NAC: Integración LDAP con el ejemplo de la configuración de ACS

Contenido

Introducción

Este documento proporciona una configuración de muestra de los pasos para configurar el faro y el ACS para habilitar los dispositivos de Cisco configurados para que el MAB de manera eficaz y eficiente autentique los dispositivos con capacidad non-802.1X en la red autenticada.

Cisco ha implementado una característica llamada puente de la autenticación de MAC (MAB) en su Switches así como soporte indispensable en el ACS para acomodar los puntos finales en las redes 802.1X-enabled que no pueden autenticar con el 802.1x. Estas funciones se aseguran de que los puntos finales que intentan la conexión a la red 802.1X-enabled que no se equipa de las funciones del 802.1x, por ejemplo, no tiene un supplicant funcional del 802.1x, se puede autenticar antes de la admisión, así como tiene política de uso de la red básica aplicada en su conexión.

El MAB habilita la red que se configurará para admitir los dispositivos identificados con el uso de su dirección MAC como los credenciales primarios cuando el dispositivo no puede participar en el protocolo del 802.1x. Para que el MAB sea desplegado y utilizado con eficacia, el entorno debe tener medios de indentify los dispositivos en el entorno que no son capaces de la autenticación del 802.1x, y de mantener una base de datos actualizada de estos dispositivos en un cierto plazo como se mueve, agrega y los cambios ocurren. Esta lista necesita ser poblada y ser mantenida en el servidor de autenticación (ACS) manualmente, o a través de algunos medios alternativos

para asegurarse de que los dispositivos que autentican en el MAC es completado y válido en cualquier momento.

El Profiler del punto final del faro puede automatizar el proceso de la identificación de NON-autenticar los puntos finales, ésos sin los suplicantes del 802.1x, y el mantenimiento de la validez de estos puntos finales en las redes de la escala diversa en la funcionalidad de monitoreo del perfilado y del comportamiento del punto final. A través de una interfaz LDAP estándar, el sistema del faro puede servir como una base de datos externa o directorio de los puntos finales que se autenticarán con el MAB. Cuando una petición MAB se recibe de la infraestructura del borde, el ACS puede preguntar el sistema del faro para determinar independientemente de si un punto final dado se debe admitir a la red basada en la mayoría de la información actual sobre el punto final conocido por el faro, para prevenir la necesidad de la configuración manual.

Refiera al NAC: Integración LDAP con el ejemplo de configuración ACS 5.x y posterior para 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

El MAB es funciones esenciales para el soporte dinámico de los dispositivos tales como impresoras, Teléfonos IP, máquinas de fax y otros dispositivos con capacidad non-802.1X en el despliegue del entorno post-802.1X. Sin una capacidad MAB, los puertos de acceso a la red que proporcionan Conectividad a los puntos finales capaces non-802.1X deben ser aprovisionado estáticamente para no intentar la autenticación del 802.1x o con el uso de las otras funciones que proporcionan las opciones muy limitadas de la directiva. Por las razones obvias, esto no es intrínsecamente scalable en los entornos para empresas grandes. Con el MAB habilitado conjuntamente con el 802.1x en todos los puertos de acceso, los puntos finales capaces

conocidos non-802.1X se pueden mover dondequiera en el entorno y todavía conecte confiablemente (y con seguridad) con la red. Porque los dispositivos admitidos a la red se están autenticando, diversas directivas se pueden aplicar a diversos dispositivos

Además, los puntos finales capaces non-802.1X que no se conocen en el entorno, tal como laptopes que pertenezcan a los visitantes o a los contratistas, pueden ser acceso restringido proporcionado a la red con el MAB si están deseados.

Mientras que el nombre sugiere, puente de la autenticación de MAC utiliza la dirección MAC del punto final como los credenciales primarios. Con puente de la autenticación de MAC habilitado en un puerto de acceso, si un punto final conecta y no puede responder al desafío de autenticación del 802.1x, el puerto invierte al modo MAB. El Switch que intenta el MAB de un punto final hace un pedido de RADIUS estándar al ACS con el MAC de la estación. Intenta conectar con la red y pide la autenticación del punto final del ACS antes de la admisión del punto final a la red.

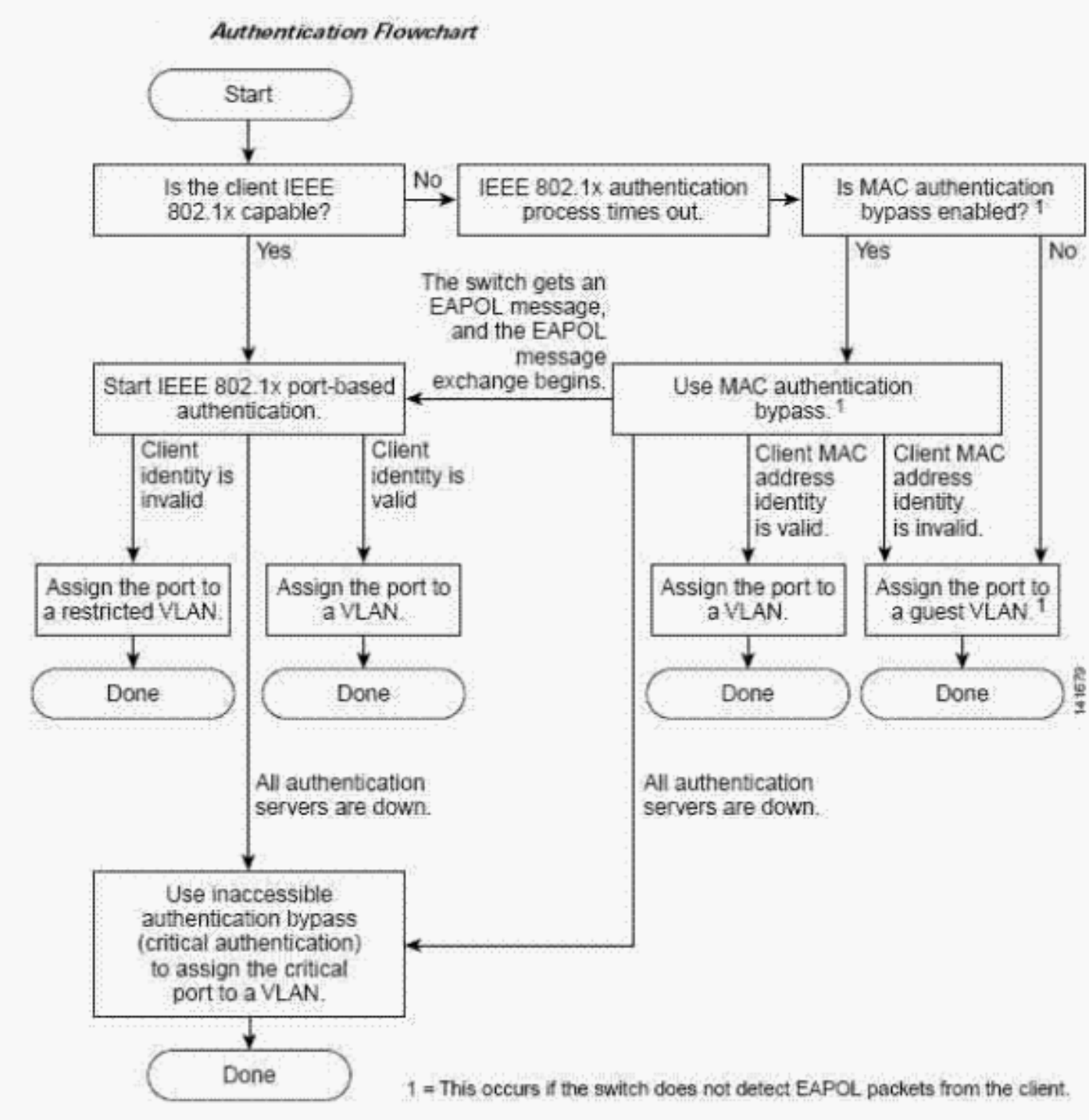
Configuración

Diagrama de organigrama

Este organigrama tomado de la documentación de Cisco Systems ilustra cómo el MAB se utiliza conjuntamente con la autenticación del 802.1x en la infraestructura del borde de Cisco mientras que los nuevos puntos finales intentan conectar con la red.

Este documento utiliza este flujo de trabajo del organigrama:

Figura 1: Flujo de la autenticación



El ACS se puede configurar para utilizar su propia base de datos interna o a un servidor LDAP externo para autenticar las peticiones del usuario de la dirección MAC. El sistema del Profiler del punto final del faro LDAP-se habilita completamente por abandono y se puede utilizar por el ACS para autenticar las peticiones del usuario de la dirección MAC con las funciones estándar LDAP. Porque el faro automatiza la detección así como el perfilado de todos los puntos finales en la red, el ACS puede preguntar el faro con el LDAP para determinar si el MAC se admite a la red, y en qué grupo debe ser asociado el punto final. Esto automatiza y aumenta perceptiblemente la característica de puente de la autenticación de MAC, determinado en los entornos para empresas grandes.

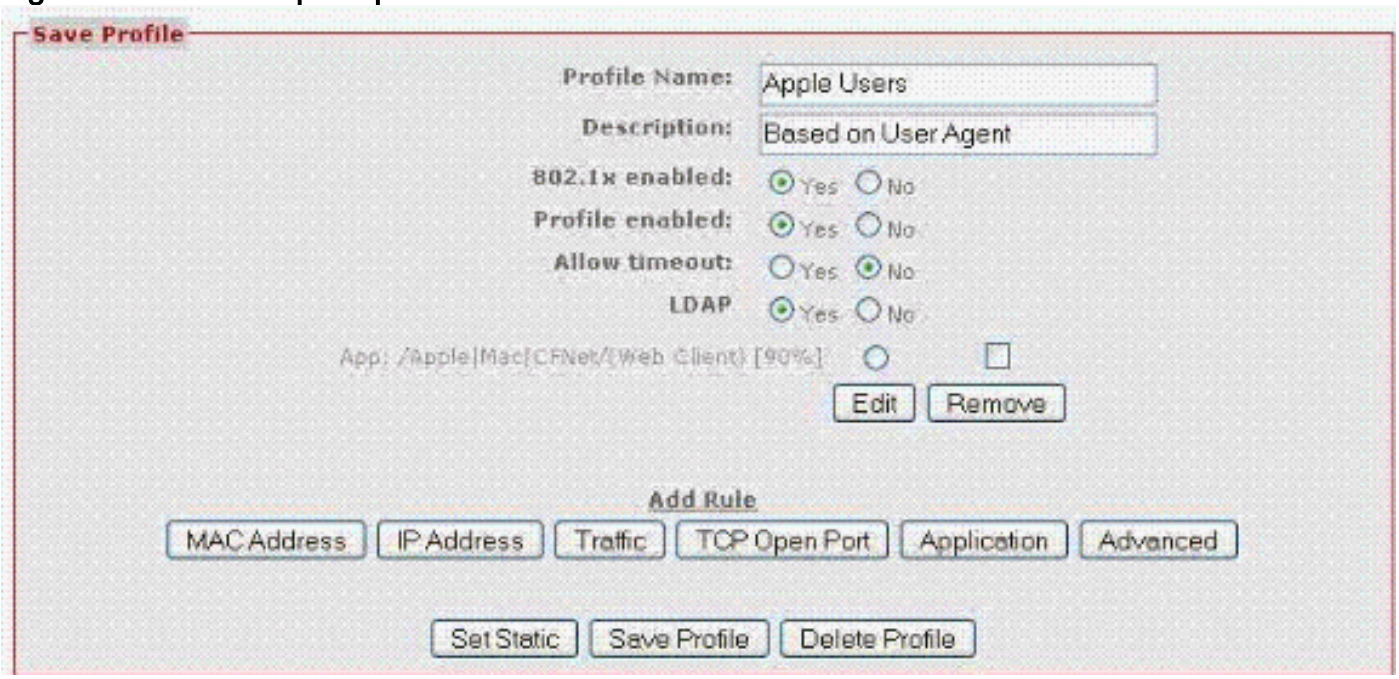
Con la funcionalidad de monitoreo del comportamiento proporcionada por el faro, los dispositivos que se observan para comportarse contrario con los perfiles habilitados para el MAB son transitioned fuera de 4 perfiles LDAP-habilitados y fallar posteriormente la tentativa regular siguiente de la reautentificación.

