NAC: Integração LDAP com exemplo da configuração ACS

Índice

Introdução

Este documento fornece uma configuração de exemplo das etapas a fim configurar a baliza e o ACS para permitir os dispositivos Cisco configurados para que o MAB de forma eficaz e eficiente autentique dispositivos capazes non-802.1X na rede autenticada.

Cisco executou uma característica chamada o desvio da autenticação de MAC (MAB) em seu Switches assim como apoio necessário no ACS a fim acomodar valores-limite nas redes 802.1X-enabled que são incapazes de autenticar com o 802.1X. Esta funcionalidade assegura-se de que os valores-limite que tentam a conexão à rede 802.1X-enabled que não é equipado com a funcionalidade do 802.1X, por exemplo, não tem um suplicante funcional do 802.1X, pode ser autenticado antes da admissão, assim como tem a política de utilização da rede básica reforçada durante todo sua conexão.

O MAB permite a rede de ser configurado para admitir dispositivos identificados com o uso de seu MAC address como as credenciais preliminares quando o dispositivo não participa no protocolo do 802.1X. Para que o MAB seja distribuído e utilizado eficazmente, o ambiente deve ter meios indentify os dispositivos no ambiente que não são capazes da autenticação do 802.1X, e manter ao longo do tempo um base de dados atualizado destes dispositivos como move-se, adiciona e as mudanças ocorrem. Esta lista precisa de ser povoada manualmente e mantido no Authentication

Server (ACS), ou com alguns meios alternativos a fim assegurar-se de que os dispositivos que autenticam no MAC é terminado e válido em qualquer momento a tempo.

O perfilador do valor-limite da baliza pode automatizar o processo da identificação de NON-autenticar valores-limite, aqueles sem suplicantes do 802.1X, e a manutenção da validez destes valores-limite nas redes da escala de variação na funcionalidade de monitoramento do perfilamento e do comportamento do valor-limite. Através de uma interface ldap padrão, o sistema da baliza pode servir como um base de dados externo ou um diretório dos valores-limite a ser autenticados com o MAB. Quando um pedido MAB é recebido da infraestrutura da borda, o ACS pode perguntar o sistema da baliza a fim determinar mesmo se um valor-limite dado deve ser admitido ao baseado na rede na maioria de informação atual sobre o valor-limite conhecido pela baliza, a fim impedir a necessidade para a configuração manual.

Refira o NAC: Integração LDAP com ACS 5.x e exemplo de configuração mais atrasado para mais informação e uma configuração similar usando ACS 5.x e mais tarde.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

O MAB é uma funcionalidade essencial para o apoio dinâmico dos dispositivos tais como impressoras, Telefones IP, máquinas de fax e outros dispositivos capazes non-802.1X no desenvolvimento do ambiente post-802.1X. Sem uma capacidade MAB, as portas do acesso de rede que fornecem Conectividade aos valores-limite capazes non-802.1X devem ser fornecida estaticamente a fim não tentar a autenticação do 802.1X ou com o uso dos outros recursos que fornecem opções muito limitadas da política. Por razões óbvias, isto não é inerentemente escalável em grandes ambientes de empreendimento. Com o MAB permitido conjuntamente com o 802.1X em todas as portas de acesso, os valores-limite capazes conhecidos non-802.1X podem ser movidos em qualquer lugar no ambiente e ainda confiantemente (e firmemente) conecte à

rede. Porque os dispositivos admitidos à rede estão sendo autenticados, as políticas diferentes podem ser aplicadas aos dispositivos diferentes

Além, os valores-limite capazes non-802.1X que não são conhecidos no ambiente, tal como os portáteis que pertencem aos visitantes ou aos contratantes, podem ser acesso restrito fornecido à rede com o MAB se desejados.

Enquanto o nome sugere, o desvio da autenticação de MAC utiliza o MAC address do valor-limite como as credenciais preliminares. Com o desvio da autenticação de MAC permitido em uma porta de acesso, se um valor-limite conecta e não responde ao desafio de autenticação do 802.1X, a porta reverte ao modo MAB. O interruptor que tenta o MAB de um valor-limite faz uma requisição RADIUS padrão ao ACS com o MAC da estação. Tenta conectar à rede e pede a autenticação do valor-limite do ACS antes da admissão do valor-limite à rede.

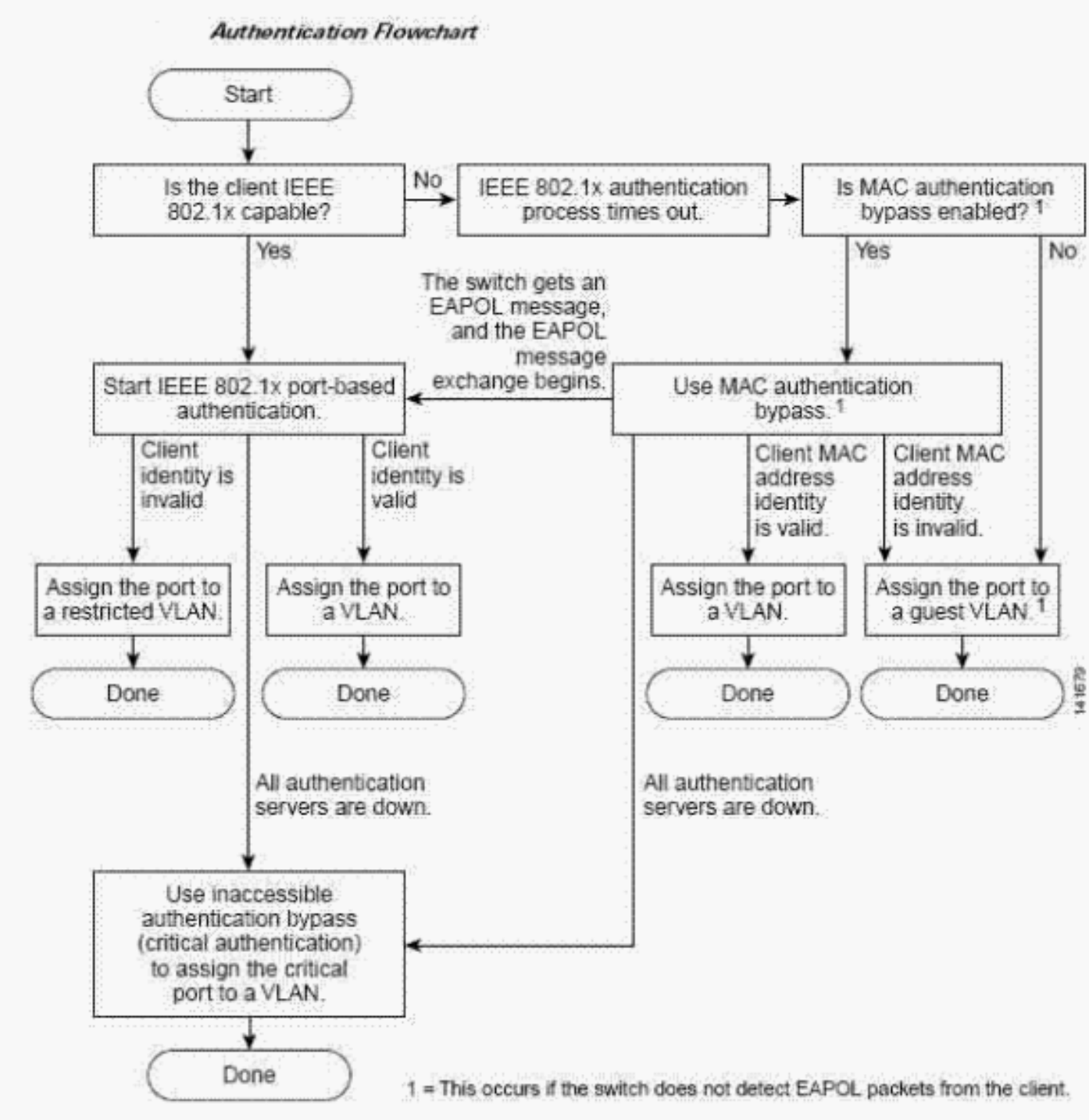
Configuração

Diagrama de fluxograma

Este fluxograma tomado da documentação do Cisco Systems ilustra como o MAB está utilizado conjuntamente com a autenticação do 802.1X na infraestrutura da borda de Cisco enquanto os valores-limite novos tentam conectar à rede.

Este documento usa este fluxo de trabalho do fluxograma:

Figura 1: Fluxo da autenticação



O ACS pode ser configurado para utilizar seu próprio base de dados interno ou um servidor ldap externo a fim autenticar requisições de usuário do MAC address. O sistema do perfilador do valor-limite da baliza LDAP-é permitido inteiramente à revelia e pode ser utilizado pelo ACS a fim autenticar requisições de usuário do MAC address com a funcionalidade do padrão LDAP. Porque a baliza automatiza a descoberta assim como o perfilamento de todos os valores-limite na rede, o ACS pode perguntar a baliza com o LDAP a fim determinar se o MAC for admitido à rede, e em que grupo o valor-limite deve ser traçado. Isto significativamente automatiza e aumenta a característica do desvio da autenticação de MAC, particularmente em grandes ambientes de empreendimento.

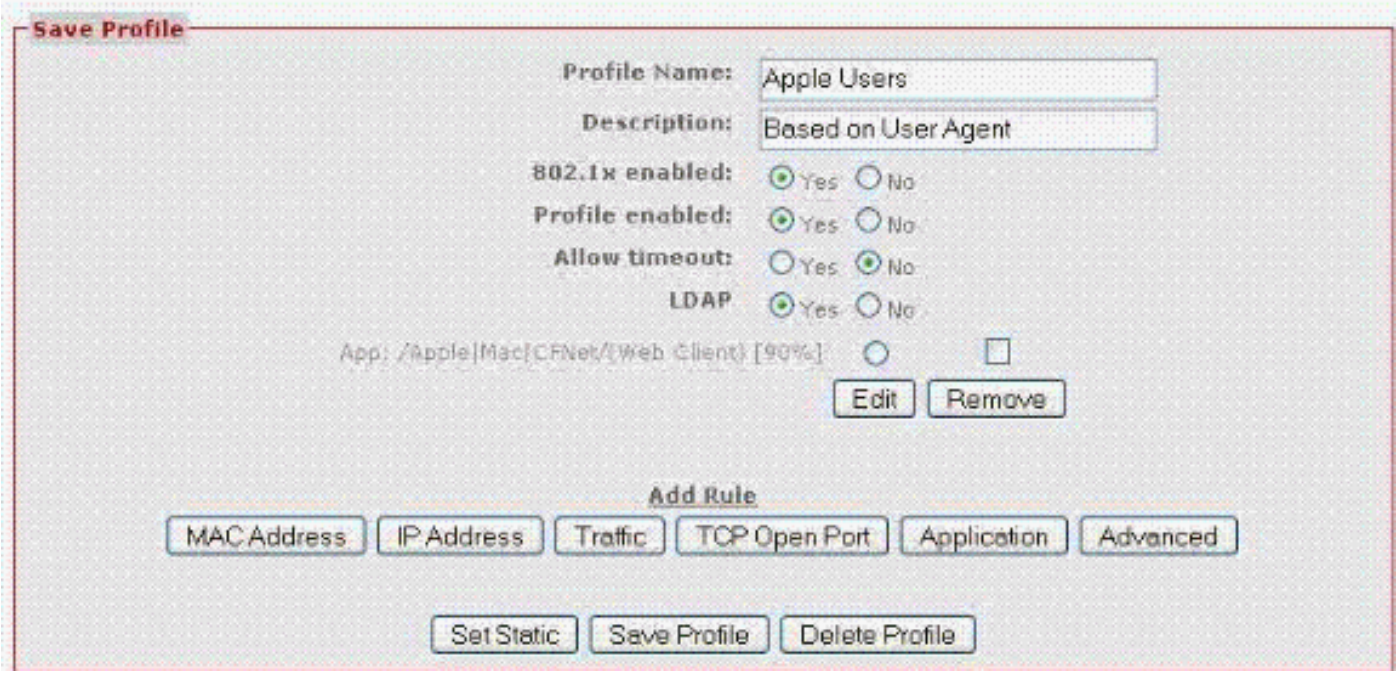
Com a funcionalidade de monitoramento comportável fornecida pela baliza, os dispositivos que são observados para se comportar incompativelmente com os perfis permitidos para o MAB são concluiu a transição fora de 4 perfis LDAP-permitidos e para falhar subseqüentemente a tentativa regular seguinte da reautenticação.

