Пример настройки RSA SecureID с контроллерами беспроводной сети и Cisco Secure ACS

Содержание

Введение
Предварительные условия
Требования
Используемые компоненты
Условные обозначения
Общие сведения
Настройка
Конфигурация узла агента
Использование Cisco Secure ACS как сервер RADIUS
Использование менеджера аутентификации RSA 6.1 серверов RADIUS
Конфигурация агента аутентификации
Настройте ACS Cisco
Настройте конфигурацию контроллера беспроводной локальной сети Cisco для 802.1x
802.11 Конфигурация беспроводного клиента
Типичные ошибки
Дополнительные сведения

Введение

Этот документ объясняет, как установить и настроить протокол Cisco LWAPP (LWAPP) - способные AP и Контроллеры беспроводной локальной сети (WLC), а также сервер Cisco Secure Access Control Server (ACS), который будет использоваться в SecurID RSA, аутентифицировал среду WLAN. RSA специфичные для SecurID руководства по внедрению может быть найден в www.rsasecured.com.

Предварительные условия

Требования

Убедитесь, что вы обеспечили выполнение следующих требований, прежде чем попробовать эту конфигурацию:

- Знание WLC и как настроить основные параметры WLC.
- Знание о том, как настроить профиль Клиента беспроводной связи Cisco с помощью служебной программы рабочего стола Aironet (ADU).

- Имейте функциональное знание Cisco Secure ACS.
- Имейте базовые знания о LWAPP.
- Имейте основное понимание сервисов Active Directory (AD) Microsoft Windows, а также понятия DNS и контроллер домена.**Примечание:** Прежде чем вы будете делать попытку этой конфигурации, будете гарантировать, что ACS и Сервер - диспетчер Аутентификации RSA находятся в том же домене, и их системные часы точно синхронизируются. При использовании Microsoft Windows AD Services обратитесь к документации microsoft для настройки ACS и Сервера - диспетчера RSA в том же домене. См. Настраивают Базу данных Active Directory и Пользователя Windows для связанных сведений.

Используемые компоненты

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

- Менеджер аутентификации RSA 6.1
- Агент аутентификации RSA 6.1 для Microsoft Windows
- Cisco Secure ACS 4.0 (1) сборка 27**Примечание:** Сервер RADIUS, который включен, может использоваться вместо ACS Cisco. См. документацию RADIUS, которая была включена с Менеджером Аутентификации RSA о том, как настроить сервер.
- WLC Cisco и облегченные точки доступа для выпуска 4.0 (версия 4.0.155.0)

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

Система SecurID RSA является решением для проверки подлинности пользователя с двумя факторами. Используемый в сочетании с Менеджером Аутентификации RSA и Агентом Аутентификации RSA, аутентификатор RSA SecurID требует, чтобы пользователи определили себя с помощью механизма двухфакторной аутентификации.

Каждый - код SecurID RSA, случайное число, генерируемое каждые 60 секунд на аутентификаторе RSA SecureID. Другой Персональный идентификационный номер (PIN).

Аутентификаторы RSA SecurID так же просты использовать как ввод пароля. Каждому конечному пользователю назначают аутентификатор RSA SecurID, который генерирует код с одним разовым использованием. При входе пользователь просто вводит этот номер и секретный PIN, который будет успешно аутентифицироваться. Как дополнительное преимущество, аппаратные устройства аутентификации RSA SecurID обычно предварительно запрограммированы, чтобы быть полностью функциональными на получение.

Эта демонстрация флэш-памяти объясняет, как использовать аутентификатор RSA secureID: демонстрация RSA.

Через SecurID RSA Готовая программа, WLC Cisco и серверы Cisco Secure ACS поддерживают Проверку подлинности с помощью secureid RSA прямо из коробки. Программное обеспечение агента Аутентификации RSA перехватывает запросы доступа, или локальный или удаленный, от пользователей (или группы пользователей) и направляет их к Менеджеру Аутентификации RSA программа для аутентификации.

Программное обеспечение менеджера Аутентификации RSA является компонентом управления решения RSA SecurID. Это используется, чтобы проверить запросы аутентификации и централизованно администрировать политику аутентификации для корпоративных сетей. Это работает в сочетании с Программным обеспечением агента Аутентификации RSA и аутентификаторами RSA SecurID.

В этом документе Сервер Cisco ACS используется в качестве Агента Аутентификации RSA путем установки программного обеспечения агента на нем. WLC является Сервер доступа к сети (NAS) (клиент AAA) который в свою очередь вперед аутентификации клиента к ACS. Документ демонстрирует понятия и настройку с помощью аутентификации клиента Защищенного расширяемого протокола аутентификации (PEAP).

Для обучения об аутентификации PEAP обратитесь к Cisco Защищенный Расширяемый протокол аутентификации.

Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Эти конфигурации используются в данном документе:

- Конфигурация узла агента
- Конфигурация агента аутентификации

Конфигурация узла агента

Использование Cisco Secure ACS как сервер RADIUS

Для упрощения связи между Cisco Secure ACS и Менеджером Аутентификации RSA / Устройство SecurID RSA, запись Узла агента должна быть добавлена к Базе данных диспетчера Аутентификации RSA. Запись Узла агента определяет Cisco Secure ACS в своей базе данных и содержит информацию о связи и шифровании.

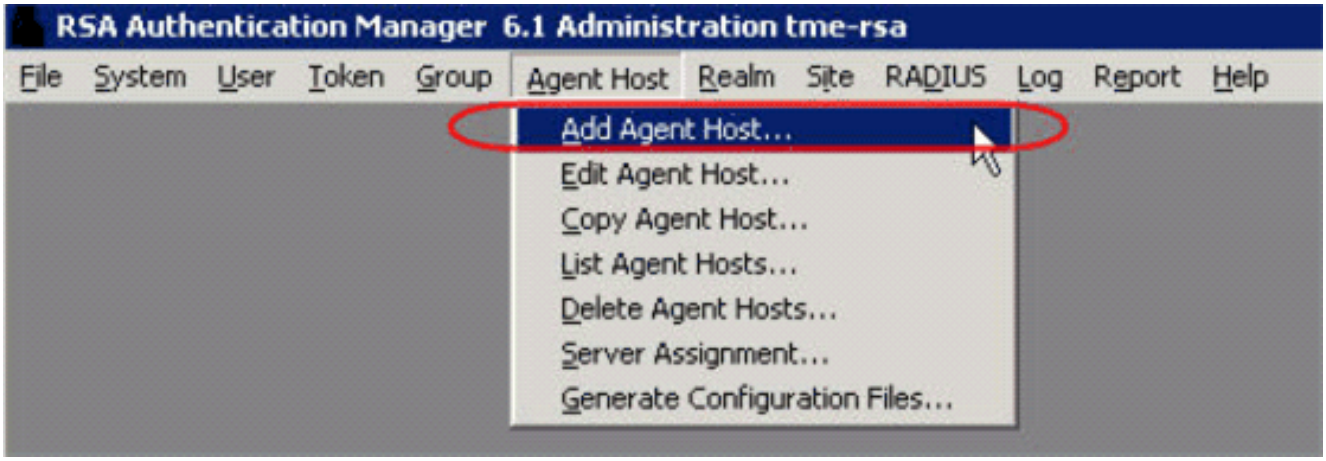
Для создания записи Узла агента вам нужна эта информация:

- Имя хоста сервера Cisco ACS
- IP-адреса для всех сетевых интерфейсов Сервера Cisco ACS

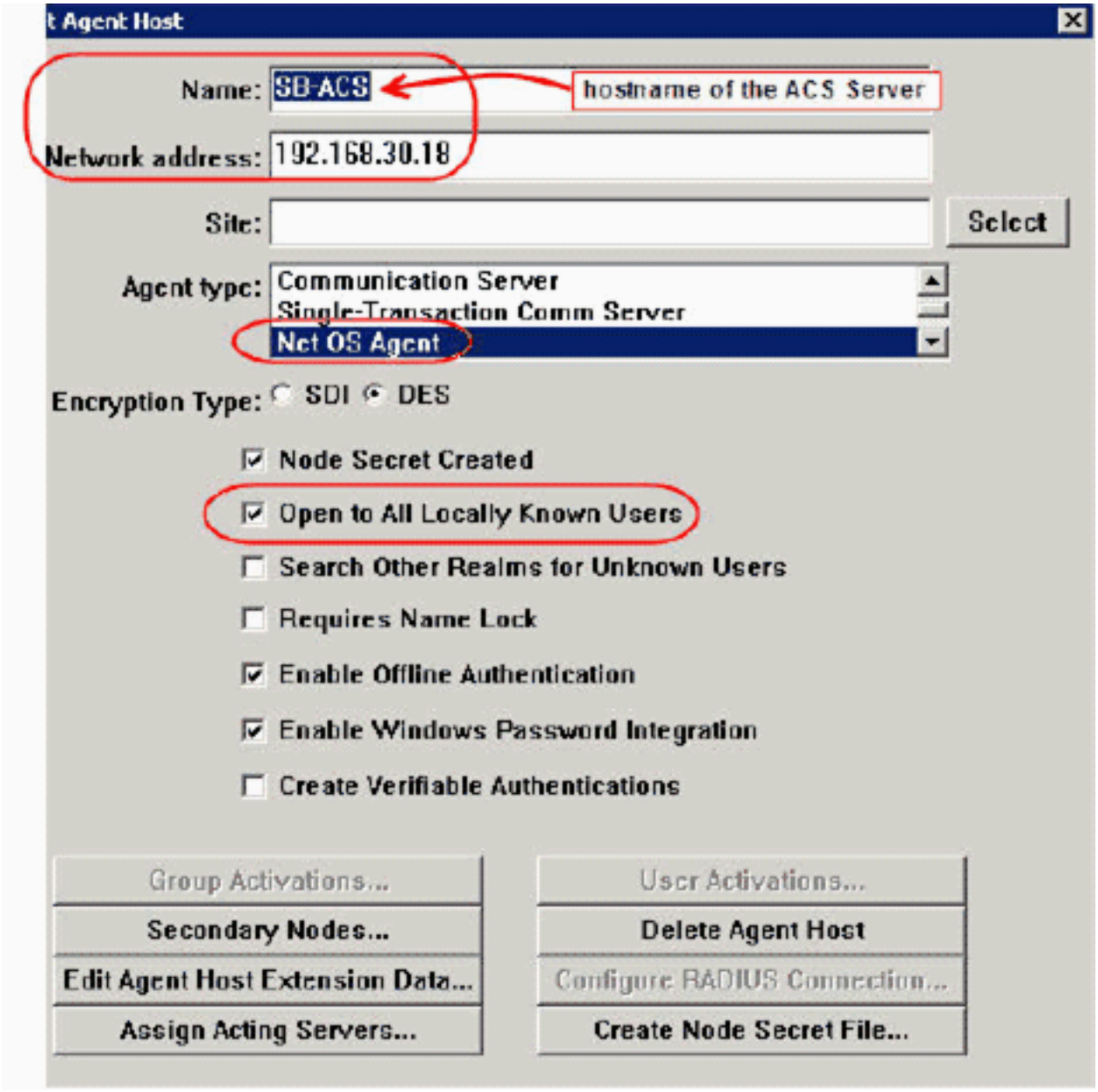
Выполните следующие действия:

