NAC : Exemple de configuration de l'intégration LDAP avec ACS

Contenu

Introduction

Ce document fournit une configuration d'échantillon des étapes afin de configurer la balise et l'ACS pour activer des périphériques de Cisco configurés pour que le MAB de manière efficace et efficiente authentifie les périphériques capables non-802.1X dans le réseau authentifié.

Cisco a mis en application une caractéristique appelée dérivation d'authentification MAC (MAB) sur leurs Commutateurs aussi bien que le support requis dans ACS afin de faciliter des points finaux dans les réseaux 802.1X-enabled qui ne peuvent pas authentifier par le 802.1X. Cette fonctionnalité s'assure que les points finaux qui tentent la connexion au réseau 802.1X-enabled qui ne sont pas équipés de la fonctionnalité de 802.1X, par exemple, n'ont pas un suppliant fonctionnel de 802.1X, peuvent être authentifiés avant l'admission, aussi bien qu'ont la stratégie d'utilisation de base de réseau imposée dans toute leur connexion.

Le MAB permet au réseau d'être configuré pour admettre les périphériques identifiés avec l'utilisation de leur adresse MAC comme laisser-passer primaire quand le périphérique ne participe pas au protocole de 802.1X. Pour que le MAB soit déployé et utilisé efficacement, l'environnement doit avoir des moyens d'indentify les périphériques dans l'environnement qui ne sont pas capables de l'authentification de 802.1X, et de mettre à jour une base de données à jour de ces périphériques au fil du temps comme se déplace, ajoute et les modifications se produisent. Cette

liste doit être remplie et mise à jour dans le serveur d'authentification (ACS) manuellement, ou par un certain alternatif signifie afin de s'assurer que les périphériques qui authentifient sur le MAC est terminé et valide à tout moment.

Le profileur de point final de balise peut automatiser le processus de l'identification de non-authentifier des points finaux, ceux sans suppliants de 802.1X, et la maintenance de la validité de ces points finaux dans les réseaux de l'échelle variable sur la fonctionnalité de surveillance de profilage et de comportement du point final. Par une interface standard de LDAP, le système de balise peut servir de base de données externe ou de répertoire des points finaux à authentifier par le MAB. Quand une demande de MAB est reçue de l'infrastructure de périphérie, ACS peut questionner le système de balise afin de déterminer si un point final donné devrait être admis au réseau basé sur la plupart des informations en cours sur le point final connu par la balise, afin d'empêcher le besoin de configuration manuelle.

Référez-vous au NAC : Intégration de LDAP avec ACS 5.x et pour en savoir plus d'exemple de configuration plus récente et une configuration semblable utilisant ACS 5.x et plus tard.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco commutent 3750 qui exécute 12.2(25)SEE2
- Cisco Secure Access Control Server pour Windows 4.1

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

Le MAB est une fonctionnalité essentielle pour le support dynamique des périphériques tels que des imprimantes, des Téléphones IP, des télécopieurs et d'autres périphériques capables non-802.1X dans le déploiement de l'environnement post-802.1X. Sans capacité de MAB, des ports d'accès au réseau qui fournissent Connectivité aux points finaux capables non-802.1X doivent provisioned statiquement afin de ne pas tenter l'authentification de 802.1X ou par l'utilisation d'autres caractéristiques qui fournissent des options très limitées de stratégie. Pour des raisons évidentes, ce n'est pas en soi extensible à de grands environnements d'entreprise. Le MAB étant

activé en même temps que le 802.1X sur tous les ports d'accès, des points finaux capables connus non-802.1X peuvent être déplacés n'importe où l'environnement et sûrement (et sécurisé) connectez toujours au réseau. Puisque les périphériques admis au réseau sont authentifiés, différentes stratégies peuvent être appliquées aux différents périphériques

En outre, les points finaux capables non-802.1X qui ne sont pas connus dans l'environnement, tel que les ordinateurs portables qui appartiennent aux visiteurs ou aux sous-traitants, peuvent être accès restreint fourni au réseau par le MAB si désirés.

Pendant que le nom suggère, la dérivation d'authentification MAC utilise l'adresse MAC du point final comme laisser-passer primaire. La dérivation d'authentification MAC étant activé sur un port d'accès, si un point final se connecte et ne relève pas le défi d'authentification de 802.1X, le port retourne au mode de MAB. Le commutateur qui tente le MAB d'un point final fait une demande RADIUS standard à ACS avec le MAC de la station. Il tente de se connecter au réseau et demande l'authentification du point final d'ACS avant l'admission du point final au réseau.

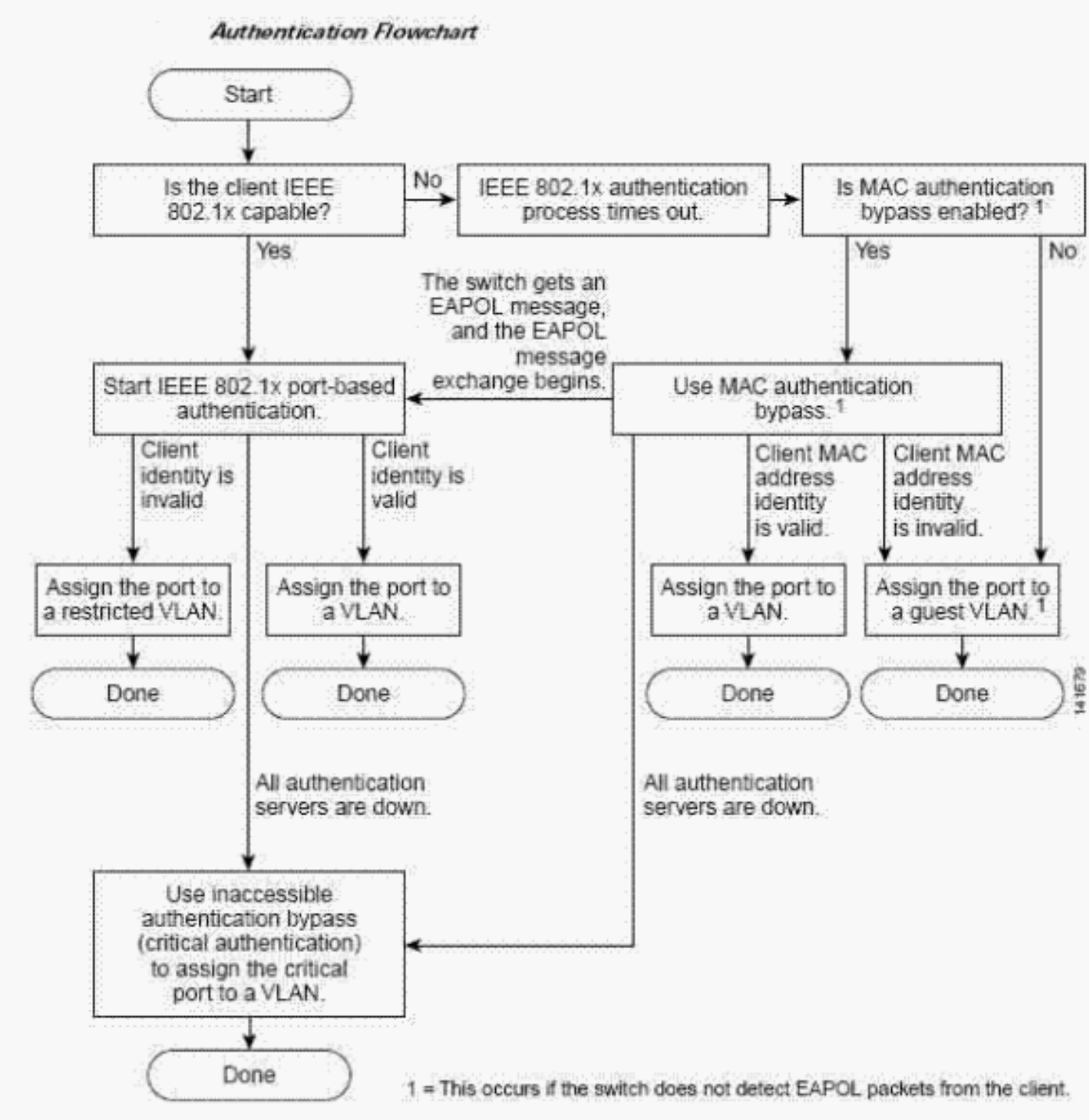
Configuration

Diagramme d'organigramme

Cet organigramme pris de la documentation de Cisco Systems montre comment le MAB est utilisé en même temps que l'authentification de 802.1X sur l'infrastructure de périphérie de Cisco pendant que nouvelle tentative de points finaux de se connecter au réseau.

Ce document utilise ce flux des tâches d'organigramme :

Figure 1 : Écoulement d'authentification



ACS peut être configuré pour utiliser sa propre base de données interne ou un serveur LDAP externe afin d'authentifier des demandes d'utilisateur d'adresse MAC. Le système de profileur de point final de balise LDAP-est entièrement activé par défaut et peut être utilisé par ACS afin d'authentifier des demandes d'utilisateur d'adresse MAC par la fonctionnalité standard de LDAP. Puisque la balise automatise la détection aussi bien que le profilage de tous les points finaux sur le réseau, ACS peut questionner la balise par le LDAP afin de déterminer si le MAC est admis au réseau, et dans quel groupe le point final devrait être tracé. Ceci de manière significative automatise et améliore la caractéristique de dérivation d'authentification MAC, en particulier dans de grands environnements d'entreprise.

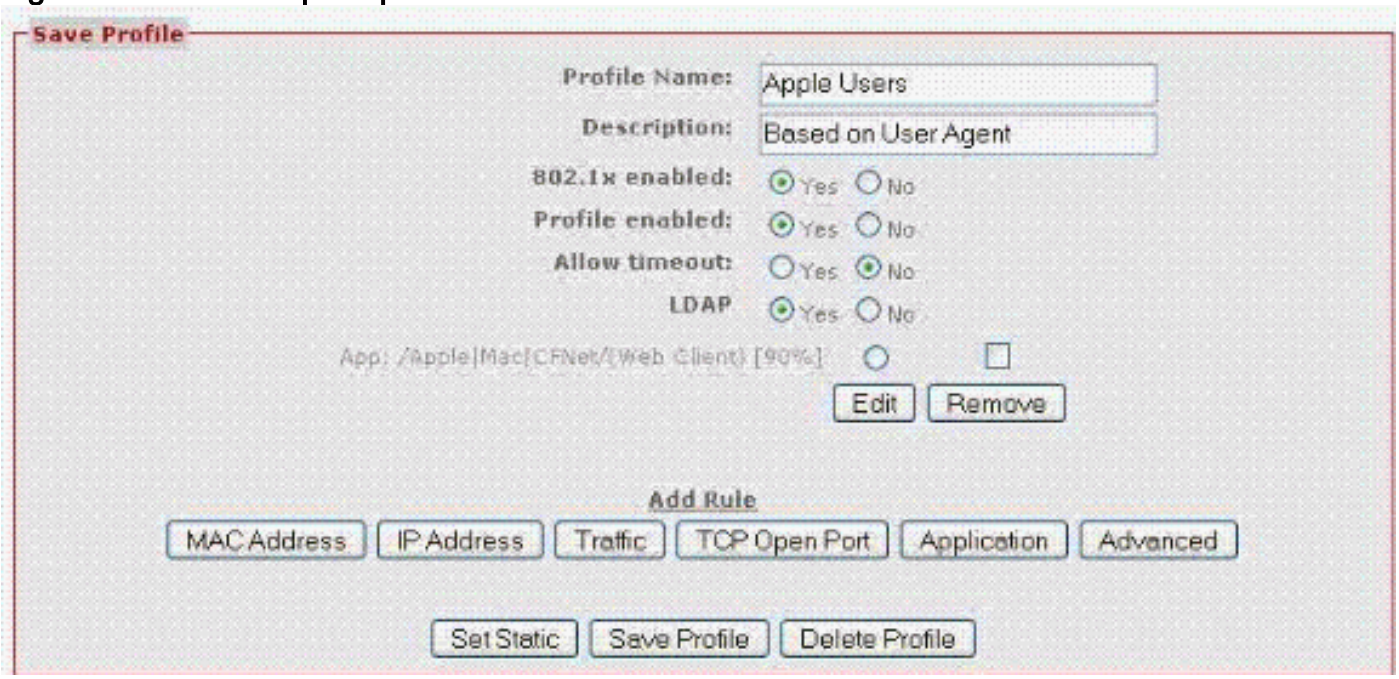
Par la fonctionnalité comportementale de surveillance fournie par la balise, des périphériques qui sont observés pour se comporter inconséquemment avec les profils activés pour le MAB transitioned sur 4 profils LDAP-activés et échouer ultérieurement la prochaine tentative régulière de ré-authentification.