Configuração de sistema do perfilador do valor-limite da baliza para o MAB

A configuração do sistema da baliza para a integração com o ACS para fins do apoio MAB é direta porque a funcionalidade LDAP é permitida à revelia. As tarefas de configuração preliminares são identificar os perfis que contêm os valores-limite que são desejados ser autenticados com o MAB no ambiente, e para permitir então aqueles perfis para o LDAP. Tipicamente, os perfis da baliza, que contêm dispositivos possuíram pela organização, devem ser acesso de rede fornecido quando considerados em uma porta contudo são sabidos para ser incapazes de autenticar com o 802.1X. Tipicamente estes são os perfis que contêm impressoras, Telefones IP ou UPSs manejável como exemplos comuns.

Se as impressoras perfiladas pela baliza foram colocadas em um perfil nomeado *Impressora*, e os Telefones IP em um perfil nomearam *Telefones IP*, por exemplo, a seguir necessidade destes perfis ser permitido para o LDAP tais que os valores-limite colocados naqueles perfis conduzem à autenticação bem sucedida como o telefone IP e impressoras conhecidos no ambiente com o MAB. Se você permite um perfil para o LDAP, este exige que o botão de rádio LDAP na configuração de perfil do valor-limite esteja selecionado, segundo as indicações deste exemplo:

Figura 2: Permita um perfil para o LDAP



Quando a autenticação de MAC dos proxys ACS a iluminar com o LDAP, a pergunta consistir em duas perguntas secundárias, ambo devem retornar um resultado válido, NON-nulo. A primeira pergunta a iluminar é mesmo se o MAC está sabido para iluminar, por exemplo, se se descobriu e foi adicionado ao base de dados da baliza. Se o valor-limite tem ser descoberto ainda pela baliza, o valor-limite está considerado ser desconhecido. A segunda pergunta não é necessária no caso dos valores-limite que a baliza não descobriu e não está em seu base de dados. Se o valor-limite foi descoberto e está no base de dados da baliza, a pergunta seguinte é determinar o perfil atual do valor-limite. Se um valor-limite tem ser perfilado ainda ou está atualmente em um perfil não 5 permitido para o LDAP, o resultado desconhecido está retornado ao ACS, e a autenticação do valor-limite pela baliza falha. Depende de como o ACS é configurado que este pode conduzir ao dispositivo com a recusa do acesso à rede completamente, ou dado uma política que seja apropriada para o desconhecido ou os dispositivos do convidado.

Somente no caso onde o MAC é um valor-limite que a baliza descubra e colocado em um perfil LDAP-permitido, a resposta é que o valor-limite está conhecido e perfilado pela baliza esteja

retornado ao ACS. Mais importante ainda, porque baliza destes valores-limite fornece o nome de perfil atual, que permite o ACS de traçar valores-limite conhecidos aos grupos de Cisco SecureAccess. Isto permite uma determinação granulada da política feita, tão granulado quanto uma política separada para cada perfil LDAP-permitido baliza, se desejado.

Configuração ACS para o MAB e utilização da baliza como uma base de dados de usuário externo

A configuração do ACS para o MAB e da utilização da baliza como uma base de dados de usuário externo exige três etapas distintas. A ordem ilustrada neste documento segue uns trabalhos que sejam eficientes quando executam a configuração MAB em sua totalidade, e possam variar para os sistemas que estiveram na operação com outros modos de autenticação já configurados.

Configurar Cisco SecureGroup

Quando você tenta o MAB para um ponto final particular que tentem conectar à rede, o ACS pergunta a baliza no LDAP a fim determinar se a baliza descobriu o MAC, e o que baliza do perfil colocou atualmente o MAC address dentro como descrito mais cedo no documento.

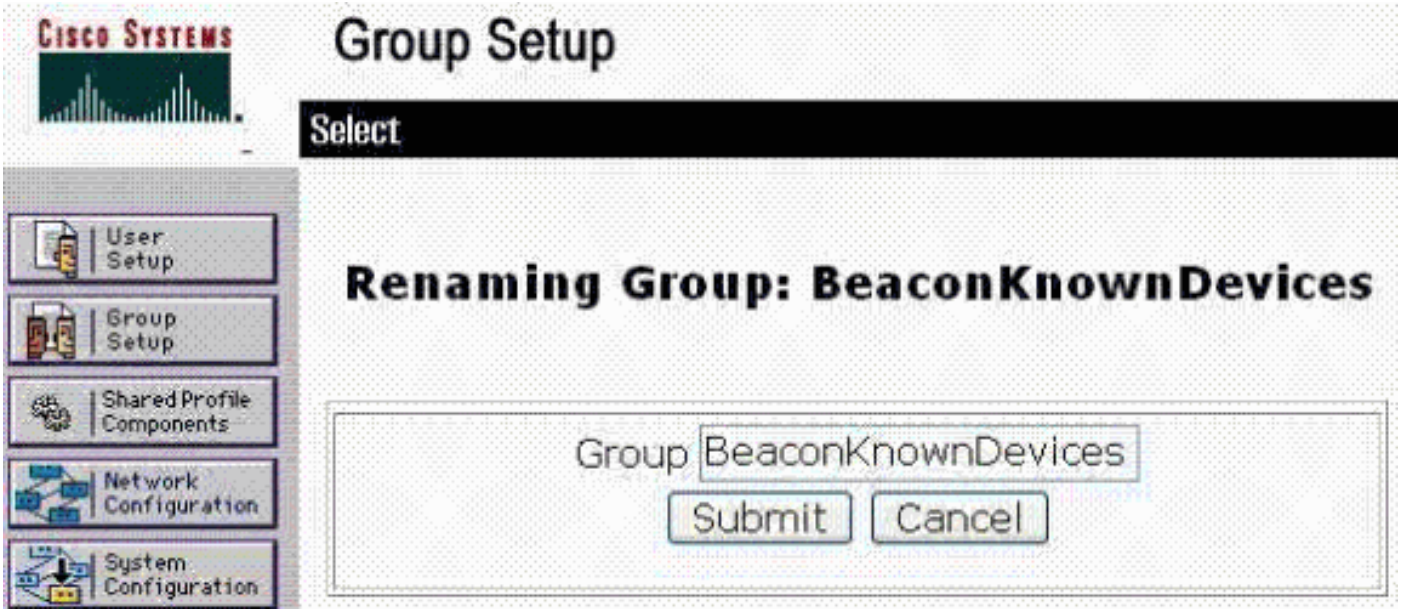
O mecanismo de Cisco SecureGroup com ACS pode ser usado a autentica e aplica a política aos valores-limite que foram descobertos e perfilados pela baliza com o MAB, assim como às falhas de autenticação — aqueles dispositivos não conhecidos ou perfilados não atualmente pela baliza.

Por exemplo, um grupo pode ser adicionado à configuração ACS para os valores-limite descobertos e perfilados a baliza e *BeaconKnownDevices* chamado, e por um outro grupo *BeaconUnknownDevices* adicionado para os dispositivos que não são sabidos atualmente pela baliza. Uma ou outra baliza não descobriu o MAC, nem não o perfilou atualmente em um perfil LDAP-permitido. Como mostrado mais tarde neste documento, os grupos permitem o aplicativo da política aos valores-limite enquanto tentam se juntar à rede.

Note que no exemplo esboçado neste documento, simplesmente dois grupos, BeaconKnown e BeaconUnknown são configurados. Mas é possível criar SecureGroups múltiplo para os valores-limite descobertos e perfilados pela baliza, tanta como porque uma para cada perfil LDAP-permitido na baliza, cada um com os parâmetros diferentes da política tais como a atribuição de VLAN. Além, o grupo do dispositivo de BeaconUnkown pode ser configurado para negar todo o acesso aos valores-limite que têm ser descobertos ou colocado ainda em um perfil permitido para o LDAP pela baliza 6. Isto é realizado se você escolhe a caixa de seleção desabilitada grupo nos parâmetros do indicador da configuração de grupo de BeaconUnknownDevices.

A criação do grupo no ACS é iniciada do botão Group Setup Button na interface do utilizador ACS. Escolha um dos grupos disponíveis, e escolha então o botão do **grupo do rebatismo** a fim mudar o nome do grupo a KnownBeaconDevices segundo as indicações deste exemplo. O clique **submete-se** a fim salvar a mudança.

