NAC: Пример конфигурации интеграции LDAP с AcS

Содержание

Введение

Этот документ предоставляет пример конфигурации шагов для настройки Маяка и ACS, чтобы позволить устройствам Cisco, настроенным для MAB эффективно и продуктивно аутентифицировать устройства с поддержкой не802.1X в аутентифицируемой сети.

Cisco реализовала опцию, названную Обходом проверки подлинности MAC (MAB) на их коммутаторах, а также необходимой поддержке в ACS для размещения оконечных точек в поддерживающих 802.1X сетях, которые неспособны аутентифицироваться через 802.1X. Эта функциональность гарантирует, что оконечные точки, которые делают попытку соединения с поддерживающей 802.1X сетью, которые не оборудованы функциональностью 802.1X, например, не имеют функционального соискателя 802.1X, могут аутентифицироваться до разрешения, а также принуждать политику использования базовой основы сети всюду по их соединению.

Когда устройство не в состоянии участвовать в протоколе 802.1X, MAB позволяет сети быть настроенной для принятия определенных устройств с использованием их MAC-адреса как основные учетные данные. Для MAB, который будет развернут и использован эффективно, среда должна иметь средство для indentify устройства в среде, которые не способны к аутентификации 802.1X и поддерживают актуальную базу данных этих устройств в течение

долгого времени как шаги, добавляет, и изменения происходят. Этот список должен заполняться и вестись в Сервере проверки подлинности (ACS) вручную, или через некоторые альтернативные средства, чтобы гарантировать, что устройства, которые аутентифицируются на MAC, завершены и допустимы в любой момент времени.

Профилировщик Оконечной точки Маяка может автоматизировать процесс идентификации неаутентифицирующихся оконечных точек, тех без соискателей 802.1X и обслуживания законности этих оконечных точек в сетях переменного масштаба на Мониторинге функциональных возможностей Профилирования и Поведения Оконечной точки. Через стандартный Интерфейс LDAP система Маяка может служить Внешней базой данных или Каталогом оконечных точек, которые будут аутентифицироваться через MAB. Когда запрос MAB получен от граничной инфраструктуры, ACS может сделать запрос системы Маяка, чтобы определить, нужно ли данную оконечную точку допустить в сетевое на актуальнейшей информации об оконечной точке, известной Маяком для предотвращения потребности в настройке вручную.

См. NAC: интеграция LDAP с ACS 5.x и Более поздний Пример конфигурации для получения дополнительной информации и подобная конфигурация с помощью ACS 5.x и позже.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Коммутатор Cisco 3750, который выполняется 12.2 (25) SEE2
- Cisco Secure Access Control Server для Windows 4.1

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Общие сведения

MAB является существенной функциональностью для динамической поддержки устройств, таких как принтеры, IP-телефоны, факсы и другие устройства с поддержкой не802.1X в развертываниях пост802.1X среды. Без возможности MAB порты доступа к сети, которые предоставляют подключение не802.1X способные оконечные точки, должны быть настроены статически для не попытки аутентификации 802.1X или с помощью других

функций, которые предоставляют очень ограниченные опции policy. По очевидным причинам это является по сути не масштабируемым в средах крупных предприятий. С MAB, включенным в сочетании с 802.1X на всех портах доступа, известный не802.1X, способные оконечные точки могут быть перемещены куда угодно в среде и все еще надежно (и надежно) соединяются с сетью. Поскольку устройства, которые допускают в сеть, аутентифицируются, другая политика может быть применена к другим устройствам

Кроме того, не802.1X способные оконечные точки, которые не известны в среде, такой как портативные ПК, которые принадлежат посетителям или подрядчикам, может быть предоставленным ограниченным доступом к сети через MAB при желании.

Как название предполагает, Обход Проверки подлинности MAC использует MAC-адрес оконечной точки как основные учетные данные. С Обходом Проверки подлинности MAC, включенным на порте доступа, если оконечная точка соединяется и не в состоянии отвечать на аутентификационное препятствие 802.1X, порт возвращается к режиму MAB. Коммутатор, который делает попытку MAB оконечной точки, делает стандартный Запрос RADIUS к ACS с MAC станции. Это пытается соединиться с сетью и запрашивает аутентификацию оконечной точки от ACS до разрешения оконечной точки к сети.

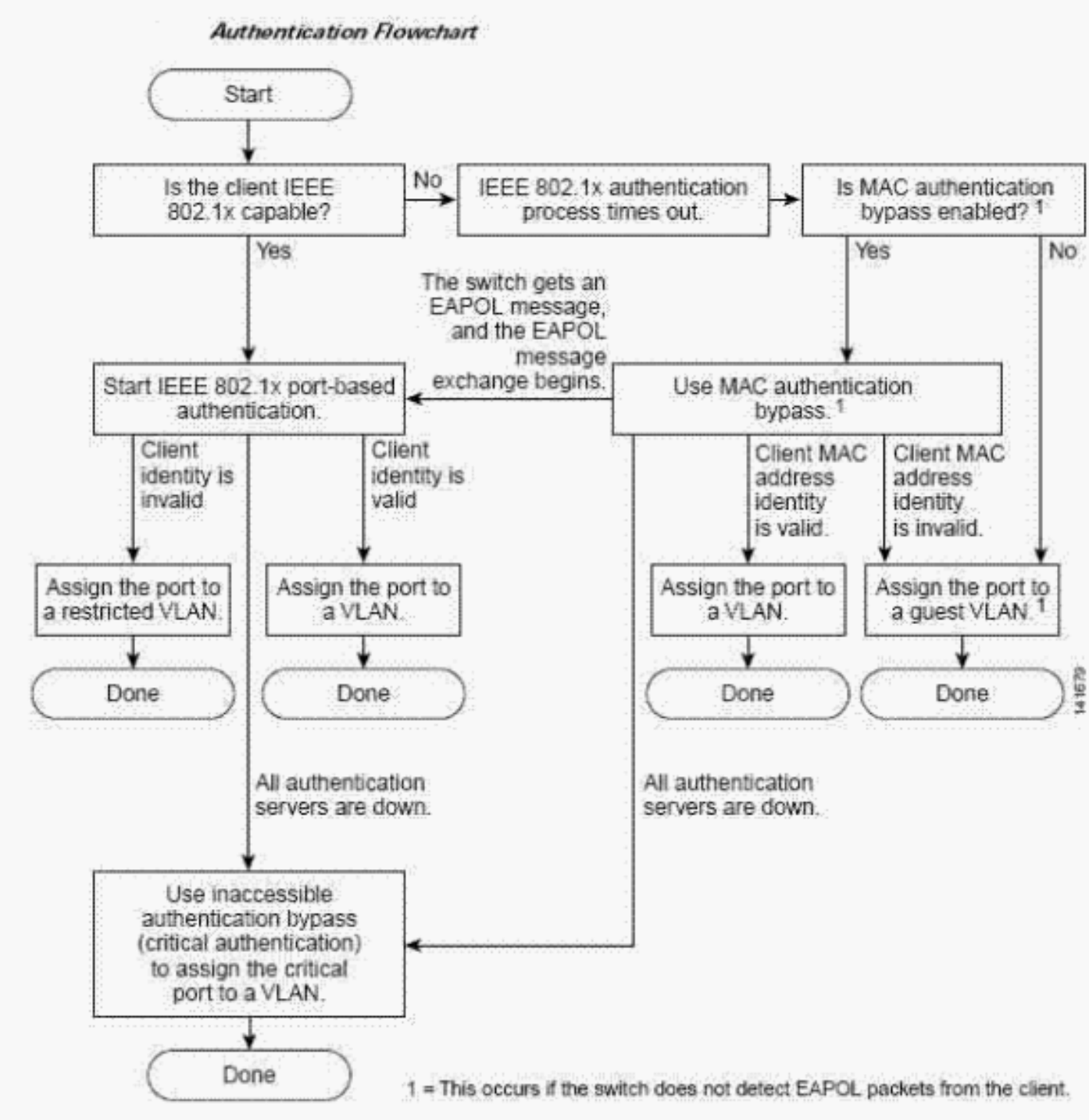
!--- конфигурацию

Схема блок-схемы

Эта блок-схема, взятая из документации Cisco Systems, иллюстрирует, как MAB используется в сочетании с аутентификацией 802.1X на граничной инфраструктуре Cisco, поскольку новые оконечные точки пытаются соединиться с сетью.

Этот документ использует этот рабочий поток Блок-схемы:

Рисунок 1: Опознавательный поток



ACS может быть настроен для использования или его собственной внутренней базы данных или внешнего Сервера LDAP для аутентификации запросов пользователя MAC-адреса. Система Профилировщика Оконечной точки Маяка является полностью поддерживающей LDAP по умолчанию и может быть использована ACS для аутентификации запросов пользователя MAC-адреса через стандартную функциональность LDAP. Поскольку Маяк автоматизирует обоих обнаружение, а также Профилирование всех оконечных точек в сети, ACS может сделать запрос Маяка через LDAP, чтобы определить, нужно ли MAC допустить в сеть, и в который группируются, оконечная точка должна быть сопоставлена. Это значительно автоматизирует и улучшает функцию Обхода Проверки подлинности MAC, особенно в средах крупных предприятий.

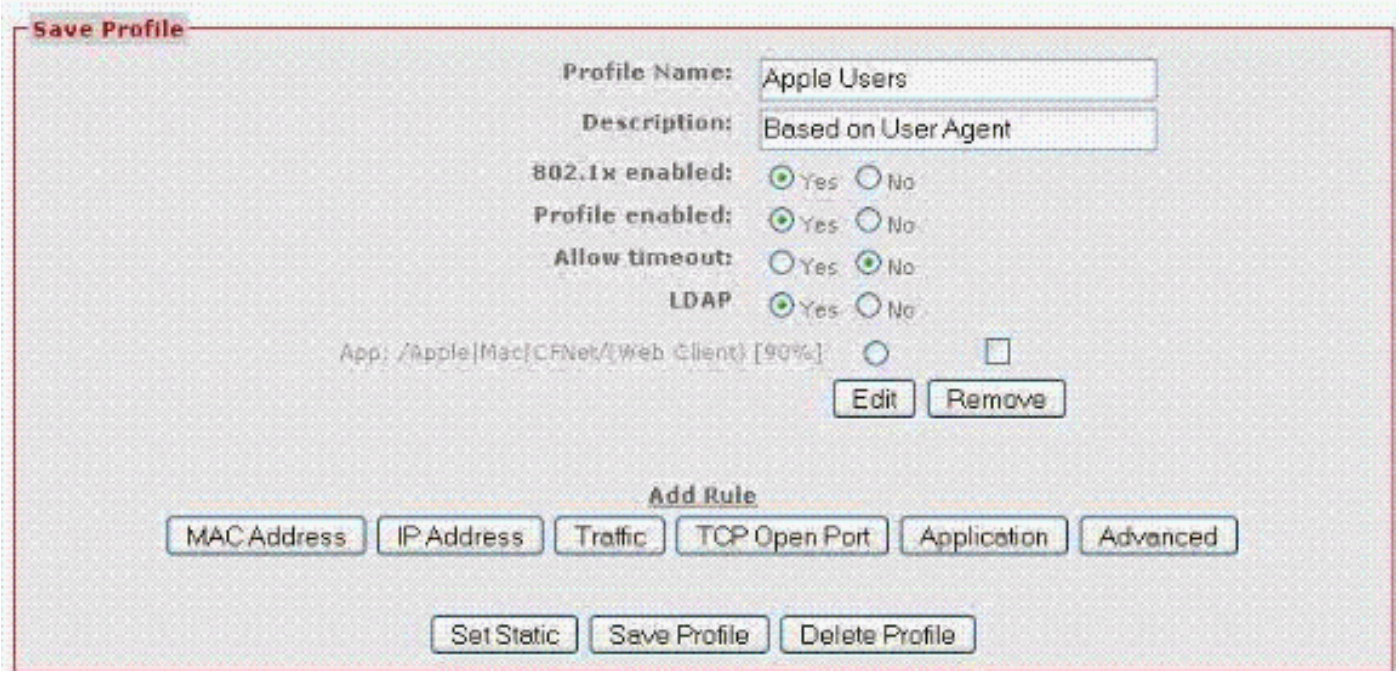
Через Поведенческий Мониторинг функциональных возможностей, предоставленный Маяком, устройства, которые, как наблюдают, ведут себя противоречиво с Профилями, включенными для MAB, переходятся из 4 поддерживающих LDAP профилей и впоследствии отказывают следующую обычную попытку повторной проверки подлинности.