Configuration système de profileur de point final de balise pour le MAB

La configuration du système de balise pour l'intégration avec ACS aux fins de support de MAB est simple car la fonctionnalité de LDAP est activée par défaut. La tâche primaire de configuration est d'identifier les profils qui contiennent les points finaux qui sont désirés pour être authentifiés par le MAB dans l'environnement, et activer alors ces profils pour le LDAP. Typiquement, les profils de balise, qui contiennent des périphériques ont possédé par l'organisation, devraient être accès au réseau fourni une fois vus sur un port pourtant sont connus pour ne pouvoir pas authentifier par le 802.1X. Typiquement ce sont des profils qui contiennent des imprimantes, des Téléphones IP ou des UPS maniables comme exemples classiques.

Si des imprimantes profilées par la balise étaient placées dans un profil nommé *Printers*, et les Téléphones IP dans un profil nommaient des *Téléphones IP*, par exemple, alors le besoin de ces profils d'être activé pour le LDAP tels que les points finaux placés dans ces profils ont comme conséquence l'authentification réussie en tant que le téléphone IP et imprimantes connus dans l'environnement par le MAB. Si vous activez un profil pour le LDAP, ceci exige que la case d'option de LDAP dans la configuration de profil de point final soit sélectionnée, suivant les indications de cet exemple :

Figure 2 : Activez un profil pour le LDAP



Quand l'authentification MAC de proxys ACS à baliser par le LDAP, la requête se compose de deux sous requêtes, qui doivent renvoyer un résultat valide et non nul. La première requête à baliser est si le MAC est connu pour baliser, par exemple, s'il a été découvert et ajouté à la base de données de balise. Si le point final a pour être découvert encore par la balise, le point final est considéré inconnu. La deuxième requête n'est pas nécessaire dans le cas des points finaux que la balise n'a pas découverts et n'est pas dans sa base de données. Si le point final a été découvert et est dans la base de données de balise, la prochaine requête est de déterminer le profil en cours du point final. Si un point final a pour être profilé encore ou est actuellement dans un profil non 5 activés pour le LDAP, le résultat inconnu est retourné à ACS, et l'authentification du point final par la balise échoue. Il dépend de la façon dont ACS est configuré que ceci peut avoir comme conséquence le périphérique avec le refus de l'accès au réseau totalement, ou soit donné une stratégie qui est appropriée pour des périphériques d'inconnu ou d'invité.

Seulement dans le cas où le MAC est un point final que la balise a découvert et placé dans un

profil LDAP-activé, la réponse est que le point final est connu et profilé par la balise soyez retourné à ACS. Avant tout, parce que balise de ces points finaux fournit le nom de profil en cours, qui permet à ACS de tracer des points finaux connus aux groupes de Cisco SecureAccess. Ceci active une détermination granulaire de stratégie faite, aussi granulaire qu'une stratégie distincte pour chaque profil LDAP-activé par balise, si désiré.

Configuration ACS pour le MAB et utilisation de balise comme base de données d'utilisateur externe

La configuration d'ACS pour le MAB et de l'utilisation de la balise comme base de données d'utilisateur externe exige trois étapes distinctes. La commande illustrée dans ce document suit un processus qui est efficace quand il exécute la configuration de MAB en sa totalité, et peut varier pour les systèmes qui ont été en fonction avec d'autres authentications mode déjà configurées.

Configurez Cisco SecureGroup

Quand vous tentez le MAB pour un point final particulier qui tente de se connecter au réseau, les requêtes ACS balisent sur le LDAP afin de déterminer si la balise a découvert le MAC, et le quel balise de profil a actuellement placé l'adresse MAC dedans comme décrit plus tôt dans le document.

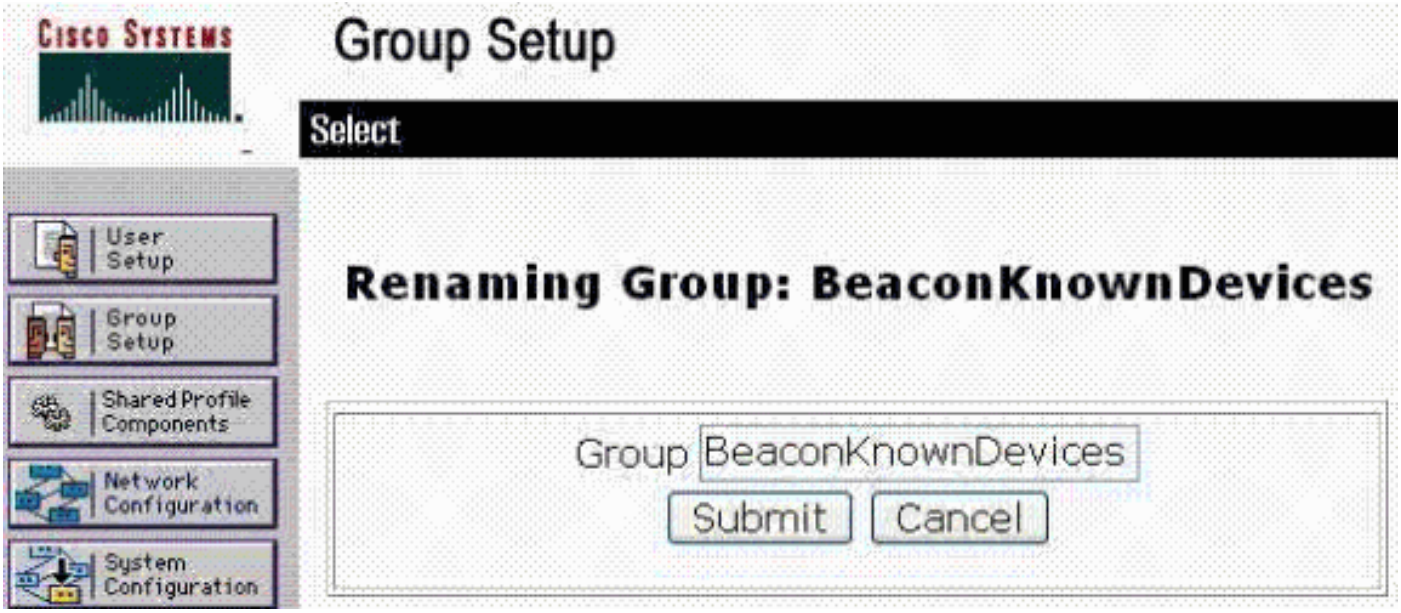
Le mécanisme de Cisco SecureGroup avec ACS peut être utilisé à authentifient et s'appliquent la stratégie aux points finaux qui ont été découverts et profilés par la balise par le MAB, aussi bien qu'aux échecs d'authentification — ces périphériques non connus ou pas actuellement profilés par la balise.

Par exemple, un groupe peut être ajouté à une configuration ACS pour des points finaux découverts et profilés par la balise et le *BeaconKnownDevices* appelé, et à un groupe différent *BeaconUnknownDevices* ajouté pour les périphériques qui ne sont pas actuellement connus par la balise. La balise n'a pas découvert le MAC, ou ne l'a pas actuellement profilé dans un profil LDAP-activé. Comme affiché plus tard dans ce document, l'enable de groupes l'application de la stratégie aux points finaux comme ils tentent de joindre le réseau.

Notez que dans l'exemple tracé les grandes lignes dans ce document, seulement deux groupes, BeaconKnown et BeaconUnknown sont configurés. Mais il est possible de créer plusieurs SecureGroups pour des points finaux découverts et profilés par la balise, autant de car une pour chaque profil LDAP-activé dans la balise, chacun avec différents paramètres de stratégie tels que l'affectation VLAN. En outre, le groupe de périphériques de BeaconUnkown peut être configuré pour refuser tout l'accès aux points finaux qui ont encore pour être découverts ou placés dans un profil activé pour le LDAP par la balise 6. Ce fait si vous choisissez la case à cocher désactivée par groupe dans les paramètres de la fenêtre de configuration de groupe de BeaconUnknownDevices.

La création de groupe sur ACS est initiée du bouton de Group Setup dans l'interface utilisateur ACS. Choisissez un des groupes disponibles, et puis choisissez le bouton de **groupe de renommer** afin de changer le nom de groupe à KnownBeaconDevices suivant les indications de cet exemple. Cliquez sur Submit afin de sauvegarder la modification.

Figure 3 : Éditez le groupe de CiscoSecure

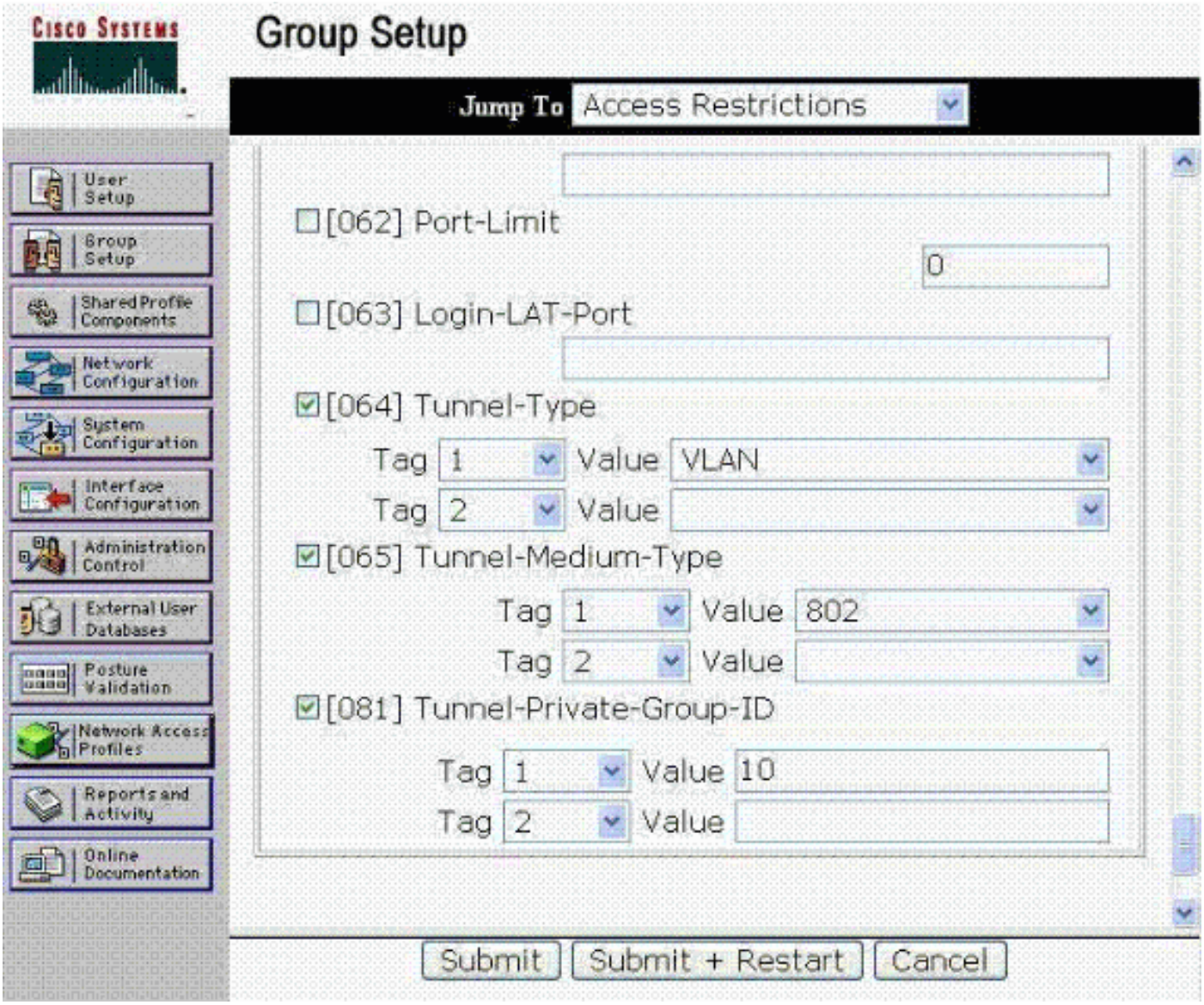


Choisissez **éditent des configurations** afin d'éditer les configurations du groupe. Éditez les paramètres du groupe de BeaconKnownDevices comme désirés. Aux fins de l'exemple dans ce document, les paramètres de groupe qui sont changés incluent seulement les attributs RADIUS IETF, fondent au bas de page.