1. Откройте менеджера Аутентификации RSA Хоста Моуда приложение.
2. Выберите **Agent Host> Add Agent**

Host.



Будет отображено следующее окно:



3. Введите соответствующую информацию для Названия Сервера Cisco ACS и Сетевого адреса. Выберите **NetOS** для Агента вводят и проверяют флажок для **Открытого для Всех Локально Известных Пользователей**.
4. **Нажмите кнопку ОК.**

Использование менеджера аутентификации RSA 6.1 серверов RADIUS

Для упрощения связи между WLC Cisco и Менеджером Аутентификации RSA, запись Узла агента должна быть добавлена к Базе данных диспетчера Аутентификации RSA и Базе данных сервера RADIUS. Запись Узла агента определяет WLC Cisco в своей базе данных и содержит информацию о связи и шифровании.

Для создания записи Узла агента вам нужна эта информация:

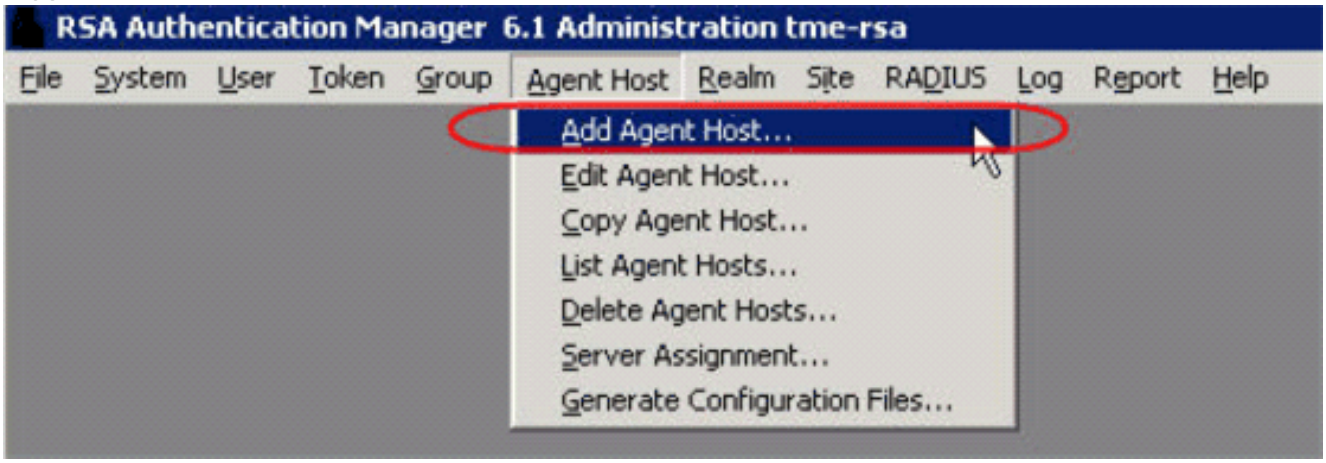
- Имя хоста WLC
- Управления IP-адресами WLC
- Тайна RADIUS, которая должна совпасть с тайной RADIUS на WLC Cisco

При добавлении Записи Узла агента роль WLC настроена как Сервер подключения. Эта установка используется Менеджером Аутентификации RSA, чтобы определить, как произойдет связь с WLC.

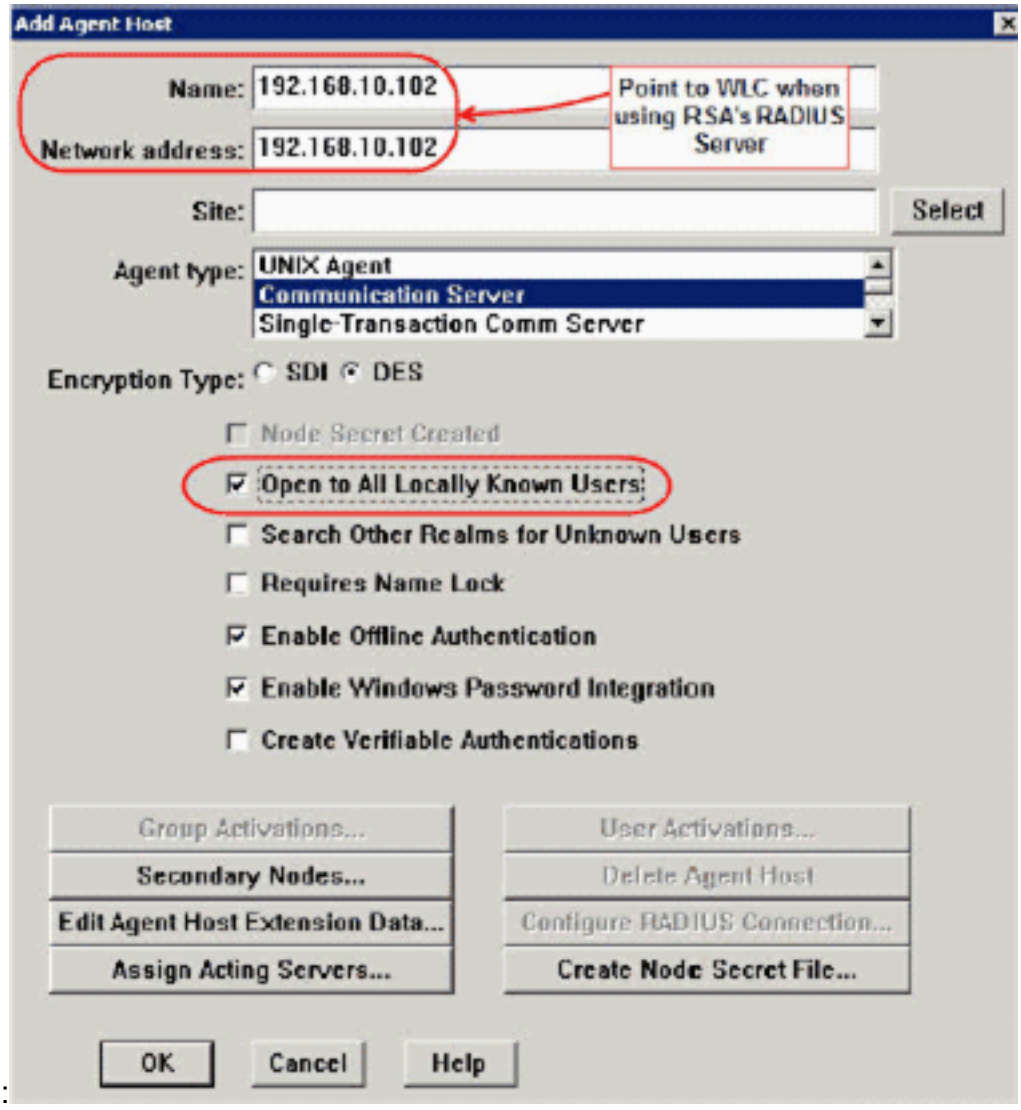
Примечание: Имена хоста в Менеджере Аутентификации RSA / Устройство SecurID RSA должны решить к действительным IP - адресам на локальной сети.

Выполните следующие действия:

1. Откройте менеджера Аутентификации RSA Хоста Моуда приложение.
2. Выберите **Agent Host> Add Agent Host**.