Конфигурация системы профилировщика оконечной точки маяка для MAB

Конфигурация системы Маяка для интеграции с ACS в целях поддержки MAB является прямой, поскольку функциональность LDAP добавлена по умолчанию. Основная задача конфигурации должна определить Профили, которые содержат оконечные точки, которые желаемы, чтобы аутентифицироваться через MAB в среде, и затем включить те Профили для LDAP. Как правило, Профили Маяка, которые содержат устройства, принадлежавшие организации, должны быть предоставленным доступом к сети, когда замечено на порту, все же, как известно, неспособны аутентифицироваться через 802.1X. Как правило, это Профили, которые содержат принтеры, IP-телефоны или управляемый UPSs как общие примеры.

Если бы принтеры, представленные Маяком, были размещены в профиль под названием *Принтеры* и IP-телефоны в профиле под названием *IP-телефоны*, например, то эти профили должны быть включены для LDAP, таким образом, что оконечные точки разместили в те Профили результат в успешной аутентификации как известный IP-телефон и Принтеры в среде через MAB. При включении профиля для LDAP это требует, чтобы переключатель LDAP в Настройке профиля Оконечной точки был установлен, как показано в данном примере:

Рис. 2: Включите профиль для LDAP



Когда проверка подлинности MAC ACS - прокси к Маяку через LDAP, запрос состоит из двух запросов sub, оба из которых должны возвратить допустимый, непустой результат. Первый запрос к Маяку - известен ли MAC Маяку, например, если это было обнаружено и добавлено к базе данных Маяка. Если оконечная точка должна все же быть обнаружена Маяком, оконечная точка, как полагают, неизвестна. Второй запрос не необходим в случае оконечных точек, которые Маяк не обнаружил и не находится в его базе данных. Если оконечная точка была обнаружена и находится в базе данных Маяка, следующий запрос должен определить текущий Профиль оконечной точки. Если оконечная точка должна все же быть представлена или в настоящее время находится в профиле не 5, включил для LDAP, неизвестный результат возвращен к ACS и аутентификации оконечной точки сбоями Маяка. Это зависит от того, как ACS настроен, что это может привести к устройству с отказом доступа к сети в целом или быть дано Политику, которая является соответствующей гостевым устройствам или неизвестному.

Только в случае, где MAC является оконечной точкой, которую Маяк обнаружил и разместил в поддерживающий LDAP Профиль, ответ состоит в том, что оконечная точка известна и Представлена Маяком, который будет возвращен к ACS. Самое главное для этих оконечных точек Маяк предоставляет текущее Имя профиля, которое позволяет ACS сопоставить известные оконечные точки с Cisco SecureAccess Groups. Это включает гранулированное сделанное определение Политики, столь же гранулированное как отдельная политика для каждого Маяка поддерживающий LDAP Профиль, при желании.

Конфигурация AcS для MAB и использования маяка как внешняя база данных пользователей

Конфигурация ACS для MAB и использования Маяка как Внешняя база данных пользователей требует трех следующих действий. Заказ, проиллюстрированный в этом документе, придерживается потока операций, который эффективен, когда это выполняет конфигурацию MAB полностью и может варьироваться для систем, которые были в действии с другими режимами аутентификации, уже настроенными.

Настройте Cisco SecureGroup (s)

Когда вы делаете попытку MAB для конкретной оконечной точки, которая пытается соединиться с сетью, ACS делает запрос Маяка на LDAP, чтобы определить, обнаружил ли Маяк MAC, и во что Маяк Профиля в настоящее время размещал MAC-адрес, как описано ранее в документе.

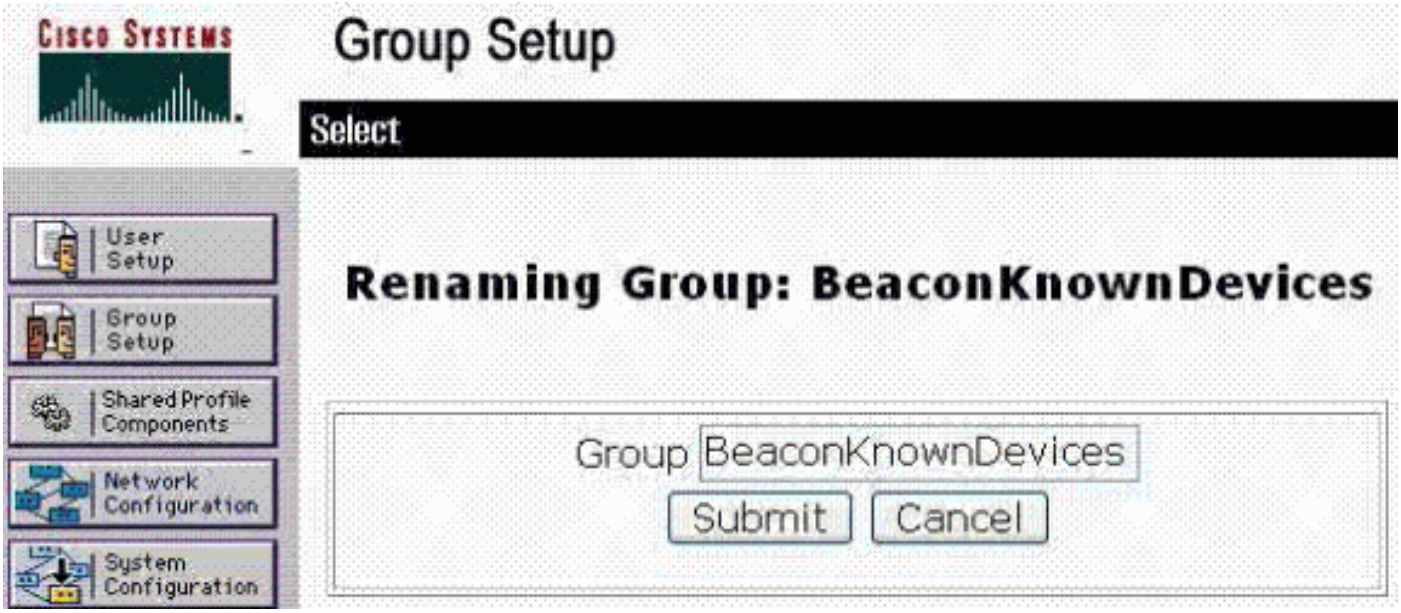
Механизм Cisco SecureGroup с ACS может использоваться, чтобы и аутентифицировать и применить политику к оконечным точкам, которые были обнаружены и Представлены Маяком через MAB, а также ошибками проверки подлинности — те устройства, не известные или не в настоящее время Представляемые Маяком.

Например, Группа может быть добавлена к конфигурации AcS для оконечных точек, обнаруженных и Представленных Маяком, и вызвала *BeaconKnownDevices* и другую группу *BeaconUnknownDevices* добавленный для устройств, которые не в настоящее время известны Маяком. Или Маяк не обнаружил MAC или в настоящее время не представлял его в поддерживающий LDAP профиль. Как показано позже в этом документе, Группы включают приложение политики к оконечным точкам, поскольку они пытаются присоединиться к сети.

Обратите внимание на то, что в примере, выделенном в этом документе, только две группы, BeaconKnown и BeaconUnknown настроены. Но возможно создать множественный SecureGroups для оконечных точек, обнаруженных и представленных Маяком, целым одним для каждого поддерживающего LDAP профиля в Маяке, каждом с другими параметрами политики, такими как назначение VLAN. Кроме того, группа устройств BeaconUnkown может быть настроена для запрета всего доступа к оконечным точкам, которые должны все же быть обнаружены или размещены в Профиль, включенный для LDAP 6 Маяками. Это выполнено при выборе флажка Group Disabled в параметрах окна конфигурации группы BeaconUnknownDevices.

Создание группы на ACS инициируется от кнопки Group Setup в интерфейсе пользователя ACS. Выберите одну из доступных Групп, и затем выберите кнопку **Rename Group** для изменения Имени группы на KnownBeaconDevices как показано в данном примере. Нажмите **Submit** для сохранения изменения.

Рис. 3: Edit CiscoSecure Group

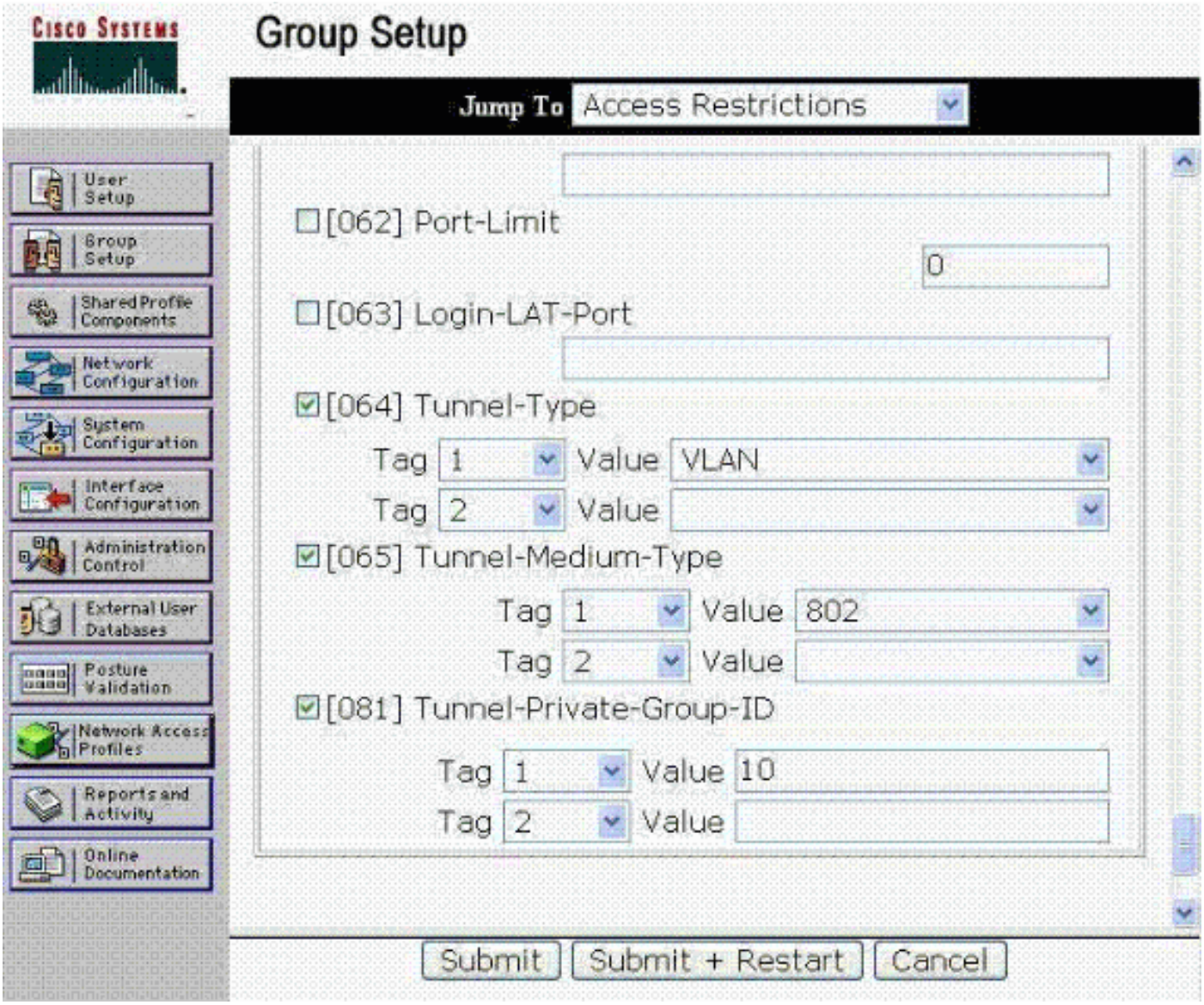


Выберите **Edit Settings** для редактирования параметров настройки Группы. Отредактируйте параметры группы BeaconKnownDevices, как желаемый. В целях примера в этом документе параметры группы, которые изменены, включают только Атрибуты RADIUS, стандартизированный IETF, найденные внизу страницы.

