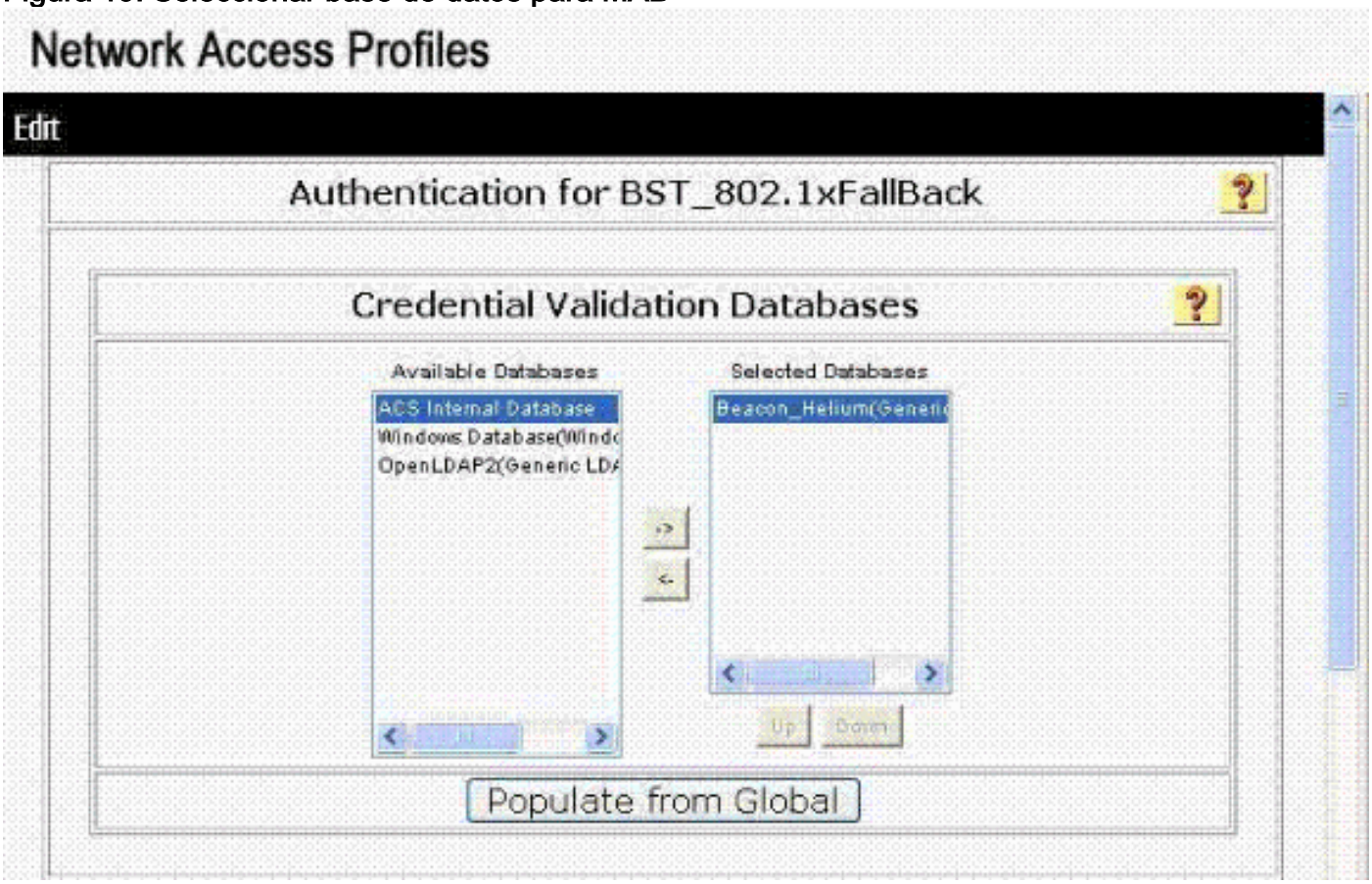
Al hacer clic en Enviar, se muestra este formulario que permite editar los parámetros del perfil que se acaba de crear, como se muestra.