Figura 3: Edite o grupo do CiscoSecure

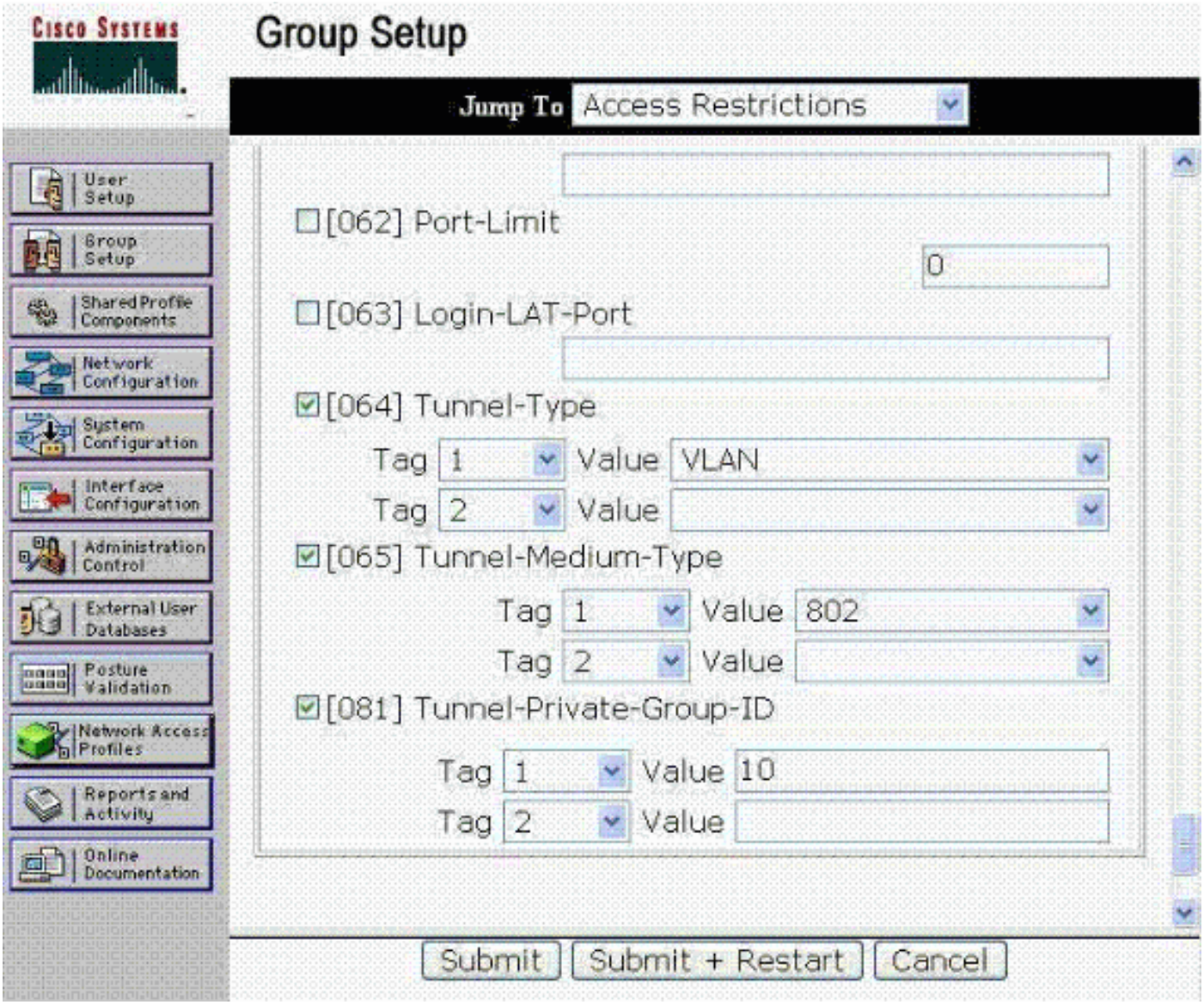


Escolha **editam ajustes** a fim editar os ajustes do grupo. Edite os parâmetros do grupo de BeaconKnownDevices como desejados. Para fins do exemplo neste documento, os parâmetros do grupo que são mudados incluem somente os atributos de raio de IETF, encontraram na parte inferior da página.

Especificamente você designa que os dispositivos autenticados a este grupo, os endereços MAC que a baliza perfilou aos perfis selecionados para o MAB e permitidos para o LDAP, têm os parâmetros da política retornados ao interruptor de autenticação que permite a admissão dos valores-limite à rede no VLAN apropriado. A fim fazer isto, o Túnel-Media-tipo 064, 065 o Tipo de túnel dos atributos RADIUS, e 081 o túnel Privado-Grupo-ID é ajustado para conduzir aos valores-limite que estão sendo colocados no VLAN desejado, segundo as indicações de figura 4.

Assegure-se de que as caixas de seleção ao lado de cada atributo RADIUS estejam verificadas.

Figura 4: Atributos do grupo VLAN

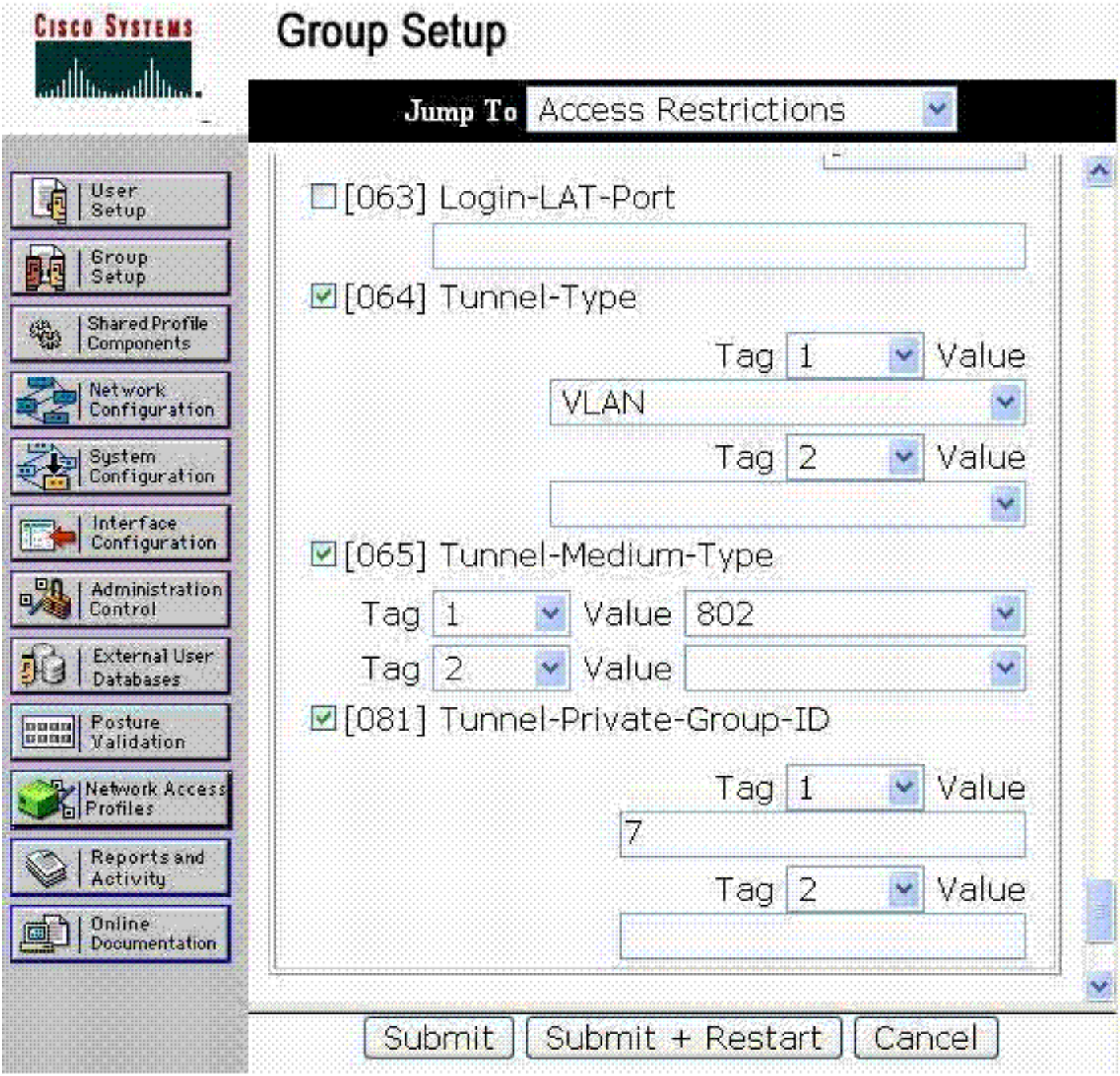


No exemplo mostrado, os valores-limite autenticados com sucesso pela baliza e atribuídos subseqüentemente ao grupo ACS BeaconKnownDevices são colocados no VLAN10, o VLAN autorizado na configuração de rede de exemplo, durante a conexão à rede e autenticados com sucesso no MAB pelo ACS com o uso da baliza como uma base de dados de usuário externo.

O grupo de BeaconUnknownDevices é criado similarmente para os dispositivos que não são sabidos atualmente pela baliza como mostrado. Além disso, se estes dispositivos não obtiverem nenhum acesso à rede, verifique simplesmente a caixa de seleção **desabilitada grupo na** parte superior do formulário. Valores-limite que não foram descobertos pela baliza nem atualmente não são perfilados pela baliza em uma falha LDAP-permitida MAB do perfil e não são admitidos à rede.

Esta figura mostra a alternativa do que o uso da caixa de seleção desabilitada grupo. Neste caso, os valores-limite que não podem ser autenticados pela baliza são atribuídos a um grupo que seja permitido, mas têm uma política diferente do que isso para os valores-limite que são conhecidos. Consulte para figurar o 5.

Figura 5: Parâmetros VLAN para BeaconUnknownDevices



Note que para dispositivos desconhecidos neste exemplo, são admitidos à rede mas relegados a um convidado ou a um VLAN restrito, VLAN 7. Na rede de exemplo, o VLAN 7 é o convidado VLAN, que permite o acesso ao Internet dos valores-limite somente, e proibe o acesso aos recursos internos.

Quando o ACS pede a autenticação da baliza de um MAC de um valor-limite que tenha ser descoberto ou perfilado ainda pela baliza, o ACS coloca o MAC neste grupo e retorna o resultado ao interruptor de autenticação permitido para o MAB.

Configuração externa de bando de dados de usuário ACS

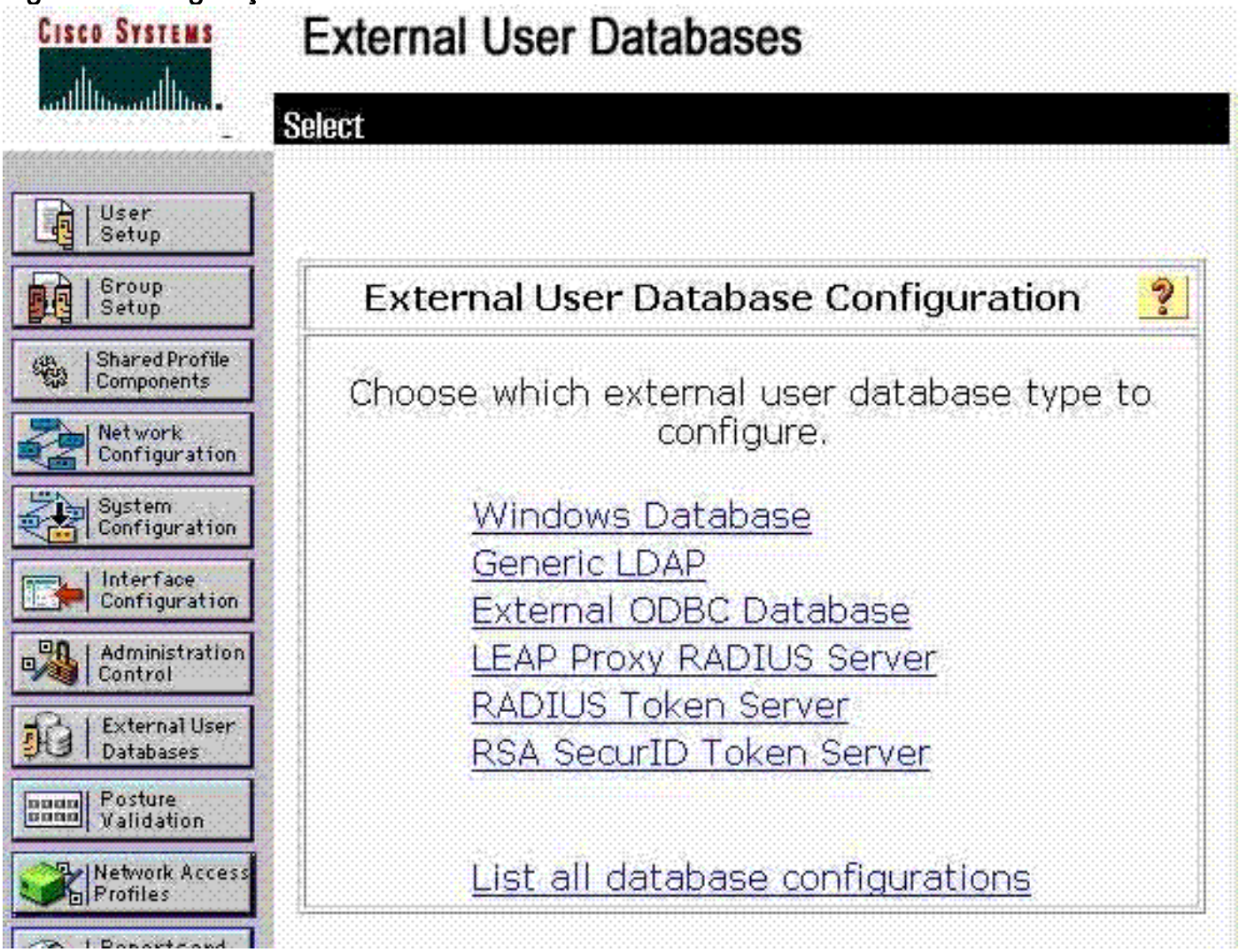
O ACS deve ser configurado aos pedidos MAB do proxy dos switch de acesso iluminar através do LDAP. Isto exige que a configuração ACS inclui o sistema da baliza como uma base de dados de usuário externo genérica LDAP. As etapas esboçadas nesta seção ilustram como adicionar o sistema do perfilador do valor-limite da baliza 9 como uma base de dados de usuário externo a ser perguntada pelo ACS quando recebe pedidos MAB. Escolha a **base de dados de usuário externo no** painel de navegação global a fim trazer acima o indicador da base de dados de

usuário externo ilustrado na figura 6.