В частности вы называете это устройствами аутентифицируемый на этой группе, MAC-адресам, которые Маяк Представил к Профилям, выбранным для MAB, и включил для LDAP, возвратили параметры политики к аутентифицирующемуся коммутатору, который включает разрешение оконечных точек к сети на надлежащей VLAN. Чтобы сделать это, атрибуты RADIUS 064 Tunnel-Type, 065 Туннельных Средних Типов и 081 Туннель - Частный идентификатор группы собирается привести к оконечным точкам, размещаемым в желаемую VLAN, как показано на рисунке 4.

Гарантируйте, что проверены флажки рядом с каждым атрибутом RADIUS.

Рис. 4: Атрибуты VLAN группы

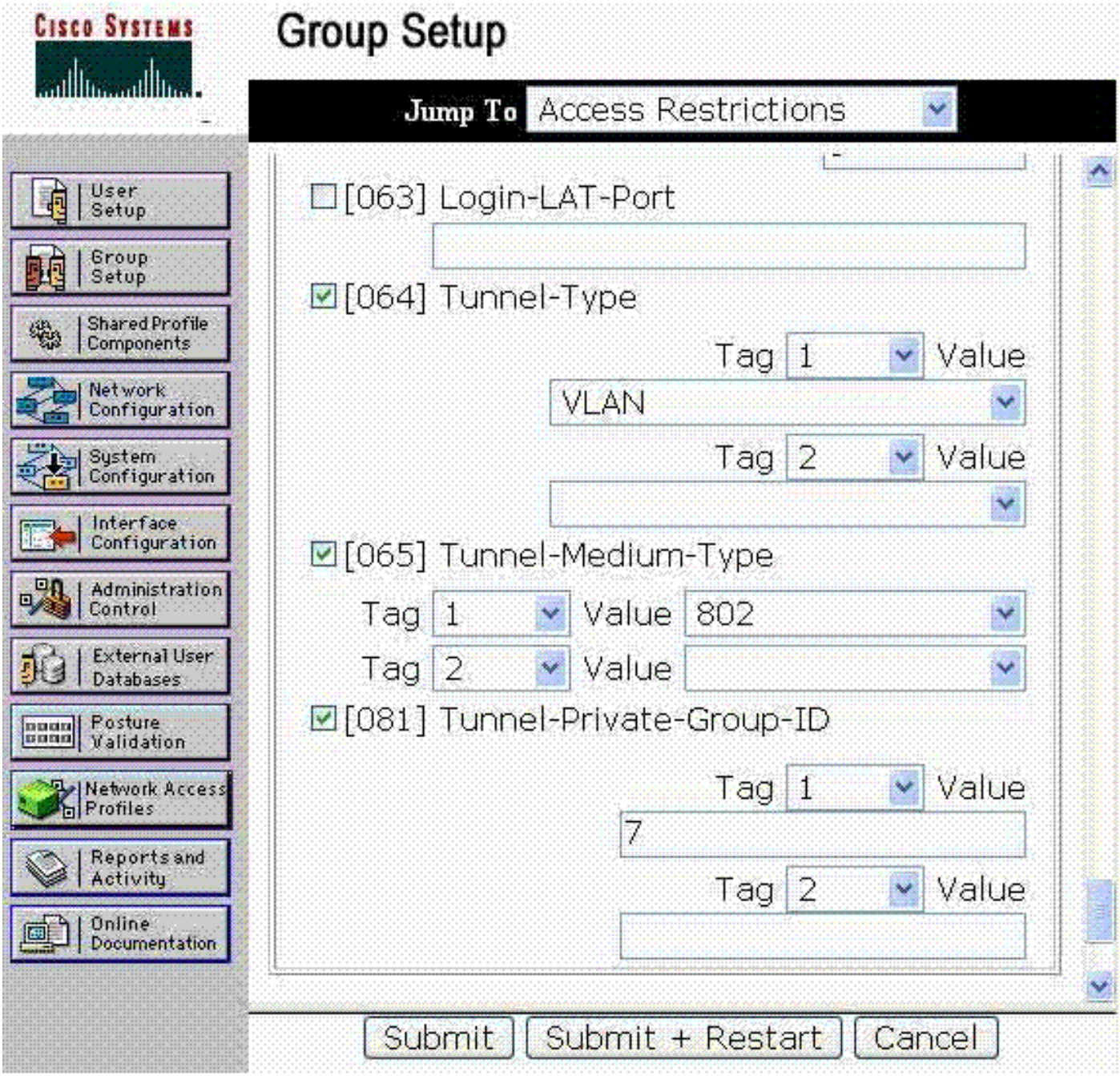


В показанном примере оконечные точки, аутентифицируемые успешно Маяком и впоследствии назначенные на группу ACS BeaconKnownDevices, размещаются в VLAN 10, санкционированную VLAN в конфигурации примера сети, во время соединения с сетью и успешно аутентифицируются на MAB ACS с использованием Маяка как Внешняя база данных пользователей.

Так же группа BeaconUnknownDevices создана для устройств, которые не в настоящее время известны Маяком как показано. Снова, если эти устройства не должны получать доступ к сети, просто проверьте флажок **Group Disabled** наверху формы. Оконечные точки, которые не были обнаружены Маяком или в настоящее время не Представляются Маяком в поддерживающий LDAP Профиль, отказывают MAB и не допущены в сеть.

Эти данные показывают альтернативу, чем использование флажка Group Disabled. В этом случае оконечные точки, которые не могут аутентифицироваться Маяком, назначены на группу, которая включена, но имеет другую политику, чем это для оконечных точек, которые известны. См. рисунок 5.

Рис. 5: Параметры VLAN для BeaconUnknownDevices



Обратите внимание на то, что для неизвестных устройств в данном примере, их допускают в сеть, но понижают Гостю или Ограниченному VLAN, VLAN 7. В примере сети VLAN 7 является Гостевой VLAN, который позволяет оконечным точкам только доступ в Интернет и запрещает доступ к внутренним ресурсам.

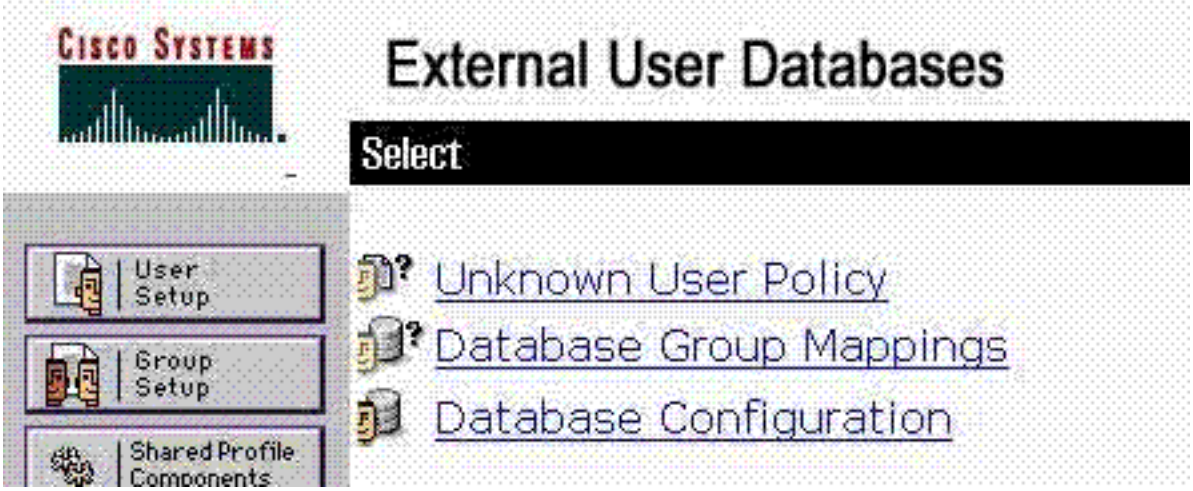
Когда ACS запрашивает аутентификацию от Маяка MAC оконечной точки, которая должна все же быть обнаружена или Представлена Маяком, ACS размещает MAC в эту группу и возвращается, результат к аутентифицирующемуся коммутатору включил для MAB.

Конфигурация базы данных внешних пользователей ACS

ACS должен быть настроен для проксирования запросов MAB от коммутаторов доступа до Маяка через LDAP. Это требует, чтобы конфигурация AcS включала систему Маяка как Внешнюю базу данных пользователей LDAP Общего назначения. Шаги, выделенные в этом разделе, иллюстрируют, как добавить 9 систем Профилировщика Оконечной точки Маяка как внешнюю базу данных пользователей, которая будет делать запрос ACS, когда это получает запросы MAB. Выберите **External User Database** на глобальной панели переходов