Figura 18: Editar NAP para MAB



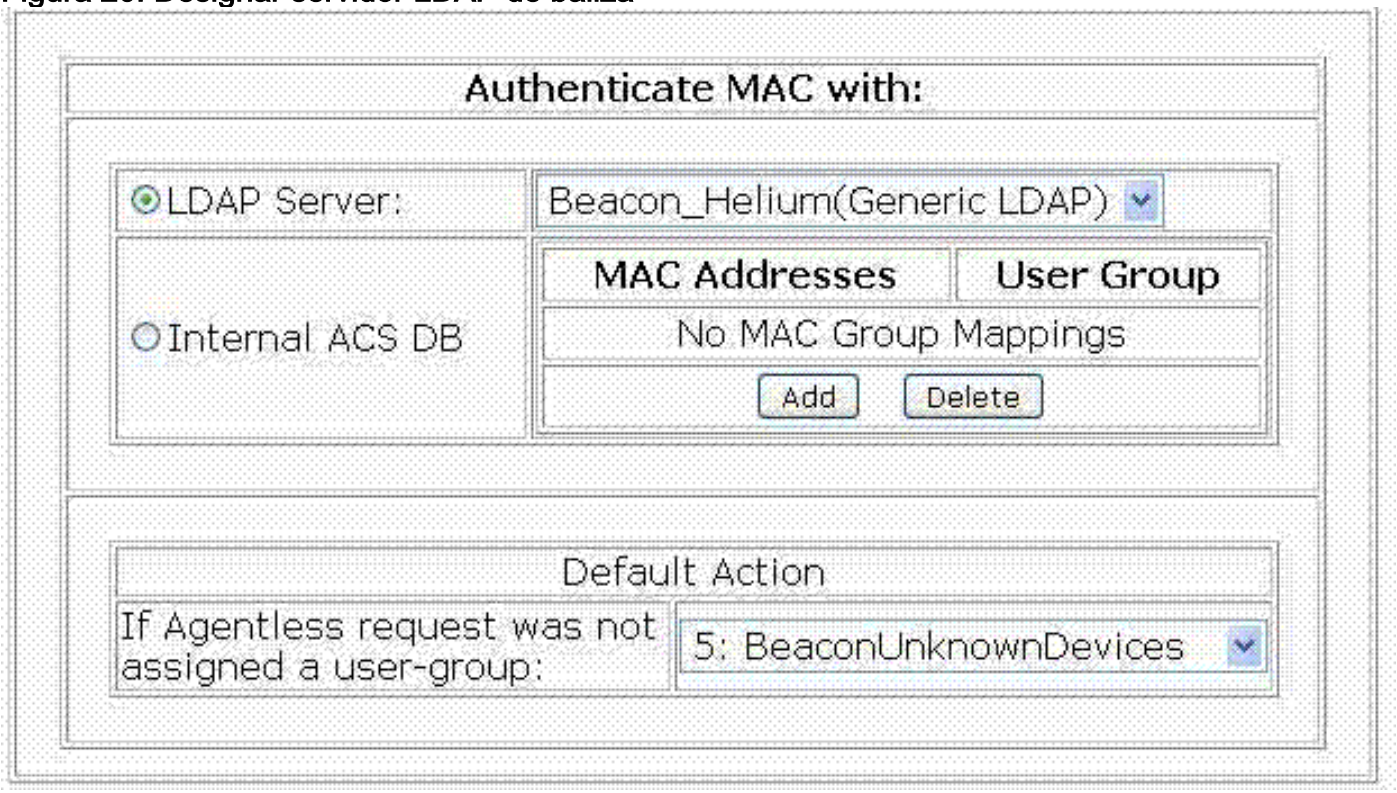
La política de autenticación para el perfil recientemente configurado se debe configurar para utilizar el sistema Beacon como base de datos de validación de credenciales. Elija el enlace Authentication en la columna Policies (Políticas) para el perfil de acceso a la red creado recientemente (802.1x FallBack en el ejemplo). Se presentan estos formularios.

Figura 19: Seleccionar base de datos para MAB



En primer lugar, elija la base de datos de usuario externa de baliza de la tabla Bases de datos disponibles y utilice el botón **->** para agregarla a Bases de datos seleccionadas. Desplácese hacia abajo hasta la sección Authenticate MAC del formulario y elija el botón de opción **LDAP Server**. Elija la base de datos **Beacon** de la lista desplegable. Por último, elija el grupo **BeaconUnknownDevice** para la acción predeterminada, como se muestra en la siguiente figura.

Figura 20: Designar servidor LDAP de baliza



Este paso completa la configuración ACS necesaria para la derivación de autenticación MAC con baliza como base de datos de usuario externa. Reinicie el servicio ACS para asegurarse de que todos los cambios de configuración se registren en la configuración en ejecución.

El sistema debe estar listo para probar el MAB, si los switches están configurados correctamente. Un terminal que se encuentra actualmente en un perfil de baliza habilitado para LDAP puede desconectarse de la red y volver a enviarse con los parámetros de política especificados para el grupo BeaconKnownDevices.

Configuración del Switch para la Omisión de Autenticación MAC

La tercera configuración del switch proporciona una configuración de ejemplo para la autenticación 802.1X con la autenticación MAC Bypass habilitada, y la reasignación de VLAN dinámica requerida para aplicar los atributos RADIUS devueltos desde ACS.