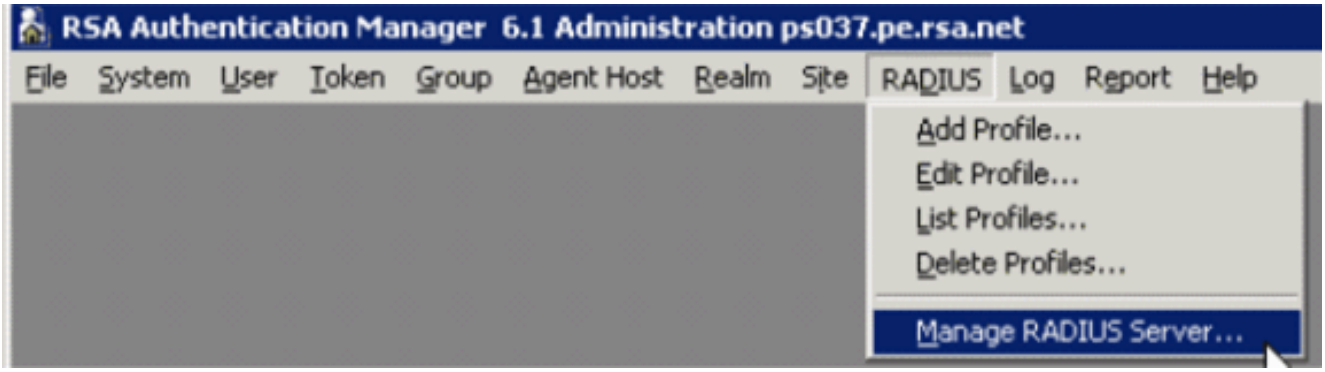


Будет отображено следующее



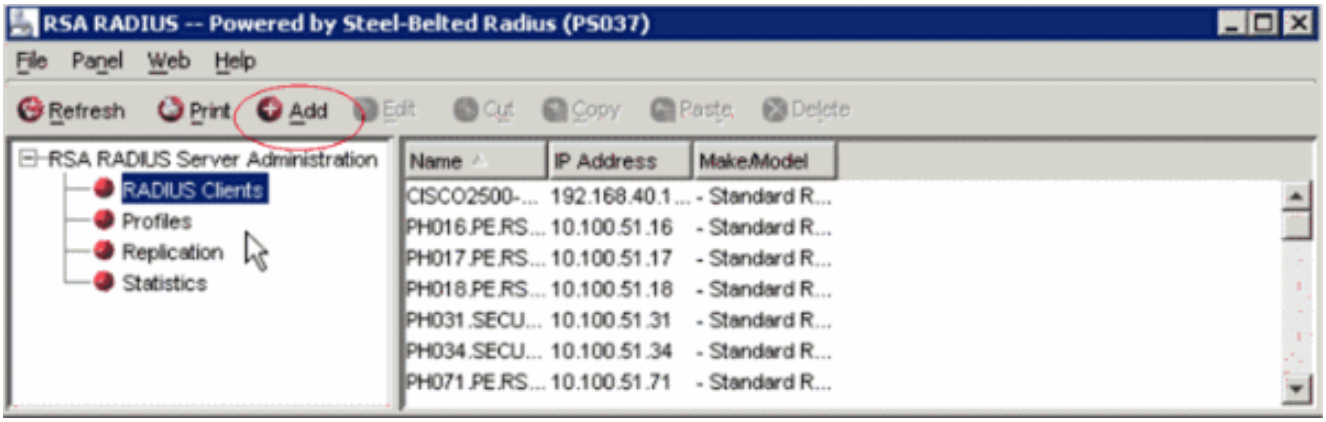
окно:

3. Введите соответствующую информацию для имени хоста WLC (разрешимый FQDN, если необходимый) и Сетевой адрес. Выберите тип **Communication Server for Agent** и проверьте флажок для **Открытого для Всех Локально Известных Пользователей**.
4. **Нажмите кнопку ОК.**
5. Из меню выберите **RADIUS> Manage RADIUS Server**.

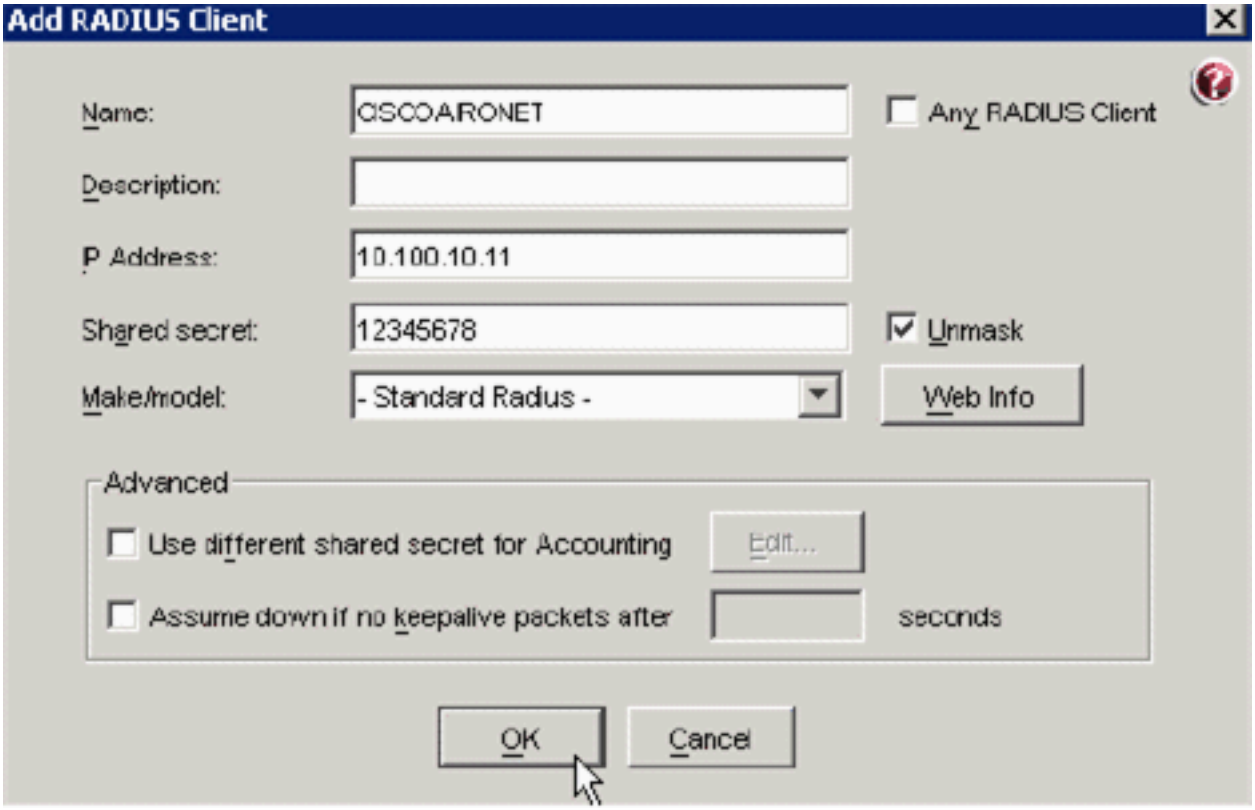


Окно нового правительства открывается.

6. В этом окне выберите **RADIUS Clients**, затем **нажмите Add**.



7. Введите соответствующую информацию для WLC Cisco. Общий секретный ключ должен совпасть с общим секретным ключом, определенным на WLC Cisco.



8. **Нажмите кнопку OK.**

Конфигурация агента аутентификации

Эта таблица представляет функциональность Агента Аутентификации RSA ACS:

Partner Integration Overview	
Authentication Methods Supported	Native RSA SecurID Authentication, RADIUS, Both
List Library Version Used	5.0.3
RSA Authentication Manager Name Locking	Yes
RSA Authentication Manager Replica Support	Full Replica Support
Secondary RADIUS Server Support	N/A
Location of Node Secret on Agent	'None stored'
RSA Authentication Agent Host Type	Communication Server
RSA SecurID User Specification	Designated Users, All Users, Default Method
RSA SecurID Protection of Administrative Users	No
RSA Software Token API Integration	No
Use of Cached Domain Credentials	No