Figura 6: Tela principal externo da configuração DB

A primeira tarefa na configuração da baliza como uma base de dados de usuário externo é adicionar o sistema da baliza como uma base de dados de usuário externo genérica LDAP. Escolha a **configuração do base de dados** para que o indicador ilustrado na figura 7 aparecem.

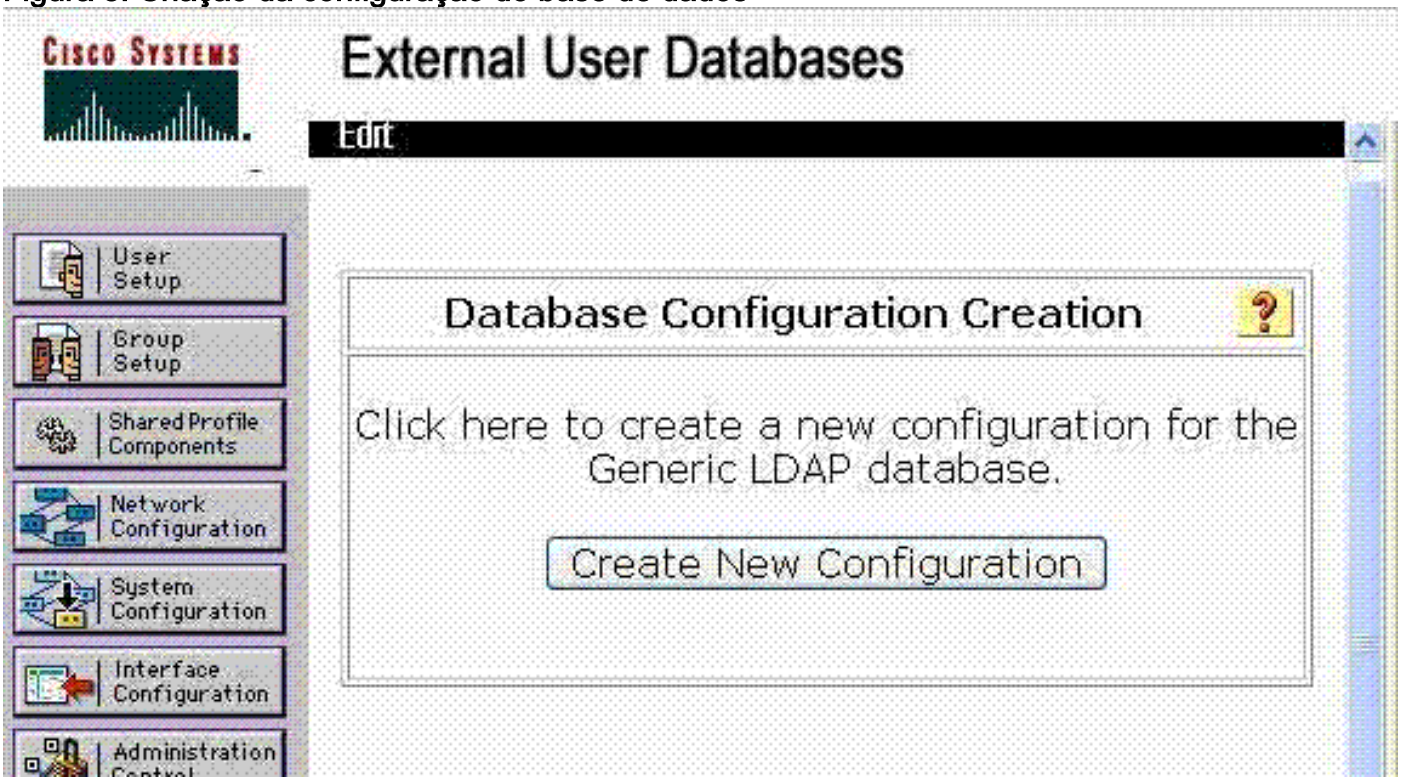
Figura 7: Configuração externa de bando de dados de usuário ACS



Escolha o **LDAP genérico** a fim abrir o formulário usado para adicionar o sistema do perfilador do valor-limite da baliza como o usuário externo DB na configuração ACS. Este indicador parece permitir a criação de uma configuração externa de bando de dados de usuário nova do tipo LDAP

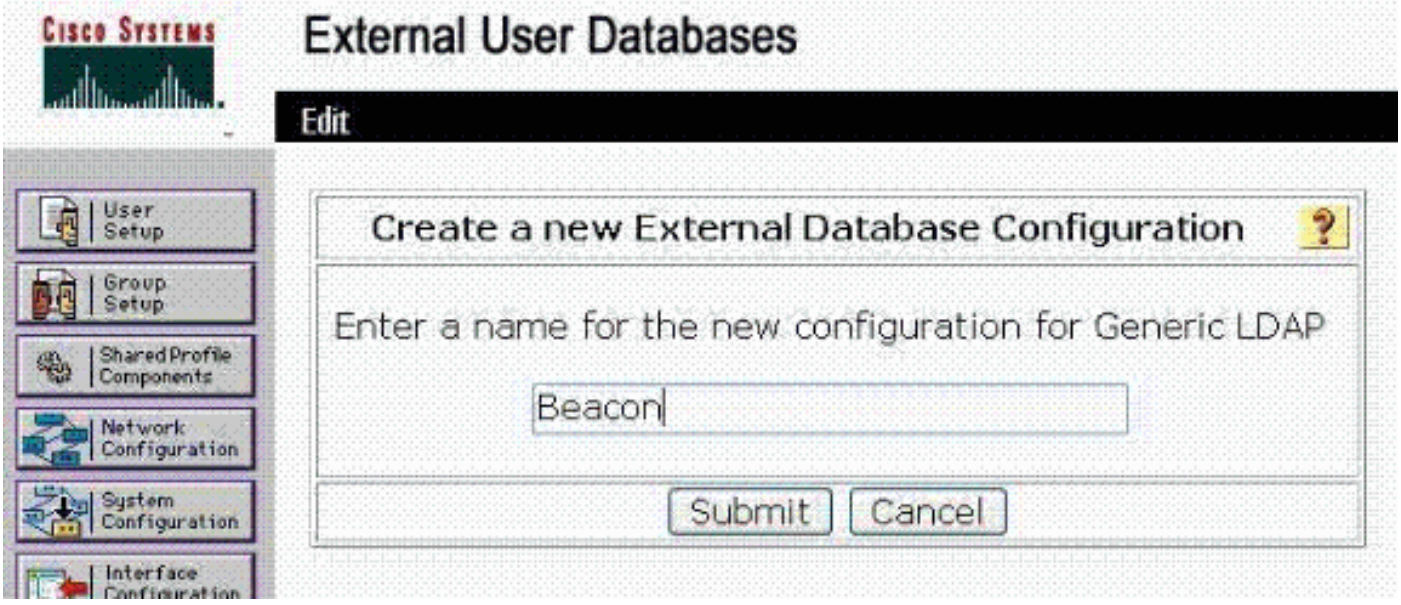
genérico.

Figura 8: Criação da configuração do base de dados



Escolha o botão **novo da configuração da criação** a fim criar o base de dados LDAP genérico para a baliza. Este indicador aparece e permite que o base de dados externo novo seja nomeado.

Figura 9: Base de dados de usuário externo da baliza do nome

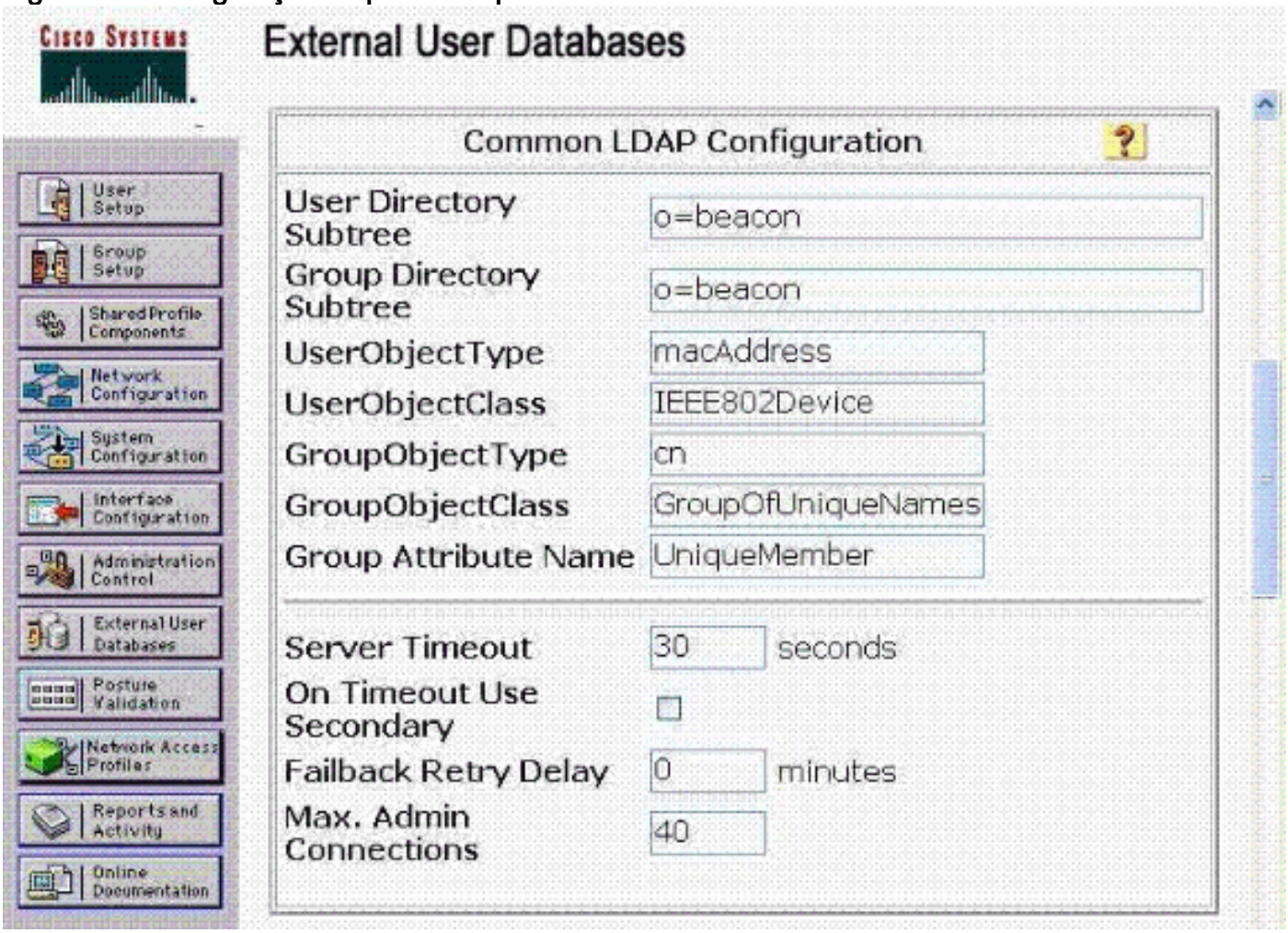


Dê entrada com um nome para o base de dados externo genérico da baliza LDAP que permite que seja diferenciado facilmente de outros bases de dados externos na configuração. Escolha **submetem-se** a fim mover-se na entrada dos parâmetros LDAP exigidos que permitem uma comunicação entre 11 ACS e baliza com a finalidade da autenticação de endereços MAC com o uso da informação de base de dados da baliza.