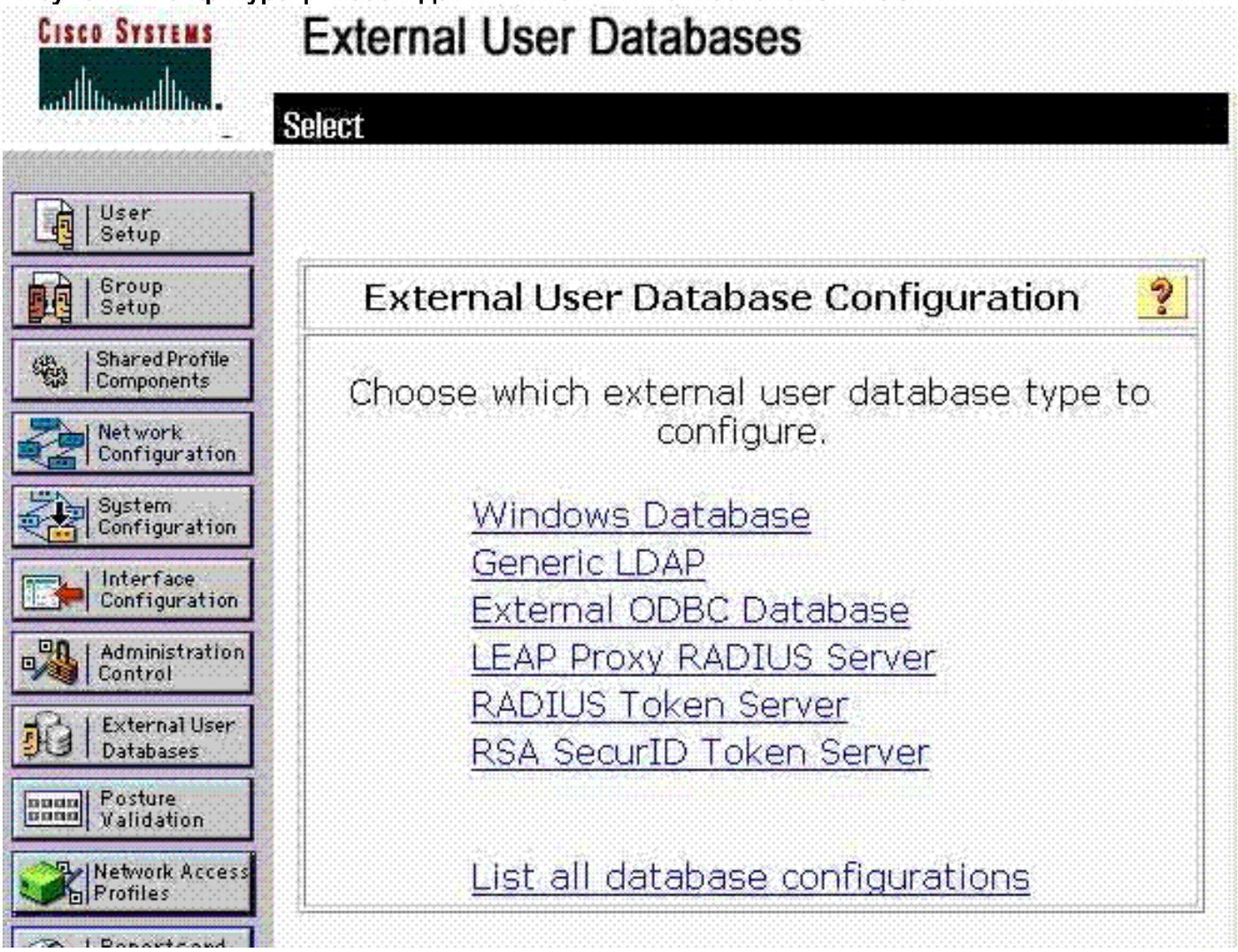
для внедрения окна External User Database, проиллюстрированного на рисунке 6.

Рис. 6: Внешний основной экран конфигурации DB



Первая задача в конфигурации Маяка как Внешняя база данных пользователей состоит в том, чтобы добавить систему Маяка как базу данных внешнего пользователя LDAP Общего назначения. Выберите **Database Configuration** для окна, проиллюстрированного на рисунке 7, появляются.

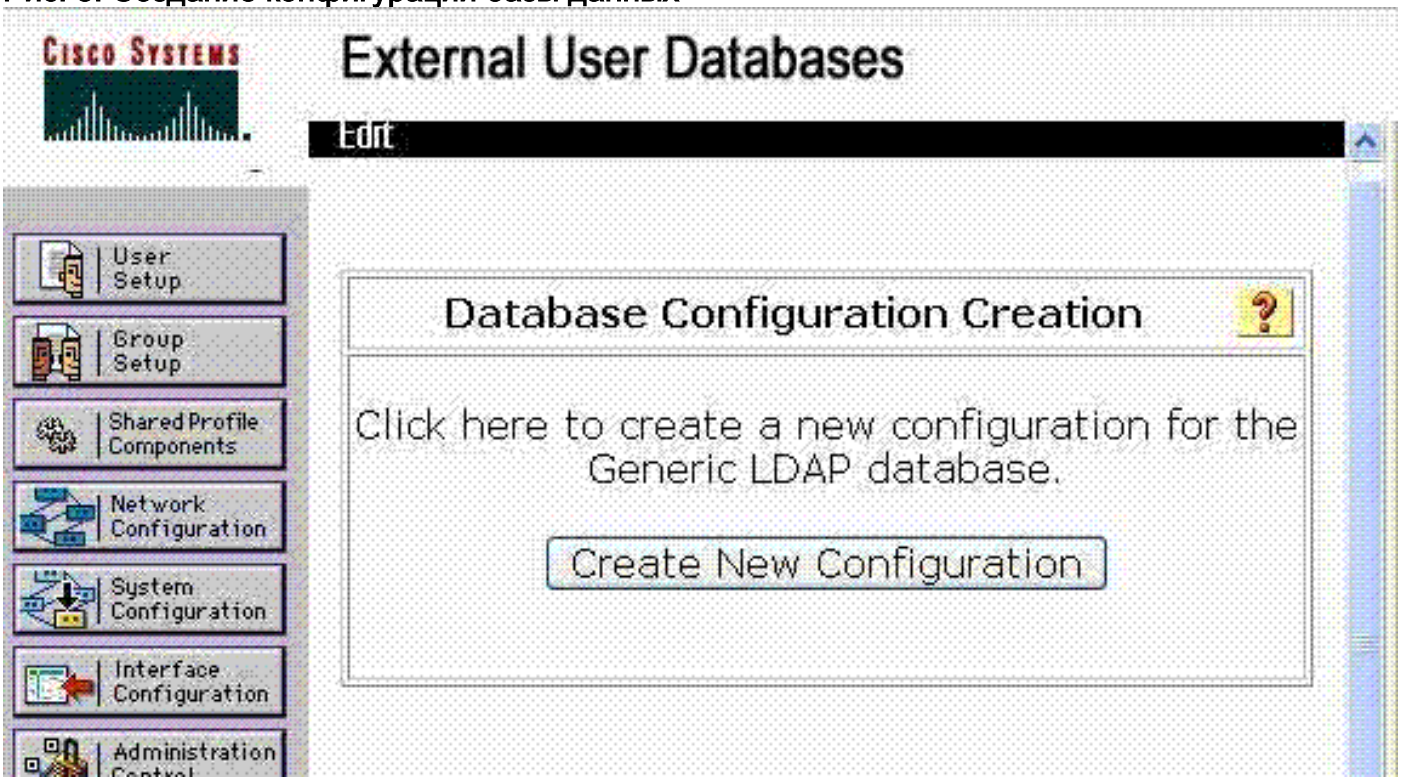
Рисунок 7: Конфигурация базы данных внешних пользователей ACS



Выберите **Generic LDAP** для открытия, форма использовала добавлять систему Профилировщика Оконечной точки Маяка как DB внешнего пользователя в конфигурации

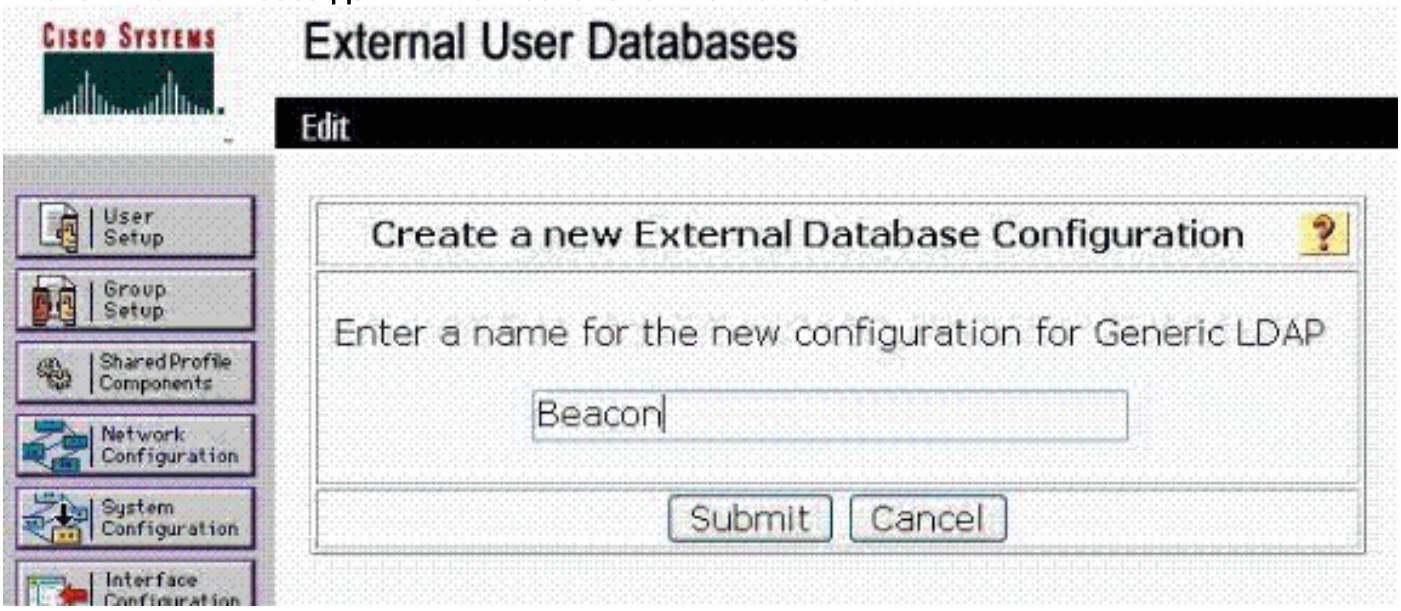
AcS. Это окно, кажется, включает создание новой Конфигурации базы данных внешних пользователей типа LDAP Общего назначения.

Рис. 8: Создание конфигурации базы данных



Выберите кнопку **Create New Configuration** для создания базы данных LDAP Общего назначения для Маяка. Это окно появляется и позволяет новой Внешней базе данных быть названной.

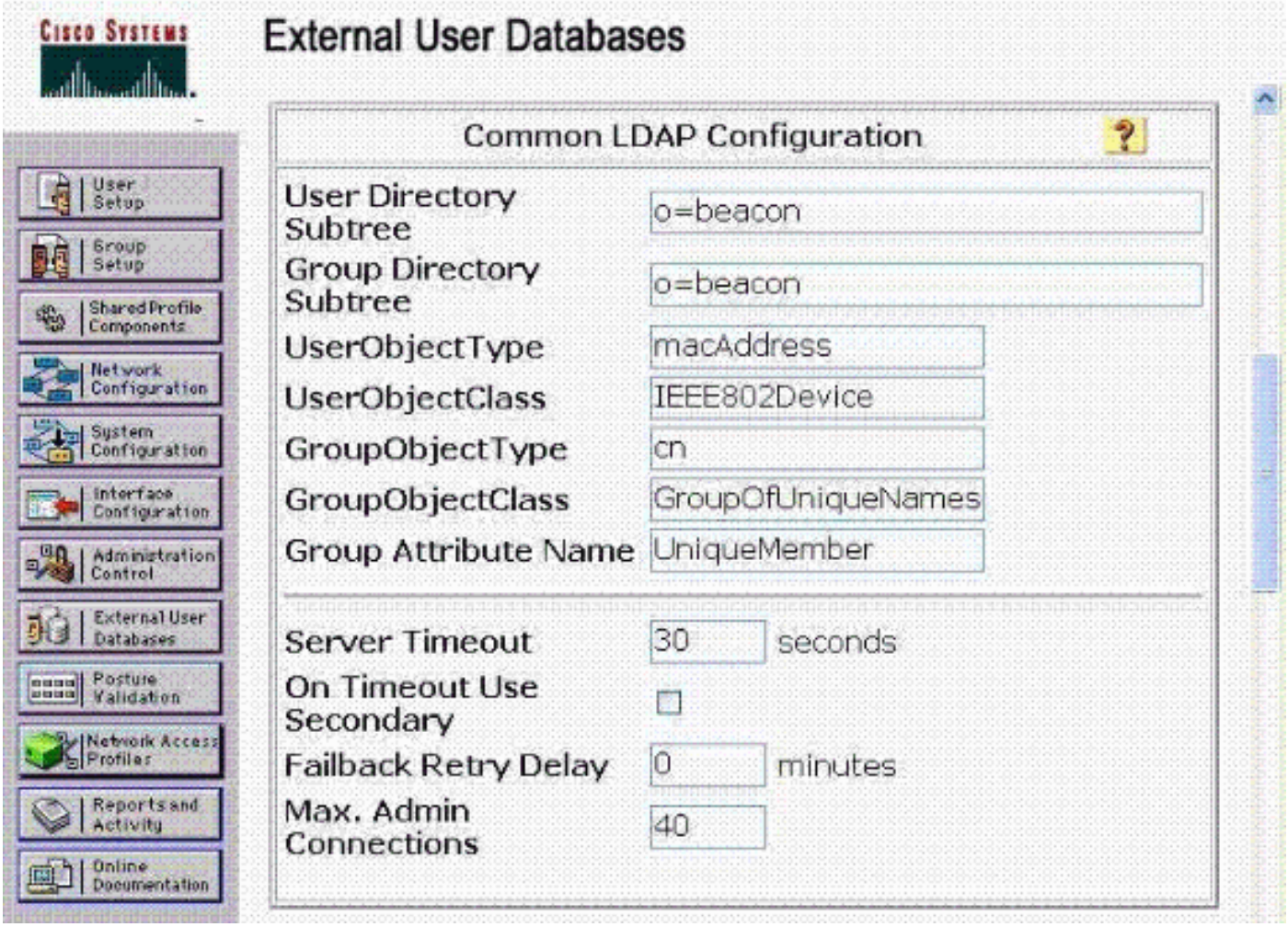
Рис. 9: Внешняя база данных пользователей маяка названия



Введите имя для Маяка внешняя база данных LDAP Общего назначения, которая позволяет ему легко дифференцироваться от других внешних баз данных в конфигурации. Выберите **Submit**, чтобы перейти на запись требуемых параметров LDAP, которые включают связь между 11 ACS и Маяком в целях аутентификации MAC-адресов с использованием информации о базе данных Маяка.