Spécifiquement vous indiquez que les périphériques authentifiés à ce groupe, les adresses MAC que la balise a profilées aux profils sélectionnés pour le MAB et activés pour le LDAP, ont des paramètres de stratégie retournés au commutateur authentifiant cette admission d'enables des points finaux au réseau sur le VLAN approprié. Afin de faire ceci, le Tunnel-Support-type 064, 065 le Tunnel-type d'attributs RADIUS, et le Tunnel-Private-Group-ID 081 sont placés pour avoir comme conséquence les points finaux étant placés sur le VLAN désiré, suivant les indications de la figure 4.

Assurez-vous que les cases à cocher à côté de chaque attribut RADIUS est vérifiées.

Figure 4 : Attributs du groupe VLAN

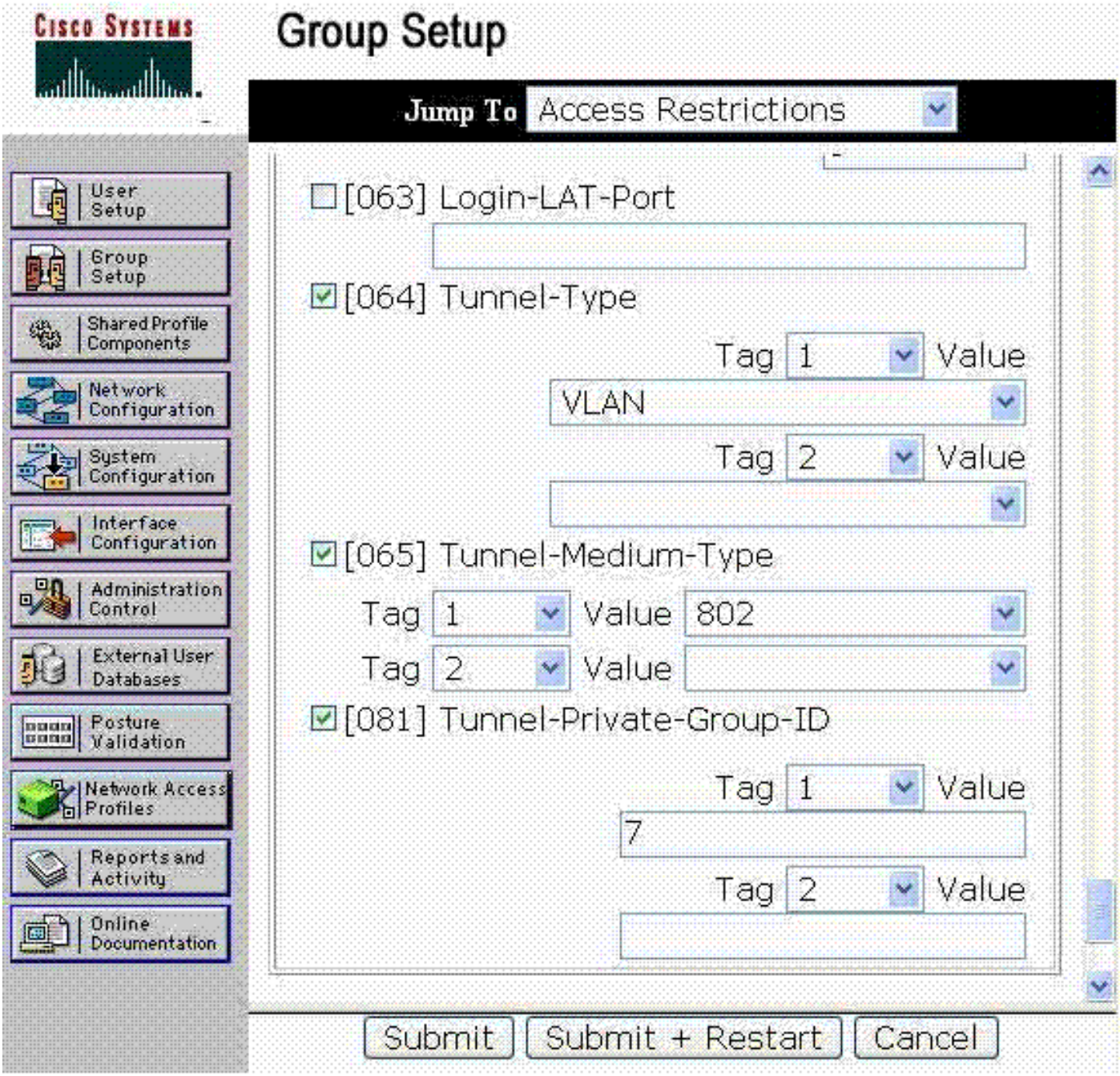


Dans l'exemple présenté, des points finaux authentifiés avec succès par la balise et ultérieurement assignés au groupe ACS BeaconKnownDevices sont placés sur le VLAN 10, le VLAN autorisé dans la configuration réseau de réseau d'exemple, pendant la connexion au réseau et avec succès authentifiés sur le MAB par ACS avec l'utilisation de la balise comme base de données d'utilisateur externe.

De même le groupe de BeaconUnknownDevices est créé pour les périphériques qui ne sont pas actuellement connus par la balise comme affichés. De nouveau, si ces périphériques n'obtiennent aucun accès au réseau, vérifiez simplement la case à cocher **désactivée par groupe** en haut de la forme. Points finaux qui n'ont pas été découverts par la balise ou ne sont pas actuellement profilés par la balise dans un MAB LDAP-activé d'échouer de profil et ne sont pas admis au réseau.

Cette figure affiche l'alternative que l'utilisation de la case à cocher désactivée par groupe. Dans ce cas, des points finaux qui ne peuvent pas être authentifiés par la balise sont assignés à un groupe qui est activé, mais ont une stratégie différente que cela pour les points finaux qui sont connus. Référez-vous à la figure 5.

Figure 5 : Paramètres VLAN pour BeaconUnknownDevices



Notez que pour les périphériques inconnus dans cet exemple, ils sont admis au réseau mais sont relégués à un invité ou à un VLAN restreint, VLAN 7. Dans le réseau d'exemple, VLAN 7 est l'invité VLAN, qui permet l'accès Internet de points finaux seulement, et interdit l'accès aux ressources internes.

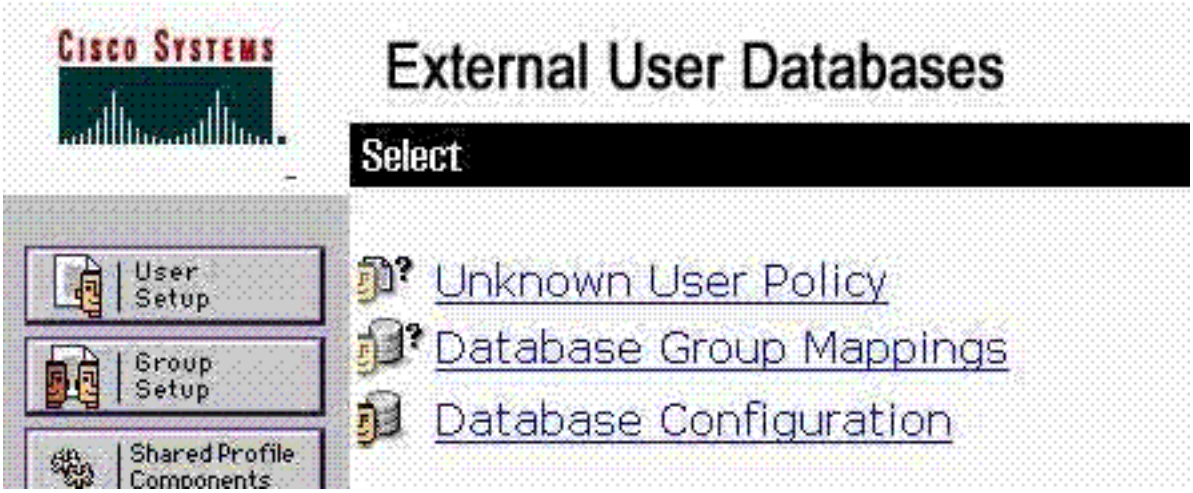
Quand ACS demande l'authentification de la balise d'un MAC d'un point final qui a encore pour être découvert ou profilé par la balise, ACS place le MAC dans ce groupe et renvoie le résultat au commutateur authentifiant activé pour le MAB.

Configuration de base de données d'utilisateur externe ACS

ACS doit être configuré aux demandes de MAB de proxy des commutateurs d'accès de baliser par l'intermédiaire du LDAP. Ceci exige que la configuration ACS inclut le système de balise comme base de données d'utilisateur externe générique de LDAP. Les étapes tracées les grandes lignes dans cette section illustrent comment ajouter le système de profileur de point final de 9 balises comme base de données d'utilisateur externe à questionner par ACS quand elle reçoit des demandes de MAB. Choisissez la **base de données d'utilisateur externe** sur le volet global de