A figura 10 ilustra os parâmetros comuns da configuração ldap que devem ser incorporados para a base de dados de usuário externo genérica da baliza LDAP que é adicionada à configuração

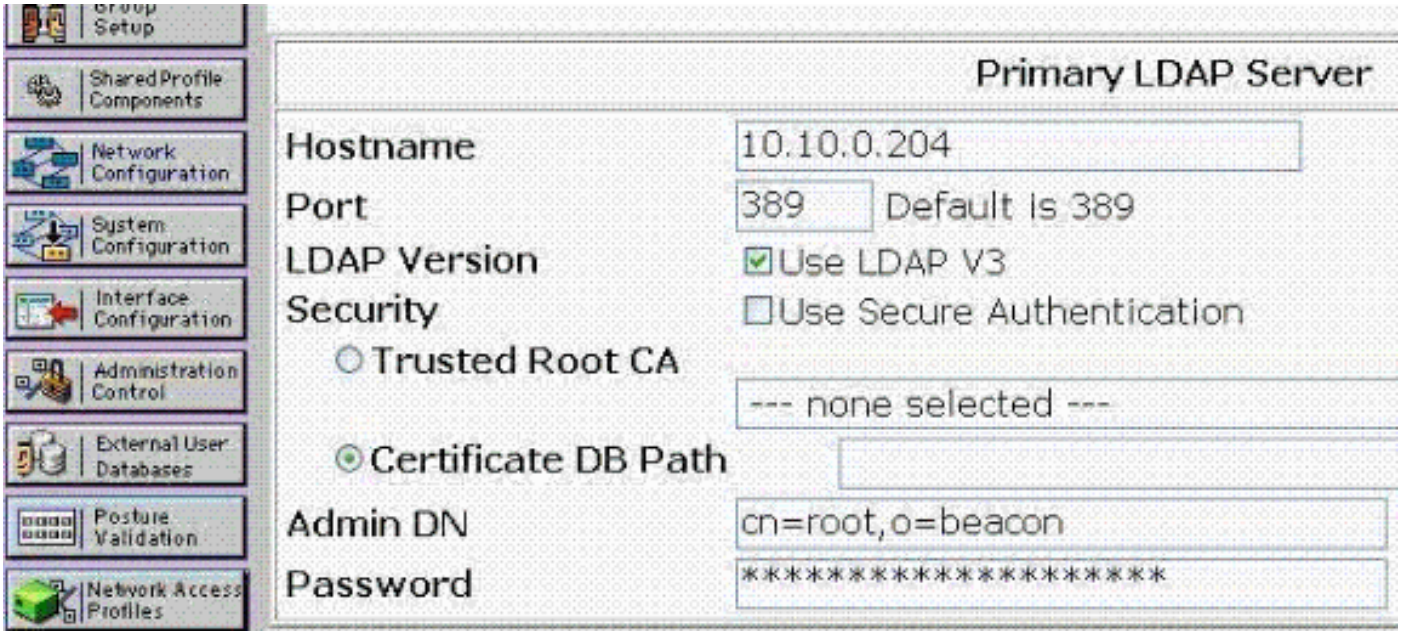
ACS. Note que estes parâmetros fornecem o ACS a informação que exige a fim perguntar a baliza com o LDAP. Estes parâmetros devem ser incorporados exatamente segundo as indicações desta figura a fim facilitar uma comunicação entre o ACS e o perfilador do valor-limite da baliza.

Figura 10: Configuração ldap comum para a baliza



Nota: Use a senha **GBSbeacon** para a senha do ligamento LDAP. A senha é incorporada no fundo do formulário mostrado em figura 11.

Figura 11: Parâmetros de servidor da baliza

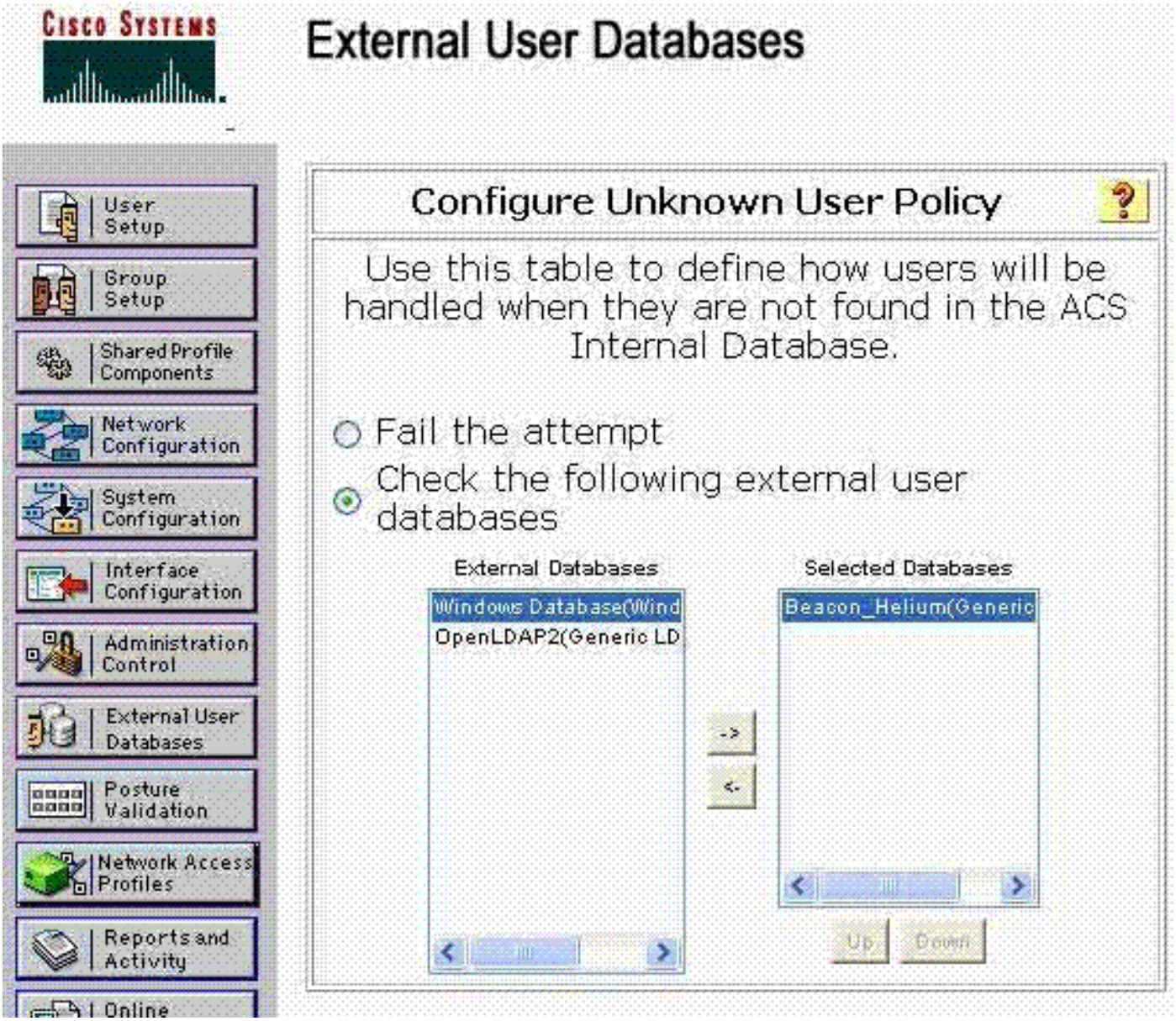


As segundas tarefas de configuração associadas com a configuração da baliza como uma base de dados de usuário externo são a configuração da política de usuário desconhecida. A política de usuário desconhecida dirige o ACS para perguntar o base de dados da baliza sempre que recebe um pedido de autenticação para um usuário, que seja um MAC address no caso do MAB, que não tem a informação para em seu próprio base de dados.

Note que em um desenvolvimento típico ACS, pode haver umas bases de dados de usuário externo existentes configuradas e pode já ser configurado para perguntar aqueles bases de dados quando as credenciais do usuário desconhecido forem submetidas. A base de dados de usuário externo da baliza deve ser adicionada à lista a fim perguntá-la quando o Switches pede o MAB de endereços individuais MAC.

Estas figuras esboçam os trabalhos para a configuração da política de usuário desconhecida, e a adição de baliza como uma base de dados de usuário externo a ser perguntada. A, escolha o link da **política de usuário desconhecida na** página principal da base de dados de usuário externo como ilustrado na figura 6 a fim começar os trabalhos.

Figura 12: Configurar a política de usuário desconhecida

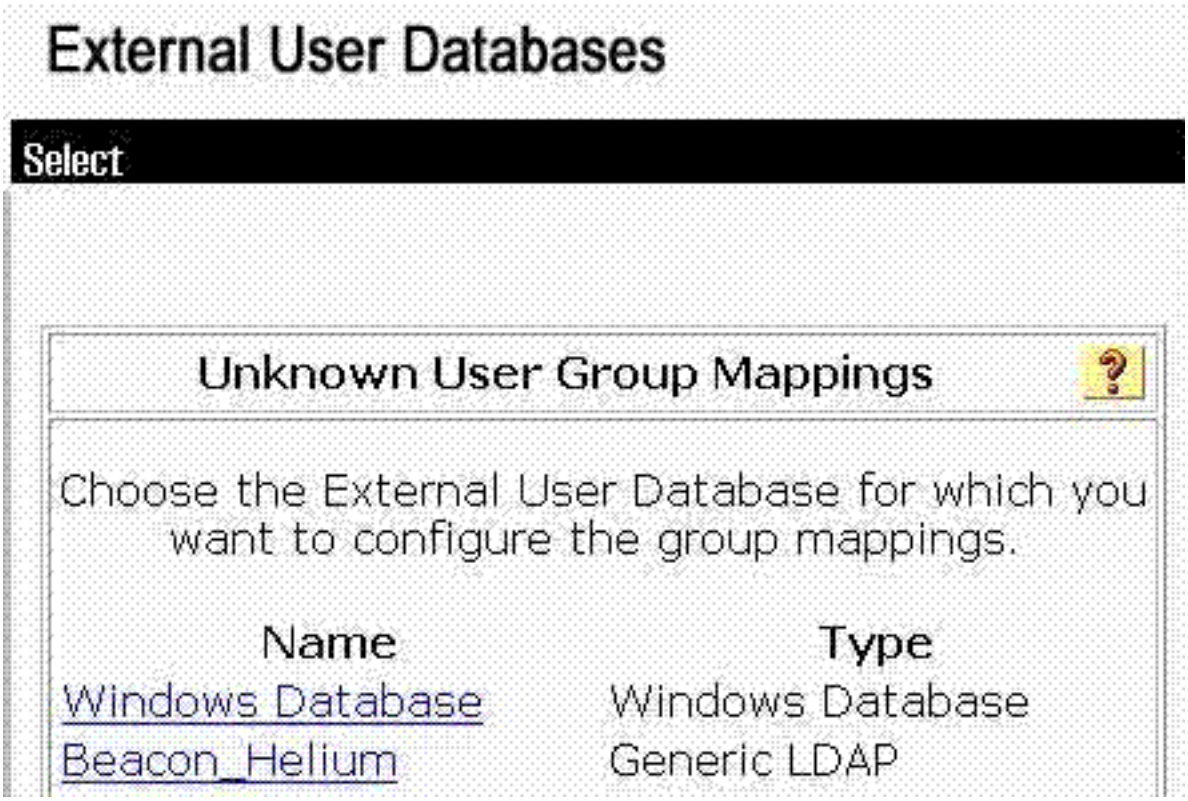


Escolha o base de dados LDAP genérico da baliza adicionado à configuração ACS na última etapa da lista de bases de dados externos à esquerda (Beacon_Helium) no exemplo. Uso **- >** a fim mover-se para bases de dados selecionado. Certifique-se de você escolher a **verificação o seguinte** botão de rádio das **bases de dados de usuário externo**. Isto assegura-se de que quando o Switches submete endereços MAC para a autenticação ao ACS, o ACS pergunte a baliza a fim determinar se o valor-limite é conhecido e tem o perfil atual, se existerem.