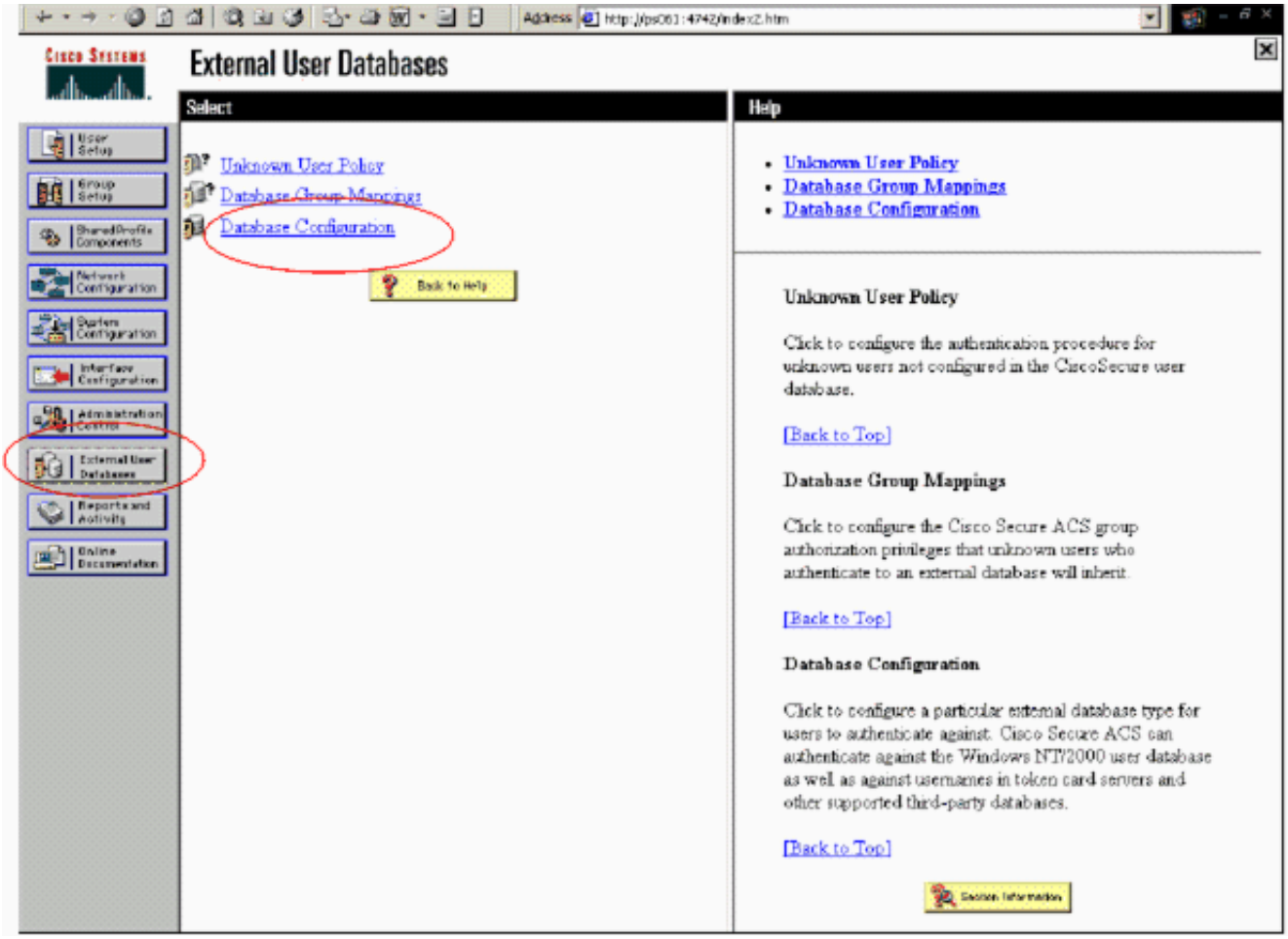
Примечание: См. документацию RADIUS, которая была включена с Менеджером Аутентификации RSA о том, как настроить сервер RADIUS, если это - сервер RADIUS, который будет использоваться.

Настройте ACS Cisco

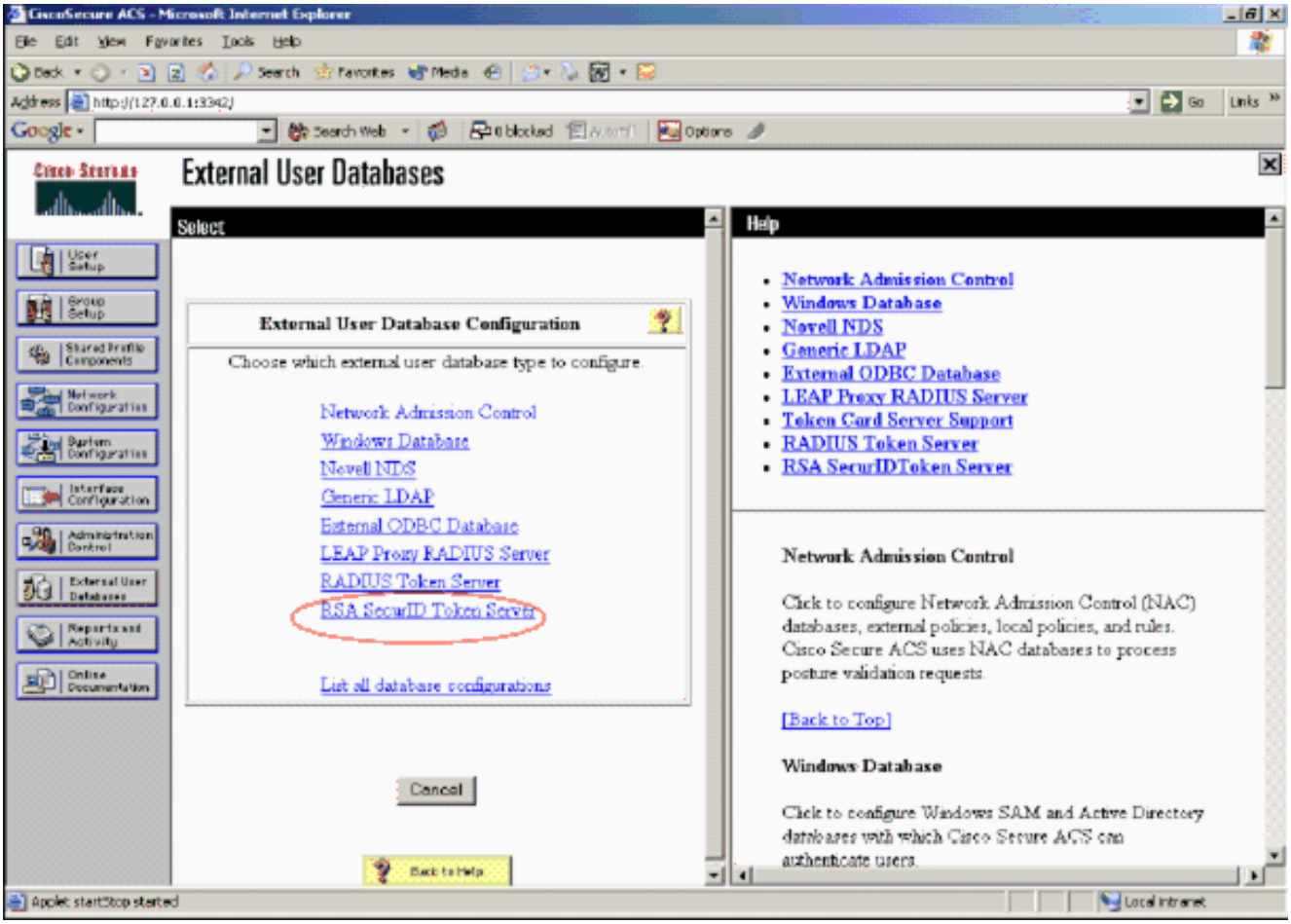
Активируйте проверку подлинности с помощью secureid RSA

Cisco Secure ACS поддерживает Проверку подлинности с помощью secureid RSA пользователей. Выполните эти шаги для настройки Cisco Secure ACS для аутентификации пользователей с Опознавательным Менеджером 6.1:

1. Установите Агента Аутентификации RSA 5.6 или позже для Windows в той же системе как сервер Cisco Secure ACS.
2. Проверьте подключение путем выполнения функции Test Authentication Агента аутентификации.
3. Скопируйте aceclnt.dll файл от каталога **c:\Program Files\RSA Security\RSA Authentication Manager\prog** сервера RSA до каталога **c:\WINNT\system32** сервера ACS.
4. В панели навигации нажмите **External User Database**. Затем нажмите **Database Configuration** на странице External Database.