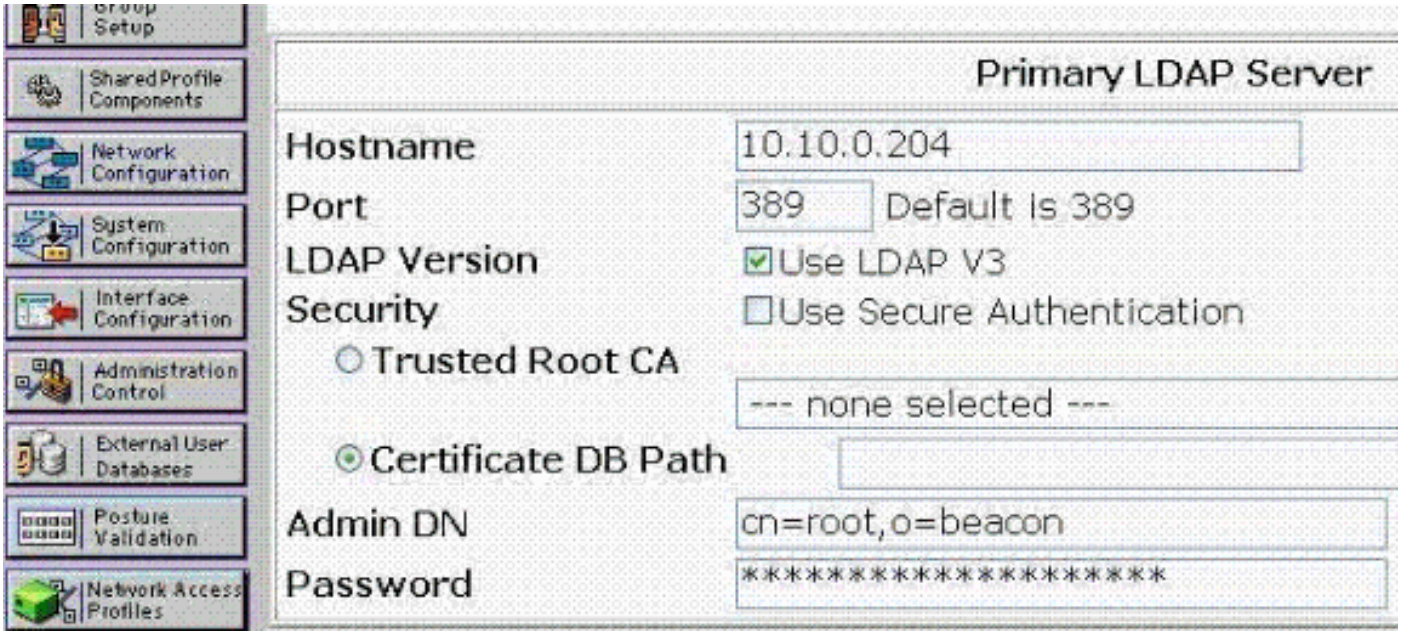
Рисунок 10 иллюстрирует Общие параметры Конфигурации LDAP, которые должны быть введены для Маяка внешняя база данных пользователей LDAP Общего назначения, которая добавлена к конфигурации AcS. Обратите внимание на то, что эти параметры предоставляют ACS информацию, которую он запрашивает для запроса Маяка через LDAP. Эти параметры должны быть введены точно как показано на этом рисунке для упрощения связи между ACS и Профилировщиком Оконечной точки Маяка.

Рис. 10: Общая конфигурация LDAP для маяка



Примечание: Используйте пароль**, GBSbeacon** для LDAP связывают пароль. Пароль введен в конце формы, показанной на рисунке 11.

Рис. 1-1: Параметры сервера маяка

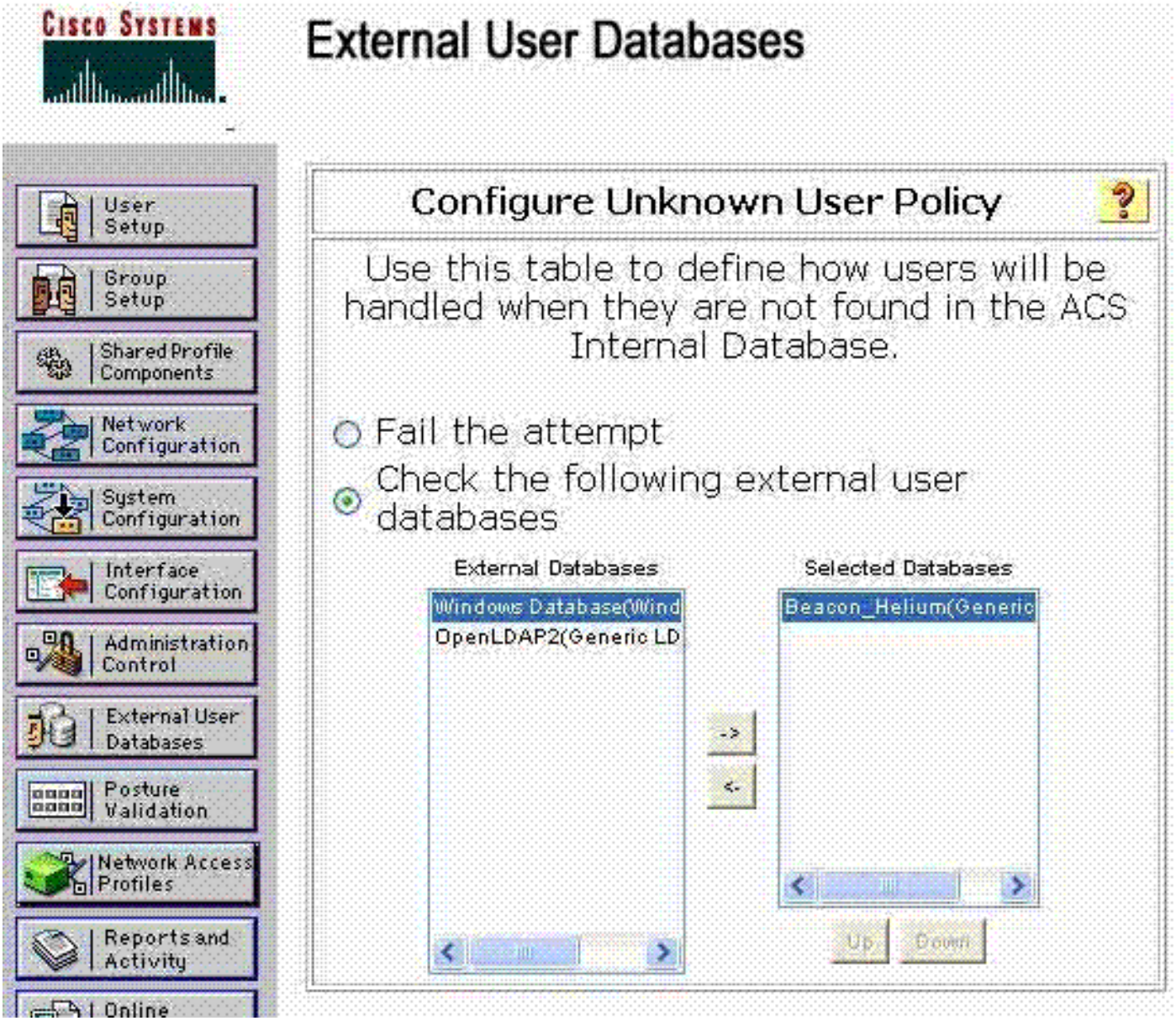


Вторая задача конфигурации, привязанная к конфигурации Маяка как Внешняя база данных пользователей, является конфигурацией Неизвестной политики пользователя. Неизвестная политика пользователя направляет ACS для запроса базы данных Маяка каждый раз, когда это получает запрос аутентификации для пользователя, который является MAC-адресом в случае MAB, для которого это не имеет информации в ее собственной базе данных.

Когда учетные данные неизвестного пользователя отправлены, Обратите внимание на то, что в типичных развертываниях ACS, могут быть существующие настроенные внешние базы данных пользователей и могут уже быть настроены для запроса тех баз данных. Когда коммутаторы запрашивают MAB отдельных MAC-адресов, внешняя база данных пользователей Маяка должна быть добавлена к списку для запроса его.

Эти рисунки выделяют поток операций для конфигурации Неизвестной политики пользователя и добавления Маяка как Внешняя база данных пользователей, которая будут делать запрос. К, выберите ссылку **Неизвестной политики пользователя** на основной странице External User Database, как проиллюстрировано на рисунке 6 для начала потока операций.