A tarefa da configuração final adicionar a baliza como uma base de dados de usuário externo é a conclusão dos mapeamentos de grupo de base de dados. Essencialmente este mapeamento amarra junto os grupos do CiscoSecure criados, por exemplo, BeaconKnownDevices e BeaconUnknownDevices, às perguntas bem sucedidas e mal sucedidas LDAP feitas para iluminar de modo que cada MAB tentado pelo Switches conduza à atribuição do valor-limite a um grupo do CiscoSecure pelo ACS. Isto permite o ACS de responder ao interruptor mesmo se o valor-limite deve ser admitido à rede, e se admitido, o que a política tal como o VLAN o atribui deve ser.

Escolha **mapeamentos de grupo de base de dados na** página principal das bases de dados de usuário externo segundo as indicações da figura 6 a fim configurar os mapeamentos.

Figura 13: Mapeamentos de grupo de base de dados

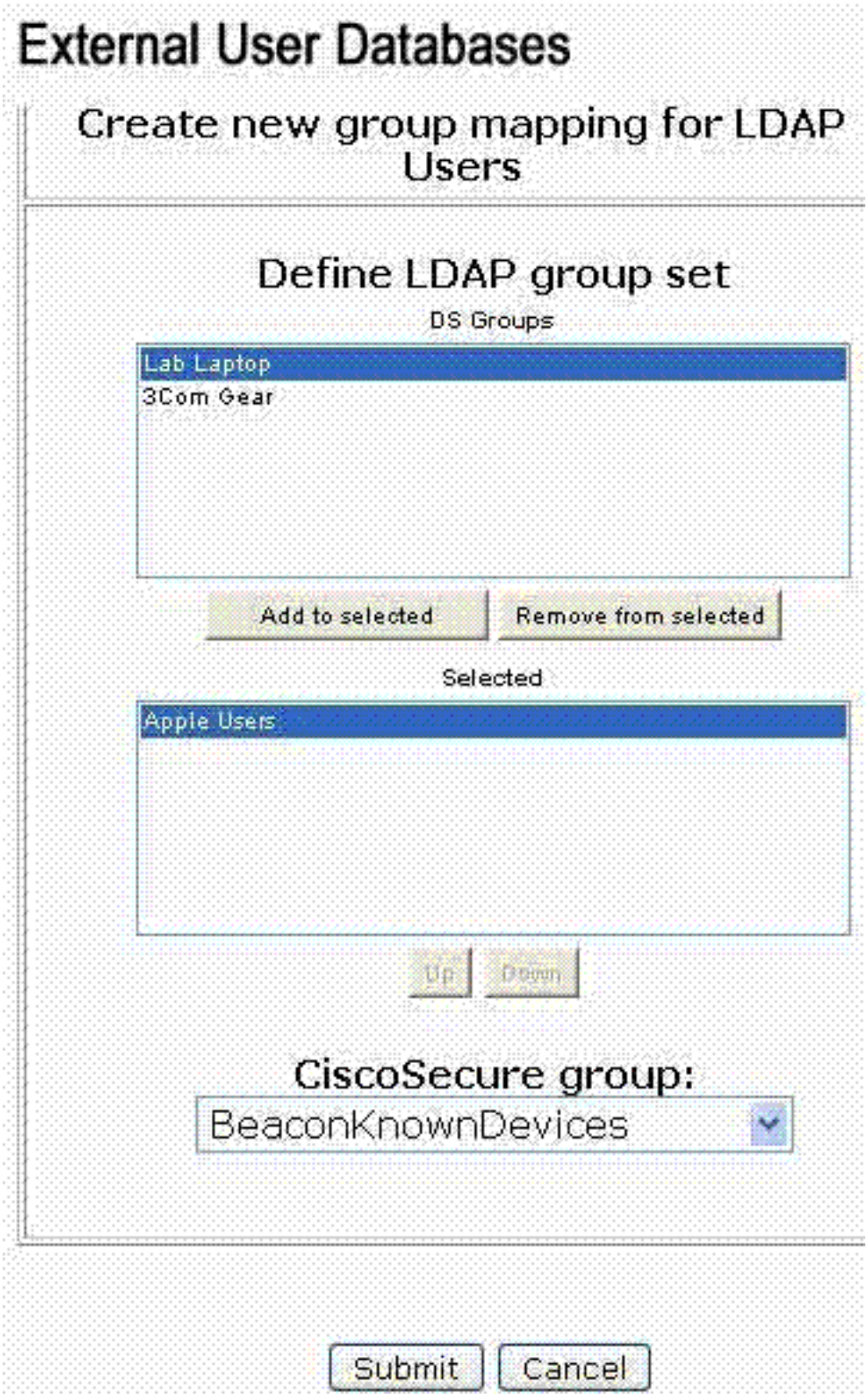


Quando você escolhe a base de dados de usuário externo da baliza criada mais cedo nesta seção com a seleção do link, Beacon_Helium no exemplo anterior, isto indica o indicador ilustrado em figura 14. Note que todos os perfis da baliza permitidos para o LDAP dentro da configuração de sistema da baliza como descrito na primeira seção destas instruções de configuração estão povoados nos grupos DS que estão disponíveis para que a seleção crie mapeamentos dentro do ACS. Se os nomes de perfil da baliza permitidos para o LDAP não são mostrados na relação ACS, este é indicativo de um problema com a configuração ldap ACS. Refira as instruções na baliza da configuração como uma base de dados de usuário externo esboçada mais cedo nesta seção, em particular os parâmetros LDAP.

Note que esta é a relação que permite o traço de perfis LDAP-permitidos individuais na baliza com os grupos do CiscoSecure configurados dentro do ACS. A relação permite o mapeamento de cada baliza individual perfil LDAP-permitido a um único grupo do CiscoSecure. Neste exemplo, somente um único grupo foi criado para dispositivos conhecidos em perfis LDAP-permitidos da baliza: BeaconKnownDevices. Mas, os grupos múltiplos, cada um com seus próprios parâmetros da política podem ser criados a fim segurar as autenticações bem sucedidas diferentemente dependentes do perfil atual da baliza do dispositivo.

Por exemplo, um grupo do CiscoSecure pode ser criado para BeaconKnownIPPhones, que retornou os atributos VLAN que atribuem valores-limite no perfil do telefone IP na baliza ao telefone VLAN quando você se junta à rede e se autentica com o MAB.

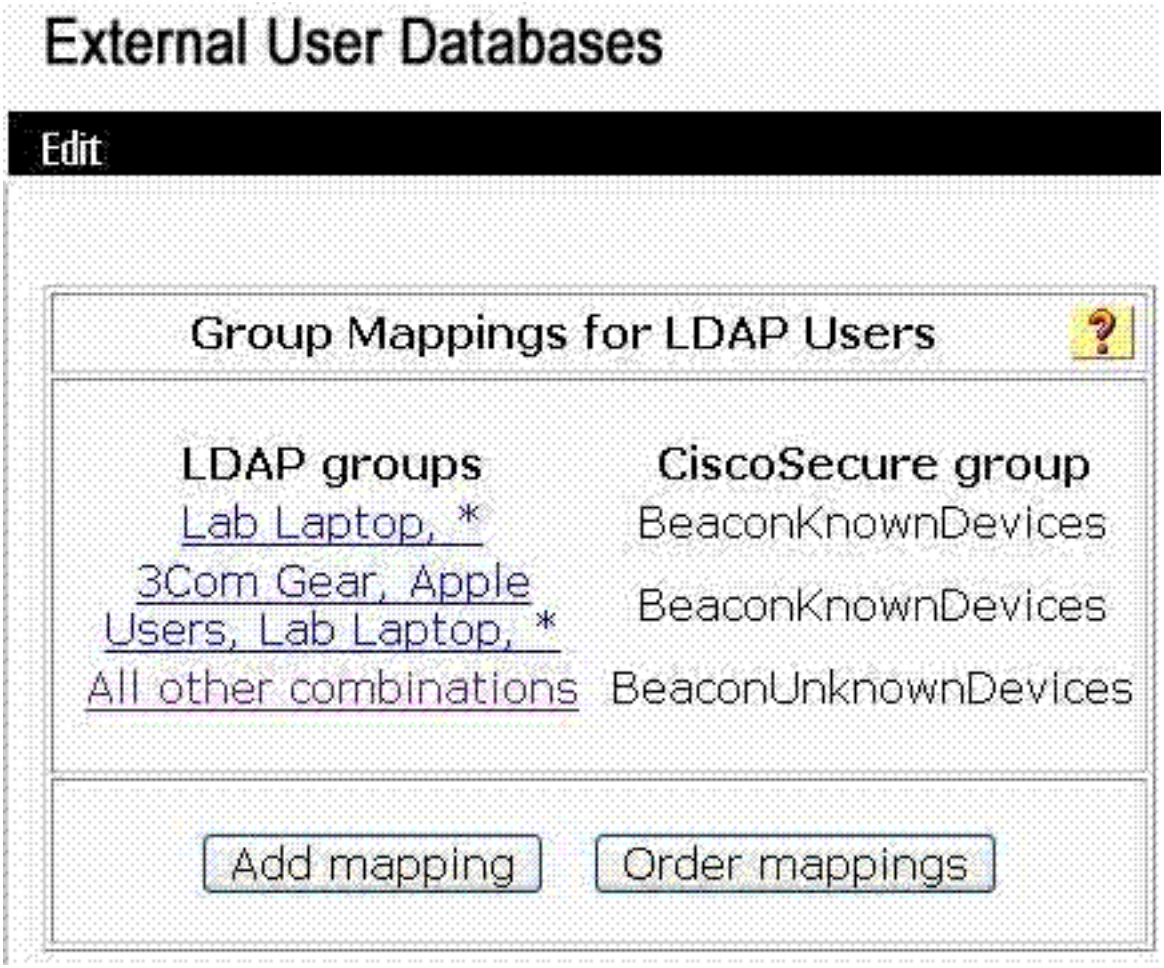
Figura 14: Mapeamento do Perfil-à-grupo



Escolha um grupo DS (perfil da baliza com o LDAP permitido), e atribua valores-limite nesse perfil ao grupo desejado do CiscoSecure do menu suspenso. No exemplo anterior, os endereços MAC no perfil de usuários de Apple na baliza são autenticados atualmente com o MAB, colocado no BeaconKnownDevices que conduz a uma autenticação bem sucedida e a uma colocação no VLAN de usuário quando você se junta à rede.