Configuración del sistema del Profiler del punto final del faro para el MAB

La configuración del sistema del faro para la integración con el ACS con el propósito del soporte MAB es directa pues las funciones LDAP se habilitan por abandono. La tarea de configuración primaria es identificar los perfiles que contienen los puntos finales que se desean para ser autenticados con el MAB en el entorno, y entonces habilitar esos perfiles para el LDAP. Típicamente, los perfiles del faro, que contienen los dispositivos poseyeron por la organización, deben ser acceso a la red proporcionado cuando estaban considerados en un puerto con todo se saben para no poder autenticar con el 802.1x. Éstos son típicamente los perfiles que contienen las impresoras, los Teléfonos IP o UPSs manejable como ejemplos comunes.

Si las impresoras perfiladas por el faro fueron colocadas en un perfil nombrado *Printers*, y los Teléfonos IP en un perfil nombraron los *Teléfonos IP*, por ejemplo, después la necesidad de estos perfiles de ser habilitado para el LDAP tales que los puntos finales puestos en esos perfiles dan lugar a la autenticación satisfactoria como el teléfono del IP e impresoras sabidos en el entorno con el MAB. Si usted habilita un perfil para el LDAP, éste requiere que el botón de radio LDAP en la configuración del perfil del punto final esté seleccionado, tal y como se muestra en de este ejemplo:

Figura 2: Habilite un perfil para el LDAP



Cuando la autenticación de MAC de los proxys ACS a balizar con el LDAP, la interrogación consiste en dos interrogaciones sub, que deben volver un resultado válido, no nulo. La primera interrogación a balizar es independientemente de si el MAC está sabido para balizar, por ejemplo, si se ha descubierto y se ha agregado a la base de datos del faro. Si el punto final tiene todavía ser descubierto por el faro, el punto final se considera ser desconocido. La segunda interrogación no es necesaria en el caso de los puntos finales que el faro no ha descubierto y no está en su base de datos. Si el punto final se ha descubierto y está en la base de datos del faro, la interrogación siguiente es determinar el perfil actual del punto final. Si un punto final tiene todavía ser perfilado o está actualmente en un perfil no 5 habilitados para el LDAP, el resultado desconocido se vuelve al ACS, y la autenticación del punto final por el faro falla. Depende de cómo se configura que éste puede dar lugar al dispositivo con la negación del acceso a la red en conjunto, o se dé el ACS una directiva que sea apropiada para los dispositivos el desconocido o del invitado.

Solamente en el caso donde está un punto final el MAC que el faro ha descubierto y colocado en un perfil LDAP-habilitado, la respuesta es que el punto final está conocido y perfilado por el faro esté vuelto al ACS. Lo que es más importante, porque faro de estos puntos finales proporciona el nombre del perfil actual, que permite al ACS para asociar los puntos finales conocidos a los grupos de Cisco SecureAccess. Esto habilita una determinación granular de la directiva hecha, tan granular como una política diferenciados para cada perfil LDAP-habilitado faro, si está deseada.

Configuración de ACS para el MAB y utilización del faro como Base de datos de usuarios externa

La configuración del ACS para el MAB y de la utilización del faro como Base de datos de usuarios externa requiere tres pasos claros. La orden ilustrada en este documento sigue un flujo de trabajo que sea eficiente cuando realiza la configuración MAB en su totalidad, y pueda variar para los sistemas que han sido en funcionamiento con otros modos de autenticación configurados ya.

Configuración Cisco SecureGroup

Cuando usted intenta el MAB para un punto final específico que intente conectar con la red, el ACS pregunta el faro en el LDAP para determinar si el faro ha descubierto el MAC, y qué faro del perfil ha puesto actualmente el MAC address adentro según lo descrito anterior en el documento.

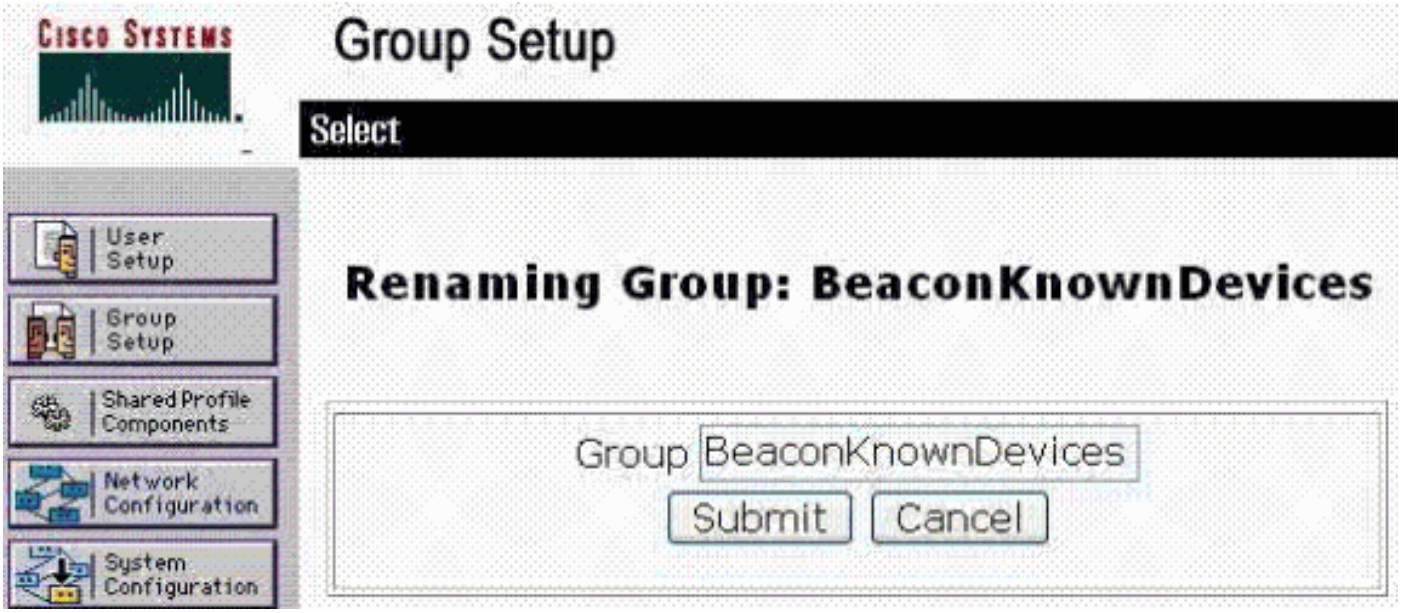
El mecanismo de Cisco SecureGroup con el ACS se puede utilizar a autentica y aplica la directiva a los puntos finales que han sido descubiertos y perfilados por el faro con el MAB, así como a las fallas de autenticación — esos dispositivos no sabidos o perfilados no no actualmente por el faro.

Por ejemplo, un grupo puede ser agregado a la configuración de ACS para los puntos finales descubiertos y perfilados por el faro y *BeaconKnownDevices* llamado, y a otro grupo *BeaconUnknownDevices* agregado para los dispositivos que no son sabidos actualmente por el faro. Cualquier faro no ha descubierto el MAC, ni lo ha perfilado actualmente en un perfil LDAP-habilitado. Como se muestra más adelante en este documento, los grupos habilitan la aplicación de la directiva a los puntos finales mientras que intentan unirse a la red.

Observe que en el ejemplo delineado en este documento, sólo configuran a dos grupos, BeaconKnown y BeaconUnknown. Pero es posible crear SecureGroups múltiple para los puntos finales descubiertos y perfilados por el faro, tanto como uno para cada perfil LDAP-habilitado en el faro, cada uno con diversos parámetros de la directiva tales como asignación VLAN. Además, el grupo de dispositivos de BeaconUnkown puede ser configurado para negar todo el acceso a los puntos finales que tienen todavía ser descubiertos o ser puestos en un perfil habilitado para el LDAP por el faro 6. Esto es realizado si usted elige el checkbox inhabilitado grupo en los parámetros de la ventana de la configuración de grupo de BeaconUnknownDevices.

La creación del grupo en el ACS se inicia del botón Group Setup Button en la interfaz del usuario de ACS. Elija a uno de los grupos disponibles, y después elija el botón del **grupo de la retitulación** para cambiar el nombre del grupo a KnownBeaconDevices tal y como se muestra en de este ejemplo. El tecleo **somete** para salvar el cambio.

Figura 3: Edite al grupo del CiscoSecure

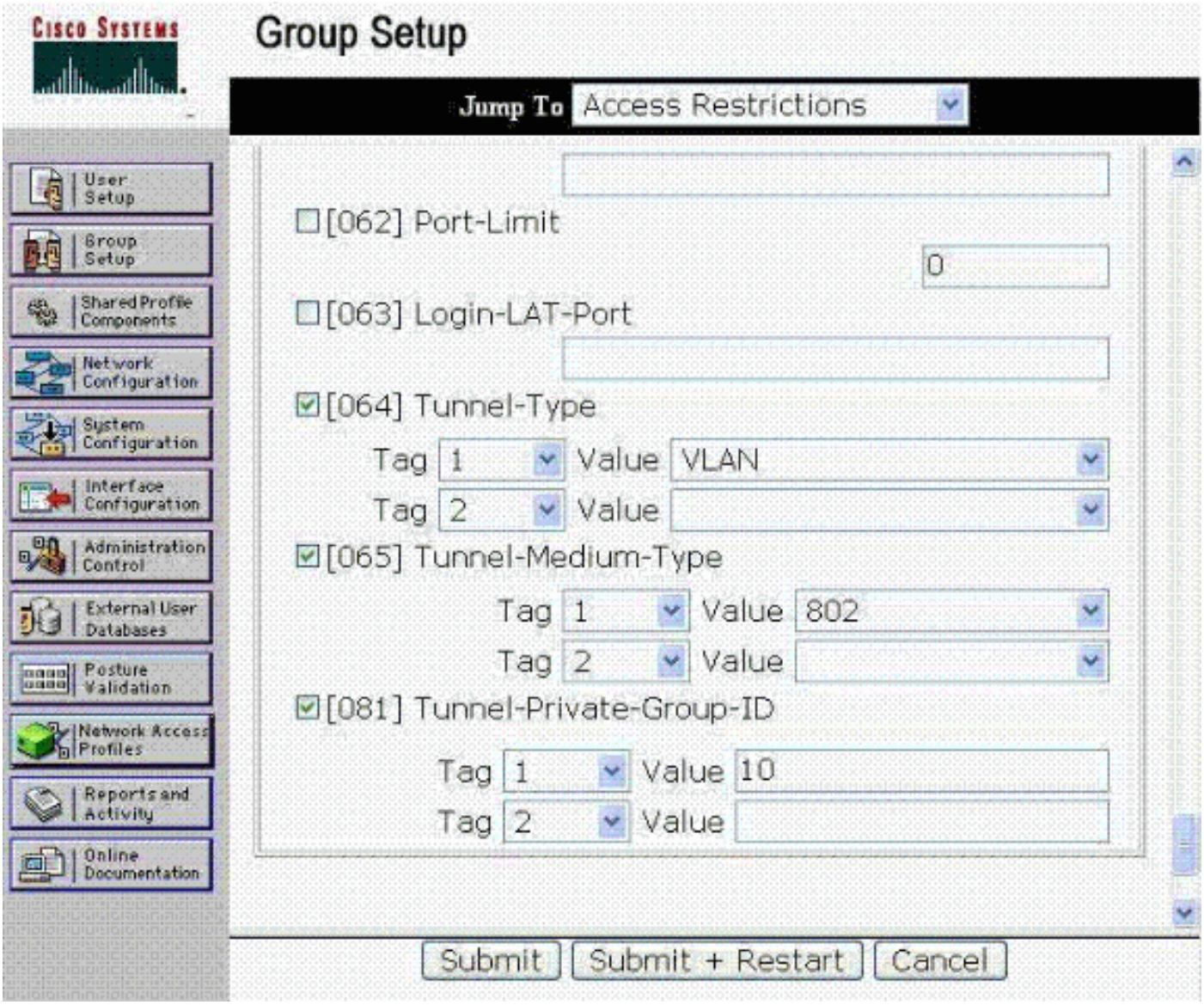


Elija **editan las configuraciones** para editar las configuraciones del grupo. Edite los parámetros del grupo de BeaconKnownDevices según lo deseado. Con el propósito del ejemplo en este documento, los parámetros del grupo se cambian que incluyen solamente los atributos IETF RADIUS, encontraron en la parte inferior de la página.

