Пример настройки ограничения доступа к WLAN на основе SSID с WLC и Cisco Secure ACS

Содержание

Введение

Этот документ содержит пример конфигурации для индивидуального ограничения доступа пользователей к сети WLAN на основе идентификаторов наборов служб (SSID).

Предварительные условия

Требования

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

- Знание того, как настроить Контроллер беспроводной локальной сети (WLC) и облегченную точку доступа (LAP) для главной операции
- Базовые знания о том, как настроить сервер Cisco Secure Access Control Server (ACS)
- Знание Протокола LWAPP и методов безопасности беспроводной связи

Используемые компоненты

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

- Cisco WLC серии 2000, который выполняет микропрограммное обеспечение 4.0
- LAP серии 1000 Cisco
- Версия сервера 3.2 Cisco Secure ACS
- Адаптер беспроводного клиента Cisco 802.11a/b/g, который выполняет микропрограммное обеспечение 2.6
- Версия 2.6 Утилиты Cisco Aironet Desktop Utility (ADU)

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

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Общие сведения

С использованием основанного на SSID доступа WLAN пользователи могут аутентифицироваться на основе SSID, который они используют для соединения с WLAN. Сервер Cisco Secure ACS используется для аутентификации пользователей. Аутентификация происходит на двух этапах на Cisco Secure ACS:

1. Аутентификация EAP
2. Аутентификация SSID на основе Ограничений доступа к сети (NAR) на Cisco Secure ACS

Если EAP и основанная на SSID аутентификация успешны, пользователю разрешают обратиться к WLAN, или иначе пользователь разъединен.

Cisco Secure ACS использует функцию NAR для ограничения пользовательского доступа на основе SSID. NAR является определением, которое вы делаете в Cisco Secure ACS дополнительных условий, которые нужно соблюдать, прежде чем пользователь может обратиться к сети. Cisco Secure ACS применяет эти условия с помощью информации от атрибутов, передаваемых клиентами AAA. Несмотря на то, что существует несколько способов, которыми можно установить NAR, они все на основе соответствующей информации об атрибутах, передаваемой клиентом AAA. Поэтому необходимо понять формат и содержание атрибутов, которые передают клиенты AAA, если вы хотите использовать эффективные NAR.

Когда вы устанавливаете NAR, можно выбрать, работает ли фильтр положительно или негативно. Т.е. в NAR вы задаете, permit ли or deny доступ к сети, на основе сравнения информации, передаваемой от клиентов AAA к информации, хранившей в NAR. Однако, если NAR не встречается с достаточными сведениями для работы, это принимает значение по умолчанию к запрещенному доступу.

Можно определить NAR для и применить его к, определенный пользователь или группа пользователей. См. Описание технологических решений Ограничений доступа к сети для

получения дополнительной информации.

Cisco Secure ACS поддерживает два типа фильтров NAR:

1. **На основе IP фильтры** — на основе IP NAR фильтруют предельный доступ, основанный на IP-адресах клиента конечного пользователя и клиента AAA. См. приблизительно на основе IP Фильтры NAR для получения дополнительной информации об этом типе фильтра NAR.
2. **Нена основе IP фильтры** — нена основе IP NAR фильтруют предельный доступ, основанный на сравнении простой строки значения, передаваемого от клиента AAA. Значение может быть номером ID вызывающей линии (CLI), номером Сервиса идентификации набранного номера (DNIS), MAC-адресом или другим значением, которое происходит от клиента. Для этого типа NAR для работы значение в описании NAR должно точно совпасть с тем, что передается от клиента, включая любой формат используется. Например, (217) 555-4534 не совпадает 217-555-4534. См. приблизительно нена основе IP Фильтры NAR для получения дополнительной информации об этом типе фильтра NAR.