Selecionar submete-se traz acima a lista de mapeamentos atuais do grupo no ACS ao autenticar usuários desconhecidos à base de dados de usuário externo da baliza.

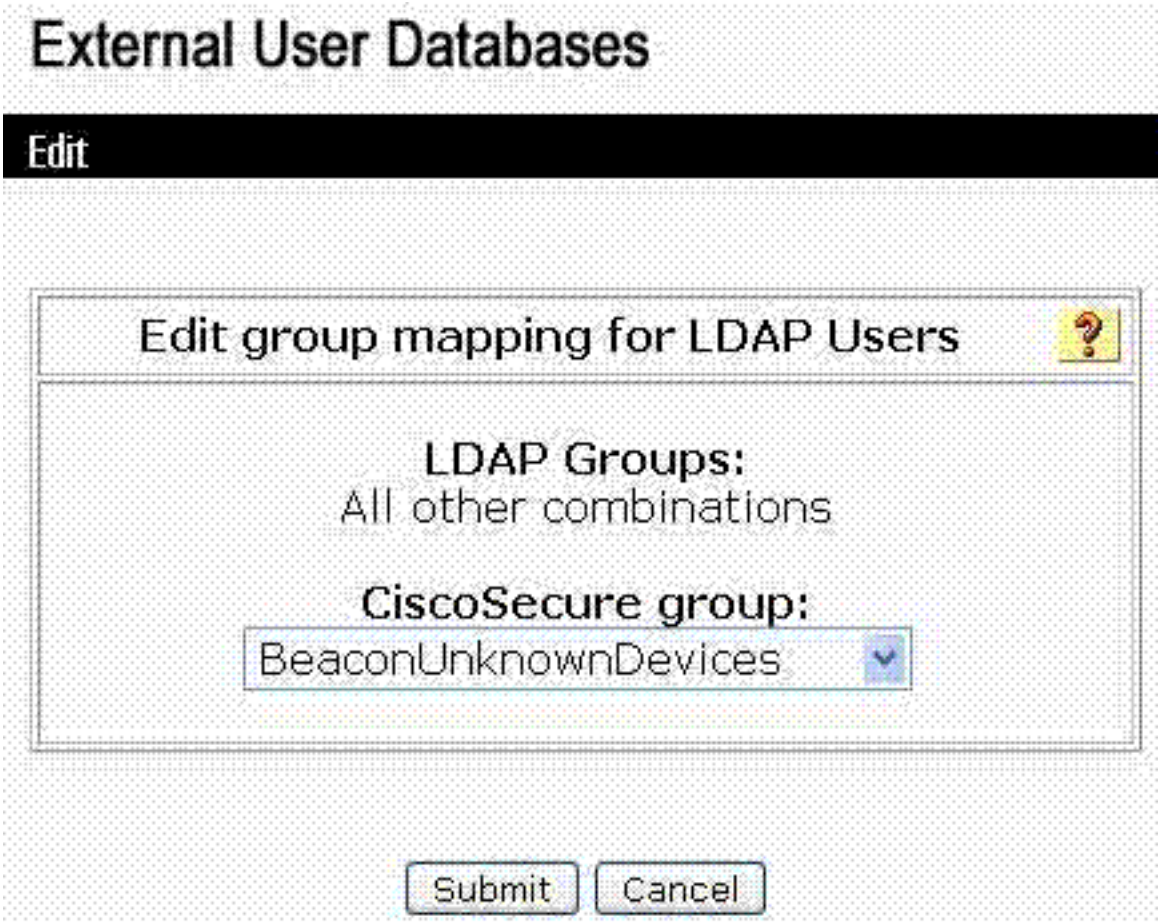
Figura 15: Mapeamentos do grupo da lista



Note que os mapeamentos feitos explicitamente com o procedimento descrito previamente estão alistados nesta vista. Alguns grupos DS (perfis LDAP-permitidos baliza) traçados não explicitamente a um grupo, que inclua os valores-limite que a baliza não descobriu ainda ou colocado em uma queda do perfil de LDAPenabled no todo outro coletor das combinações. Essencialmente isto permite valores-limite que a baliza não pode fornecer a informação sobre em um grupo do CiscoSecure, por exemplo, BeaconUnknownDevices. Como esboçado previamente, este grupo pode ser desabilitado completamente que conduz à falha MAB, ou como no exemplo anterior, pode ser projetado a fim fornecer somente Conectividade limitada aos valores-limite não conhecidos pela baliza.

Todas combinações restantes podem ser atribuídas um grupo do CiscoSecure (BeaconUnkownDevices) se você clica sobre as **todas outras combinações** liga a fim obter este indicador:

Figura 16: Atribuindo um grupo a todas combinações restantes

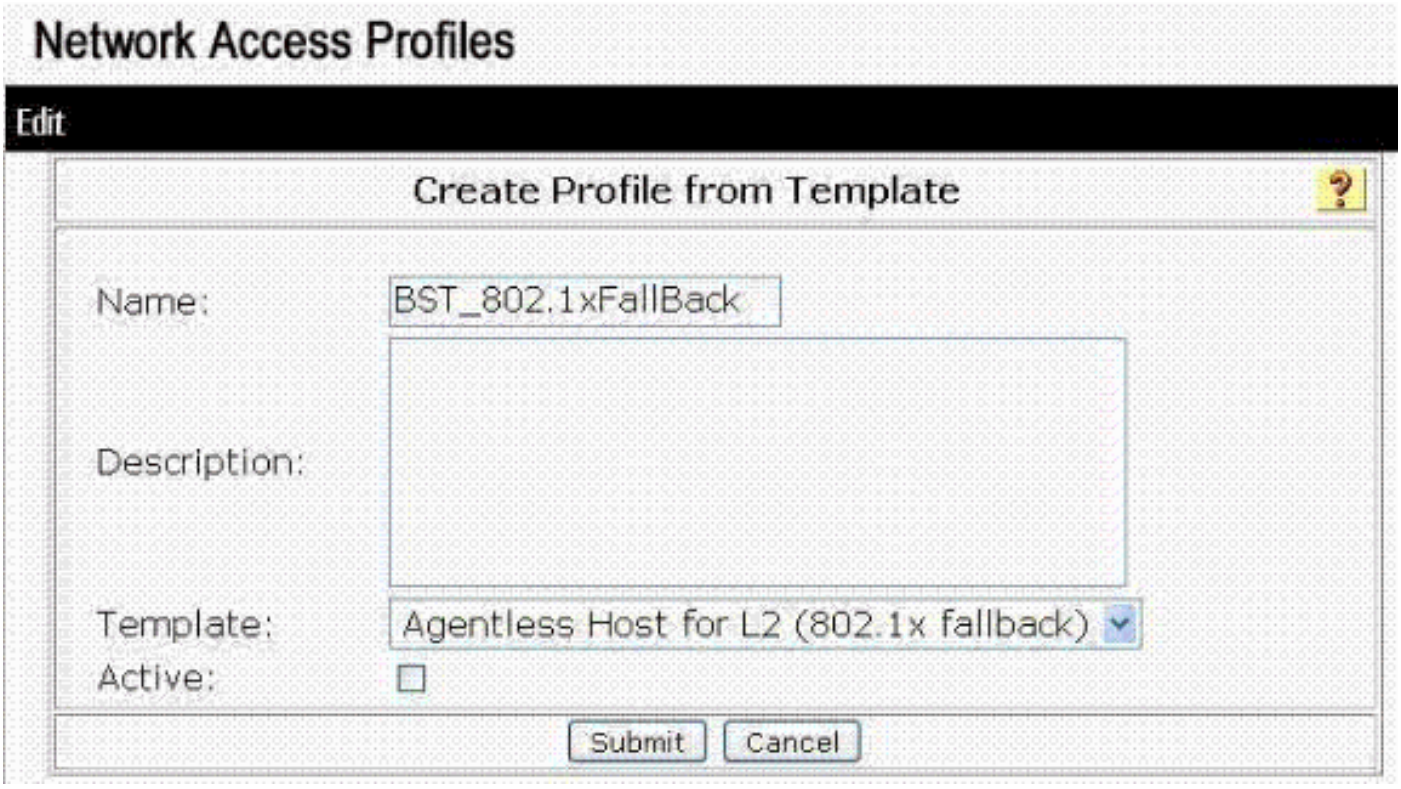


Configuração de perfil do acesso de rede

O último passo requerido na configuração ACS para que o MAB use o sistema do perfilador do valor-limite da baliza como um proxy é a configuração de um perfil do acesso de rede para a reserva do 802.1X. Termine estas etapas esboçadas a fim configurar o perfil do acesso de rede obrigatória para terminar a configuração ACS tais que o MAB está configurado e se opera de acordo com a configuração terminada previamente.

O perfil do acesso de rede a ser adicionado é um perfil do molde. Escolha os **perfis do acesso de rede da** página global da navegação. Escolha então **adicionam o perfil do molde** a fim trazer acima este formulário ilustrado.

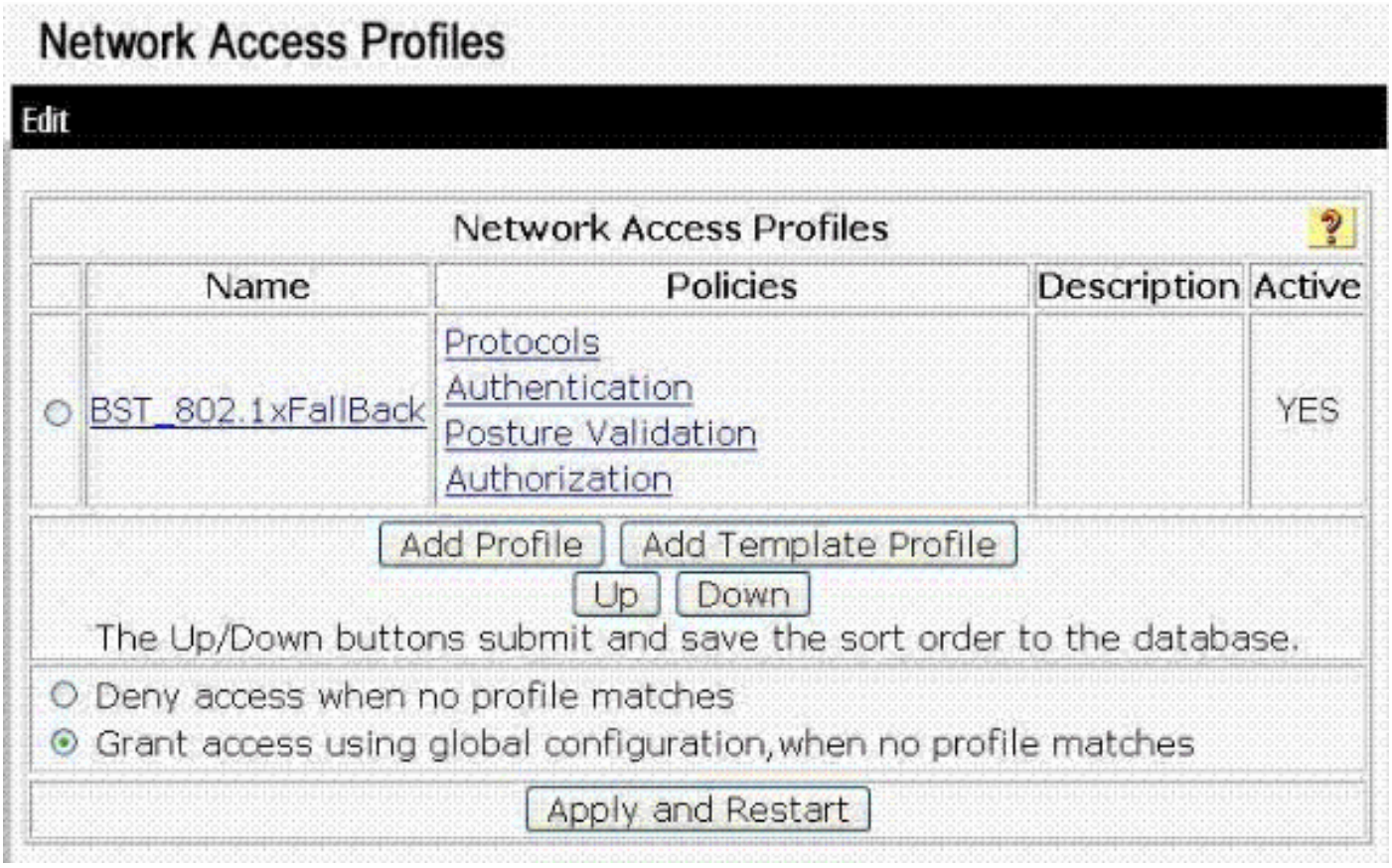
Figura 17: Adicionar um perfil do acesso de rede do molde