Usted señala específicamente que los dispositivos autenticados a este grupo, las direcciones MAC que el faro ha perfilado a los perfiles seleccionados para el MAB y habilitados para el LDAP, tienen parámetros de la directiva vueltos al Switch de autenticidad que habilita la admisión de los puntos finales a la red en el VLA N apropiado. Para hacer esto, el Túnel-Media-tipo 064, 065 fijan al Tipo de Túnel de los atributos de RADIUS, y 081 el túnel Soldado-Grupo-ID para dar lugar a los puntos finales que son colocados en el VLA N deseado, tal y como se muestra en del cuadro 4.

Asegúrese de que el checkboxes al lado de cada atributo de RADIUS esté marcado.

Figura 4: Atributos del VLA N del grupo

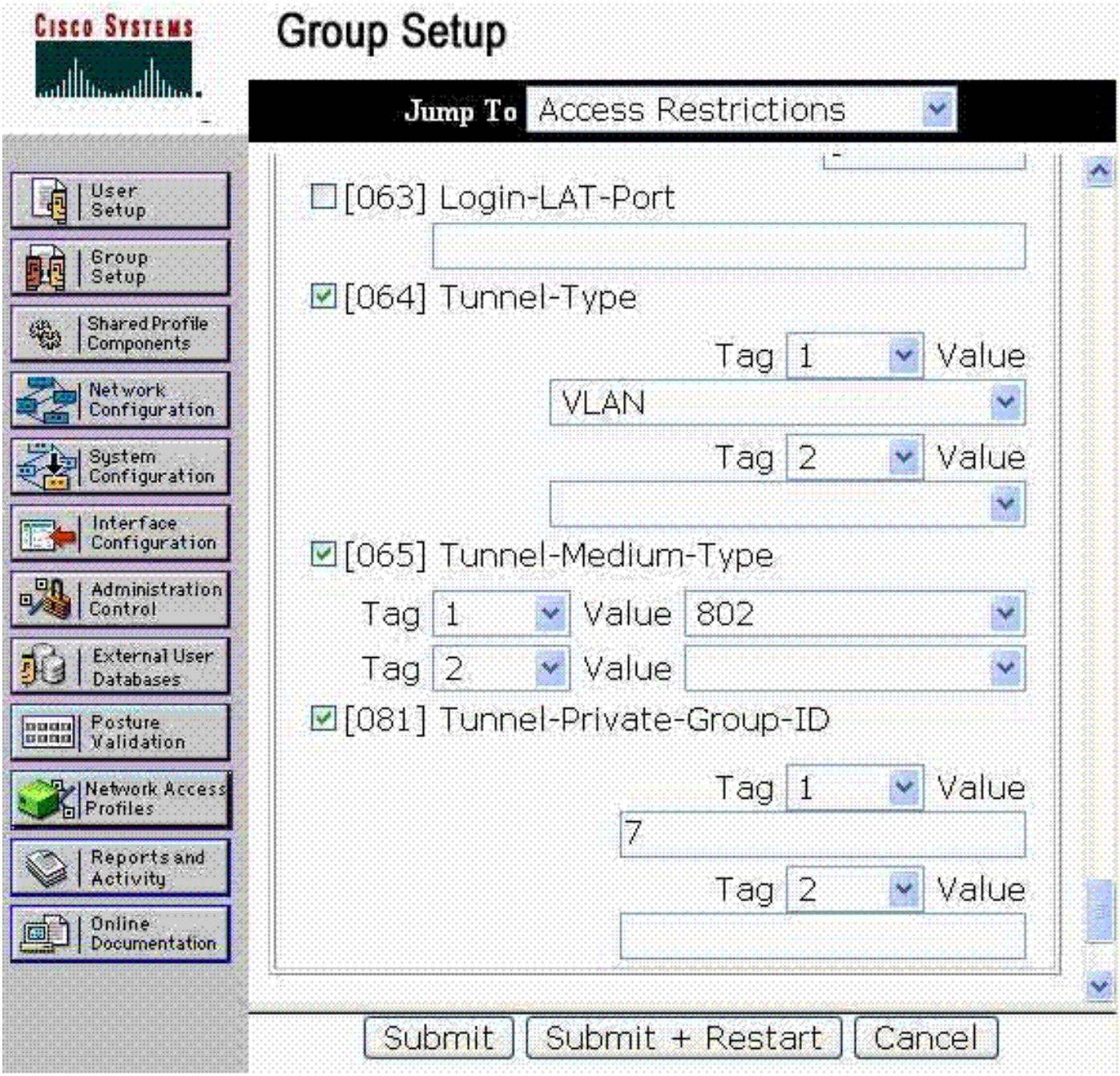


En el ejemplo mostrado, los puntos finales autenticados con éxito por el faro y asignados posteriormente al grupo ACS BeaconKnownDevices se ponen en el VLAN10, el VLA N autorizado en la configuración de red de muestra, durante la conexión a la red y son autenticados con éxito en el MAB por el ACS con el uso del faro como Base de datos de usuarios externa.

El grupo de BeaconUnknownDevices se crea semejantemente para los dispositivos que no son sabidos actualmente por el faro como se muestra. Si estos dispositivos no consiguen ningún acceso a la red, marque una vez más simplemente el checkbox **inhabilitado grupo** en la cima de la forma. Puntos finales que no han sido descubiertos por el faro ni actualmente son perfilados por el faro en un fall LDAP-habilitado MAB del perfil y no admitidos a la red.

Esta figura muestra la alternativa que el uso del checkbox inhabilitado grupo. En este caso, los puntos finales que no se pueden autenticar por el faro se asignan a un grupo se habilite que, pero tienen una diversa directiva que eso para los puntos finales se conocen que. Refiera al cuadro 5.

Figura 5: Parámetros de VLAN para BeaconUnknownDevices



Observe que para los dispositivos desconocidos en este ejemplo, se admiten a la red pero se relegan a un invitado o a un VLA N restricto, el VLA N 7. En la red de muestra, el VLA N 7 es el VLA N del invitado, que permite el acceso a internet de los puntos finales solamente, y prohíbe el acceso a los recursos internos.

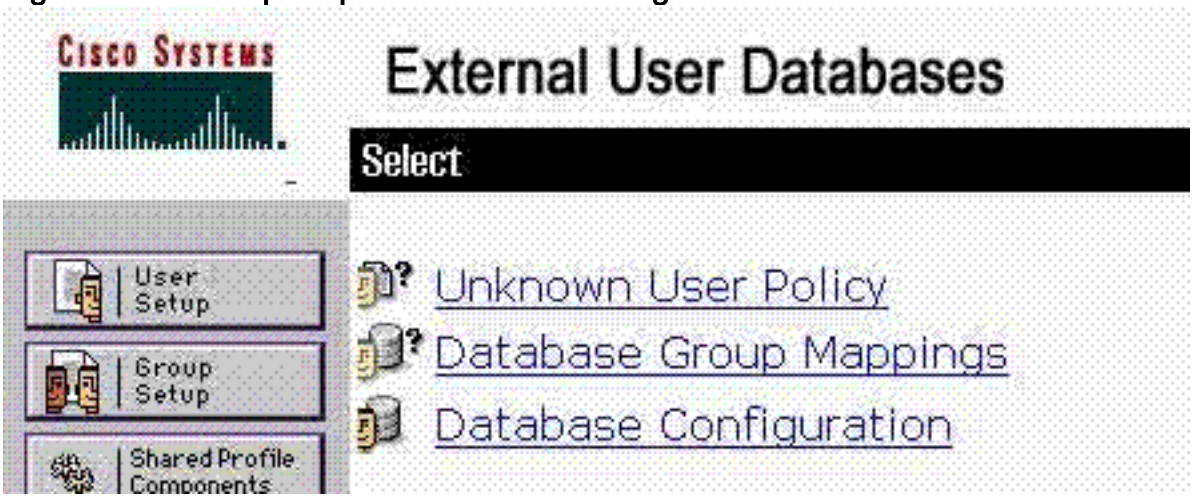
Cuando el ACS pide la autenticación del faro de un MAC de un punto final que tenga todavía ser descubierto o ser perfilado por el faro, el ACS coloca el MAC en este grupo y vuelve el resultado al Switch de autenticidad habilitado para el MAB.

Configuración de base de datos de usuarios externa ACS

El ACS se debe configurar a las peticiones MAB del proxy de los switches de acceso de balizar vía el LDAP. Esto requiere que la configuración de ACS incluya el sistema del faro como Base de datos de usuarios externa genérica LDAP. Los pasos delineados en esta sección ilustran cómo agregar el sistema del Profiler del punto final de 9 faros como Base de datos de usuarios externa que se preguntará por el ACS cuando recibe las peticiones MAB. Elija la **Base de datos de usuarios externa** en el SCR_INVALID global para traer para arriba la ventana de la Base de datos