Этот документ использует нена основе IP фильтры, чтобы сделать основанную на SSID аутентификацию. Нена основе IP фильтр NAR (т.е. фильтр NAR DNIS/CLI-based) являются списком разрешенных или Denied Calling/Point of Access Locations, который можно использовать в ограничении клиента AAA, когда у вас нет установленного на основе IP соединением. Нена основе IP функция NAR обычно использует номер CLI и Набранный номер. Существуют исключения в использовании полей DNIS/CLI. Можно ввести имя SSID в поле DNIS и сделать основанную на SSID аутентификацию. Это вызвано тем, что WLC передает в атрибуте DNIS, названии SSID, к серверу RADIUS. Таким образом, при построении NAR DNIS или в пользователе или в группе можно создать ограничения SSID для каждого пользователя.

При использовании RADIUS поля NAR перечислили здесь использование эти значения:

- **Клиент AAA** — Nas-ip-address (приписывают 4) или, если Nas-ip-address не существует, идентификатор NAS (атрибут RADIUS 32), используется.
- **Порт** — Порт NAS (приписывают 5) или, если порт NAS не существует, NAS-port-ID (приписывают 87) используется.
- **CLI** — calling-station-ID (приписывают 31) используется.
- **DNIS** — вызванный идентификатор станции (приписывают 30) используется.

См. Ограничения доступа к сети для получения дополнительной информации об использовании NAR.

Так как WLC передает в атрибуте DNIS и названии SSID, можно создать ограничения SSID для каждого пользователя. В случае WLC поля NAR имеют эти значения:

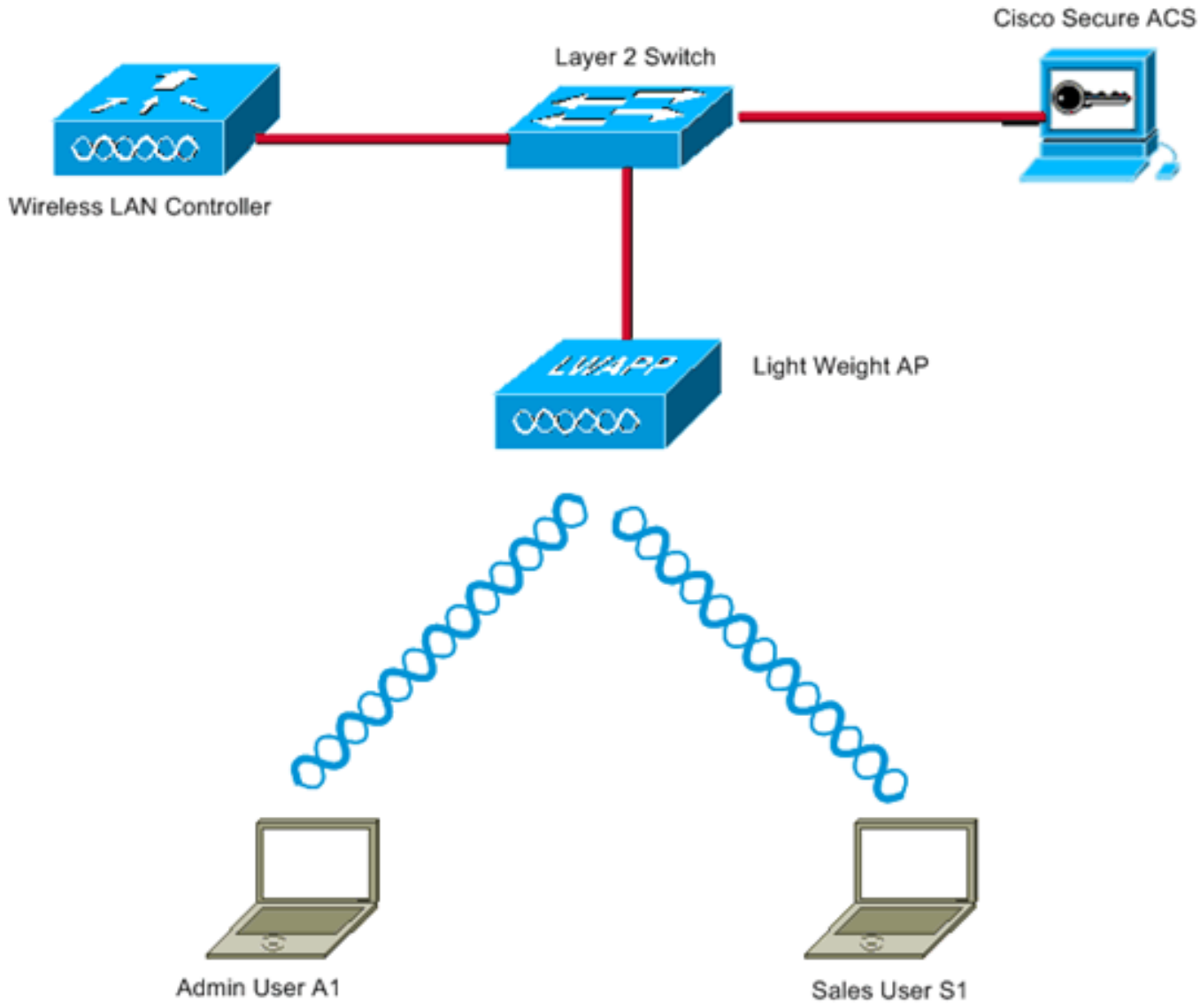
- **Клиент AAA** — IP-адрес WLC
- **порт** —*
- **CLI** —*
- **DNIS** — *ssidname