Рисунок 12: Настройте неизвестную политику пользователя

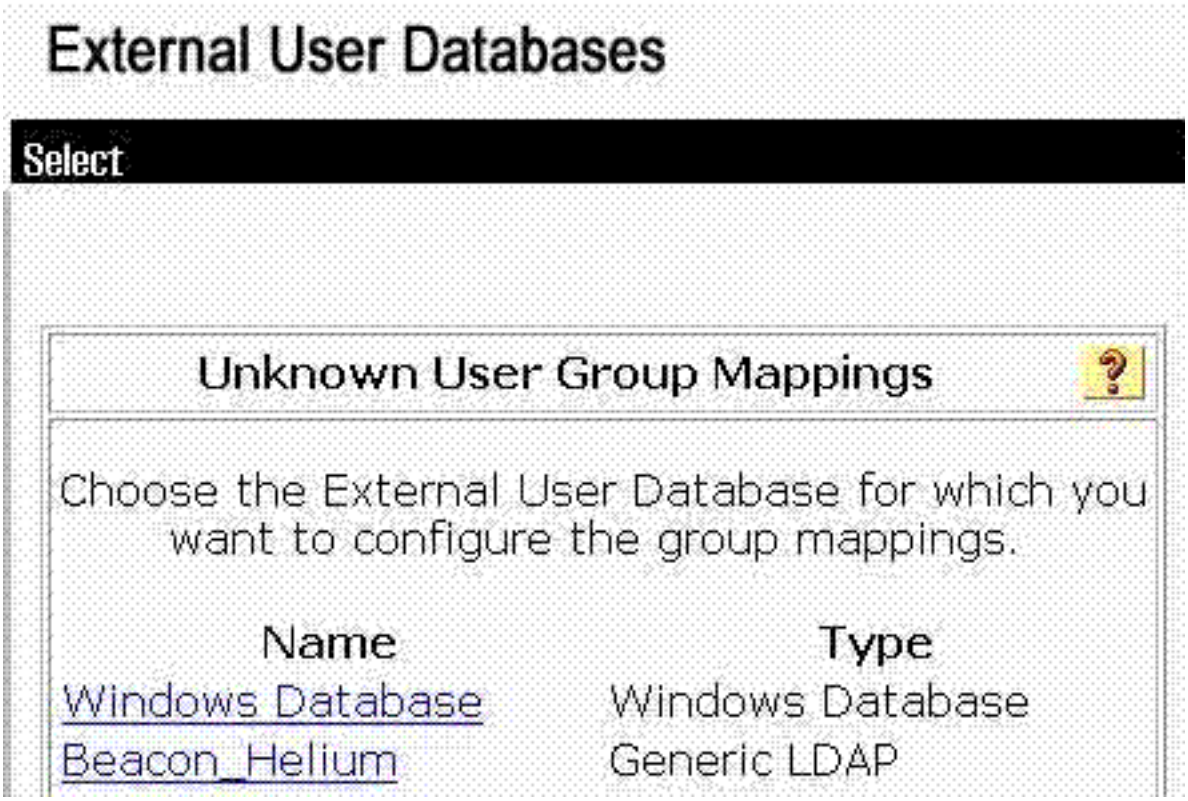


Выберите Beacon Generic LDAP database, добавленный к конфигурации AcS в последнем шаге из списка Внешних баз данных налево (Beacon_Helium) в примере. Используйте**->** для перемещения в Выбранные базы данных. Удостоверьтесь, что вы выбираете **Check следующая** кнопка с зависимой фиксацией **внешних баз данных пользователей**. Это гарантирует, что, когда коммутаторы отправляют MAC-адреса для аутентификации к ACS, ACS делает запрос Маяка, чтобы определить, известна ли оконечная точка, и это имеет текущий Профиль, если таковые имеются.

Задачей окончательной конфигурации добавить Маяк как внешнюю базу данных пользователей является завершение Сопоставлений групп баз данных. По существу это сопоставление связывает созданные группы CiscoSecure, например, BeaconKnownDevices и BeaconUnknownDevices, к успешным и неуспешным запросам LDAP, сделанным к Маяку так, чтобы каждый MAB, предпринятый коммутаторами, привел к присвоению оконечной точки группе CiscoSecure ACS. Это позволяет ACS ответить на коммутатор, нужно ли оконечную точку допустить в сеть, и, если допущено, каково политика, такая как атрибуты VLAN это должно быть.

Выберите **Database Group Mappings** на основной странице External User Databases как показано на рисунке 6 для настройки сопоставлений.

Рисунок 13: Сопоставления групп баз данных

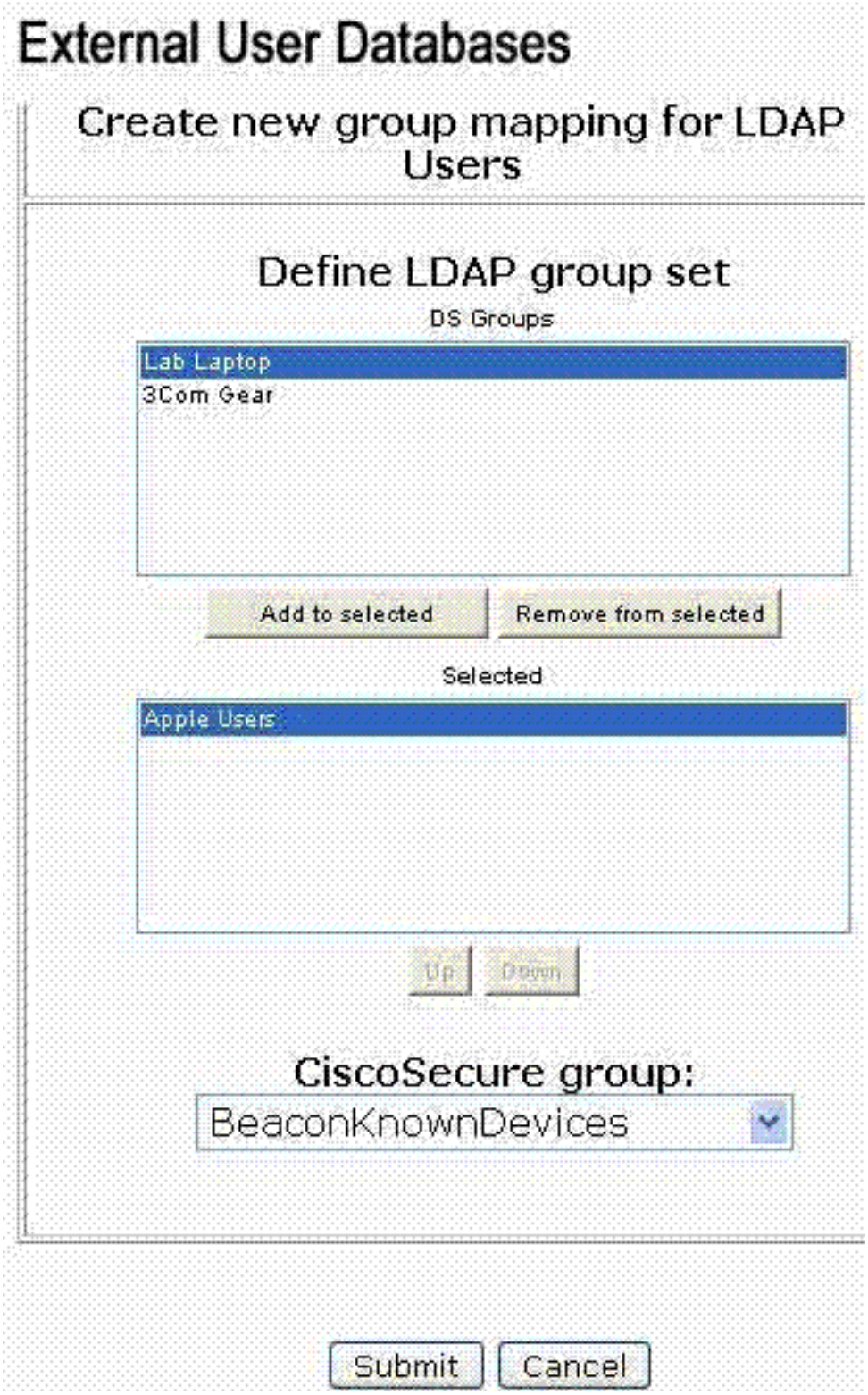


При выборе внешней базы данных пользователей Маяка, созданной ранее в этом разделе wih выбор ссылки, Beacon_Helium в предыдущем примере, это отображает окно, проиллюстрированное на рисунке 14. Обратите внимание на то, что все Профили Маяка, включенные для LDAP в конфигурации системы Маяка, как описано в первом разделе этих инструкций по конфигурации, заполнены в DS Groups, которые доступны для выбора для создания сопоставлений в ACS. Если Имена профилей Маяка, включенные для LDAP, не показывают в интерфейсе ACS, это показательно из проблемы с Конфигурацией LDAP ACS. См. инструкции по Маяку конфигурации как Внешняя база данных пользователей, выделенная ранее в этом разделе, в особенности параметры LDAP.

Обратите внимание на то, что это - интерфейс, который позволяет сопоставлять отдельных поддерживающих LDAP Профилей в Маяке с группами CiscoSecure, настроенными в ACS. Интерфейс обеспечивает сопоставление каждого отдельного Маяка поддерживающий LDAP Профиль одиночной группе CiscoSecure. В данном примере только одиночная группа была создана для известных устройств в поддерживающих LDAP Профилях Маяка: BeaconKnownDevices. Но, множественные группы, каждый с его собственными параметрами политики может быть создан для обработки успешных аутентификаций, по-другому зависящих от текущего Профиля Маяка устройства.

Например, группа CiscoSecure может быть создана для BeaconKnownIPPhones, который возвратил атрибуты VLAN, которые назначают оконечные точки в Профиле IP-телефона в Маяке к Телефонной VLAN, когда вы присоединяетесь к сети и аутентифицируетесь через MAB.

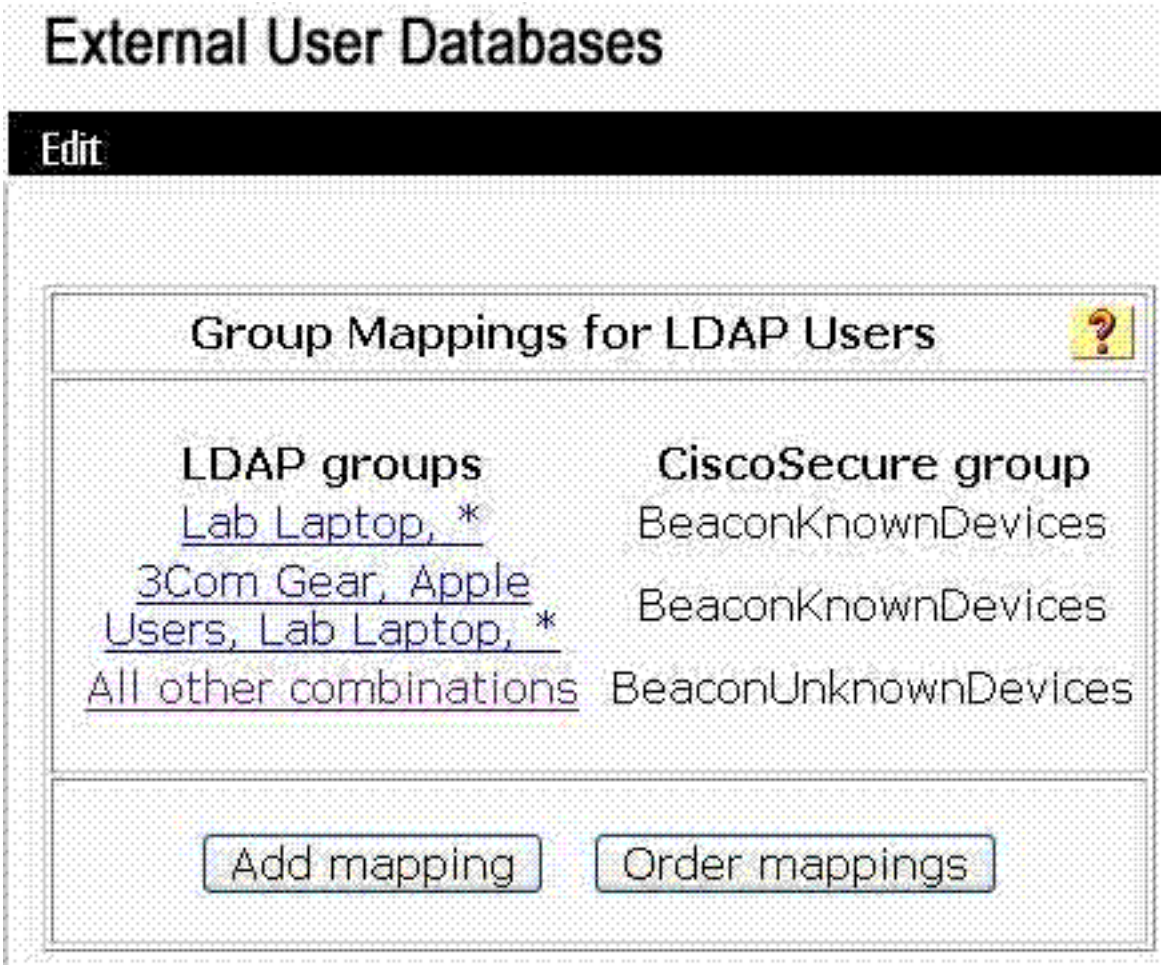
Рисунок 14: Сопоставление профиля группе



Выберите одну группу DS (Профиль маяка с включенным LDAP) и назначьте оконечные точки в том Профиле желаемой группе CiscoSecure от раскрывающегося меню. В предыдущем примере MAC-адреса в настоящее время в Пользовательском Профиле Apple в Маяке аутентифицируются через MAB, размещенного в BeaconKnownDevices, который приводит к успешной аутентификации и размещению в ПОЛЬЗОВАТЕЛЬСКОЙ LAN, когда вы присоединяетесь к сети.