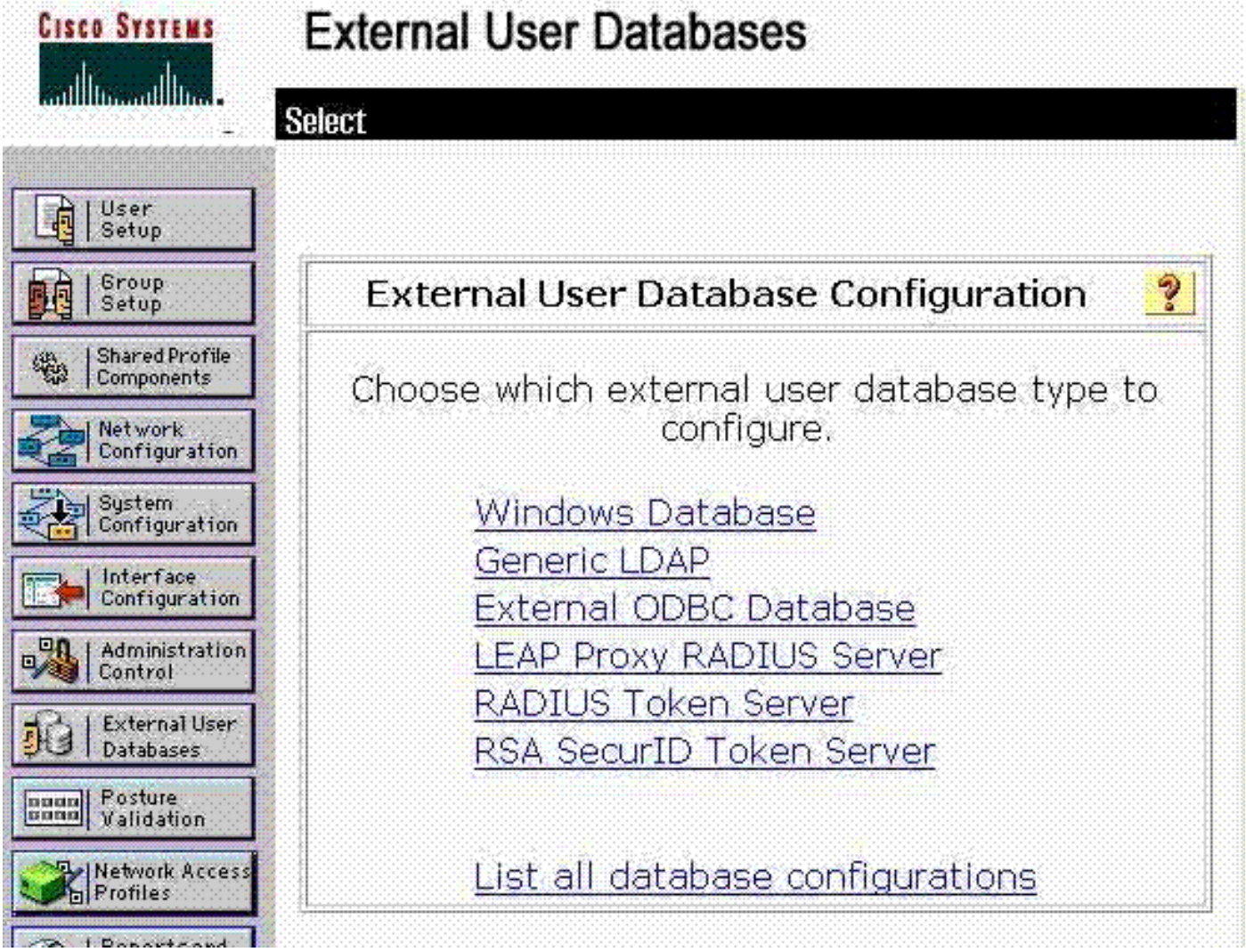
navigation afin d'apporter la fenêtre de base de données d'utilisateur externe illustrée dans la figure 6.

Figure 6 : Écran principal externe de configuration de DB



La première tâche dans la configuration de la balise comme base de données d'utilisateur externe est d'ajouter le système de balise comme base de données d'utilisateur externe générique de LDAP. Choisissez la **configuration de base de données** afin de la fenêtre illustrée dans la figure 7 apparaissent.

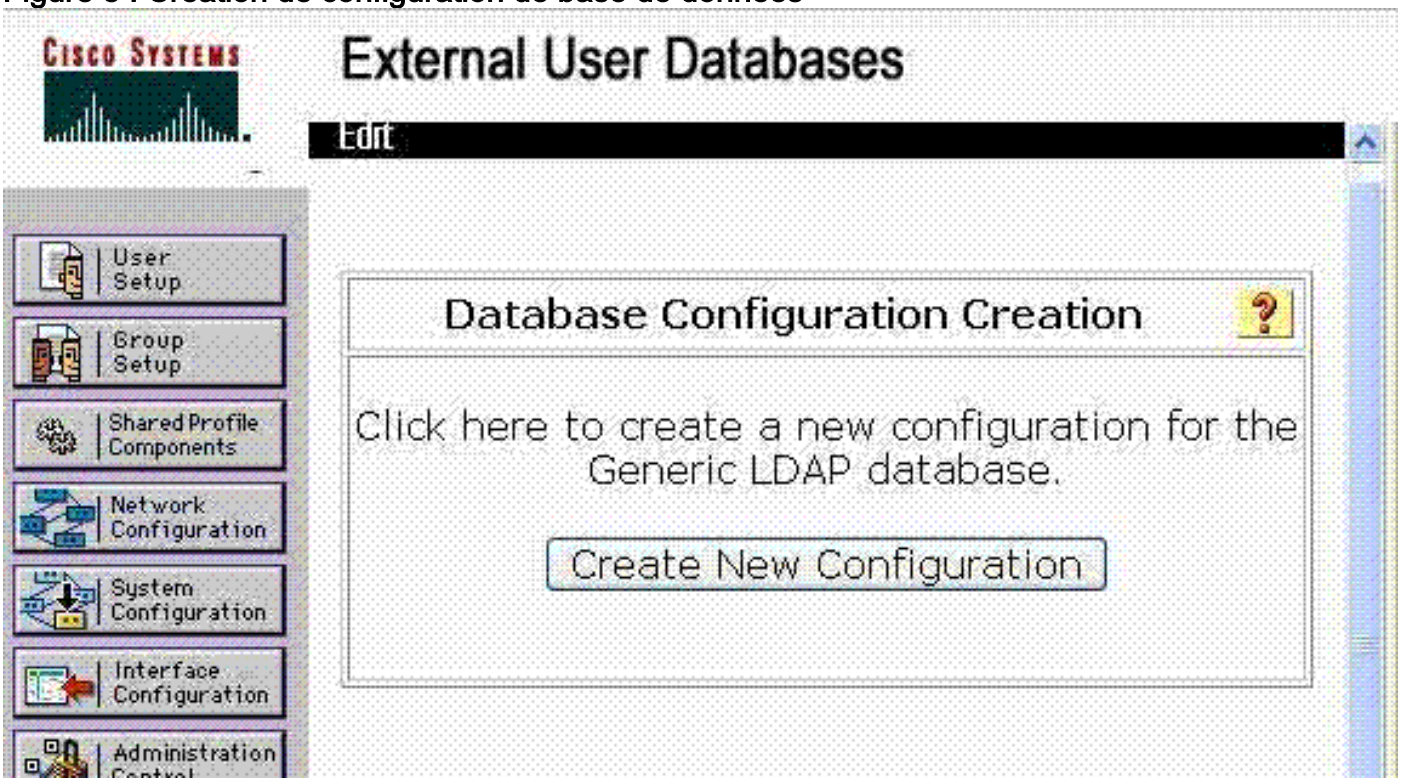
Figure 7 : Configuration de base de données d'utilisateur externe ACS



Choisissez le **LDAP générique** afin d'ouvrir la forme utilisée pour ajouter le système de profileur de

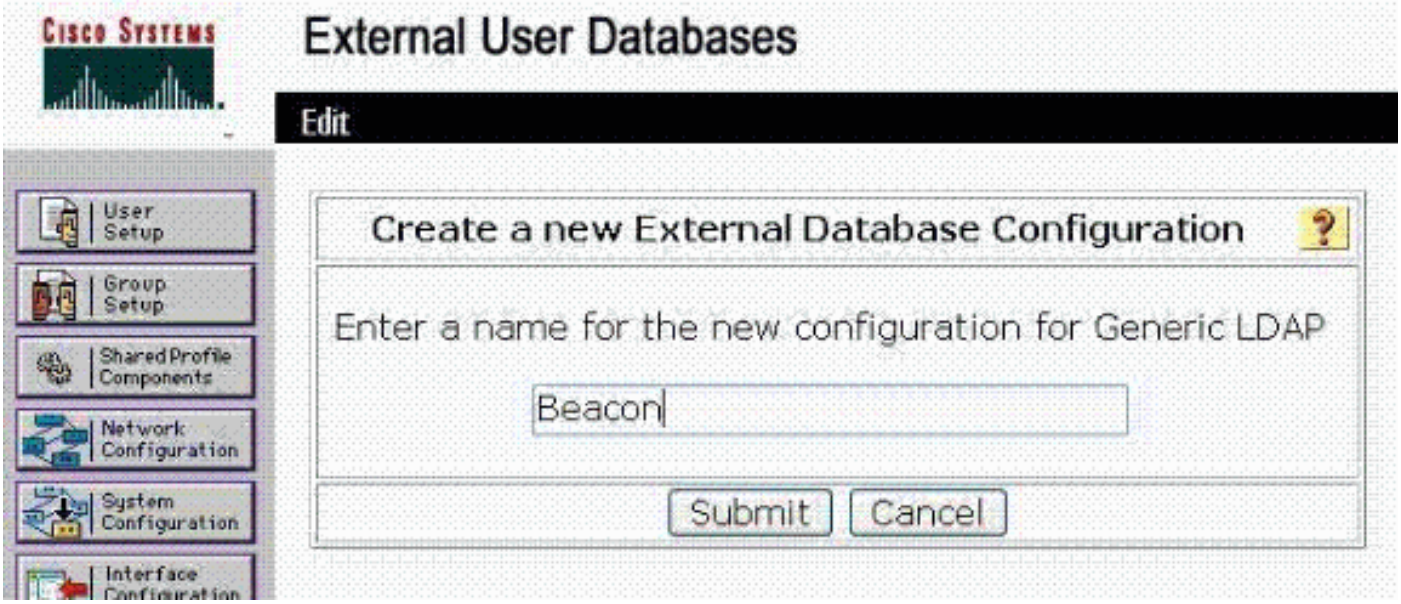
point final de balise comme DB d'utilisateur externe dans la configuration ACS. Cette fenêtre semble activer la création d'une nouvelle configuration de base de données d'utilisateur externe du LDAP générique de type.

Figure 8 : Création de configuration de base de données



Choisissez le **nouveau bouton configuration de création** afin de créer la base de données générique de LDAP pour la balise. Cette fenêtre apparaît et permet la nouvelle base de données externe à nommer.

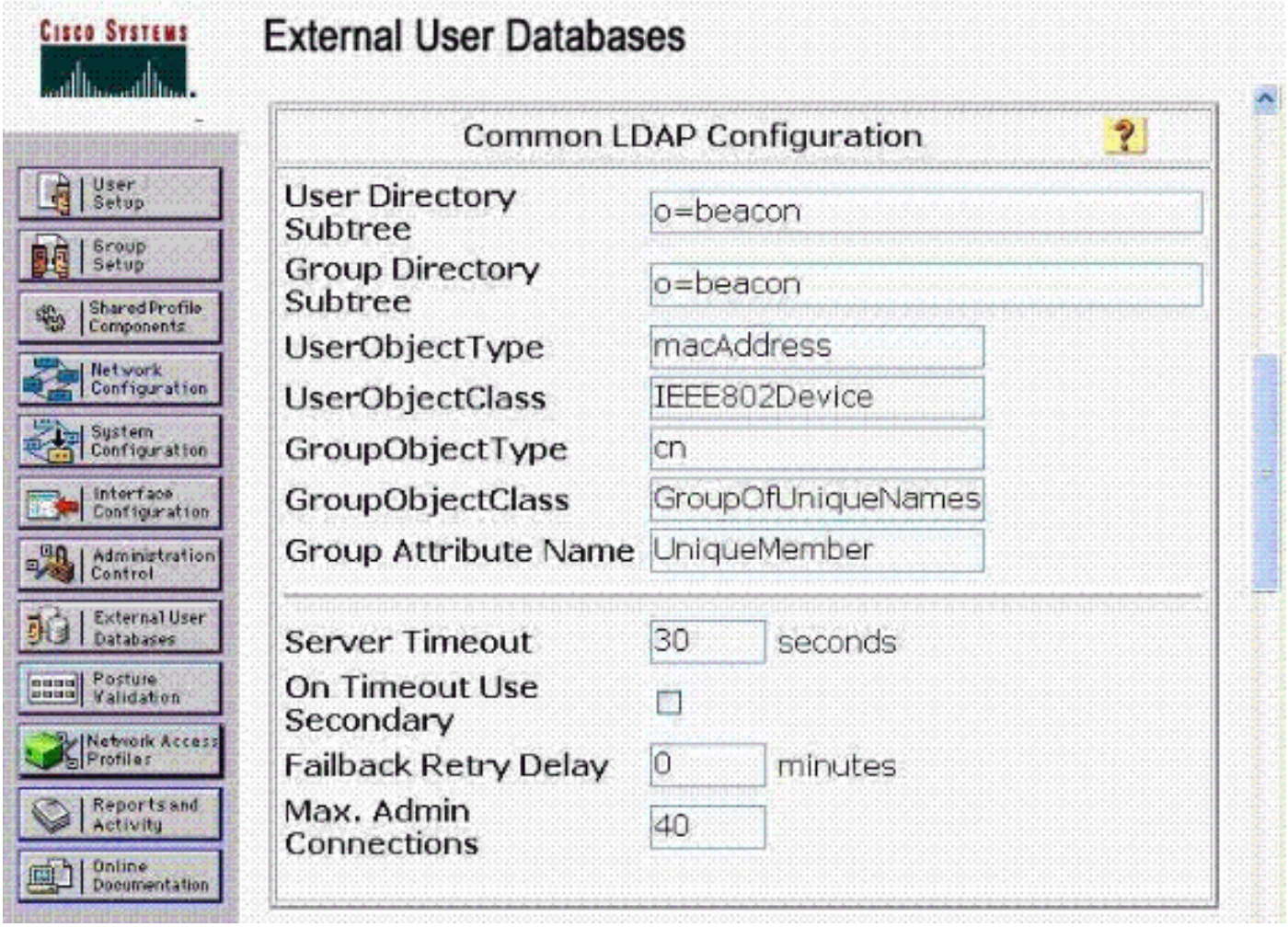
Figure 9 : Base de données d'utilisateur externe de balise de nom