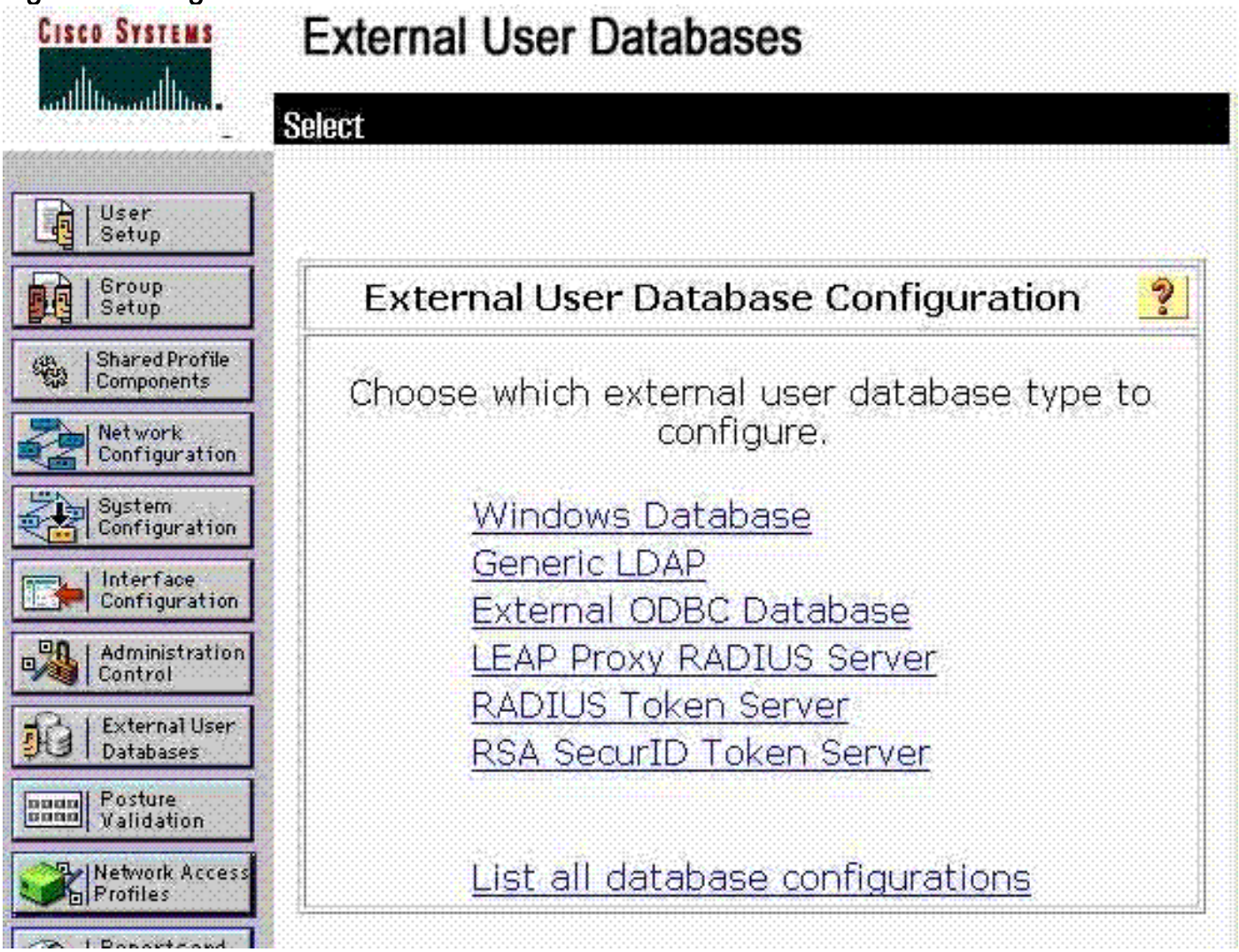
de usuarios externa ilustrada en el cuadro 6.

Figura 6: Pantalla principal externa de la configuración DB



La primera tarea en la configuración del faro como Base de datos de usuarios externa es agregar el sistema del faro como Base de datos de usuarios externa genérica LDAP. Elija la **configuración de la base de datos** para que la ventana ilustrada en el cuadro 7 aparecen.

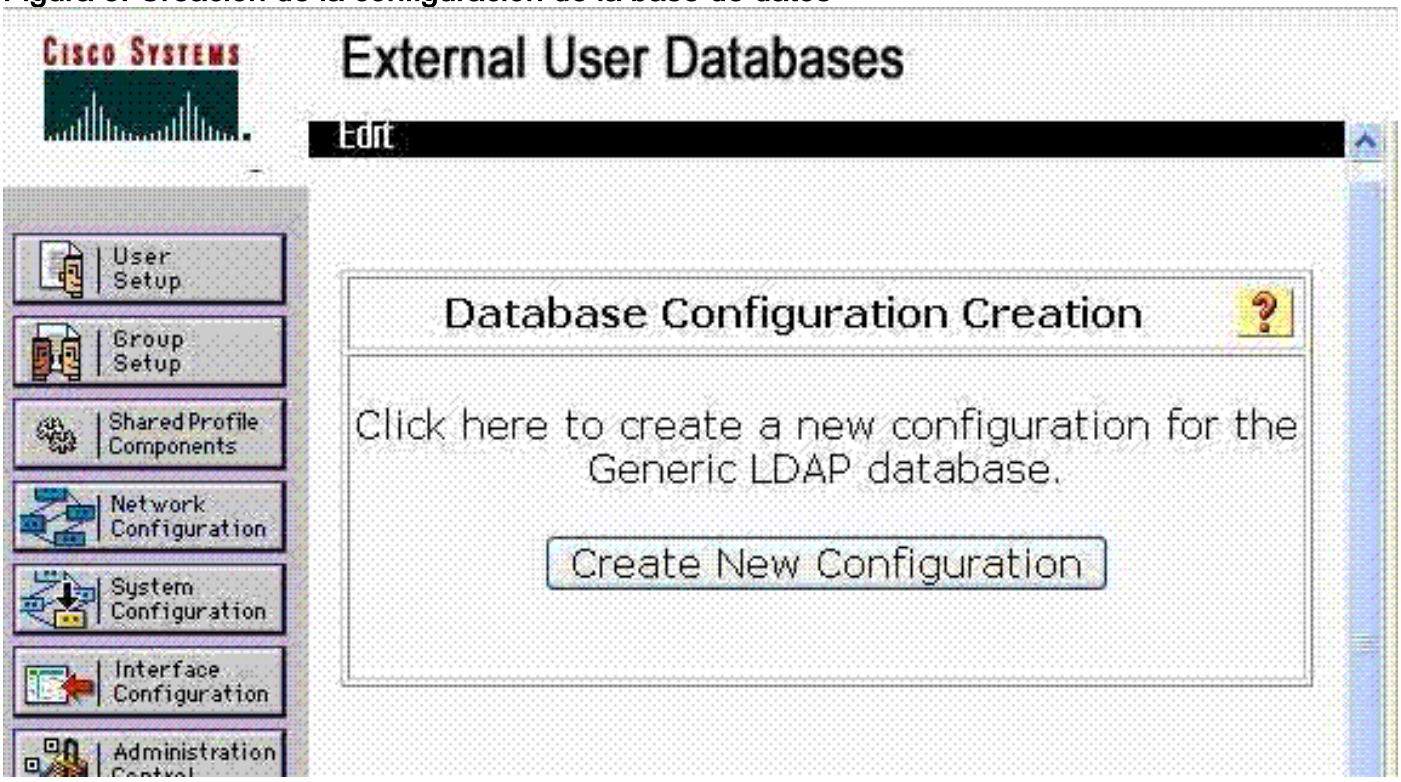
Figura 7: Configuración de base de datos de usuarios externa ACS



Elija el **LDAP genérico** para abrir la forma usada para agregar el sistema del Profiler del punto final del faro como usuario externo DB en la configuración de ACS. Esta ventana aparece habilitar la creación de una nueva Configuración de base de datos de usuarios externa del tipo LDAP

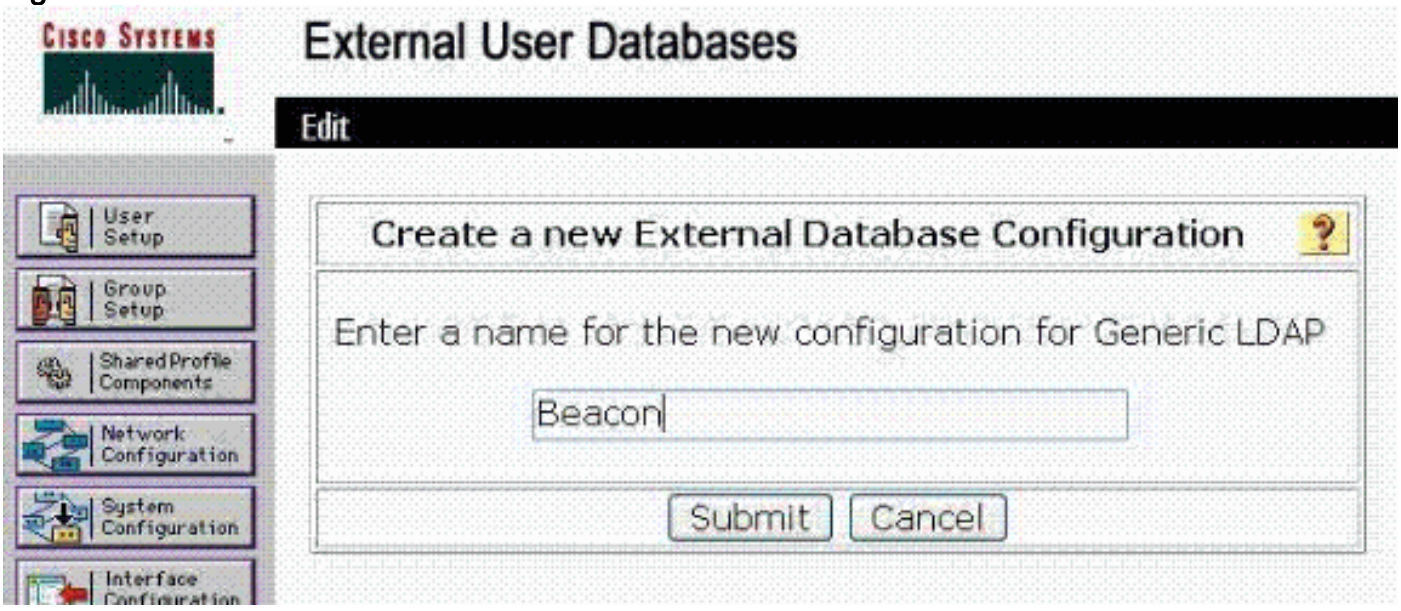
genérico.

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



Elija el **nuevo** botón de la **configuración del crear** para crear la base de datos de LDAP genérica para el faro. Esta ventana aparece y permite que la nueva base de datos externa sea nombrada.