Nomeie o perfil do acesso de rede a fim permitir de distingui-lo de outro, e adicionar uma descrição se desejado. O molde para este perfil é selecionado da lista de drop-down. Assegure-se de que o **host Agentless para L2 (reserva do 802.1x)** esteja selecionado, e verifique-se a caixa de seleção **ativa**. Clique o **botão Submit Button** quando terminado a fim salvar o perfil do acesso de rede.

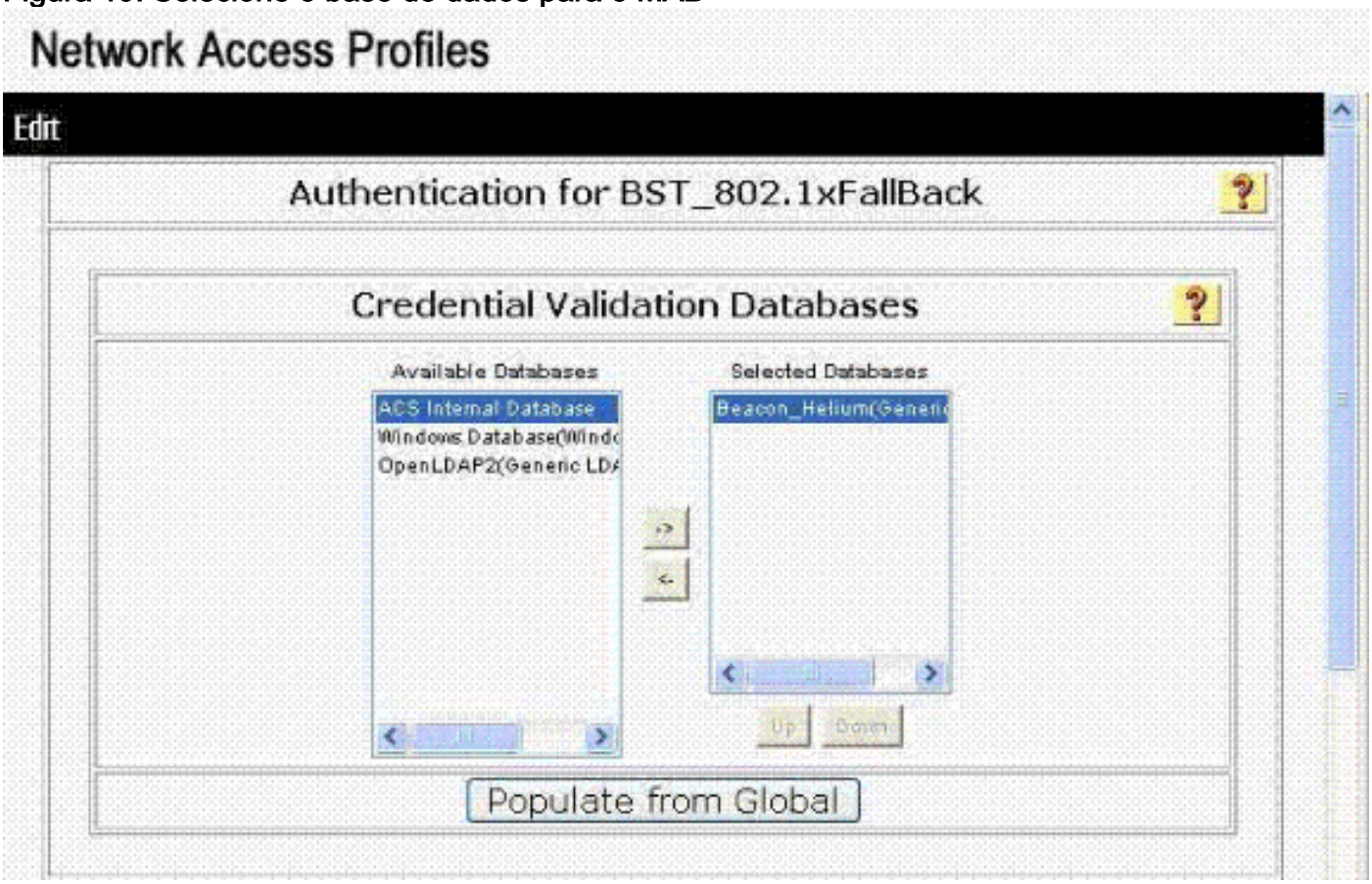
Quando você clique se submete, este formulário está apresentado que permite que você edite os parâmetros para o perfil apenas criado como mostrado.

Figura 18: Edite a SESTA para o MAB



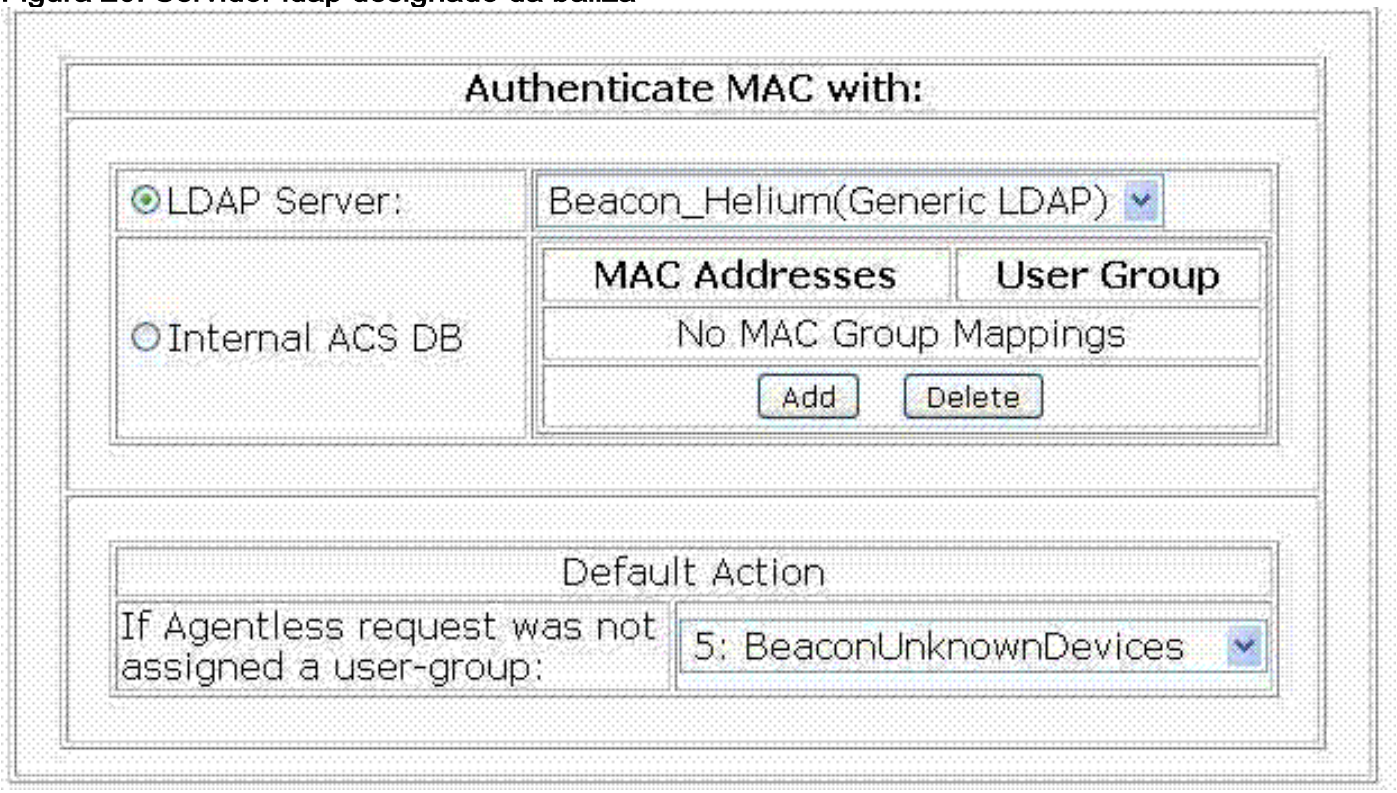
A política de autenticação para o perfil recentemente configurado deve ser configurada a fim utilizar o sistema da baliza como um base de dados credencial da validação. Escolha o link da autenticação na coluna das políticas para o perfil recém-criado do acesso de rede (reserva do 802.1x no exemplo). Estes formulários são apresentados.

Figura 19: Selecione o base de dados para o MAB



Primeiramente, escolha a base de dados de usuário externo da baliza da tabela de bases de dados disponível e use **- >** botão a fim adicionar-lo aos bases de dados selecionado. Enrole para baixo a seção MAC da autenticação do formulário, e escolha o botão de rádio do **servidor ldap**. Escolha o base de dados da **baliza da** lista de drop-down. Ultimamente, escolha o grupo de **BeaconUnknownDevice** para a ação padrão segundo as indicações da figura seguinte.

Figura 20: Servidor ldap designado da baliza



Esta etapa termina a configuração ACS exigida para o desvio da autenticação de MAC com baliza como uma base de dados de usuário externo. Reinicie o serviço ACS a fim assegurar-se de que todas as alterações de configuração estejam comprometidas à configuração running.

O sistema deve estar pronto para testar o MAB, se o Switches é configurado corretamente. Um valor-limite atualmente em um perfil LDAP-permitido da baliza pode ser desligado da rede e ser readmitido com os parâmetros da política especificados para o grupo de BeaconKnownDevices.

Configuração de switch para o desvio da autenticação de MAC

A configuração de switch de Thid fornece um exemplo de configuração para a autenticação do 802.1X o desvio da autenticação de MAC permitido, e o reafectação do VLAN dinâmico exigido a fim aplicar os atributos RADIUS retornados do 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
```

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Informações Relacionadas

- Cisco NAC Appliance (Clean Access)
- Cisco Secure Access Control Server for Windows
- Suporte Técnico e Documentação - Cisco Systems