Оставшаяся часть этого документа предоставляет пример конфигурации о том, как выполнить это.

Настройка сети

В настройке данного примера WLC зарегистрирован к LAP. Используются два WLAN. Один WLAN для Пользователей административного отдела, и другой WLAN для пользователей Отдела продаж. Беспроводной клиент A1 (пользователь Admin) и S1 (Пользователь продаж) соединяется с беспроводной сетью. Необходимо настроить WLC и сервер RADIUS таким способом, которым пользователем Admin A1 в состоянии обратиться только **к Admin** WLAN и является ограниченным доступом к **Продажам** WLAN, и пользовательский S1 Продаж должен быть в состоянии обратиться **к Продажам** WLAN и должен иметь ограниченный доступ **Admin** WLAN. Все пользователи используют Аутентификацию LEAP в качестве метода аутентификации Уровня 2.

Примечание: Этот документ предполагает, что WLC зарегистрирован к контроллеру. Если вы плохо знакомы с WLC и не знаете, как настроить WLC для главной операции, обратитесь к регистрации облегченных точек доступа к Контроллеру беспроводной локальной сети (WLC).



WLC Management Interface IP address : 172.16.1.30/16
WLC AP-Manager Interface IP address: 172.16.1.31/16
Cisco Secure ACS server IP address: 172.16.1.60/16

SSID for the Admin department users : Admin
SSID for Sales department users: Sales