Выбор подвергается, переводит распечатку в рабочее состояние текущих Сопоставлений Группы на ACS при аутентификации неизвестных пользователей на внешней базе данных пользователей Маяка.

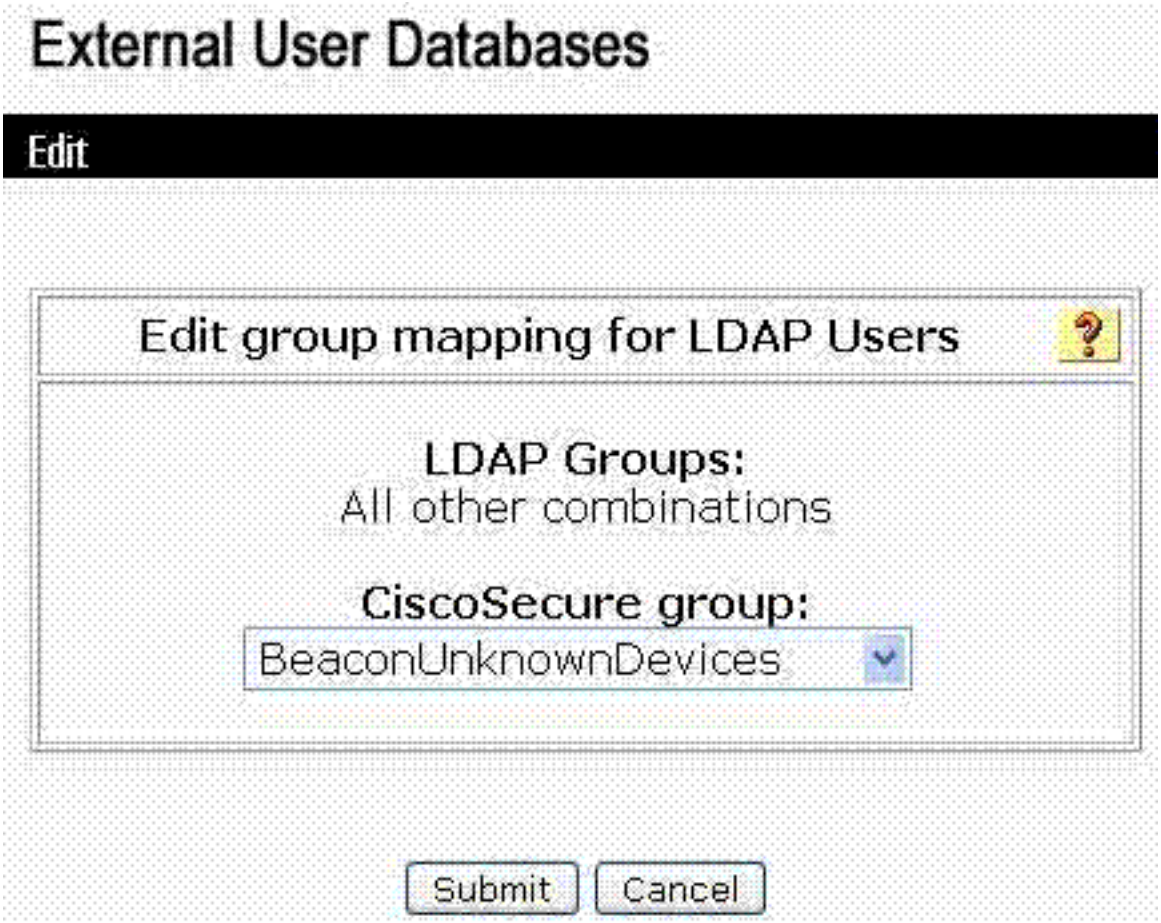
Рисунок 15: Сопоставления List Group



Обратите внимание на то, что сопоставления, явно сделанные с процедурой, ранее описанной, перечислены в этом представлении. Любая DS Groups (Маяк поддерживающие LDAP Профили) не явно сопоставленный с группой, которая включает оконечные точки, которые Маяк еще не обнаружил или разместил в падение Профиля LDAPenabled Всего другого коллектора комбинаций. По существу это позволяет оконечные точки, что Маяк не может предоставить сведения о в группу CiscoSecure, например, BeaconUnknownDevices. Как ранее выделено, эта группа может быть отключена в целом, который приводит к сбою MAB, или как в предыдущем примере, это может быть разработано для обеспечения только ограниченного подключения оконечным точкам, не известным Маяком.

Если вы нажимаете **на Всю другую** ссылку **комбинаций** для получения этого окна, **всем другим комбинациям** можно назначить CiscoSecure Group (BeaconUnkownDevices):

Рисунок 16: Присвоение Группы ко Всем другим комбинациям

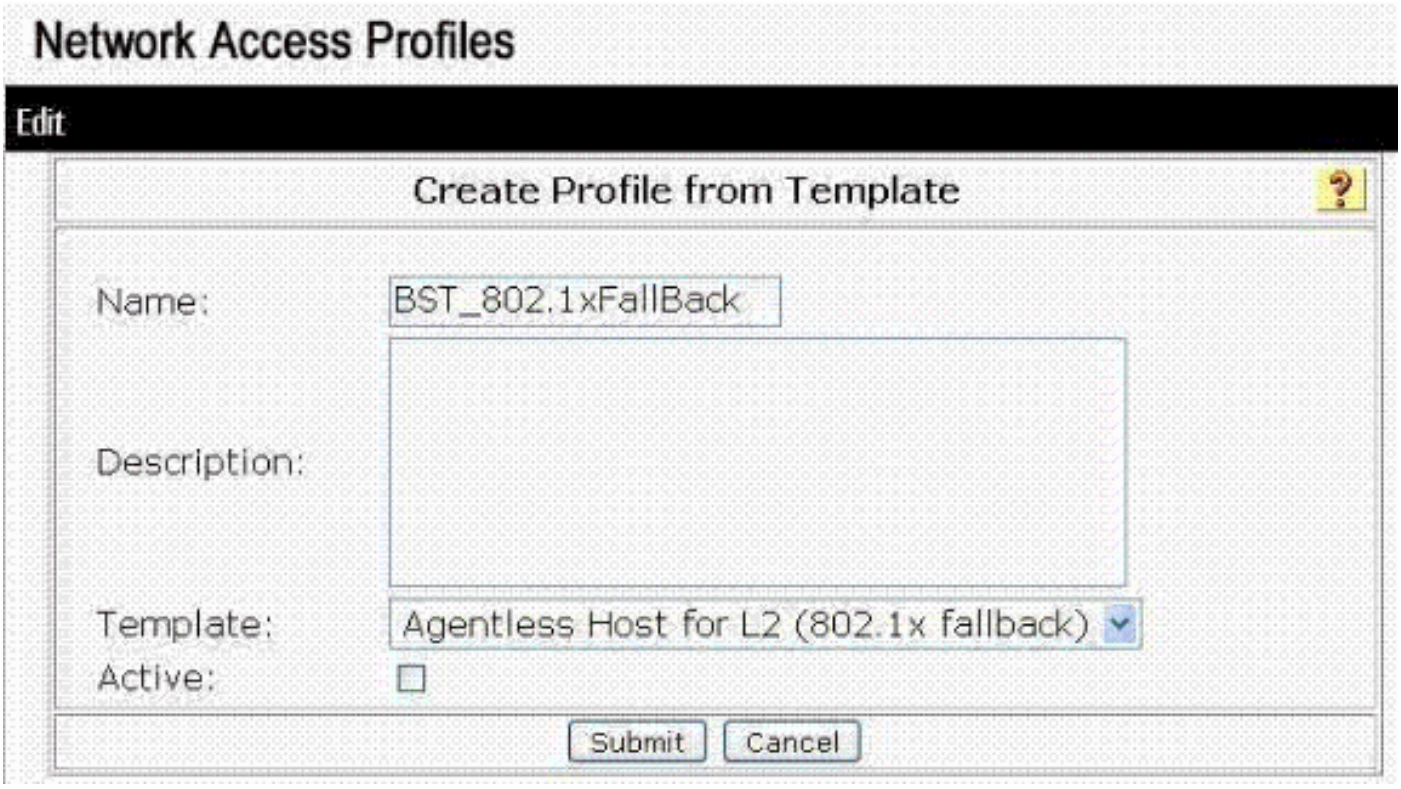


Настройка профиля доступа к сети

Последний обязательный шаг в конфигурации AcS для MAB, который будет использовать систему Профилировщика Оконечной точки Маяка в качестве прокси, является конфигурацией Профиля Доступа к сети для нейтрализации 802.1X. Выполните эти шаги, выделенные для настройки Профиля Доступа нужной сети для завершения Конфигурации AcS, таким образом, что MAB настроен и работает согласно конфигурации, завершенной ранее.

Профиль Доступа к сети, который будет добавлен, является Профилем Шаблона. Выберите **Network Access Profiles** из глобальной страницы навигации. Затем выберите **Add Template Profile** для внедрения этой проиллюстрированной формы.

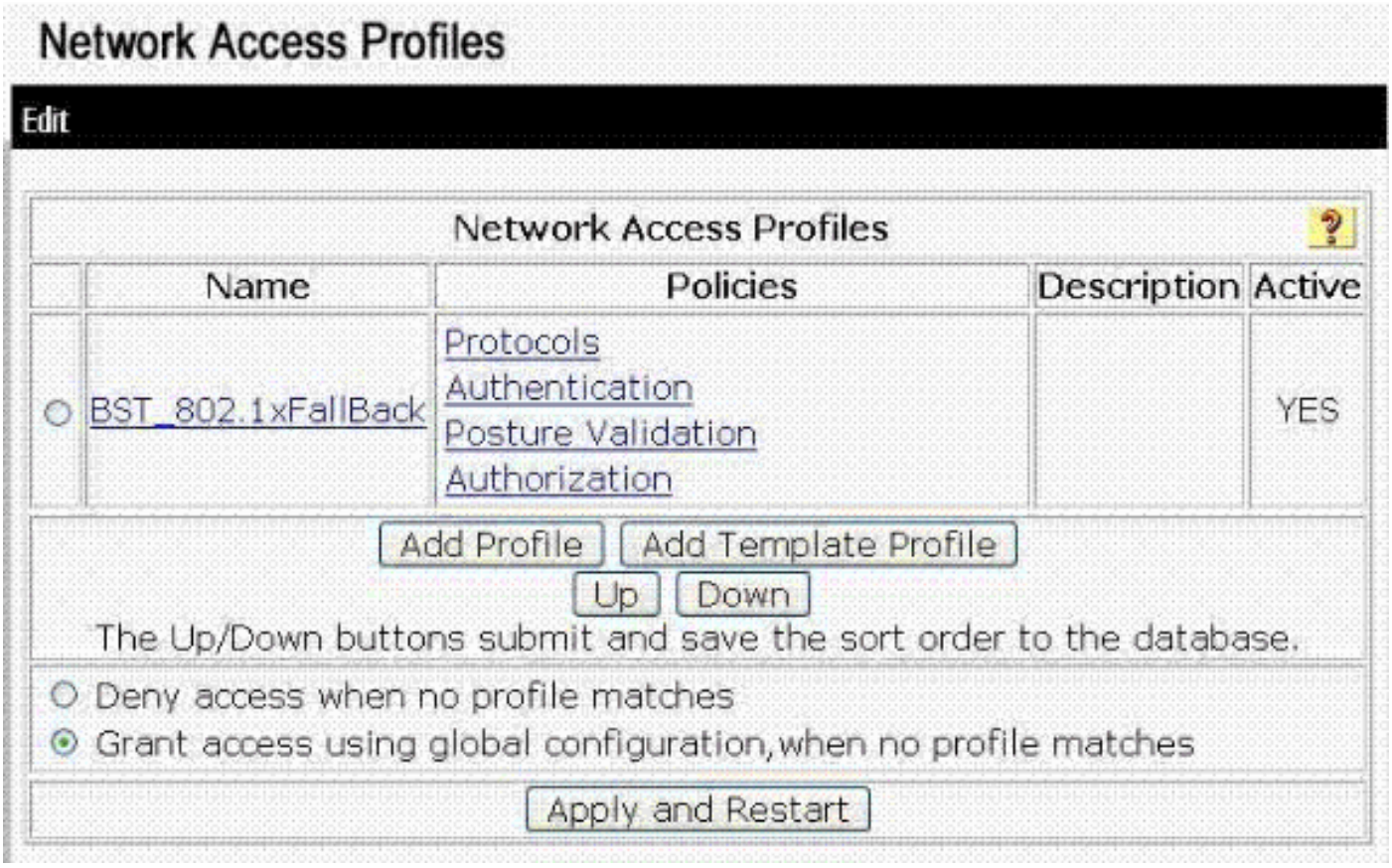
Рисунок 17: Добавьте профиль доступа к сети шаблона