Figura 9: Base de datos de usuarios externa del faro del nombre

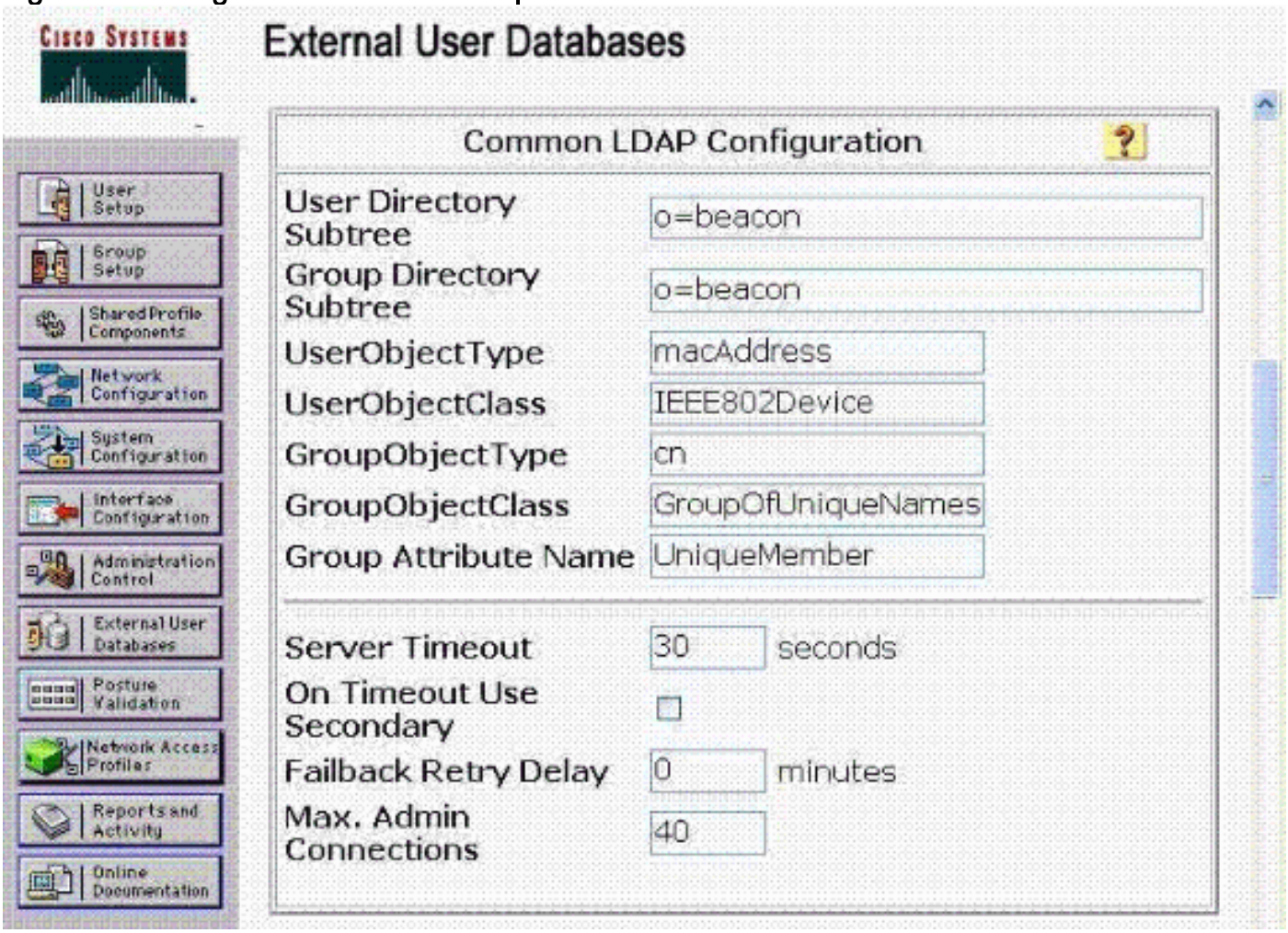


Ingrese un nombre para la base de datos externa genérica del LDAP del faro que permite que sea distinguido fácilmente de otras bases de datos externas en la configuración. Elija **someten** para moverse sobre la entrada de los Parámetros de LDAP requeridos que habilitan la comunicación entre 11 ACS y faro con el fin de la autenticación de las direcciones MAC con el uso de la Información de la base de datos del faro.

El cuadro 10 ilustra los parámetros comunes de la Configuración LDAP que se deben ingresar para la Base de datos de usuarios externa genérica del LDAP del faro que se agrega a la

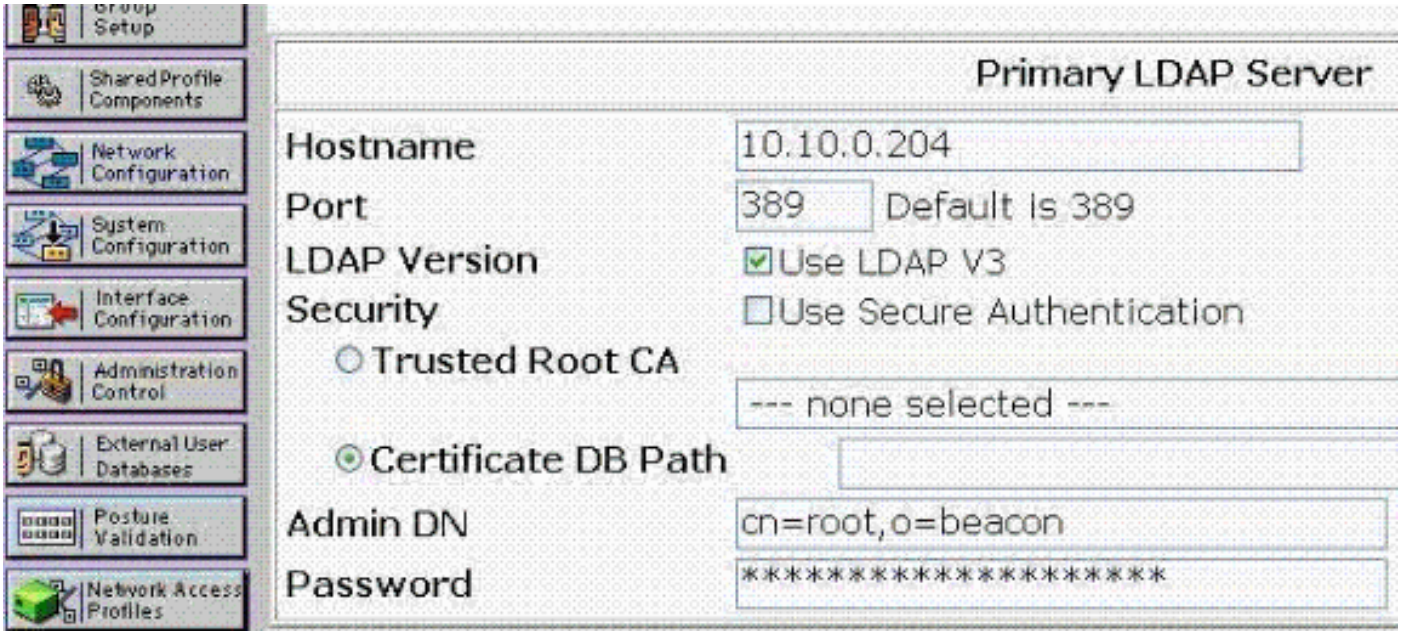
configuración de ACS. Observe que estos parámetros proporcionan el ACS con la información que requiere para preguntar el faro con el LDAP. Estos parámetros se deben ingresar exactamente tal y como se muestra en de esta figura para facilitar la comunicación entre el ACS y el Profiler del punto final del faro.

Figura 10: Configuración LDAP común para el faro



Nota: Utilice la contraseña **GBSbeacon** para la contraseña del lazo LDAP. La contraseña se ingresa en la parte inferior de la forma mostrada en el cuadro 11.

Cuadro 11: Parámetros del servidor del faro

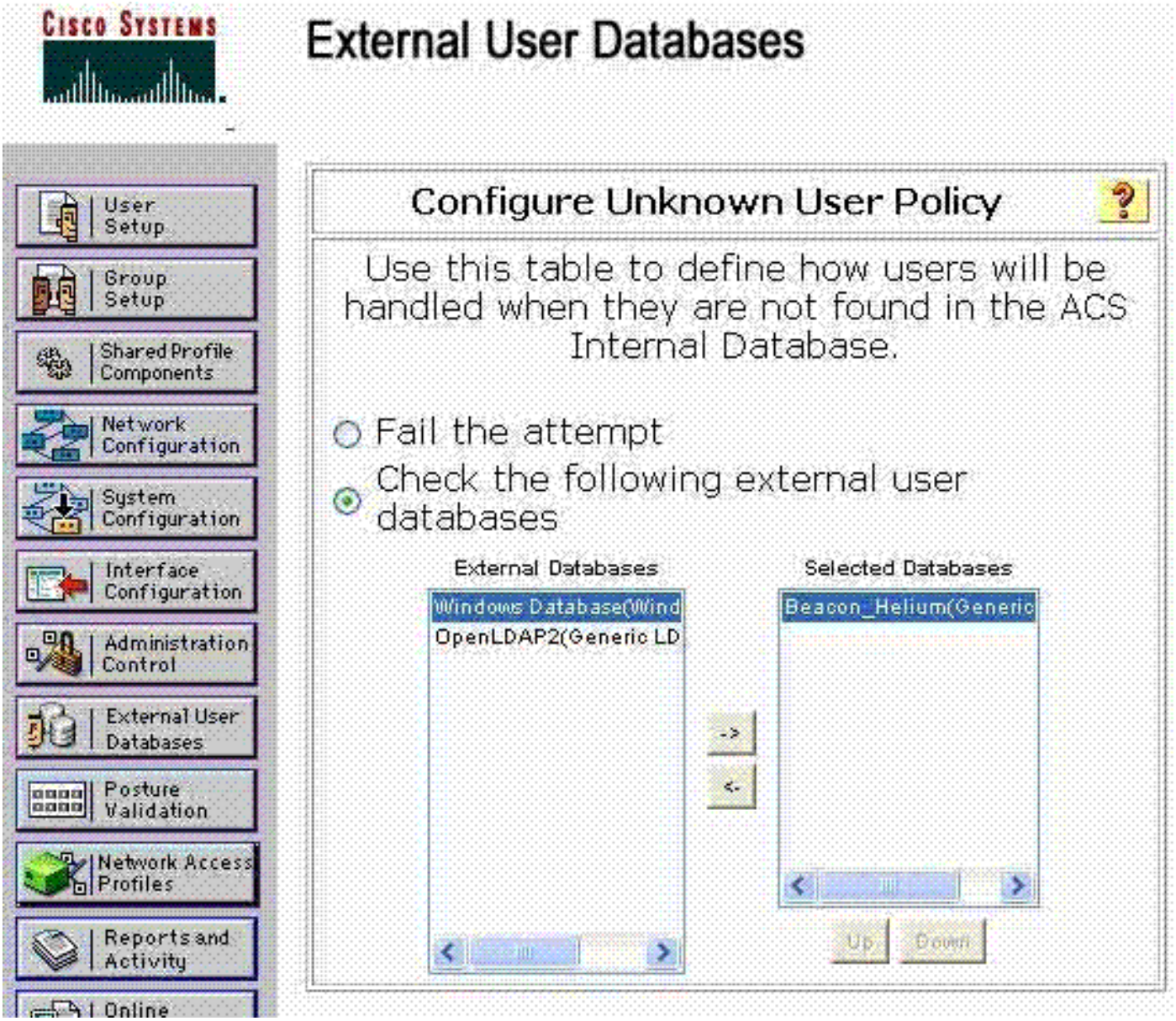


La segunda tarea de configuración asociada a la configuración del faro como Base de datos de usuarios externa es la configuración de la Política de usuario desconocido. La Política de usuario desconocido ordena el ACS para preguntar la base de datos del faro siempre que reciba un pedido de autenticación para un usuario, que es una dirección MAC en el caso de MAB, que no tiene información para en su propia base de datos.

Observe que en un despliegue típico ACS, puede haber Bases de datos de usuarios externas existentes configuradas y se puede configurar ya para preguntar esas bases de datos cuando se someten las credenciales del usuario desconocido. La Base de datos de usuarios externa del faro se debe agregar a la lista para preguntarla cuando el Switches pide el MAB de las direcciones MAC individuales.

Estas figuras delinean el flujo de trabajo para la configuración de la Política de usuario desconocido, y la adición de faro como una Base de datos de usuarios externa que se preguntará. A, elija el link de la **Política de usuario desconocido** en la página principal de la Base de datos de usuarios externa como se ilustra en el cuadro 6 para comenzar el flujo de trabajo.