Настройка

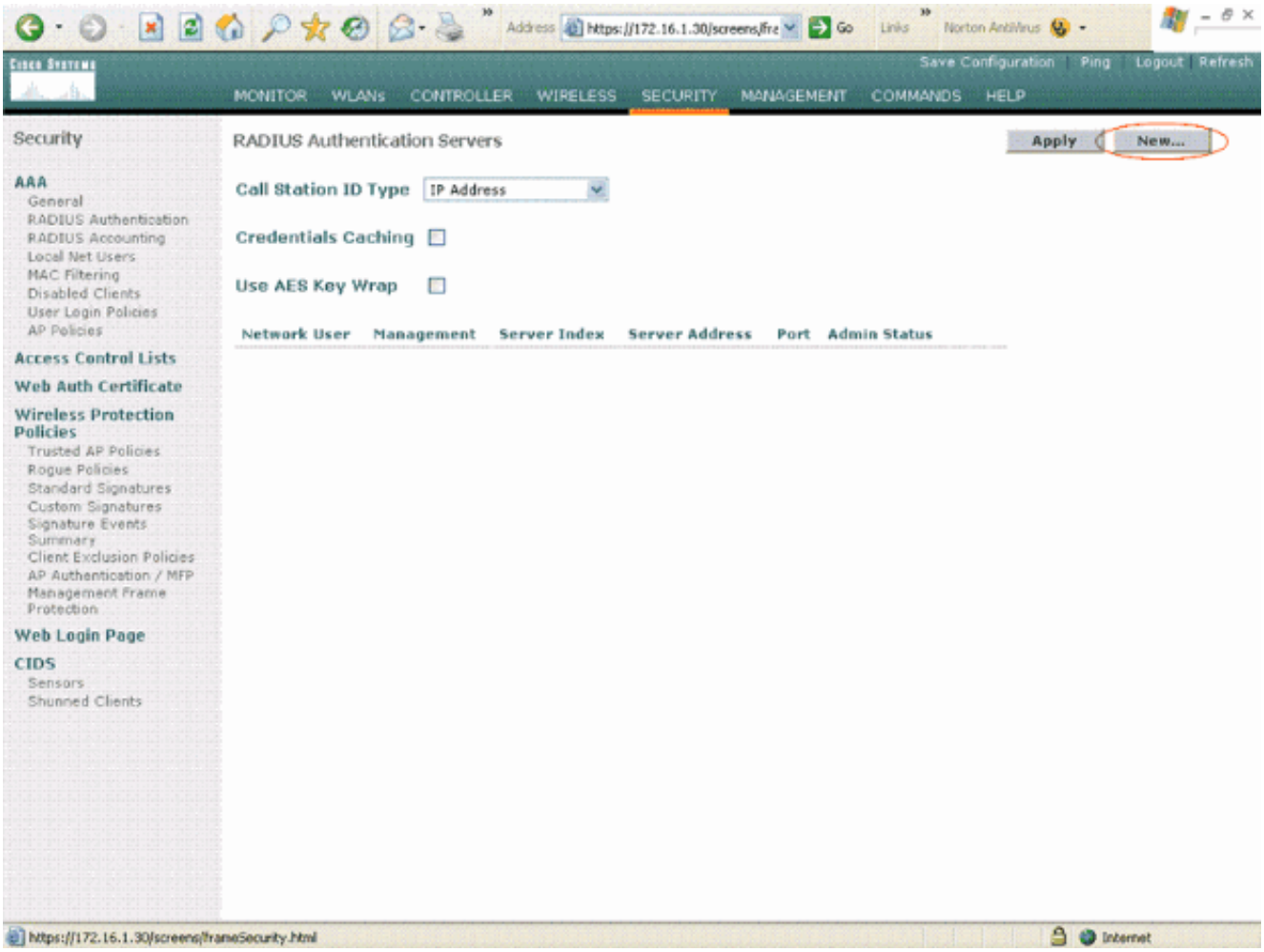
Для настройки устройств для этой настройки вы должны:

1. Настройте WLC для этих двух WLAN и сервера RADIUS.
2. Настройте Cisco Secure ACS.
3. Настройте беспроводных клиентов и проверьте.