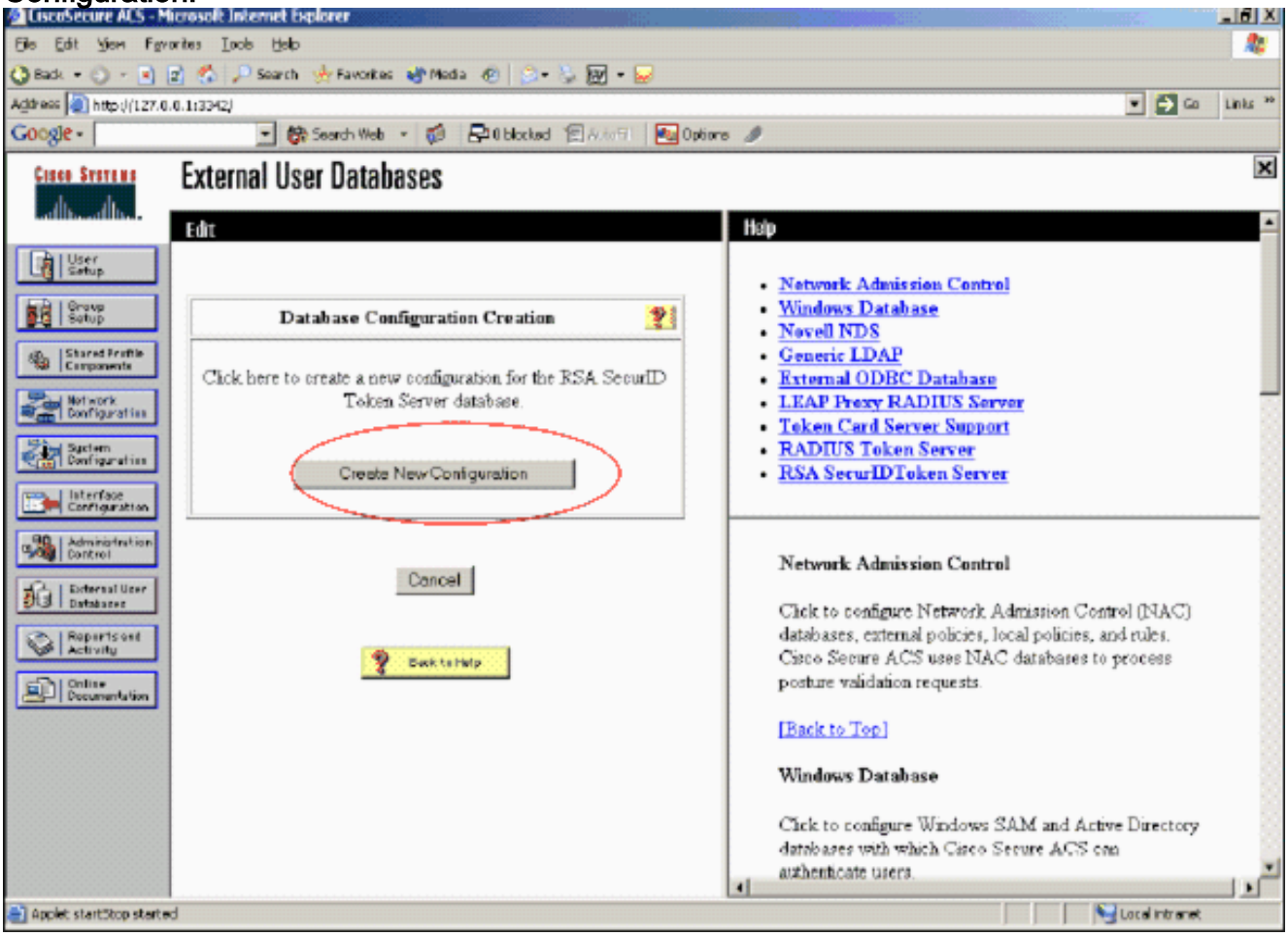


5. На странице External User Database Configuration нажмите **RSA SecurID Token Server**.

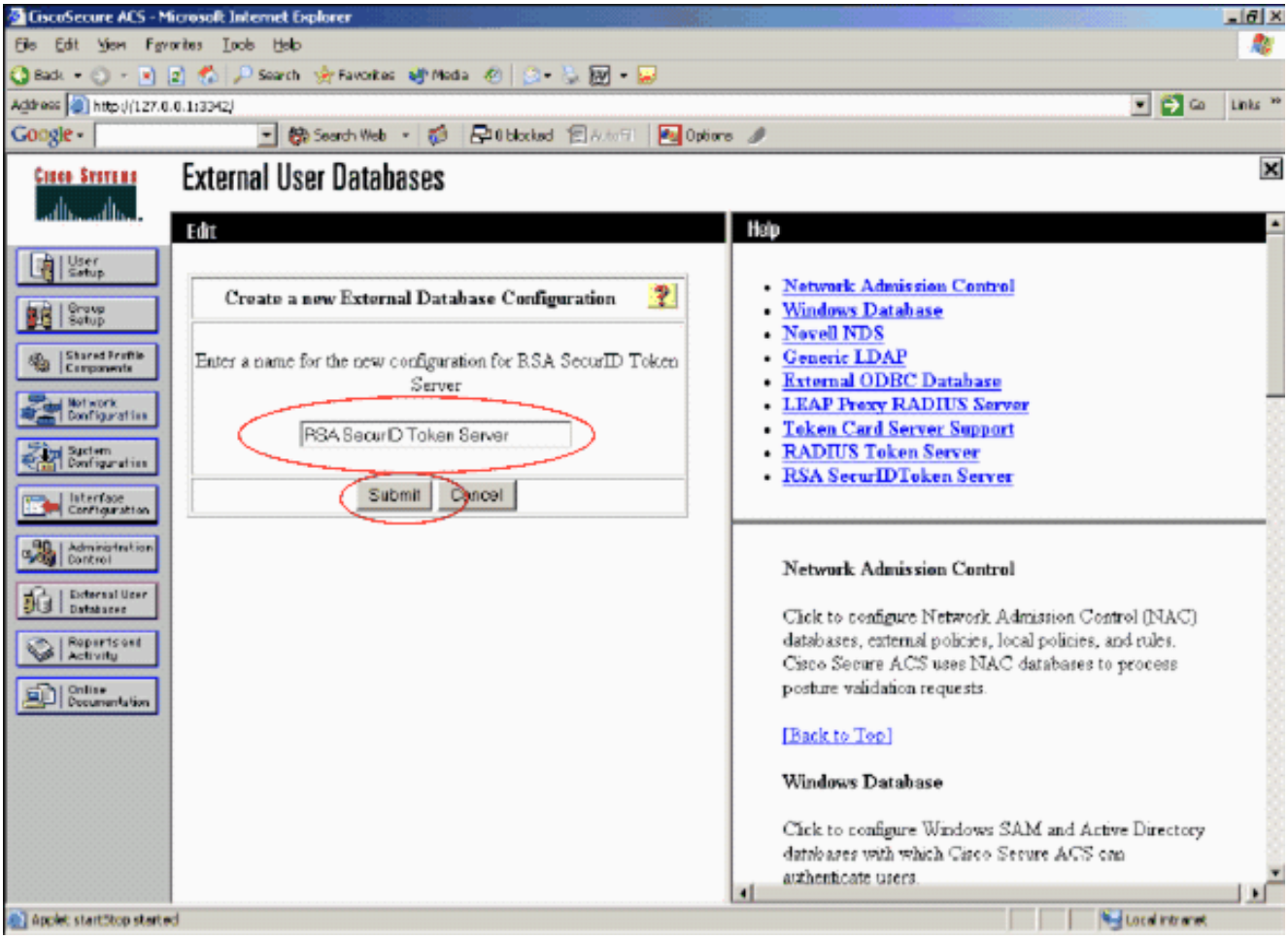


6. **Нажмите кнопку Create New**

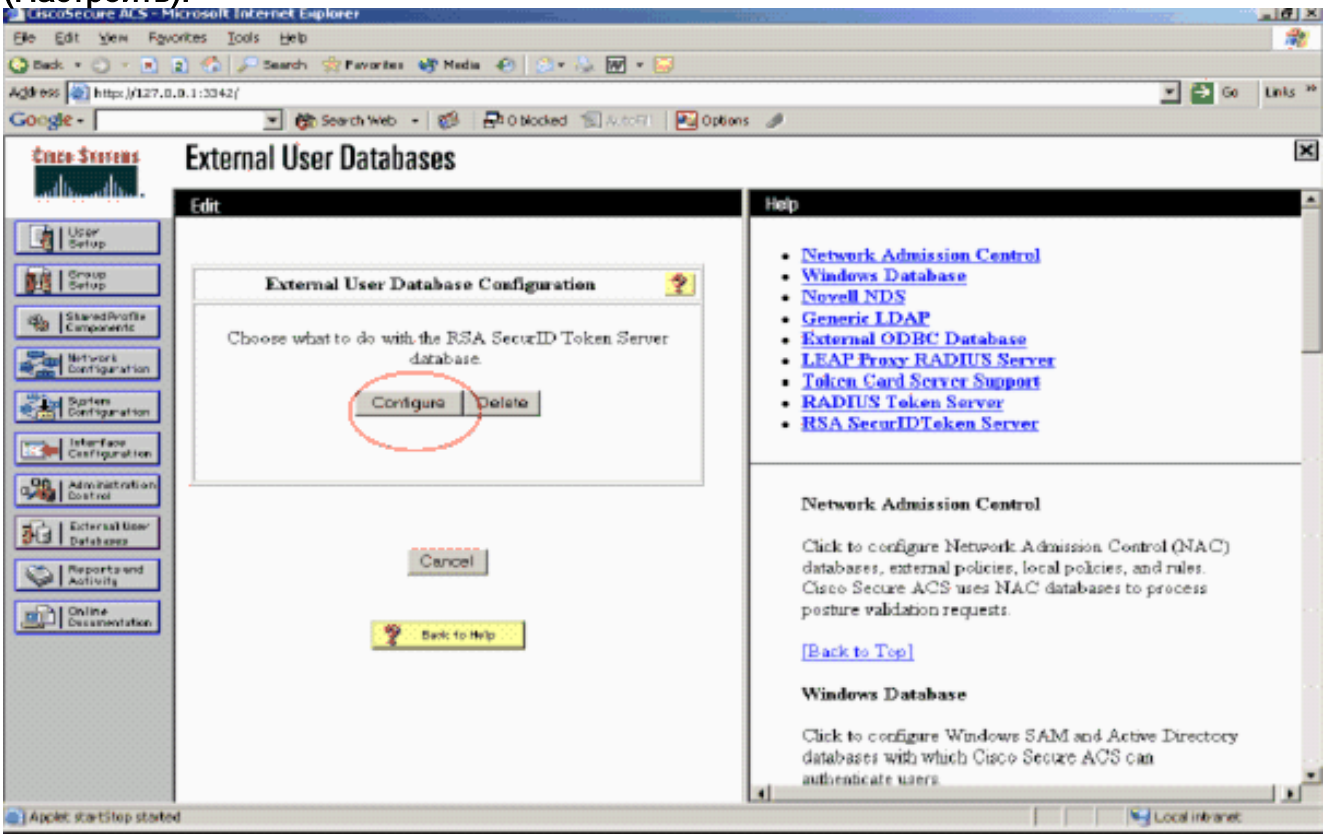
Configuration.