Cuadro 12: Política de usuario desconocido de la configuración

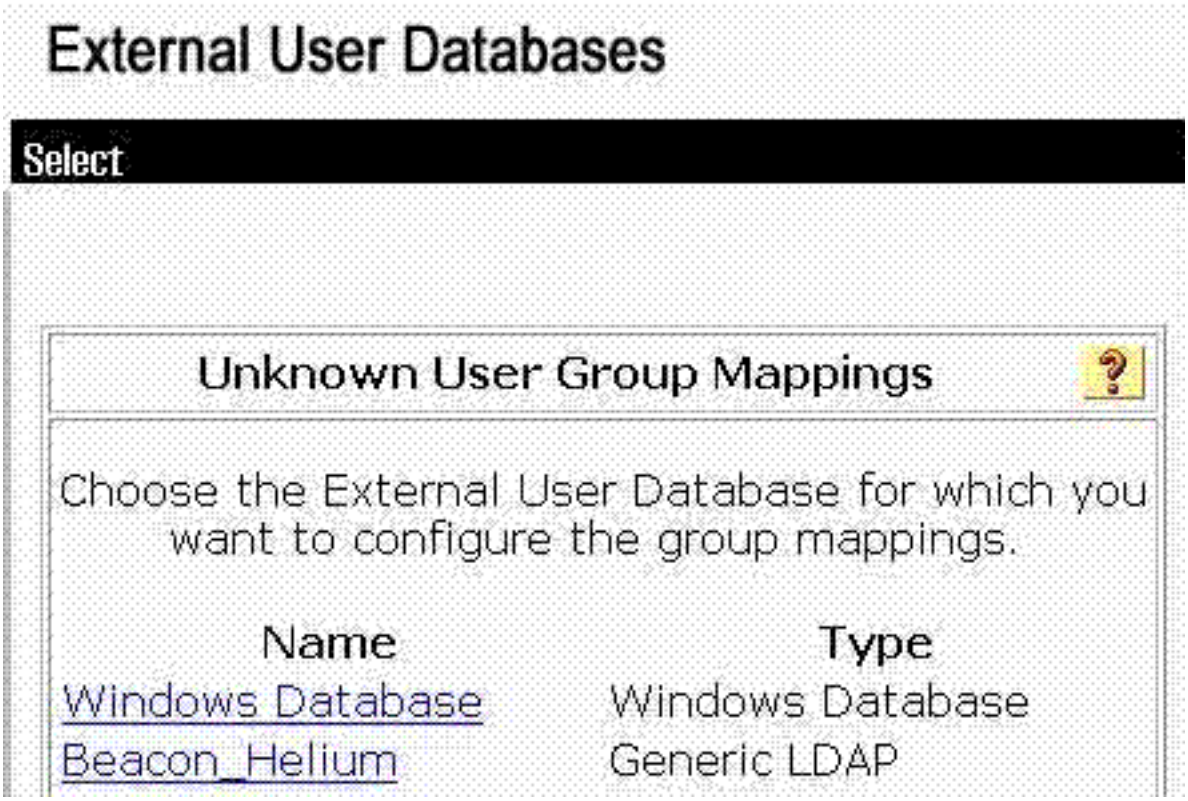


Elija la base de datos de LDAP genérica del faro agregada a la configuración de ACS en el paso más reciente de la lista de bases de datos externas a la izquierda (Beacon_Helium) en el ejemplo. Uso **- >** para moverse a las bases de datos seleccionadas. Aseegurese le elegir el **control el** botón de radio **siguiente de las Bases de datos de usuarios externas**. Esto se asegura de que cuando el Switches somete los direccionamientos MAC para la autenticación al ACS, el ACS pregunte el faro para determinar si se conoce el punto final y tiene perfil actual, si lo hay.

La tarea de la configuración final de agregar el faro como Base de datos de usuarios externa es la realización de los Mapeo de grupo de base de datos. Esencialmente esta asignación une los grupos del CiscoSecure creados, por ejemplo, BeaconKnownDevices y BeaconUnknownDevices, a las interrogaciones acertadas y fracasadas LDAP hechas para balizar de modo que cada MAB frustrado por el Switches dé lugar a la asignación del punto final a un grupo del CiscoSecure por el ACS. Esto permite al ACS para responder al Switch independientemente de si el punto final se debe admitir a la red, y si está admitido, qué la directiva tal como VLA N lo atribuye debe ser.

Elija los **Mapeo de grupo de base de datos** en la página principal de las Bases de datos de usuarios externas tal y como se muestra en del cuadro 6 para configurar las asignaciones.

Cuadro 13: Mapeo de grupo de base de datos

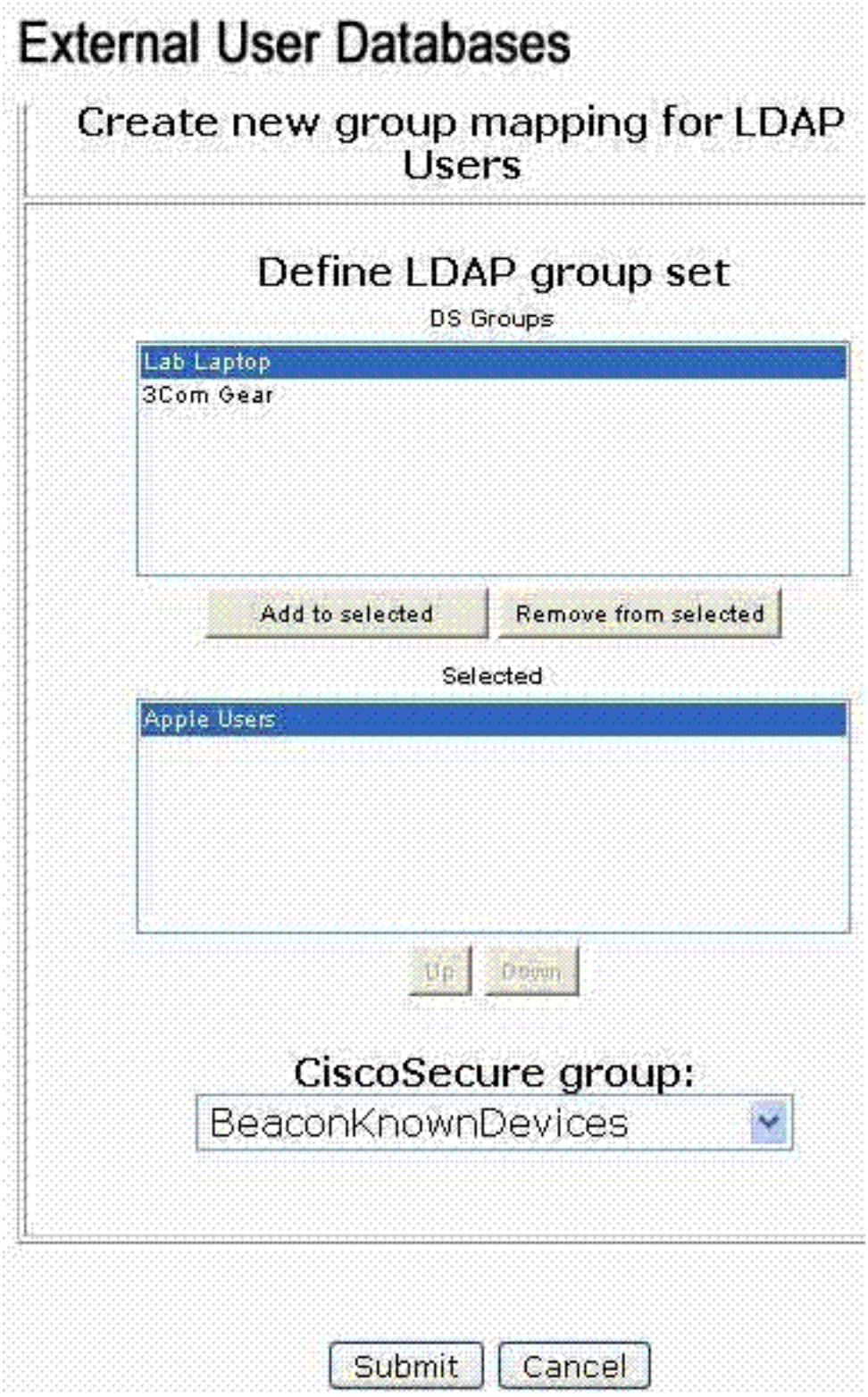


Cuando usted elige la Base de datos de usuarios externa del faro creada anterior en esta sección con la selección del link, Beacon_Helium en el ejemplo anterior, esto visualiza la ventana ilustrada en el cuadro 14. Observe que todos los perfiles del faro habilitados para el LDAP dentro de la configuración del sistema del faro según lo descrito en la primera sección de estas instrucciones de configuración están poblados en los grupos DS que están disponibles para que la selección cree las asignaciones dentro del ACS. Si los nombres del perfil del faro habilitados para el LDAP no se muestran en la interfaz ACS, éste es indicativo de un problema con la Configuración LDAP ACS. Refiera a las instrucciones en el faro de la configuración como una Base de datos de usuarios externa delineada anterior en esta sección, particularmente los Parámetros de LDAP.

Observe que ésta es la interfaz que permite asociar de los perfiles LDAP-habilitados individuales en el faro con los grupos del CiscoSecure configurados dentro del ACS. La interfaz permite la asignación de cada perfil LDAP-habilitado faro individual a un solo grupo del CiscoSecure. En este ejemplo, solamente crearon a un solo grupo para los dispositivos sabidos en los perfiles LDAP-habilitados del faro: BeaconKnownDevices. Pero, los múltiples grupos, cada uno con sus propios parámetros de la directiva pueden ser creados para manejar las autenticaciones satisfactorias diverso dependientes sobre el perfil actual del faro del dispositivo.

Por ejemplo, un grupo del CiscoSecure puede ser creado para BeaconKnownIPPhones, que volvió los atributos del VLA N que asignan los puntos finales en el perfil del teléfono del IP en el faro al VLA N del teléfono cuando usted se une a la red y la autentica con el MAB.

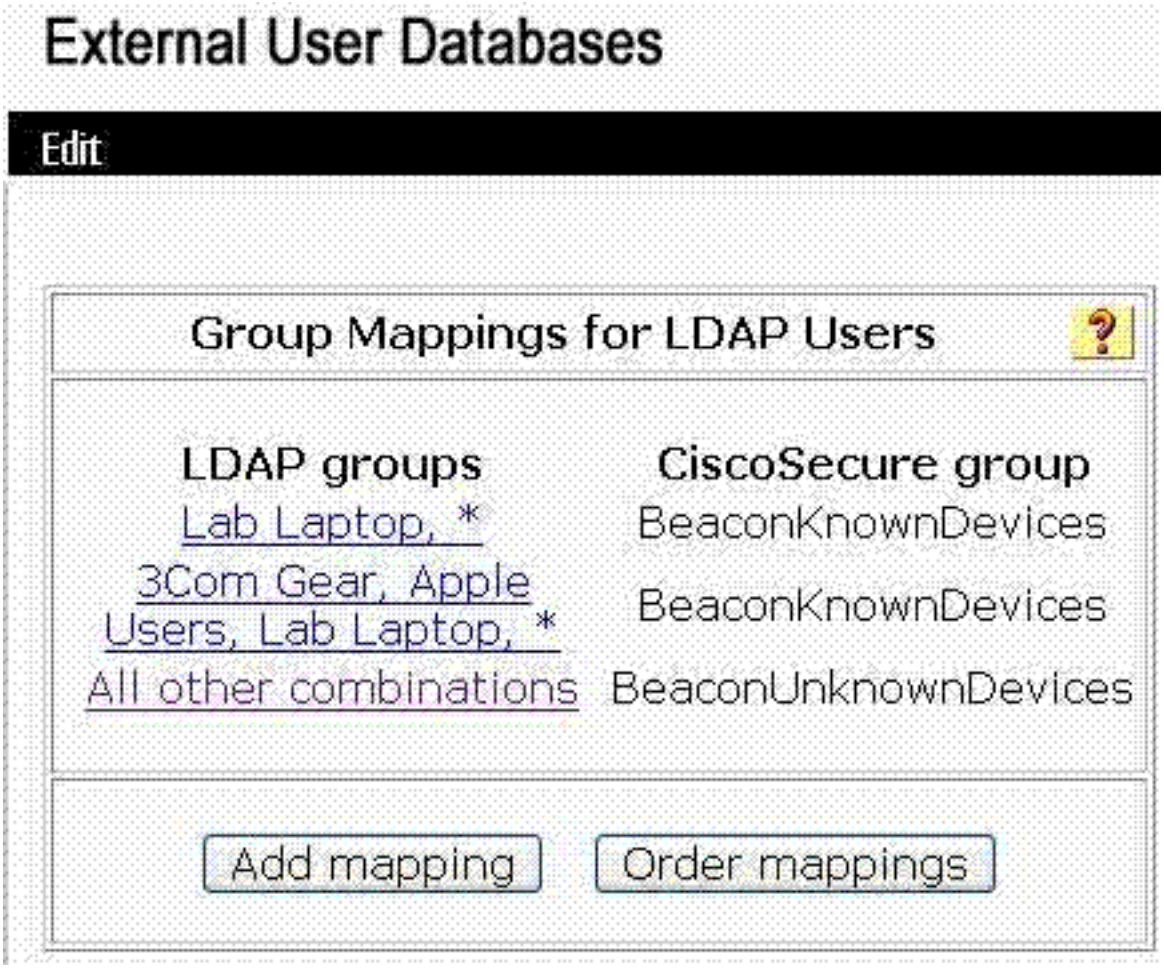
Figura 14: Asignación del Perfil-a-grupo



Elija un grupo DS (perfil del faro con el LDAP habilitado), y asigne los puntos finales en ese perfil al grupo deseado del CiscoSecure del menú desplegable. En el ejemplo anterior, las direcciones MAC en el perfil de usuarios de Apple en el faro se autentican actualmente con el MAB, colocado en el BeaconKnownDevices que da lugar a una autenticación satisfactoria y a una colocación en el VLAN de usuario cuando usted se une a la red.