Écrivez un nom pour la base de données externe générique de LDAP de balise qui le permet à différencier facilement d'autres bases de données externes dans la configuration. Choisissez **soumettent** afin de passer à l'entrée des paramètres requis de LDAP qui activent la transmission entre 11 ACS et balisent afin de l'authentification des adresses MAC avec l'utilisation des informations de base de données de balise.

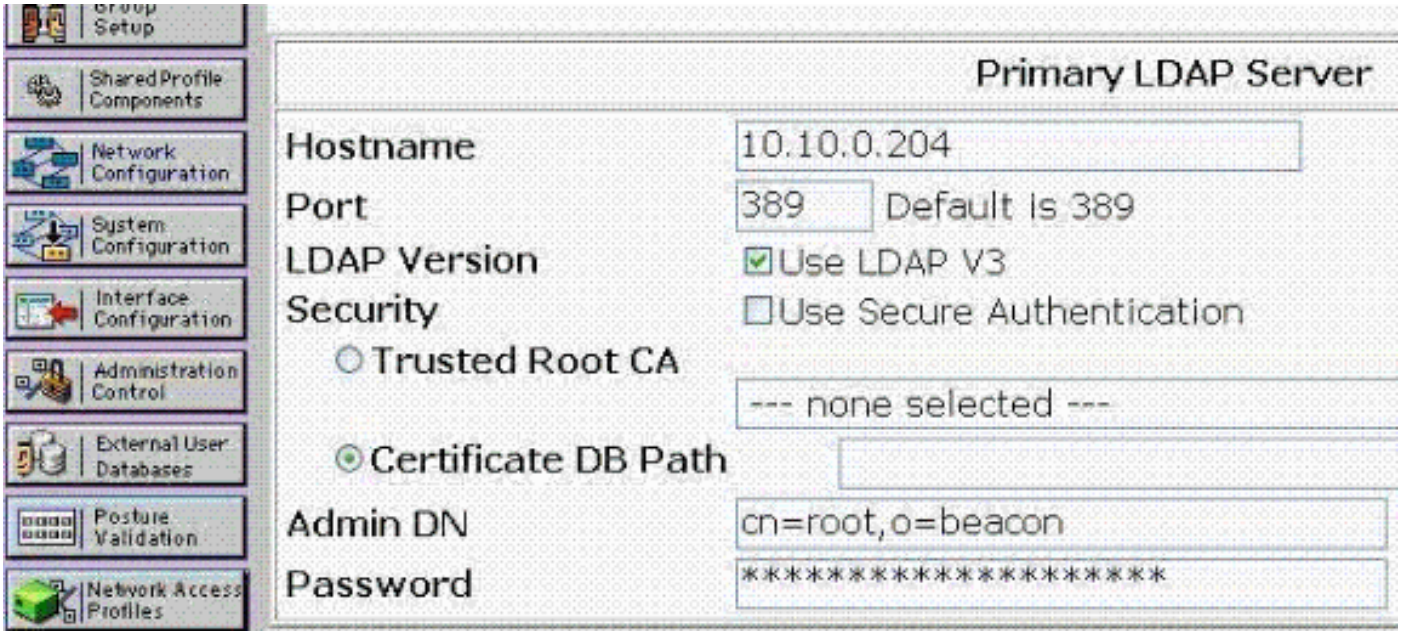
La figure 10 montre les paramètres de configuration communs de LDAP qui doivent être entrés pour la base de données d'utilisateur externe générique de LDAP de balise qui est ajoutée à la configuration ACS. Notez que ces paramètres fournissent à ACS les informations qu'il exige afin de questionner la balise par le LDAP. Ces paramètres devraient être entrés exactement suivant les indications de cette figure afin de faciliter la transmission entre ACS et le profileur de point final de balise.

Figure 10 : Configuration commune de LDAP pour la balise



Remarque: Utilisez le mot de passe **GBSbeacon** pour le mot de passe de grippage de LDAP. Le mot de passe est entré en bas de la forme affichée dans la figure 11.

Figure 11 : Paramètres de serveur de balise

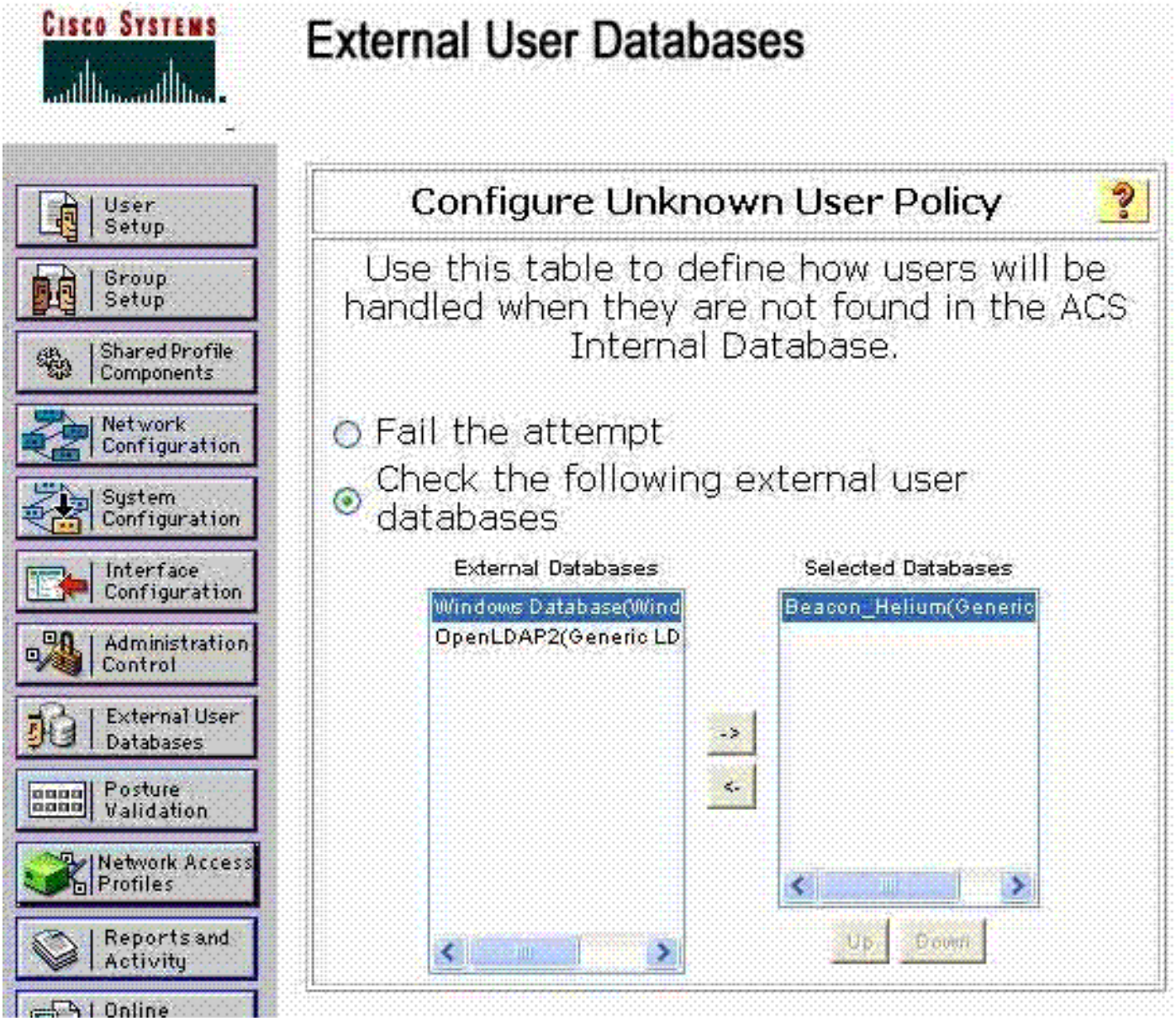


La deuxième tâche associée de configuration avec la configuration de la balise comme base de données d'utilisateur externe est la configuration de la stratégie inconnue d'utilisateur. La stratégie inconnue d'utilisateur dirige ACS pour questionner la base de données de balise toutes les fois qu'elle reçoit une demande d'authentification pour un utilisateur, qui est une adresse MAC dans le cas de MAB, qu'il n'a pas les informations pour dans sa propre base de données.

Notez que dans un déploiement typique ACS, il peut y avoir les bases de données d'utilisateur externe existantes configurées et peut déjà être configuré pour questionner bases de données quand des identifiants utilisateurs inconnus sont soumis. La base de données d'utilisateur externe de balise doit être ajoutée à la liste afin de la questionner quand les Commutateurs demandent le MAB de différentes adresses MAC.

Ces figures tracent les grandes lignes du processus pour la configuration de la stratégie inconnue d'utilisateur, et de l'ajout de la balise comme une base de données d'utilisateur externe à questionner. À, choisissez le lien **inconnu de stratégie d'utilisateur à la** page principale de base de données d'utilisateur externe comme illustrée dans la figure 6 afin de commencer le processus.