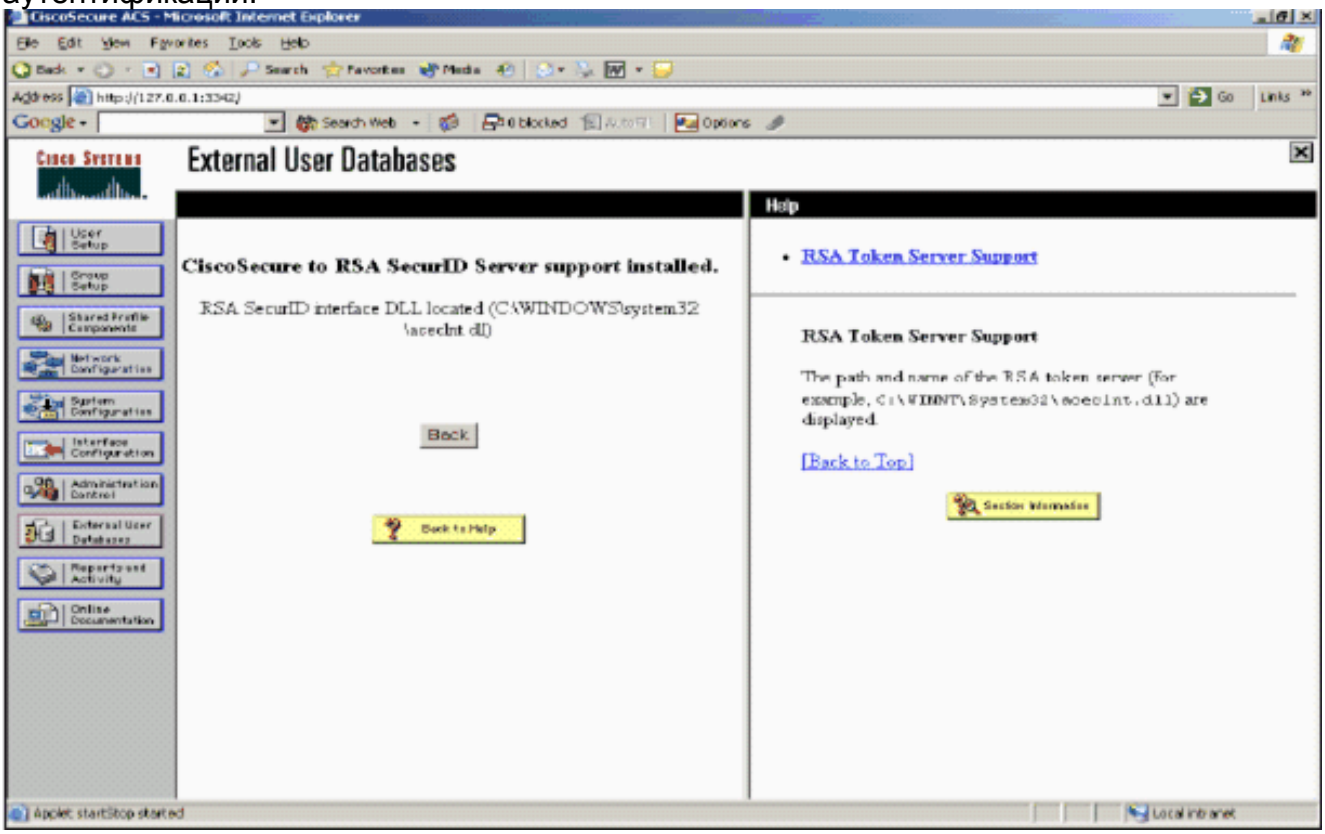
7. Введите имя, затем нажмите **Submit**.



8. Нажмите кнопку Configure (Настроить).



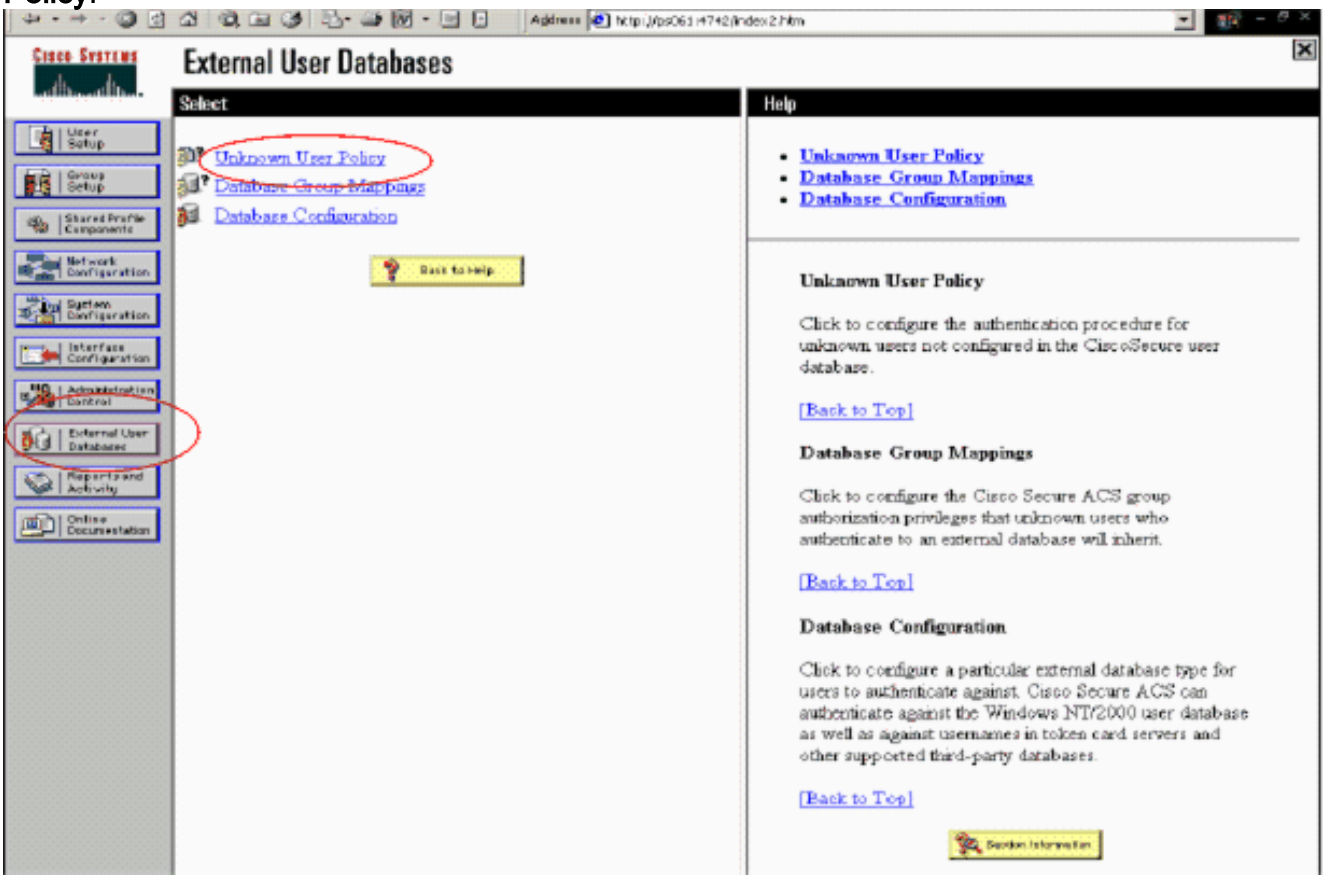
Cisco Secure ACS отображает название символического сервера и пути к DLL средства проверки подлинности. Эта информация подтверждает, что Cisco Secure ACS может связаться с Агентом Аутентификации RSA. Можно добавить внешнюю базу данных пользователей SecurID RSA к Неизвестной политике пользователя или назначить определенные учетные записи пользователя использовать эту базу данных для аутентификации.



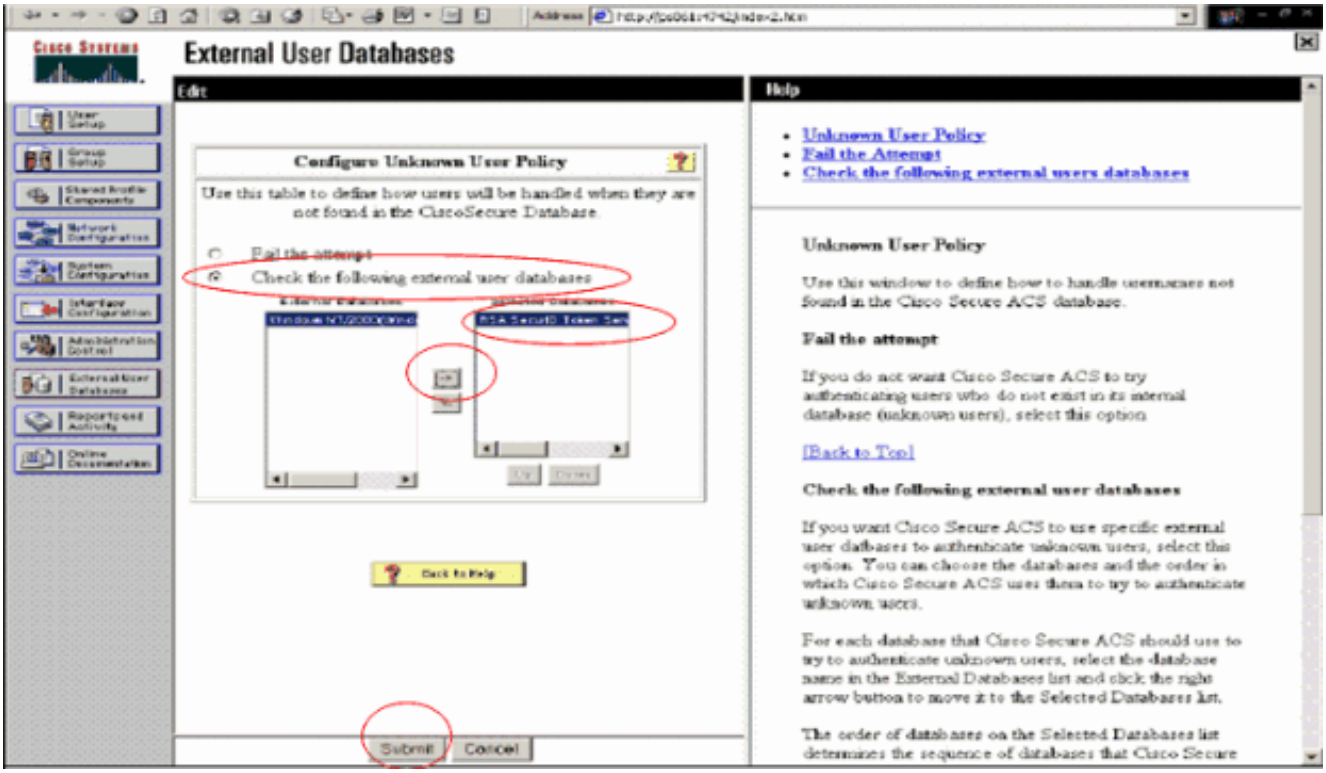
Добавьте/Настройте Проверку подлинности с помощью secureid RSA к Своей Неизвестной политике пользователя

Выполните следующие действия:

1. В панели навигации ACS нажмите **External User Database> Unknown User Policy**.