Switch
switch#**show running-config** ! version 12.2 no service pad service timestamps debug uptime service timestamps log datetime service password-encryption service sequence-numbers

```
!
!
aaa new-model
aaa authentication login default line
aaa authentication enable default enable
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
!
aaa session-id common
switch 1 provision ws-c3750g-24ts
ip subnet-zero
ip routing
no ip domain-lookup
!
!
!
!
!
!
dot1x system-auth-control
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
interface Port-channel1
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 5,7,9,10
!
interface Port-channel2
description LAG/trunk to einstein
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 5,9,10
switchport mode trunk
!
interface Port-channel3
description "LAG to Edison"
switchport access vlan 5
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 5,9,11
switchport mode trunk
!
interface GigabitEthernet1/0/1
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 5,7,9,10
channel-group 1 mode passive
!
interface GigabitEthernet1/0/2
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 5,7,9,10
channel-group 1 mode passive
!
interface GigabitEthernet1/0/3
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 5,7,9,10
channel-group 1 mode passive
!
interface GigabitEthernet1/0/4
switchport access vlan 7
switchport mode access
!
```

```
interface GigabitEthernet1/0/5
switchport access vlan 5
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet1/0/6
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 5,7,9
switchport mode trunk
switchport nonegotiate
!
interface GigabitEthernet1/0/7
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 5,9,10
switchport mode trunk
channel-group 2 mode active
!
interface GigabitEthernet1/0/8
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 5,9,10
switchport mode trunk
channel-group 2 mode active
!
interface GigabitEthernet1/0/9
switchport access vlan 5
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet1/0/10
switchport access vlan 5
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet1/0/11
switchport access vlan 5
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet1/0/12
switchport access vlan 5
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet1/0/13
switchport access vlan 5
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet1/0/14
switchport access vlan 5
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet1/0/15
switchport access vlan 5
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet1/0/16
switchport access vlan 5
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet1/0/17
```

```
switchport access vlan 5
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 5,9,11
switchport mode trunk
channel-group 3 mode active
spanning-tree portfast
!
interface GigabitEthernet1/0/18
switchport access vlan 5
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 5,9,11
switchport mode trunk
channel-group 3 mode active
spanning-tree portfast
!
interface GigabitEthernet1/0/19
switchport mode access
dot1x mac-auth-bypass
dot1x pae authenticator
dot1x port-control auto
dot1x timeout quiet-period 10
dot1x timeout reauth-period 60
dot1x timeout tx-period 10
dot1x timeout supp-timeout 10
dot1x max-req 1
dot1x reauthentication
dot1x auth-fail max-attempts 1
spanning-tree portfast
!
interface GigabitEthernet1/0/20
switchport mode access
dot1x mac-auth-bypass
dot1x pae authenticator
dot1x port-control auto
dot1x timeout quiet-period 10
dot1x timeout reauth-period 60
dot1x timeout tx-period 10
dot1x timeout supp-timeout 10
dot1x max-req 1
dot1x reauthentication
dot1x auth-fail max-attempts 1
spanning-tree portfast
!
interface GigabitEthernet1/0/21
switchport access vlan 10
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet1/0/22
switchport access vlan 10
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet1/0/23
switchport access vlan 10
spanning-tree portfast
!
interface GigabitEthernet1/0/24
switchport access vlan 10
spanning-tree portfast
!
interface GigabitEthernet1/0/25
!
interface GigabitEthernet1/0/26
```

```
!
interface GigabitEthernet1/0/27
!
interface GigabitEthernet1/0/28
!
interface Vlan1
no ip address
shutdown
!
interface Vlan5
ip address 10.1.1.10 255.255.255.0
!
interface Vlan9
ip address 10.9.0.1 255.255.0.0
!
interface Vlan10
ip address 10.10.0.1 255.255.0.0
ip helper-address 10.1.1.1
ip helper-address 10.10.0.204
!
interface Vlan11
ip address 10.11.0.1 255.255.0.0
ip helper-address 10.1.1.1
ip helper-address 10.10.0.204
!
ip default-gateway 10.1.1.1
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.1
ip route 10.30.0.0 255.255.0.0 10.10.0.2
ip route 10.40.0.0 255.255.0.0 10.10.0.2
ip http server
ip http secure-server
!
!
snmp-server community public RW
snmp-server host 10.1.1.191 public
radius-server host 10.10.0.100 auth-port 1645 acct-port
1646 key 7
05090A1A245F5E1B0C0612
radius-server source-ports 1645-1646
!
control-plane
!
!
line con 0
password 7 02020D550C240E351F1B
line vty 0 4
password 7 00001A0803790A125C74
line vty 5 15
password 7 00001A0803790A125C74
!
end
```

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Información Relacionada

- Cisco NAC Appliance (Clean Access)
- Cisco Secure Access Control Server para Windows
- Soporte Técnico y Documentación - Cisco Systems