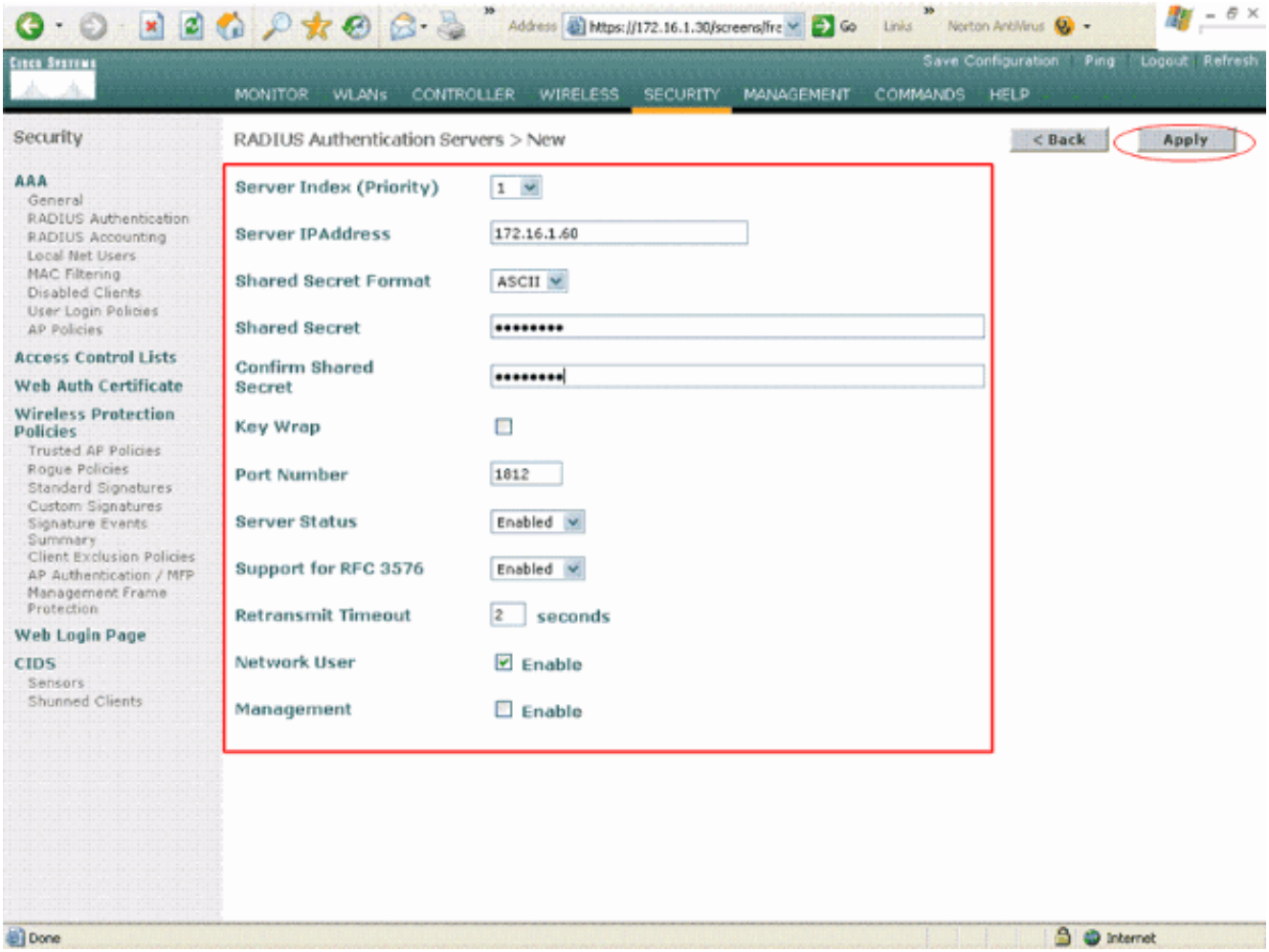
Настройте WLC

Выполните эти шаги для настройки WLC для этой настройки:

1. WLC должен быть настроен для передачи учетных данных пользователя внешнему серверу RADIUS. Внешний сервер RADIUS (Cisco Secure ACS в этом случае) тогда проверяет учетные данные пользователя и предоставляет доступ к беспроводным клиентам. Выполните следующие действия:Выберите **Security> RADIUS Authentication** от графического интерфейса контроллера для отображения страницы RADIUS Authentication
Servers.