Figure 12 : Configurez la stratégie inconnue d'utilisateur

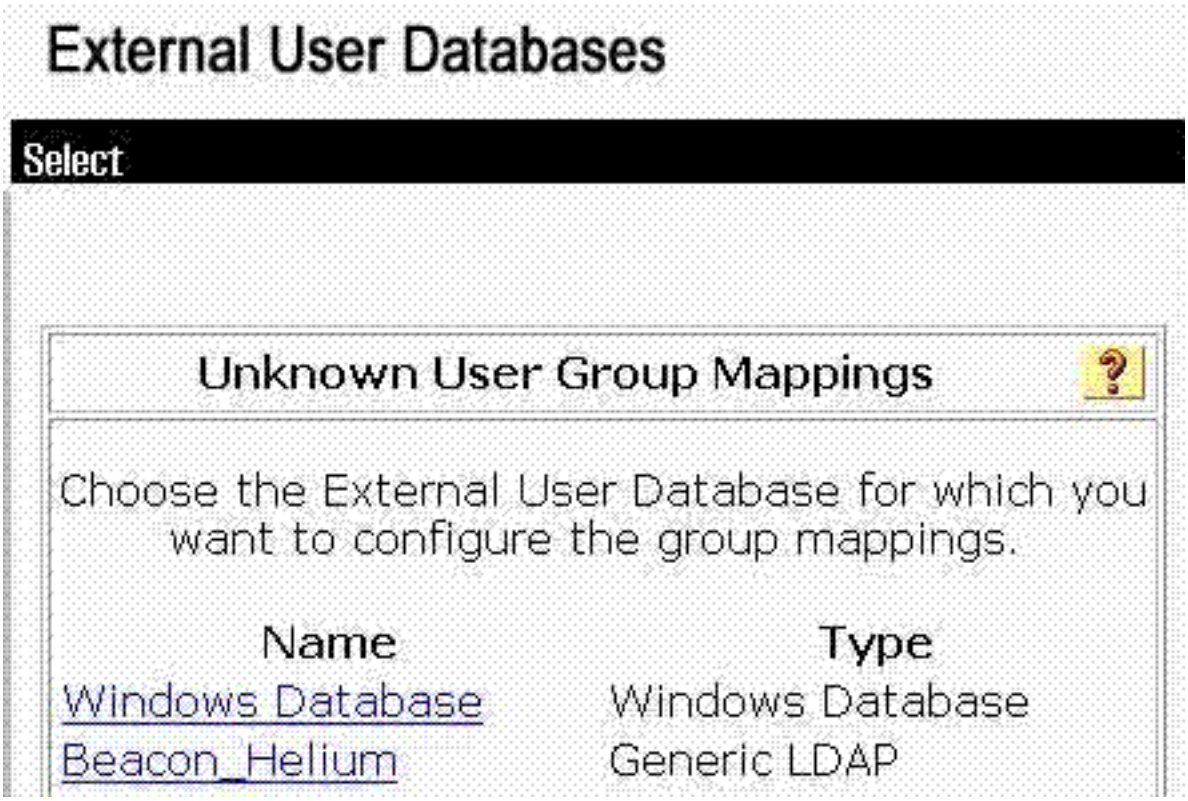


Choisissez la base de données générique de LDAP de balise ajoutée à la configuration ACS dans la dernière étape de la liste de bases de données externes vers le gauche (Beacon_Helium) dans l'exemple. Utilisation **- >** afin de se déplacer aux bases de données sélectionnées. Veillez-vous pour choisir le **contrôle la** case d'option **suivante de bases de données d'utilisateur externe**. Ceci s'assure que quand les Commutateurs soumettent des adresses MAC pour l'authentification à ACS, les requêtes ACS balisent afin de déterminer si le point final est connu et il a le profil en cours éventuel.

La tâche de configuration finale d'ajouter la balise comme base de données d'utilisateur externe est la fin des mappages de groupe de base de données. Essentiellement ce mappage attache ensemble les groupes de CiscoSecure créés, par exemple, BeaconKnownDevices et BeaconUnknownDevices, aux requêtes réussies et infructueuses de LDAP faites pour baliser de sorte que chaque MAB tenté par les Commutateurs ait comme conséquence l'attribution du point final à un groupe de CiscoSecure par ACS. Ceci permet à ACS de répondre au commutateur si le point final devrait être admis au réseau, et si admis, ce qui la stratégie telle que le VLAN l'attribue devrait être.

Choisissez les **tracés de groupe de base de données à la** page principale de bases de données d'utilisateur externe suivant les indications de la figure 6 afin de configurer les tracés.

Figure 13 : Mappages de groupe de base de données

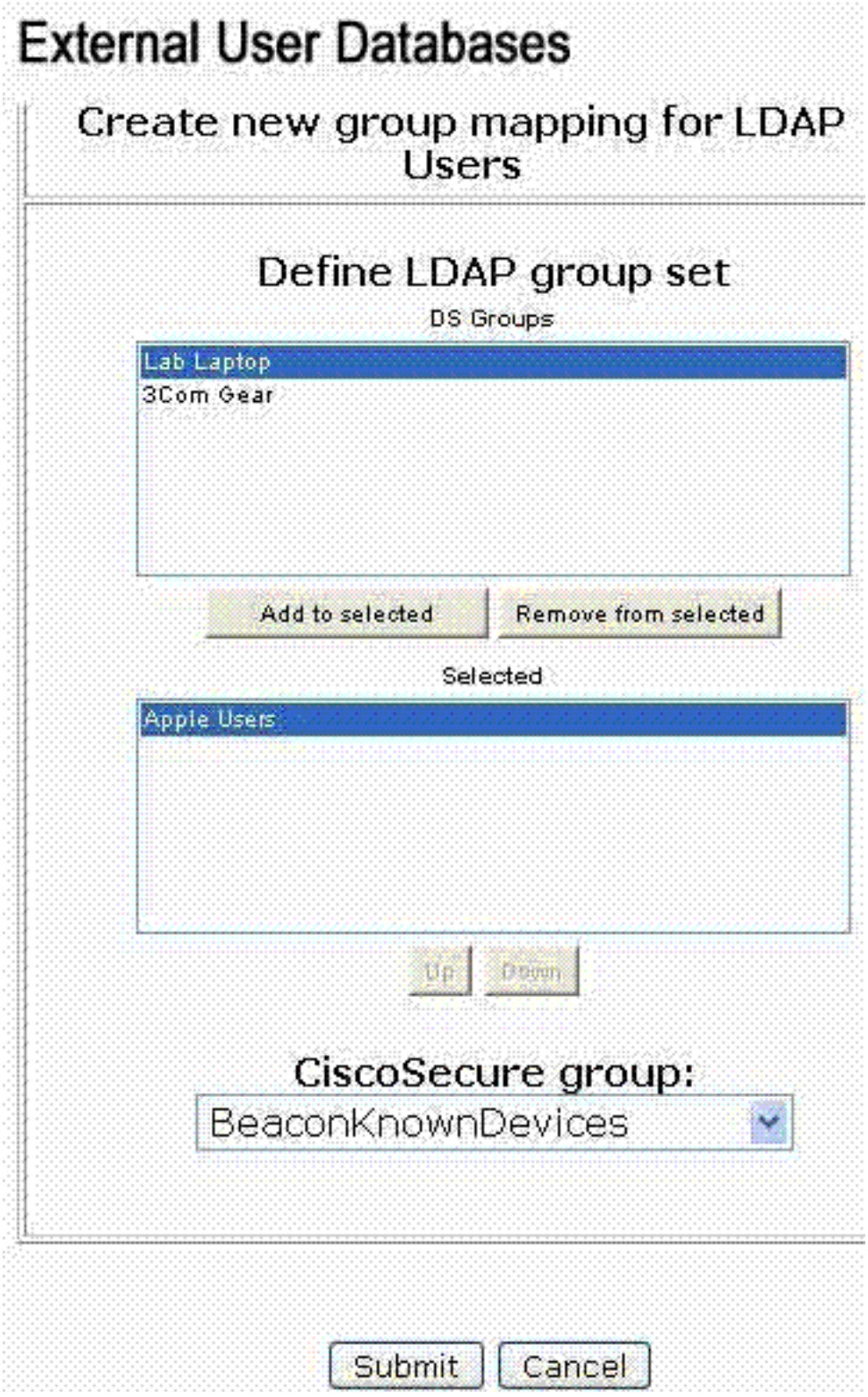


Quand vous choisissez la base de données d'utilisateur externe de balise créée plus tôt dans cette section avec la sélection du lien, Beacon_Helium dans l'exemple précédent, ceci affiche la fenêtre illustrée dans la figure 14. Notez que tous les profils de balise activés pour le LDAP dans la configuration de système de balise comme décrit dans la première section de ces instructions de configuration sont remplis dans les groupes DS qui sont disponibles pour que la sélection crée des mappages dans ACS. Si les noms de profil de balise activés pour le LDAP ne sont pas affichés dans l'interface ACS, c'est indicatif d'un problème avec la configuration de LDAP ACS. Référez-vous aux instructions sur la balise de configuration comme une base de données d'utilisateur externe tracée les grandes lignes plus tôt dans cette section, en particulier les paramètres de LDAP.

Notez que c'est l'interface qui permet le mappage de différents profils LDAP-activés dans la balise avec les groupes de CiscoSecure configurés dans ACS. L'interface tient compte du mappage de chaque profil LDAP-activé par balise individuelle à un seul groupe de CiscoSecure. Dans cet exemple, seulement un seul groupe a été créé pour les périphériques connus dans des profils LDAP-activés de balise : BeaconKnownDevices. Mais, de plusieurs groupes, chacun avec ses propres paramètres de stratégie peuvent être créés afin de manipuler des authentifications réussies différemment dépendantes sur le profil en cours de balise du périphérique.

Par exemple, un groupe de CiscoSecure peut être créé pour BeaconKnownIPPhones, qui a renvoyé les attributs VLAN qui assignent des points finaux dans le profil de téléphone IP dans la balise au téléphone VLAN quand vous joignez le réseau et l'authentifiez par le MAB.

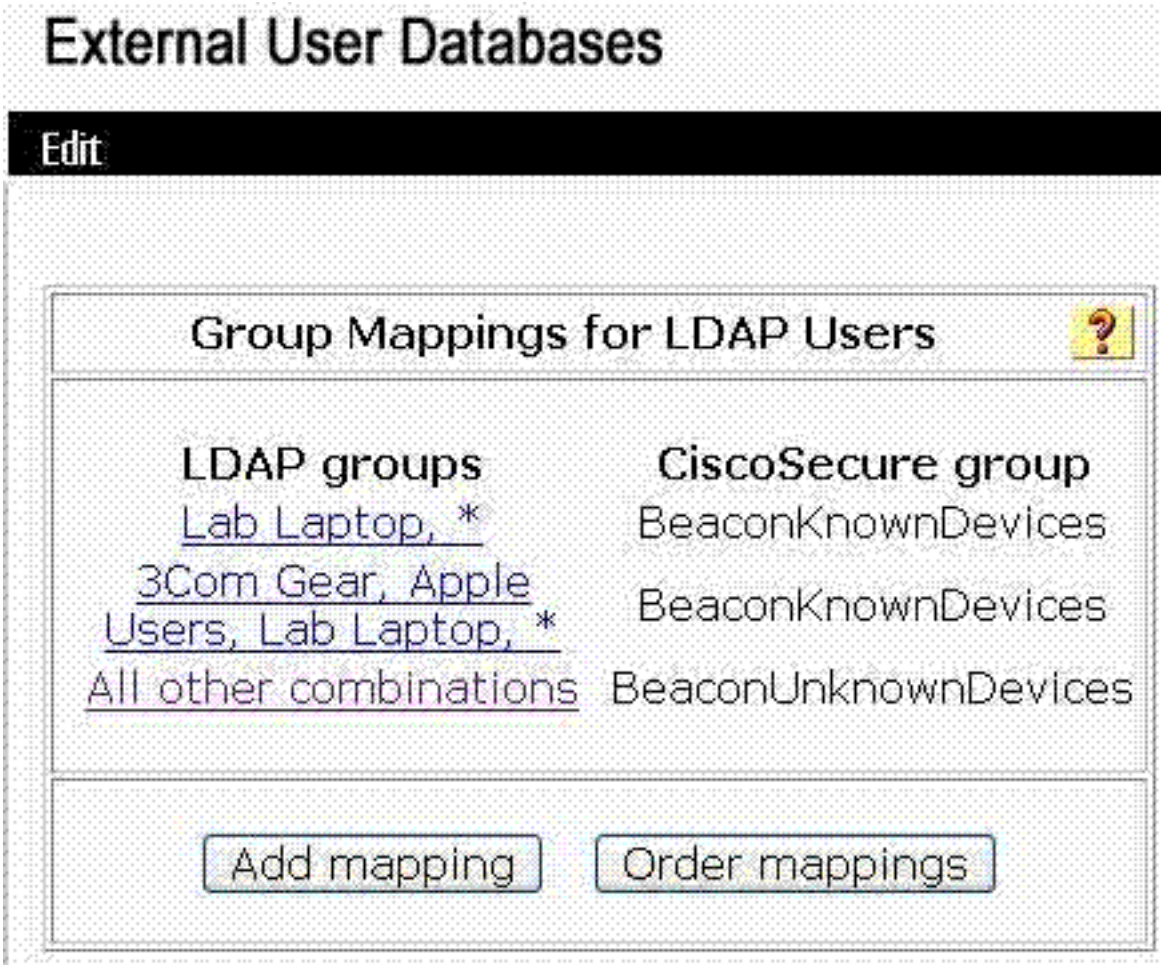
Figure 14 : Mappage de Profil-à-groupe



Choisissez un groupe DS (profil de balise avec le LDAP activé), et assignez les points finaux dans ce profil au groupe désiré de CiscoSecure du menu déroulant. Dans l'exemple précédent, des adresses MAC actuellement dans le profil d'utilisateur d'Apple dans la balise sont authentifiées par le MAB, placé dans le BeaconKnownDevices qui a comme conséquence une authentification et un placement réussis dans l'utilisateur VLAN quand vous joignez le réseau.