Назовите Профиль Доступа к сети для включения, чтобы отличить его от других и добавить описание при желании. Шаблон для этого профиля выбран от выпадающего списка. Гарантируйте, что **Бессубъектный Хост к L2 (Нейтрализация 802.1x)** выбран, и проверьте флажок **Active**. Нажмите **кнопку отправки** по окончании для сохранения Профиля Доступа к сети.

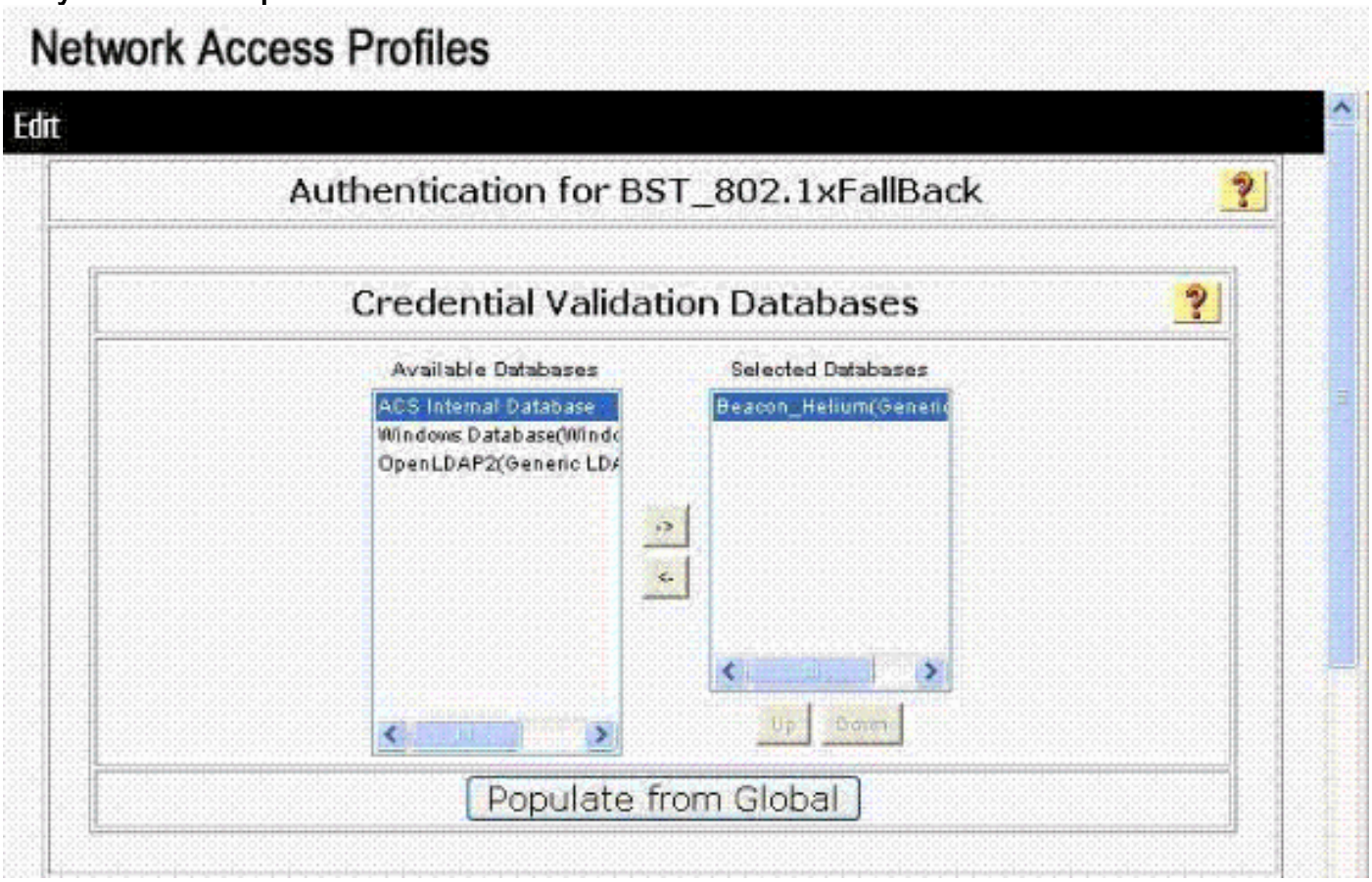
Когда вы нажимаете, подвергаются, эта форма представлена, который позволяет вам редактировать параметры для Профиля, просто созданного как показано.

Рисунок 18: Отредактируйте NAP для MAB



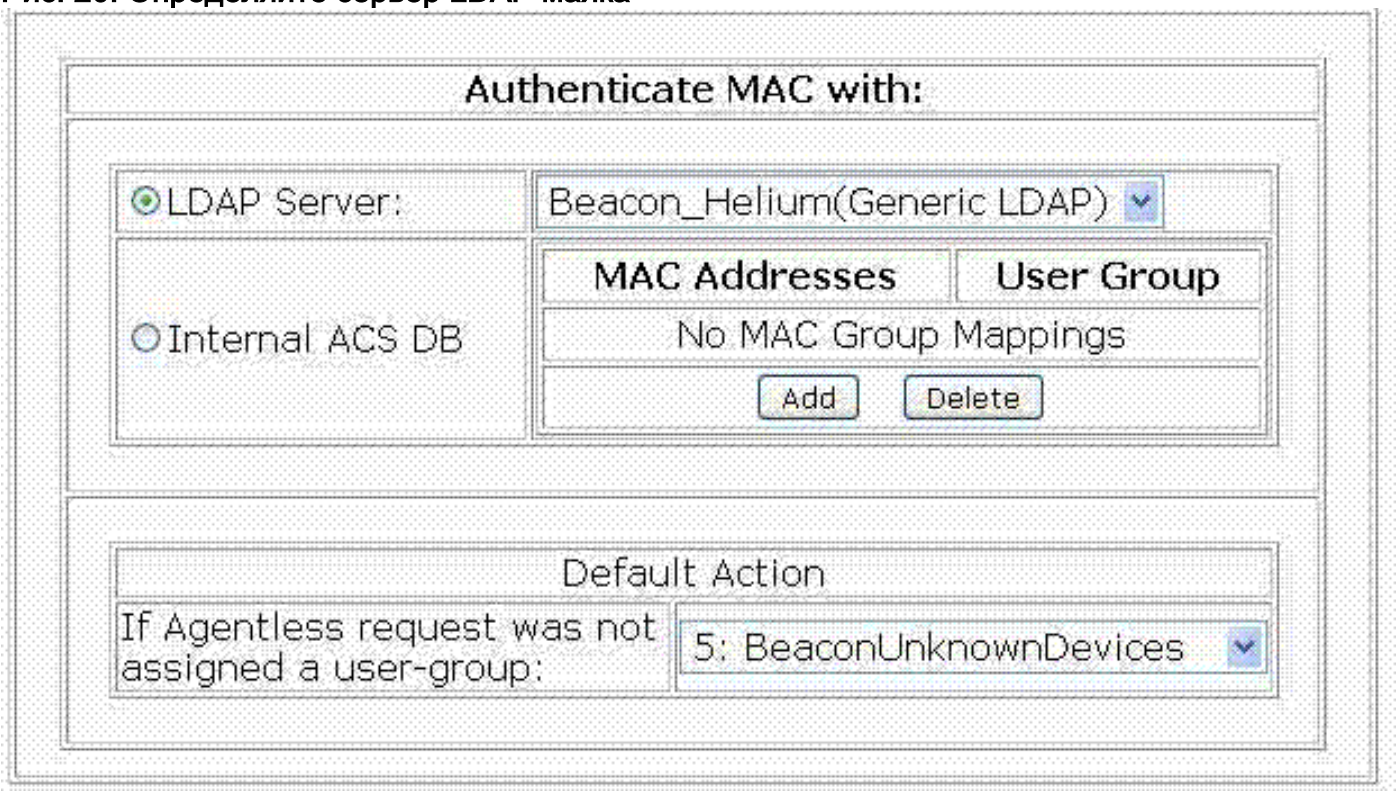
Политика аутентификации для недавно настроенного Профиля должна быть настроена для использования системы Маяка как Учетной Базы данных Проверки. Выберите Опознавательную ссылку в столбце Policies для недавно созданного Профиля Доступа к сети (802.1x FallBack в примере). Эти формы представлены.

Рисунок 19: Выберите Database for MAB



Во-первых, выберите внешнюю базу данных пользователей Маяка из Доступной таблицы баз данных и используйте**->** кнопка для добавления его к Выбранным базам данных. Прокрутите вниз к Аутентифицировать разделу MAC формы и выберите кнопку с зависимой фиксацией **LDAP Server**. Выберите базу данных **Маяка** из выпадающего списка. Наконец, выберите группу **BeaconUnknownDevice** для действия по умолчанию как показано на следующем рисунке.

Рис. 20: Определяйте сервер LDAP маяка



Этот шаг завершает требуемую конфигурацию AcS для Обхода Проверки подлинности MAC с Маяком как Внешняя база данных пользователей. Перезапустите сервис ACS, чтобы гарантировать, что все изменения конфигурации посвящают себя рабочей конфигурации.

Если коммутаторы настроены правильно, система должна быть готова протестировать MAB. Оконечную точку в настоящее время в поддерживающем LDAP Профиле Маяка можно разъединить от сети и повторно допустить с параметрами Политики, заданными для группы BeaconKnownDevices.

Конфигурация коммутатора для обхода проверки подлинности MAC

Конфигурация коммутатора Thid предоставляет пример конфигурации для аутентификации 802.1X с Обходом Проверки подлинности MAC, включенным, и перевод по службе динамической LAN потребовал для применения, атрибуты RADIUS возвратились из ACS.

Коммутатор
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
```

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Дополнительные сведения

- Cisco NAC Appliance (Clean Access)
- Cisco Secure Access Control Server for Windows
- Cisco Systems – техническая поддержка и документация