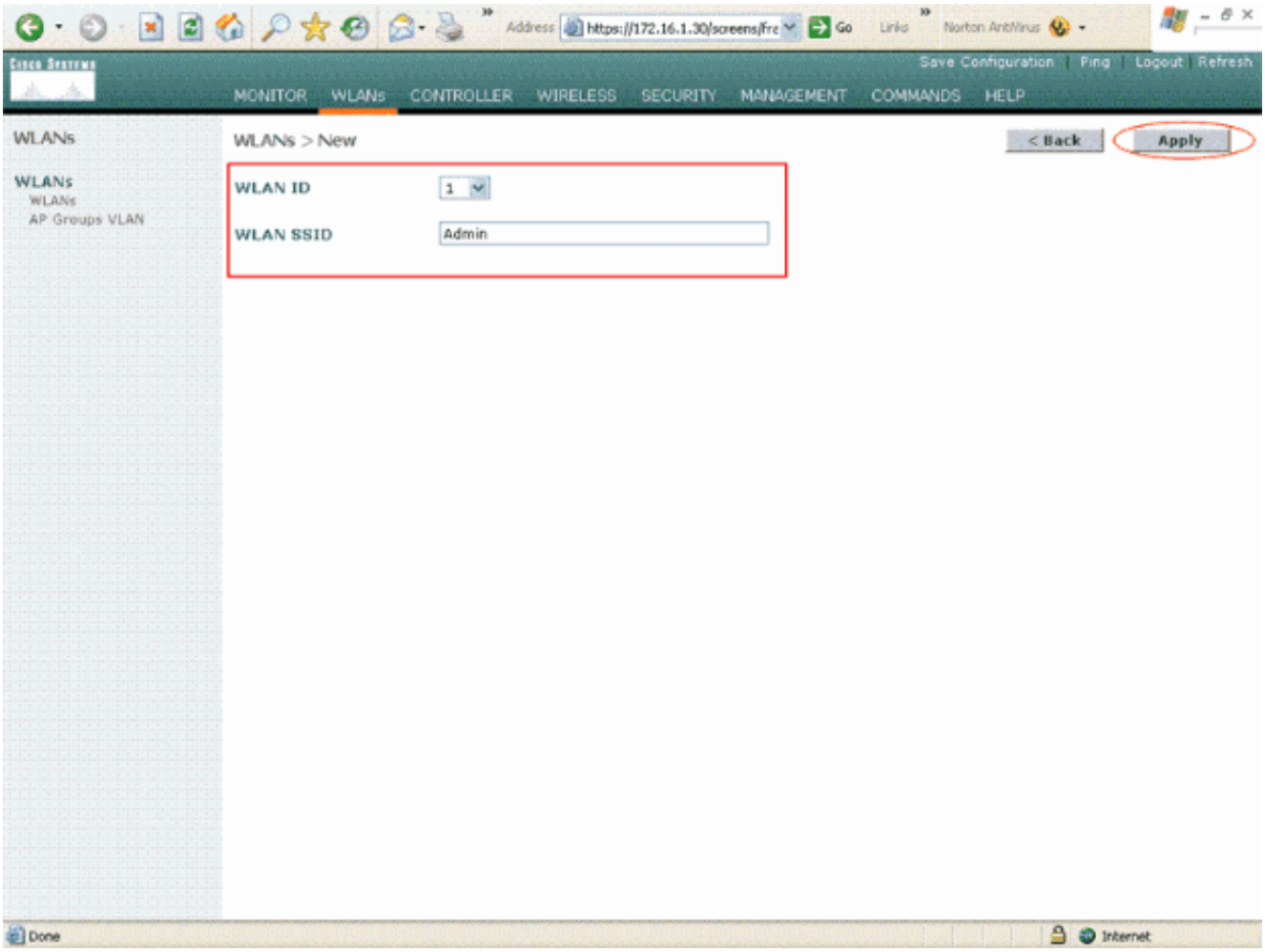


Нажмите **New** для определения параметров сервера RADIUS.В их числе: RADIUS Server IP Address, Shared Secret, Port Number и Server Status. С помощью флажков Network User и Management можно определить, применяется ли аутентификация на основе сервера RADIUS для управления и сетевых пользователей. Данный пример использует Cisco Secure ACS в качестве сервера RADIUS с IP-адресом 172.16.1.60.