Sélectionner soumettent apporte la liste des mappages en cours de groupe sur ACS en authentifiant les utilisateurs inconnus à la base de données d'utilisateur externe de balise.

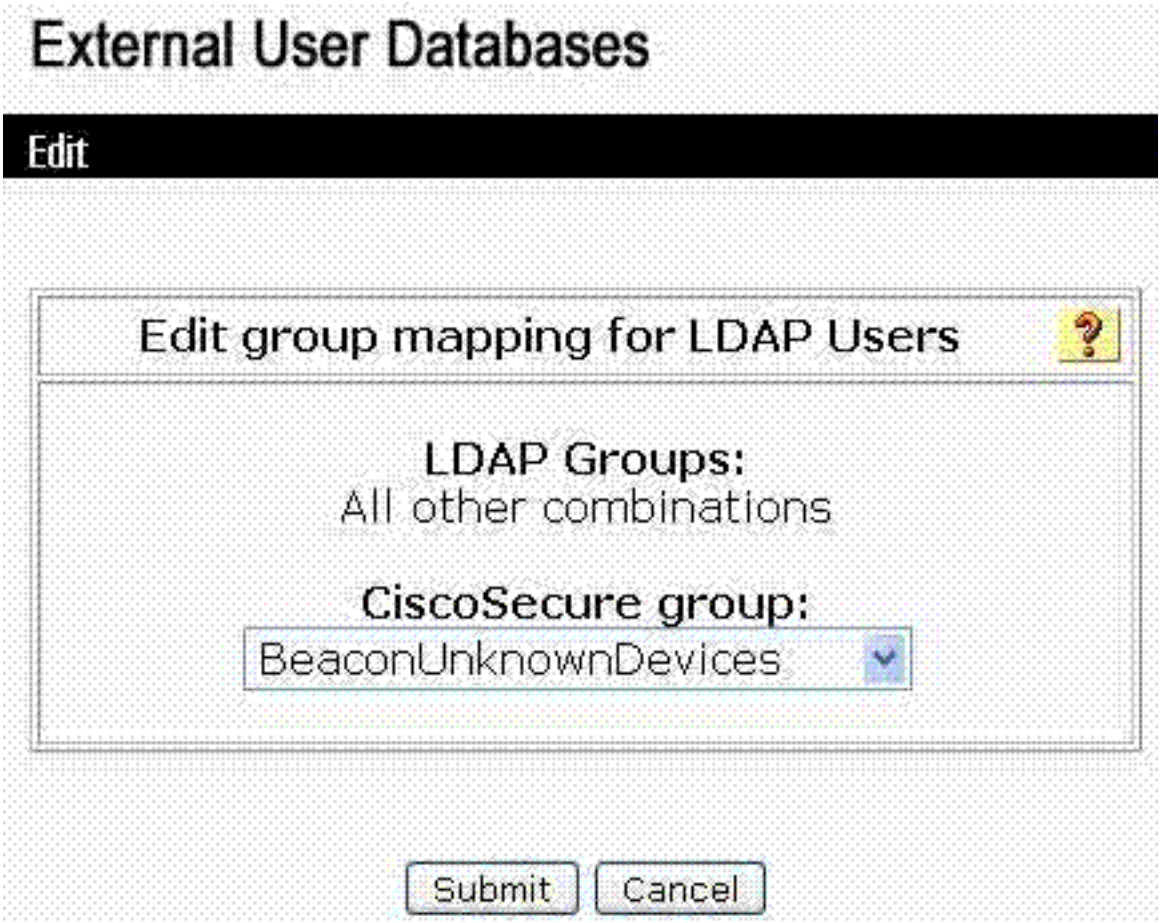
Figure 15 : Mappages de groupe de liste



Notez que les mappages explicitement faits avec la procédure précédemment décrite sont répertoriés dans cette vue. Tous groupes DS (profils LDAP-activés par balise) pas explicitement tracés à un groupe, qui inclut les points finaux que la balise n'a pas encore découverts ou placé dans une chute de profil de LDAPenabled dans le tout autre collecteur de combinaisons. Essentiellement ceci permet les points finaux que la balise ne peut pas fournir des informations au sujet de dans un groupe de CiscoSecure, par exemple, BeaconUnknownDevices. Comme précédemment tracé les grandes lignes, ce groupe peut être désactivé totalement qui a comme conséquence la panne de MAB, ou comme dans l'exemple précédent, il peut être conçu afin de fournir seulement la Connectivité limitée aux points finaux non connus par la balise.

Toutes autres combinaisons peuvent être assignées un groupe de CiscoSecure (BeaconUnkownDevices) si vous cliquez sur en fonction les **toutes autres combinaisons** joignez afin d'obtenir cette fenêtre :

Figure 16 : Assigner un groupe à toutes autres combinaisons

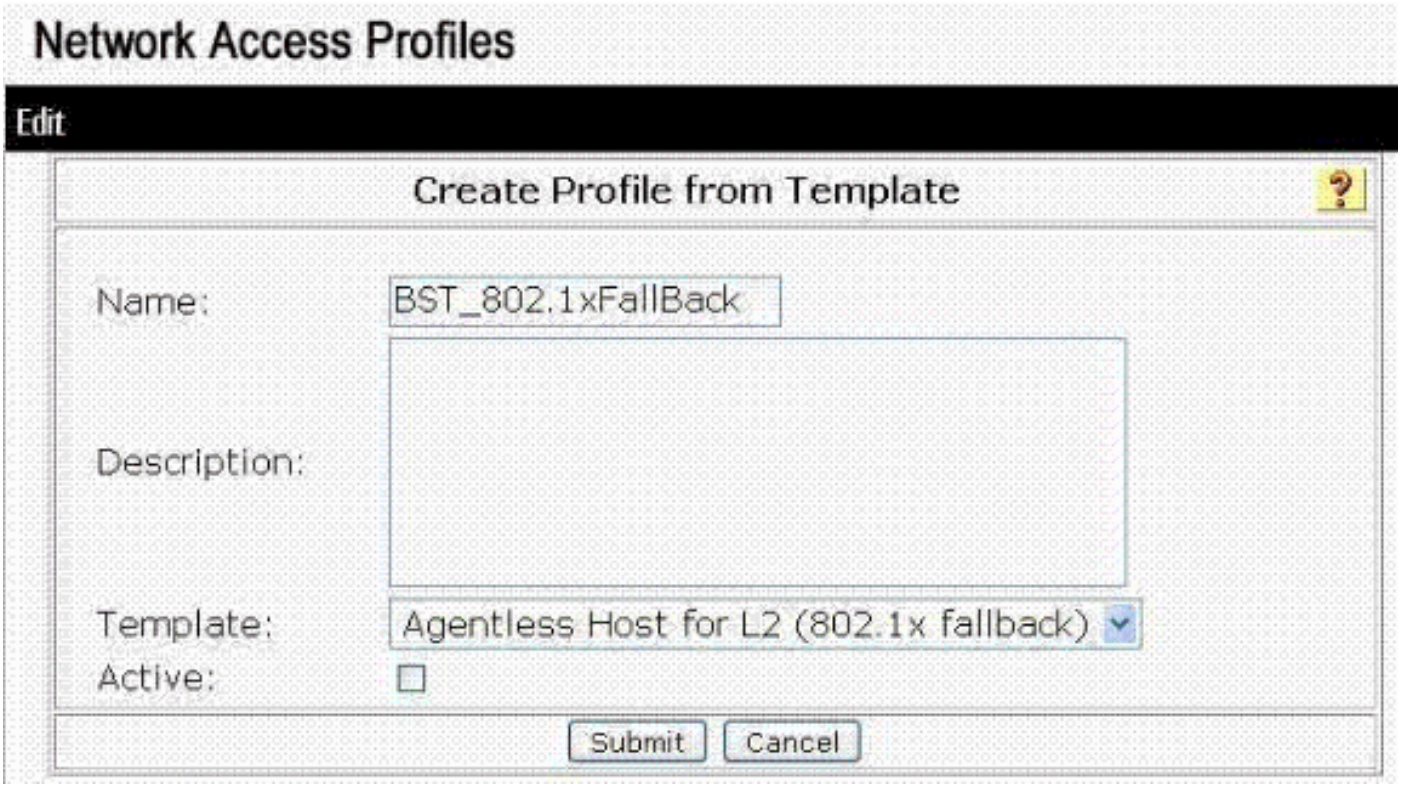


Configuration de profil d'accès au réseau

La dernière étape exigée dans la configuration ACS pour que le MAB utilise le système de profileur de point final de balise comme proxy est la configuration d'un profil d'accès au réseau pour le retour de 802.1X. Terminez-vous ces étapes tracées les grandes lignes afin de configurer le profil requis d'accès au réseau pour se terminer la configuration ACS tels que le MAB est configuré et fonctionne selon la configuration terminée précédemment.

Le profil d'accès au réseau à ajouter est un profil de modèle. Choisissez les **profils d'accès au réseau de la** page globale de navigation. Choisissez alors **ajoutent le profil de modèle** afin d'évoquer cette forme illustrée.

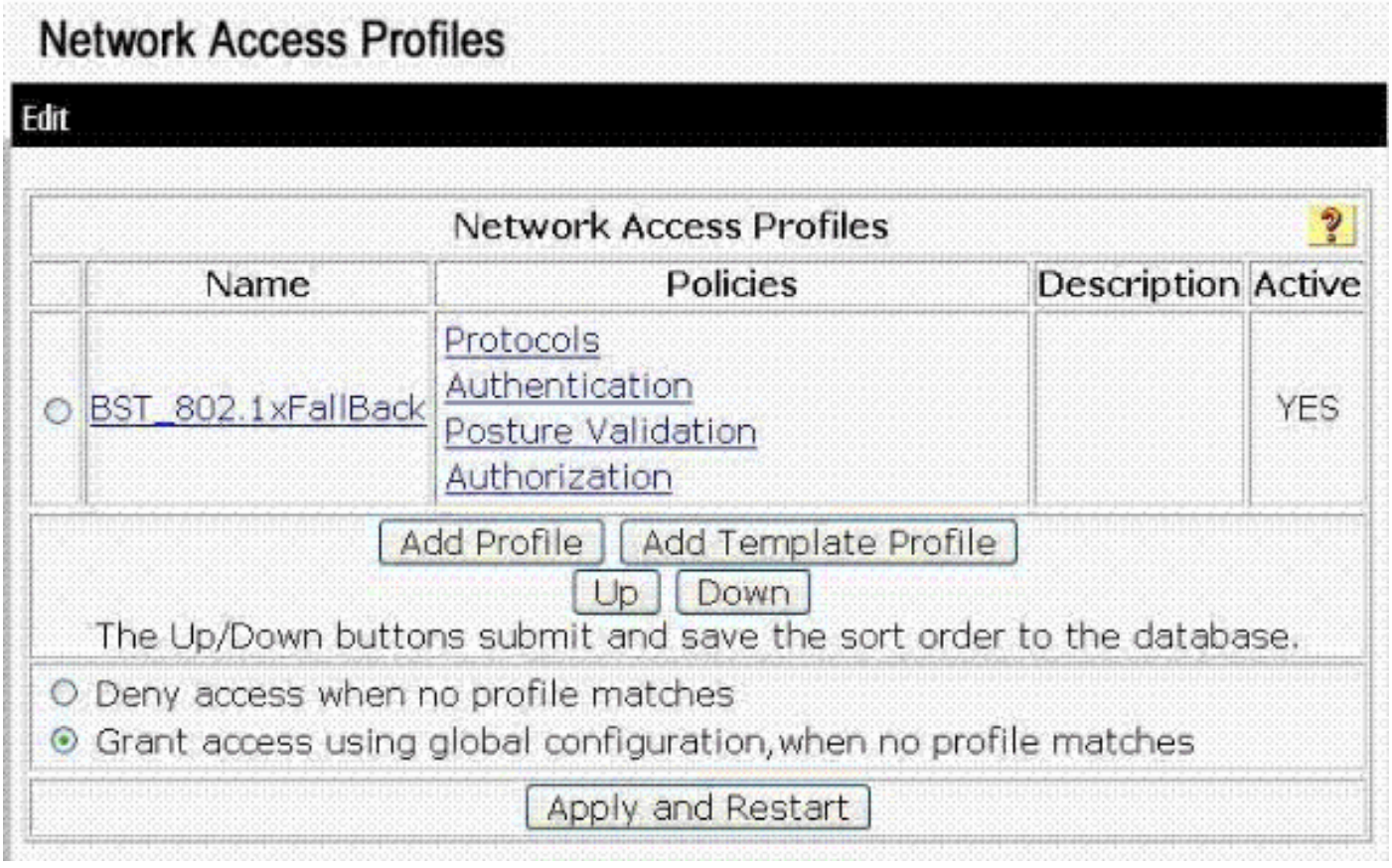
Figure 17 : Ajoutez un profil d'accès au réseau de modèle