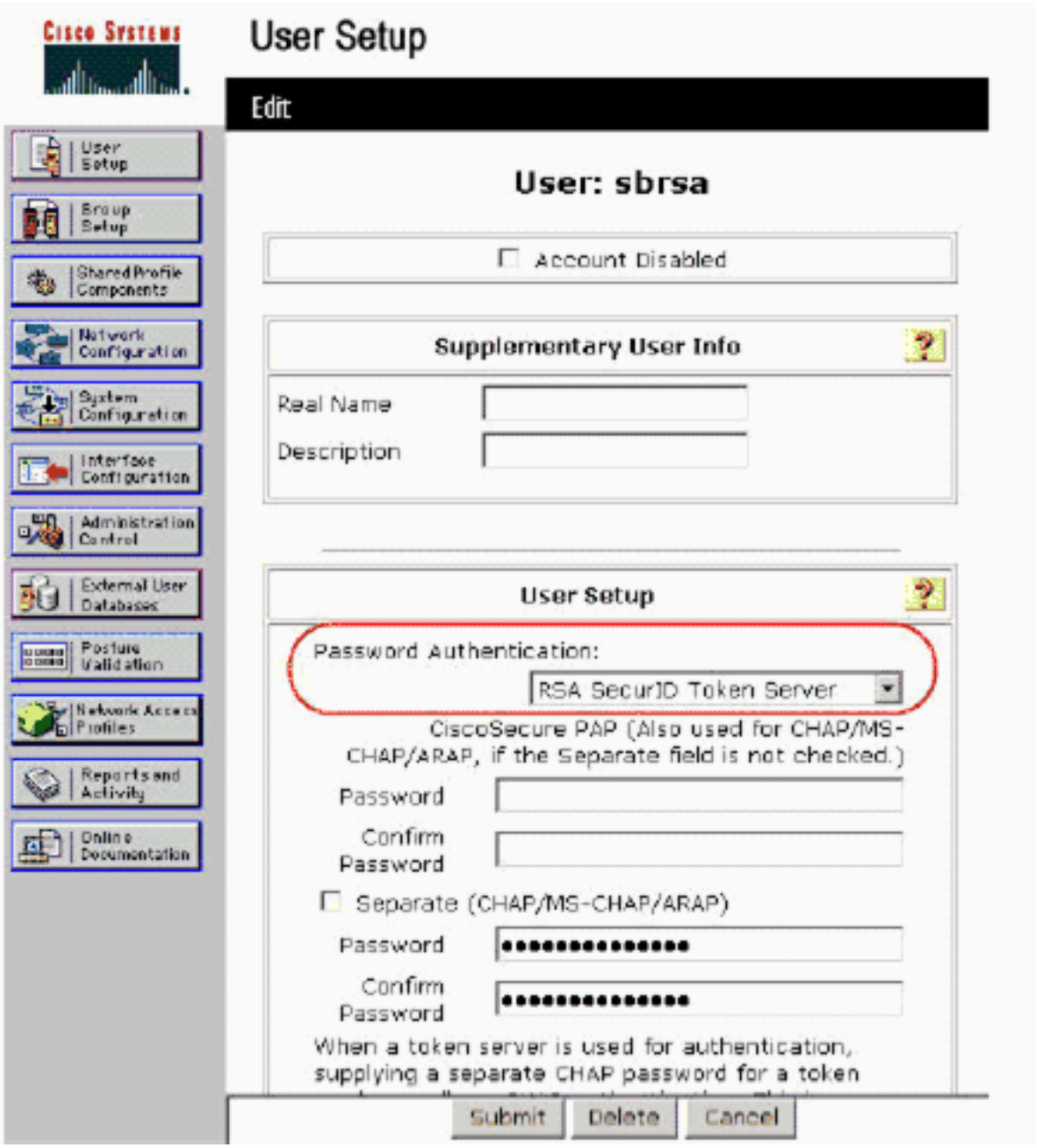
2. На странице **Unknown User Policy** выберите **Check следующие внешние базы данных пользователей**, выделите **Символический сервер SecurID RSA** и переместите его в коробку Выбранных баз данных. **Затем щелкните Submit (Отправить).**



Добавьте/Настройте Проверку подлинности с помощью secureid RSA для Определенных Учетных записей пользователя

Выполните следующие действия:

1. Нажмите **User Setup** от основного GUI Admin ACS. Введите имя пользователя и **нажмите Add** (или выберите существующего пользователя, которого вы хотите модифицировать).
2. При Настройке пользователя> Проверка подлинности с помощью пароля, выберите **RSA SecurID Token Server**. **Затем щелкните Submit (Отправить).**

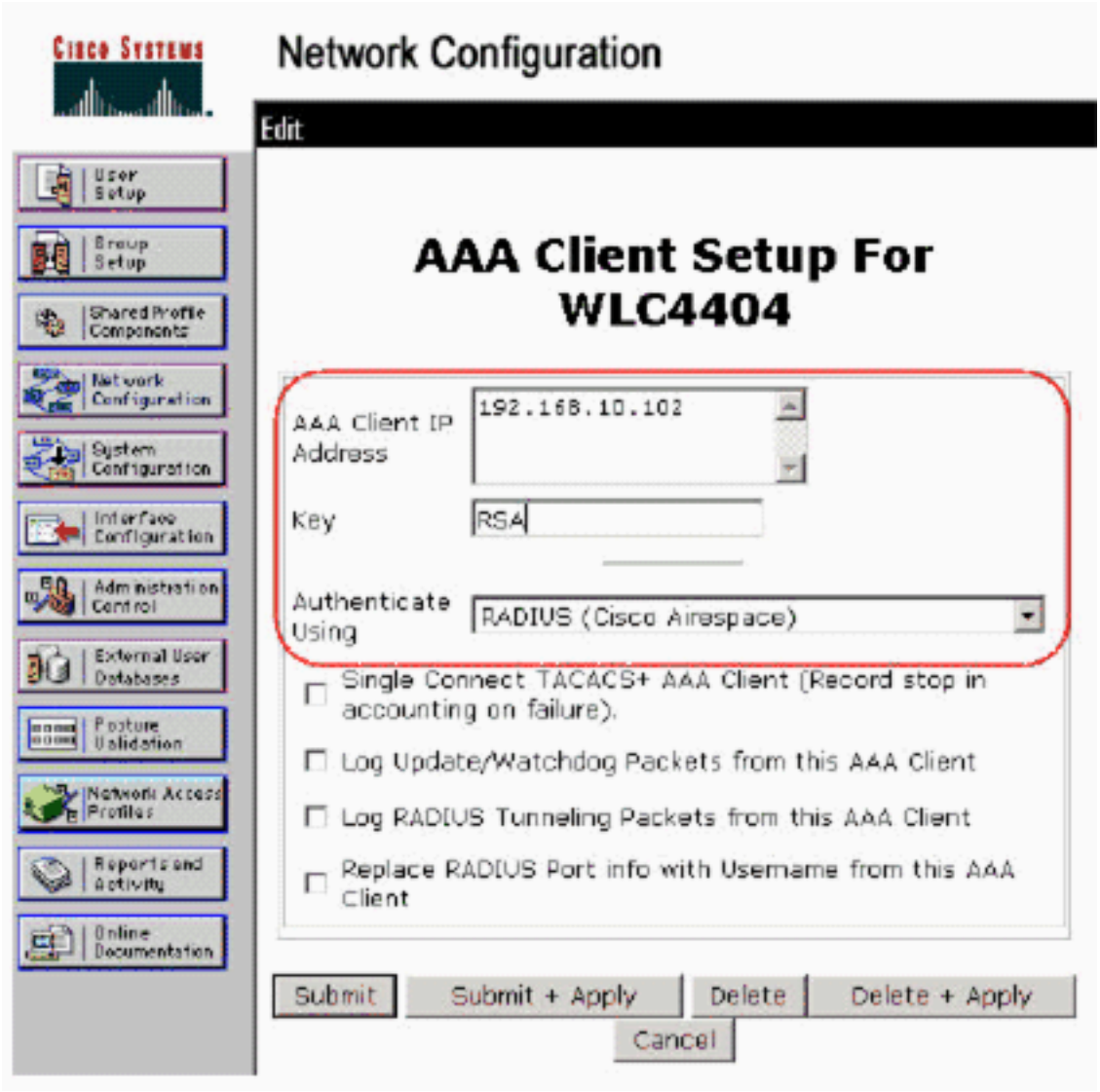


[Добавьте КЛИЕНТА RADIUS в ACS Cisco]