La selección somete trae para arriba el anuncio de las asignaciones actuales del grupo en el ACS al autenticar a los usuarios desconocidos a la Base de datos de usuarios externa del faro.

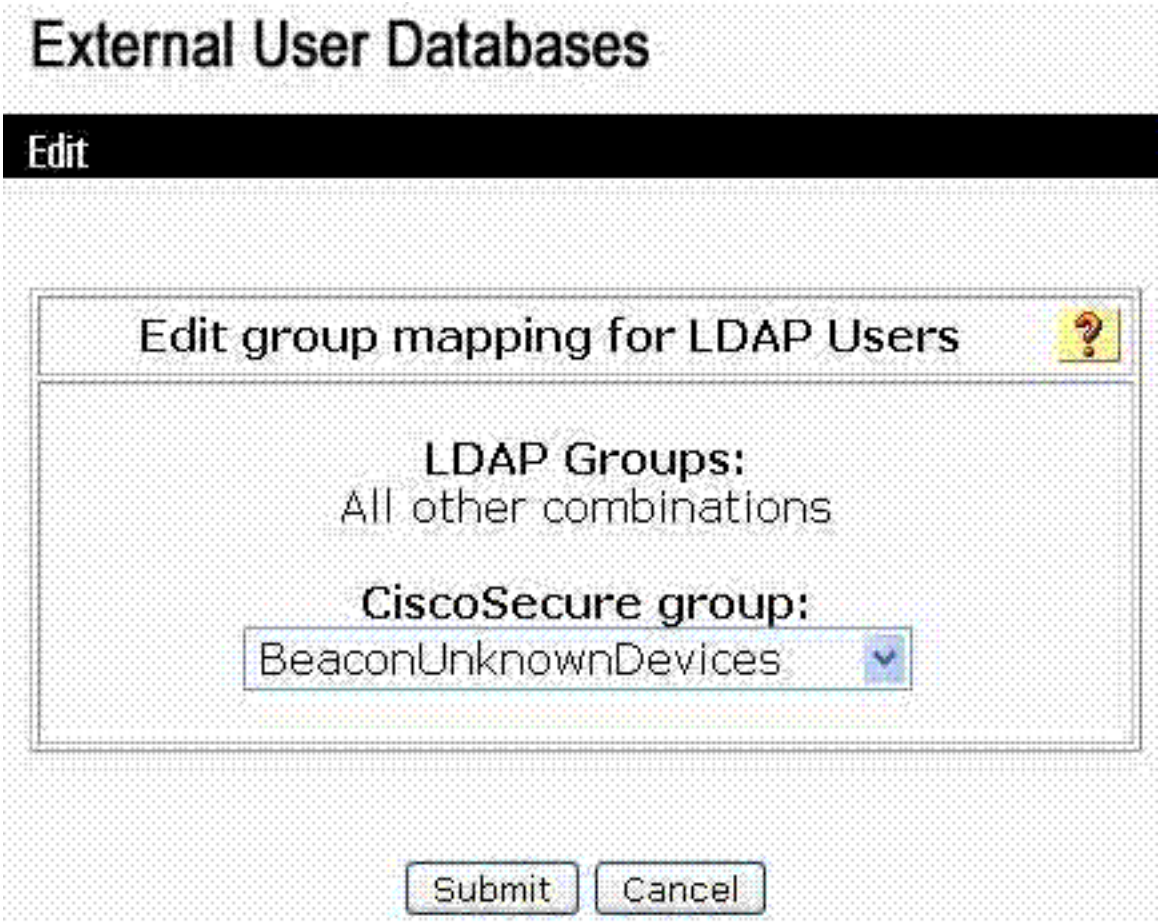
Figura 15: Asignaciones del grupo de la lista



Observe que las asignaciones hechas explícitamente con el procedimiento descrito previamente están enumeradas en esta visión. Cualquier grupos DS (perfiles LDAP-habilitados faro) asociados no explícitamente a un grupo, que incluye los puntos finales que el faro todavía no ha descubierto o colocado en una caída del perfil de LDAPenabled en el todo otro colector de las combinaciones. Esencialmente esto permite los puntos finales que el faro no puede proporcionar la información sobre en un grupo del CiscoSecure, por ejemplo, BeaconUnknownDevices. Según lo delineado previamente, este grupo se puede inhabilitar en conjunto que da lugar al incidente MAB, o como en el ejemplo anterior, puede ser diseñado para proporcionar solamente la Conectividad limitada a los puntos finales no conocidos por el faro.

El resto de las combinaciones se pueden asignar un grupo del CiscoSecure (BeaconUnkownDevices) si usted hace clic en las **todas otras combinaciones** conecta para conseguir esta ventana:

Figura 16: Asignación de un grupo al resto de las combinaciones

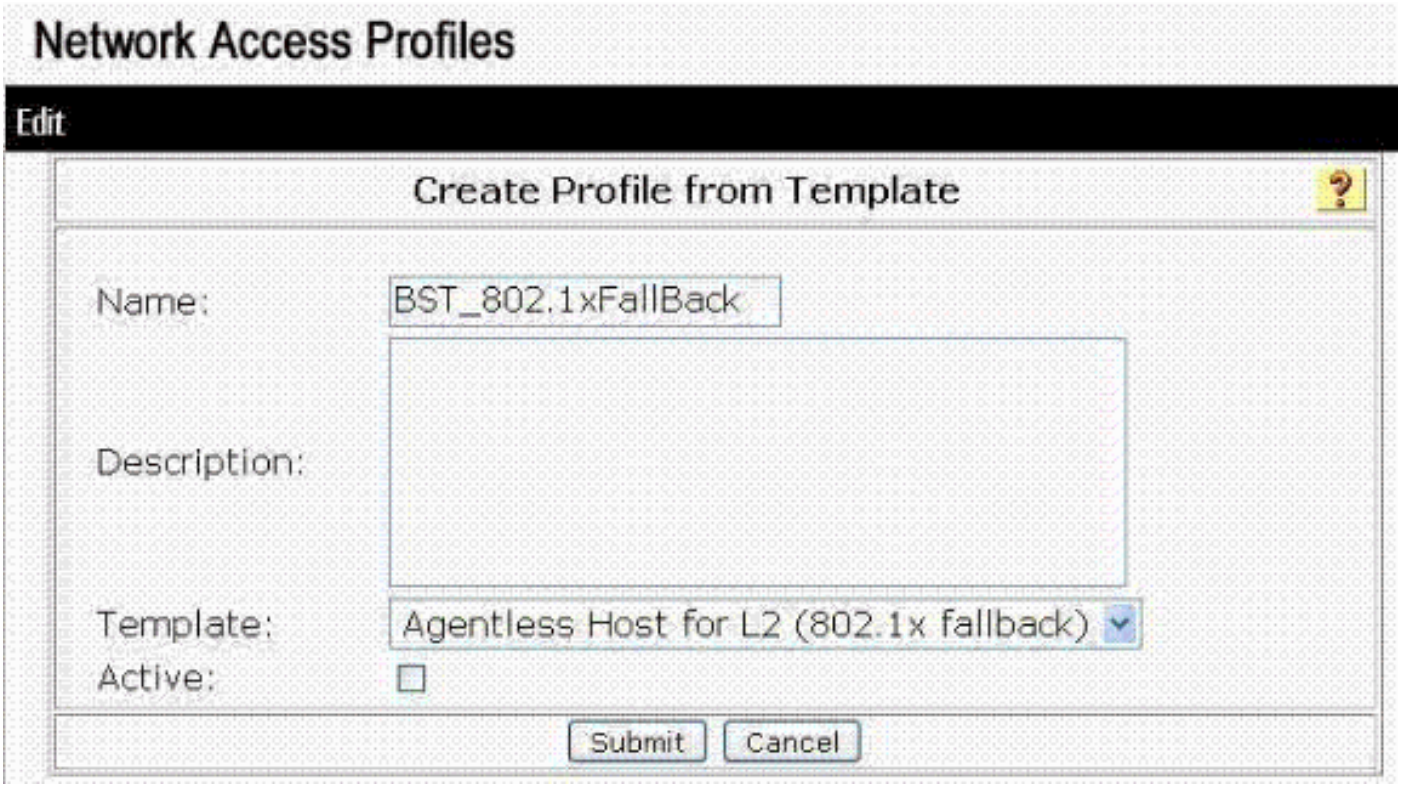


Configuración del perfil del acceso a la red

El paso obligatorio más reciente en configuración de ACS para que el MAB utilice el sistema del Profiler del punto final del faro como proxy es la configuración de un perfil del acceso a la red para el retraso del 802.1x. Complete estos pasos delineados para configurar el perfil del acceso de red requerida para completar la configuración de ACS tales que el MAB está configurado y actúa según la configuración completada previamente.

El perfil del acceso a la red que se agregará es un perfil de la plantilla. Elija los **perfiles del acceso a la red de la** página global de la navegación. Entonces elija **agregan el perfil de la plantilla** para sacar a colación esta forma ilustrada.