Nommez le profil d'accès au réseau afin d'activer pour le distinguer d'autres, et ajoutez une description si désiré. Le modèle pour ce profil est sélectionné de la liste déroulante. Assurez-vous que l'**hôte Agentless pour L2 (retour de 802.1x)** est sélectionné, et vérifiez la case à cocher **active**. Cliquez sur le bouton de **soumission** si de finition afin de sauvegarder le profil d'accès au réseau.

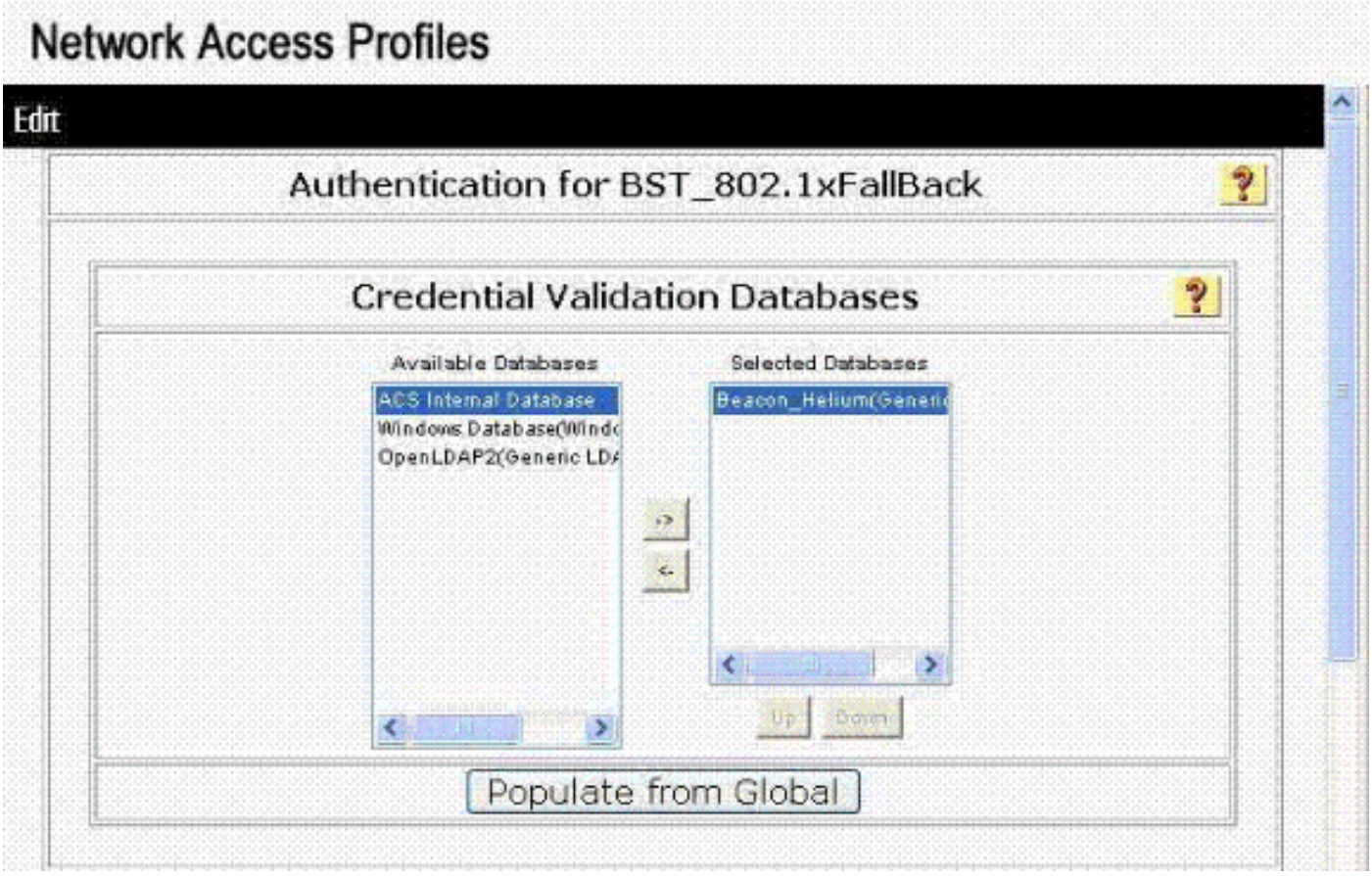
Quand vous clic soumettez, on présente cette forme qui te permet pour éditer les paramètres pour le profil juste créé comme affiché.

Figure 18 : Éditez le PETIT SOMME pour le MAB



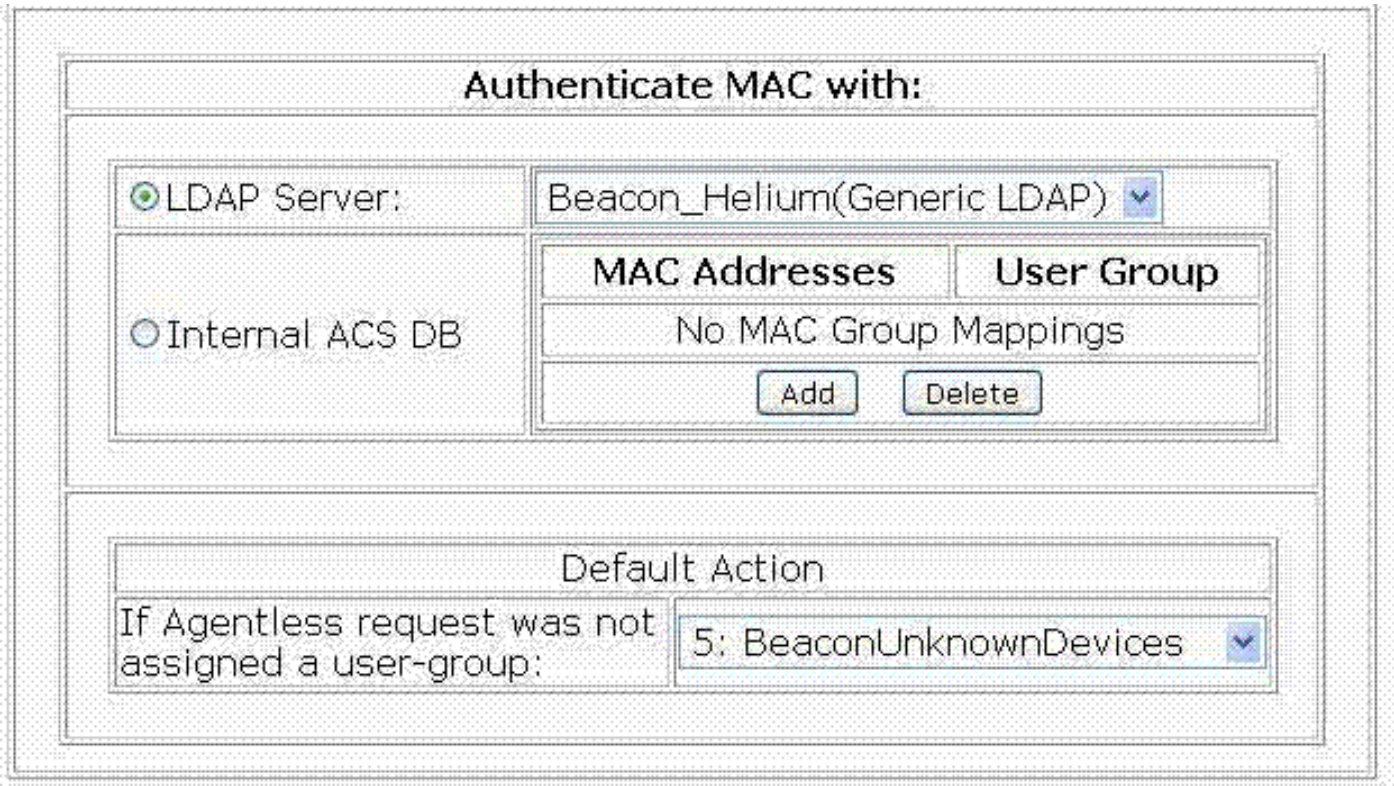
La stratégie d'authentification pour le profil nouvellement configuré doit être configurée afin d'utiliser le système de balise comme base de données de créance de validation. Choisissez le lien d'authentification dans la colonne de stratégies pour le profil de création récente d'accès au réseau (retour de 802.1x dans l'exemple). Ces formes sont présentées.

Figure 19 : Base de données choisie pour le MAB



D'abord, choisissez la base de données d'utilisateur externe de balise de la table de bases de données disponible et utilisez **- >** bouton afin de l'ajouter aux bases de données sélectionnées. Faites descendre l'écran à la section de MAC d'authentifier de la forme, et choisissez la case d'option de **serveur LDAP**. Choisissez la base de données de **balise de la** liste déroulante. Pour finir, choisissez le groupe de **BeaconUnknownDevice** pour l'action par défaut suivant les indications de la prochaine figure.

Figure 20 : Indiquez le serveur LDAP de balise



Cette étape se termine la configuration exigée ACS pour la dérivation d'authentification MAC avec la balise comme base de données d'utilisateur externe. Redémarrez le service ACS afin de s'assurer que toutes les modifications de configuration sont investies dans la configuration en cours.

Le système devrait être prêt à tester le MAB, si les Commutateurs sont configurés correctement. Un point final actuellement dans un profil LDAP-activé de balise peut être déconnecté du réseau et être réadmis avec les paramètres de stratégie spécifiés pour le groupe de BeaconKnownDevices.

Commutez la configuration pour la dérivation d'authentification MAC

La configuration de commutateur de Thid fournit à un exemple de configuration pour l'authentification de 802.1X la dérivation d'authentification MAC activée, et à la réaffectation dynamique VLAN exigée afin d'appliquer des attributs RADIUS retournés d'ACS.

Commutateur
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
```

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Informations connexes

- Dispositif Cisco NAC (Clean Access)
- Cisco Secure Access Control Server pour Windows
- Support et documentation techniques - Cisco Systems