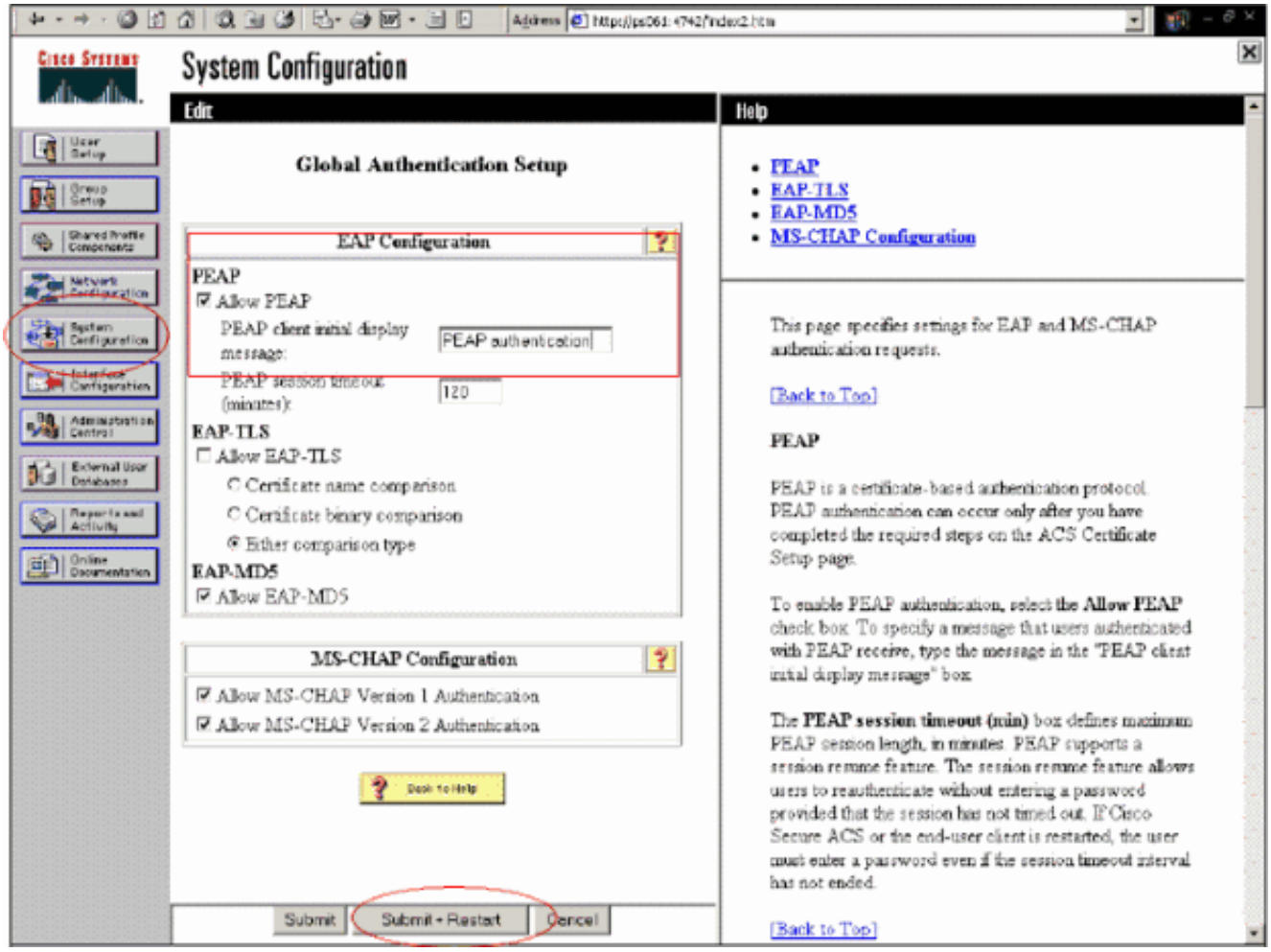
Для установки Сервера Cisco ACS будут нужны IP-адреса WLC для служения в качестве NAS для передачи клиентских аутентификаций PEAP к ACS.

Выполните следующие действия:

1. Под **Конфигурацией сети** добавляйте/редактируйте клиента AAA для WLC, который будет использоваться. Введите ключ “общего секретного ключа” (характерный для WLC), который используется между клиентом AAA и ACS. Выберите **Authenticate Using> RADIUS (Cisco Airespace)** для этого клиента AAA. Затем нажмите**, Submit + Применяются**.



2. Просите и установите серверный сертификат от известного, доверенный центр сертификации, такой как RSA Центр сертификации Keon.Для получения дополнительной информации об этом процессе обратитесь к документации, которая отправляет с ACS Cisco. При использовании Менеджера сертификатов RSA можно просмотреть RSA руководство по внедрению Aironet Keon для дополнительной справки. Необходимо успешно выполнить эту задачу перед продолжением.**Примечание:** Подписанные сертификаты могут также использоваться. См. документацию Cisco Secure ACS относительно того, как использовать их.
3. Под **Конфигурацией системы> Настройка Глобальной аутентификации**, проверьте, что флажок для **Позволяет аутентификацию PEAP**.



Настройте конфигурацию контроллера беспроводной локальной сети Cisco для 802.1x

Выполните следующие действия:

1. Соединитесь с интерфейсом командной строки WLC для настройки контроллера, таким образом, это может быть настроено для соединения с Сервером Cisco Secure ACS.
2. Введите **команду config radius auth ip-address** от WLC для настройки сервера RADIUS для аутентификации.**Примечание:** При тестировании с Менеджером Аутентификации RSA сервера RADIUS введите IP-адрес сервера RADIUS Менеджера Аутентификации RSA. Когда вы протестируете с Сервером Cisco ACS, введите IP-адрес сервера Cisco Secure ACS.
3. Введите **команду config radius auth port** от WLC для определения порта UDP для аутентификации. Порты 1645 или 1812 активны по умолчанию и в Менеджере Аутентификации RSA и в Сервере Cisco ACS.
4. Введите **команду config radius auth secret** от WLC для настройки общего секретного ключа на WLC. Это должно совпасть с общим секретным ключом, созданным в серверах RADIUS для этого Клиента RADIUS.
5. Введите **команду config radius auth enable** от WLC для включения аутентификации. Когда желаемый, введите **команду config radius auth disable** для отключения аутентификации. Обратите внимание на то, что аутентификация отключена по умолчанию.
6. Выберите соответствующую опцию безопасности уровня 2 для желаемого WLAN в WLC.

7. Используйте **команды show radius auth statistics и show radius summary**, чтобы проверить, что правильно настроены параметры настройки RADIUS.**Примечание:** Таймеры по умолчанию для Request-timeout EAP низки и, возможно, должны были бы модифицироваться. Это может быть сделано с помощью команды *<seconds>* **request-timeout config advanced eap**. Это могло бы также помочь настраивать идентификационный таймаут запроса на основе требований. Это может быть сделано с помощью команды *<seconds>* **идентификационного request-timeout config advanced eap**.

802.11 Конфигурация беспроводного клиента

Для подробного объяснения того, как настроить ваши беспроводные аппаратные средства и клиентского соискателя, обратитесь к различной документации Cisco.

Типичные ошибки

Это некоторые известные проблемы с аутентификацией RSA SecureID:

- Программный маркер RSA. Новый режим Контакта и Следующие режимы маркерного кода не поддерживаются при использовании этой формы проверки подлинности с XP2. (ИСПРАВЛЕННЫЙ в результате ACS-4.0.1-RSA-SW-CSCsc12614-CSCsd41866.zip)
- Если ваша реализация ACS будет более старой, или у вас нет вышеупомянутого исправления, то клиент не будет в состоянии аутентифицироваться до пользовательских переходов от “Включенного; Новый Режим PIN” к “Включенному”. Можно выполнить это при наличии пользователя, завершенного небеспроводная аутентификация, или при помощи приложения RSA “тестовой аутентификации”.
- Запретите 4 цифры / Алфавитно-цифровые PIN. Если пользователь в Новом режиме Контакта идет вразрез с политикой PIN, сбоями процесса проверки подлинности, и пользователь не знает как или почему. Как правило, если пользователь будет идти вразрез с политикой, то они будут передаваться сообщение, что PIN был отклонен и быть предложенным снова при показе пользователю снова, что политика PIN (Например, если политика PIN является 5-7 цифрами, все же пользователь вводит 4 цифры).

Дополнительные сведения

- Пример конфигурации динамического назначения VLAN с WLC на основе сопоставления групп ACS и Active Directory
- Пример конфигурации VPN клиента по беспроводной LAN с WLC
- Примеры настройки проверки подлинности на контроллерах беспроводной сети
- Пример конфигурации проверки подлинности EAP-FAST с контроллерами беспроводной сети и внешним сервером RADIUS
- Пример настройки типов аутентификации на фиксированном ISR с помощью SDM
- Пример настройки типов аутентификации беспроводной связи на фиксированном ISR
- Cisco защищенный расширяемый протокол аутентификации
- Аутентификация EAP с помощью сервера RADIUS
- Cisco Systems – техническая поддержка и документация