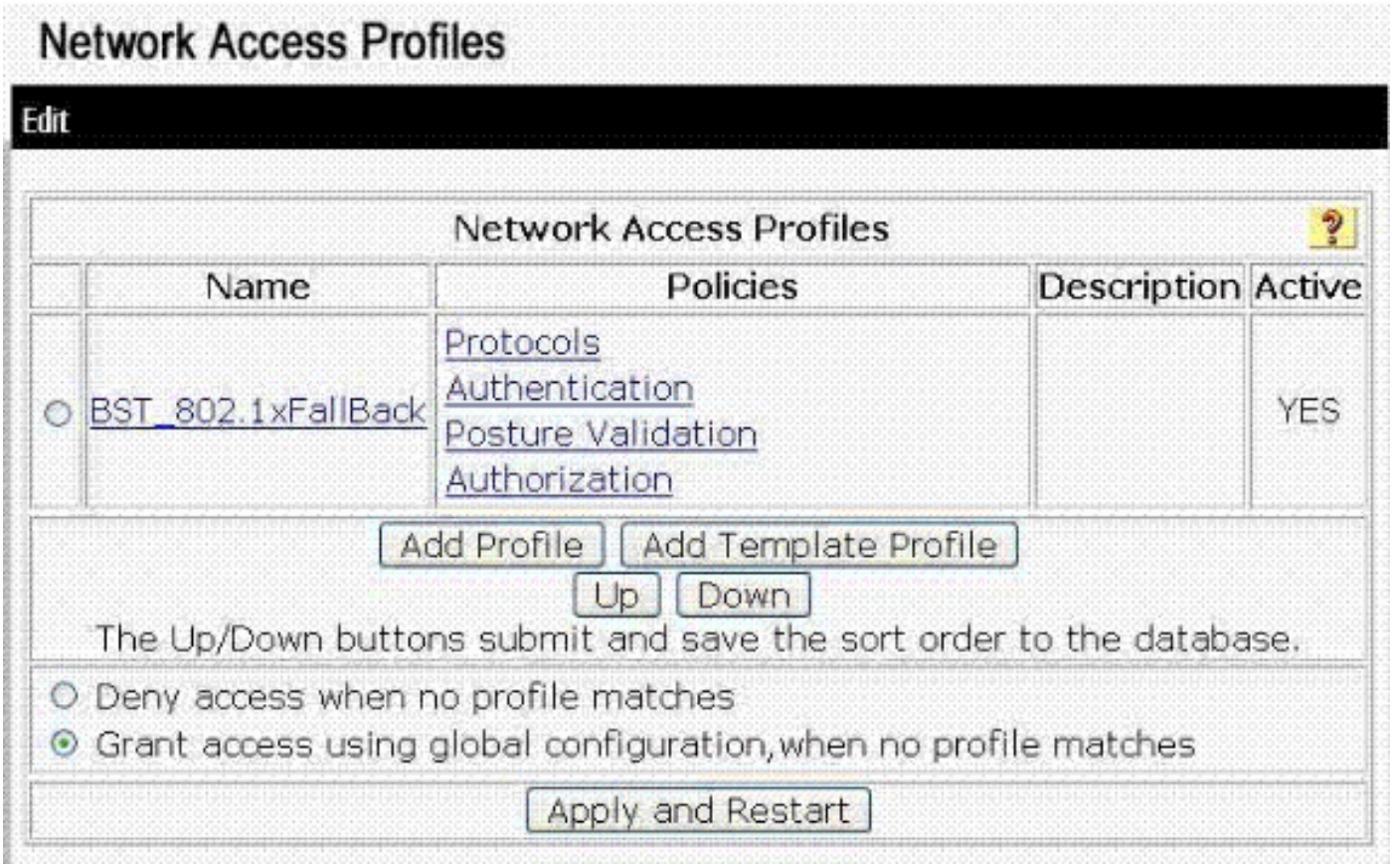
Figura 17: Agregue un perfil del acceso a la red de la plantilla



Nombre el perfil del acceso a la red para habilitar para distinguirlo de otros, y agregue una descripción si está deseado. La plantilla para este perfil se selecciona de la lista desplegable. Asegúrese de que el **host Agentless para L2 (retraso del 802.1x)** esté seleccionado, y marque **casilla de verificación activa**. Haga clic el **botón Submit Button** cuando está acabado para salvar el perfil del acceso a la red.

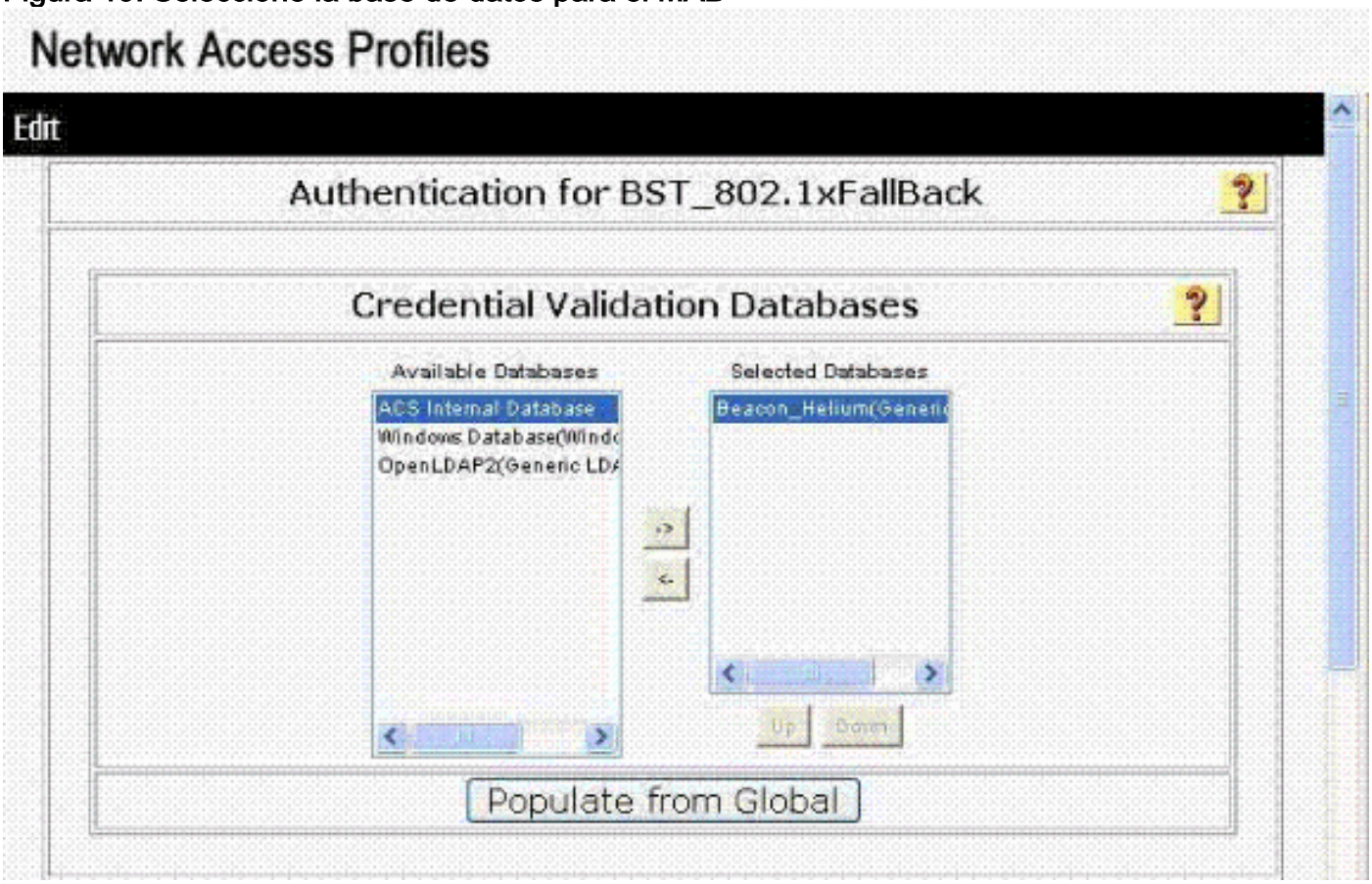
Cuando usted tecleo somete, se presenta esta forma que permite que usted edite los parámetros para el perfil apenas creado como se muestra.

Figura 18: Edite la SIESTA para el MAB



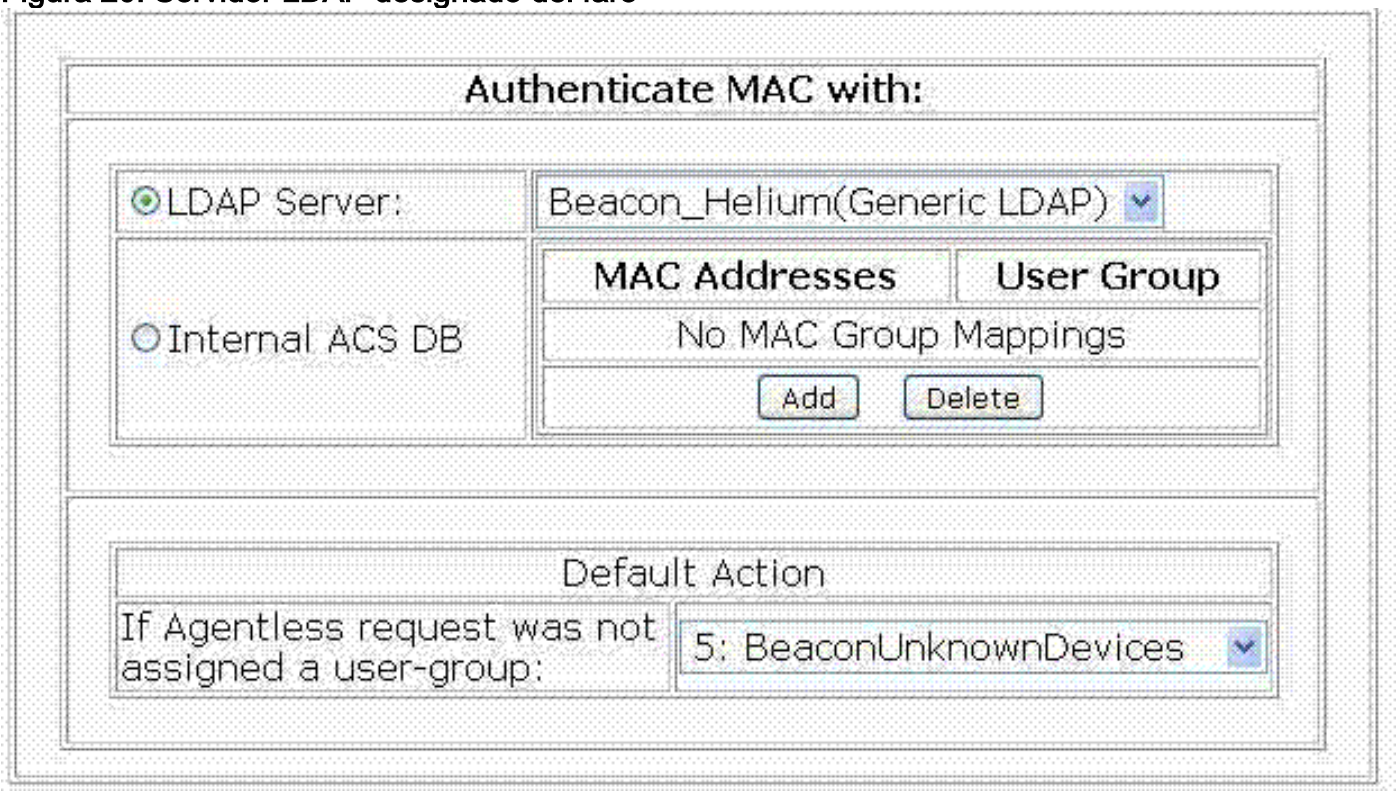
La política de autenticación para el perfil nuevamente configurado se debe configurar para utilizar el sistema del faro como base de datos credencial de la validación. Elija el link de la autenticación en la columna de las directivas para el perfil creado recientemente del acceso a la red (retraso del 802.1x en el ejemplo). Se presentan estas formas.

Figura 19: Seleccione la base de datos para el MAB



Primero, elija la Base de datos de usuarios externa del faro de la tabla de bases de datos disponible y utilice **- >** botón para agregarlo a las bases de datos seleccionadas. Navegue hacia abajo a la sección MAC de la autenticidad de la forma, y elija el botón de radio del **servidor LDAP**. Elija la base de datos del **faro de la** lista desplegable. Pasado, elija el grupo de **BeaconUnknownDevice** para la acción predeterminada tal y como se muestra en de la figura siguiente.

Figura 20: Servidor LDAP designado del faro



Este paso completa la configuración de ACS requerida para puente de la autenticación de MAC con el faro como Base de datos de usuarios externa. Recomience el servicio ACS para asegurarse que todos los cambios de configuración están confiados a la configuración corriente.

El sistema debe estar listo para probar el MAB, si el Switches se configura correctamente. Un punto final actualmente en un perfil LDAP-habilitado del faro se puede ser disconnected de la red y readmitir con los parámetros de la directiva especificados para el grupo de BeaconKnownDevices.

Configuración del switch para puente de la autenticación de MAC

La configuración del switch de Thid proporciona un ejemplo de configuración para la autenticación del 802.1x con puente de la autenticación de MAC habilitado, y la reasignación del VLAN dinámico requerida para aplicar los atributos de RADIUS vueltos del 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