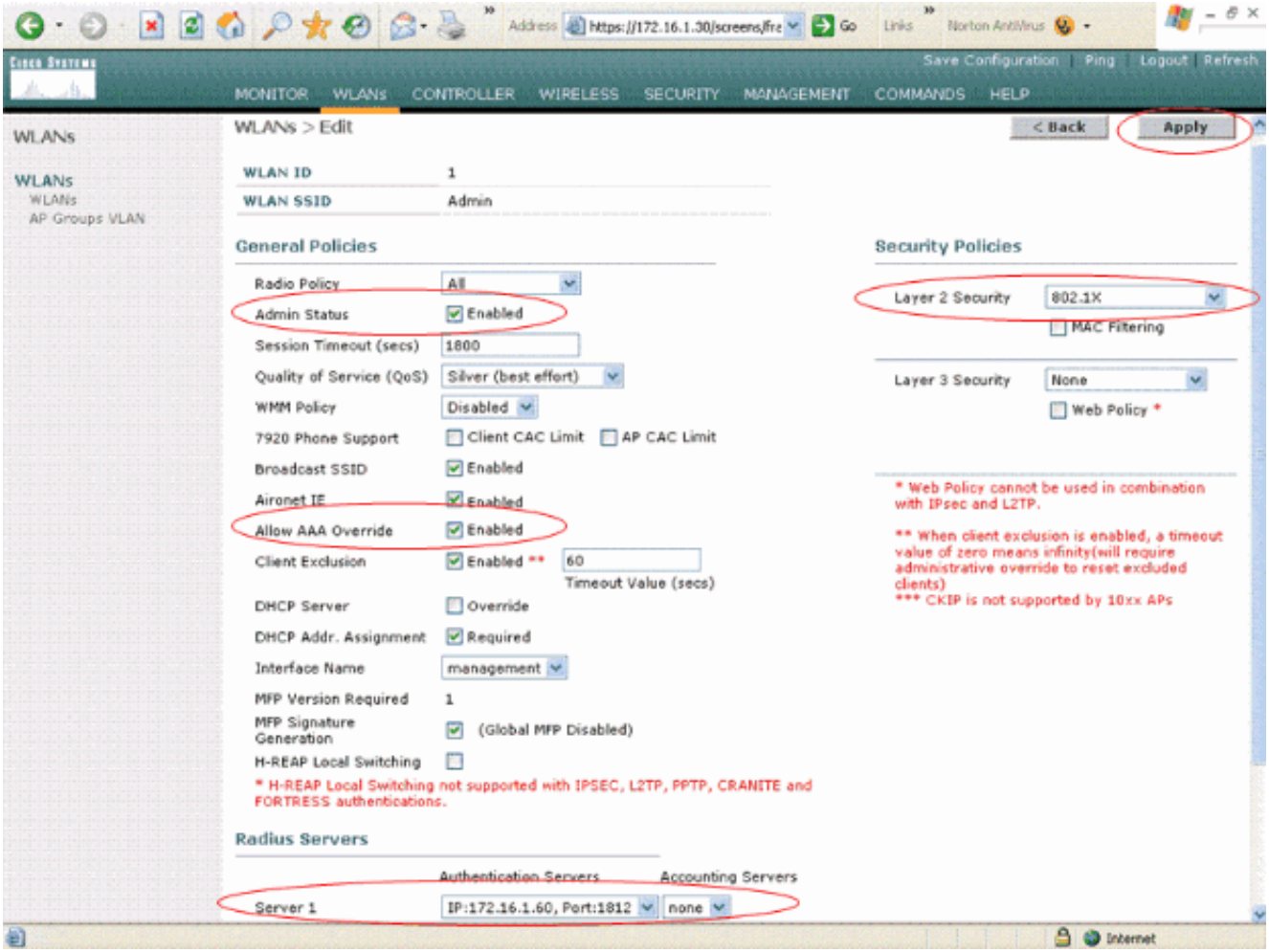


Щелкните "Применить".

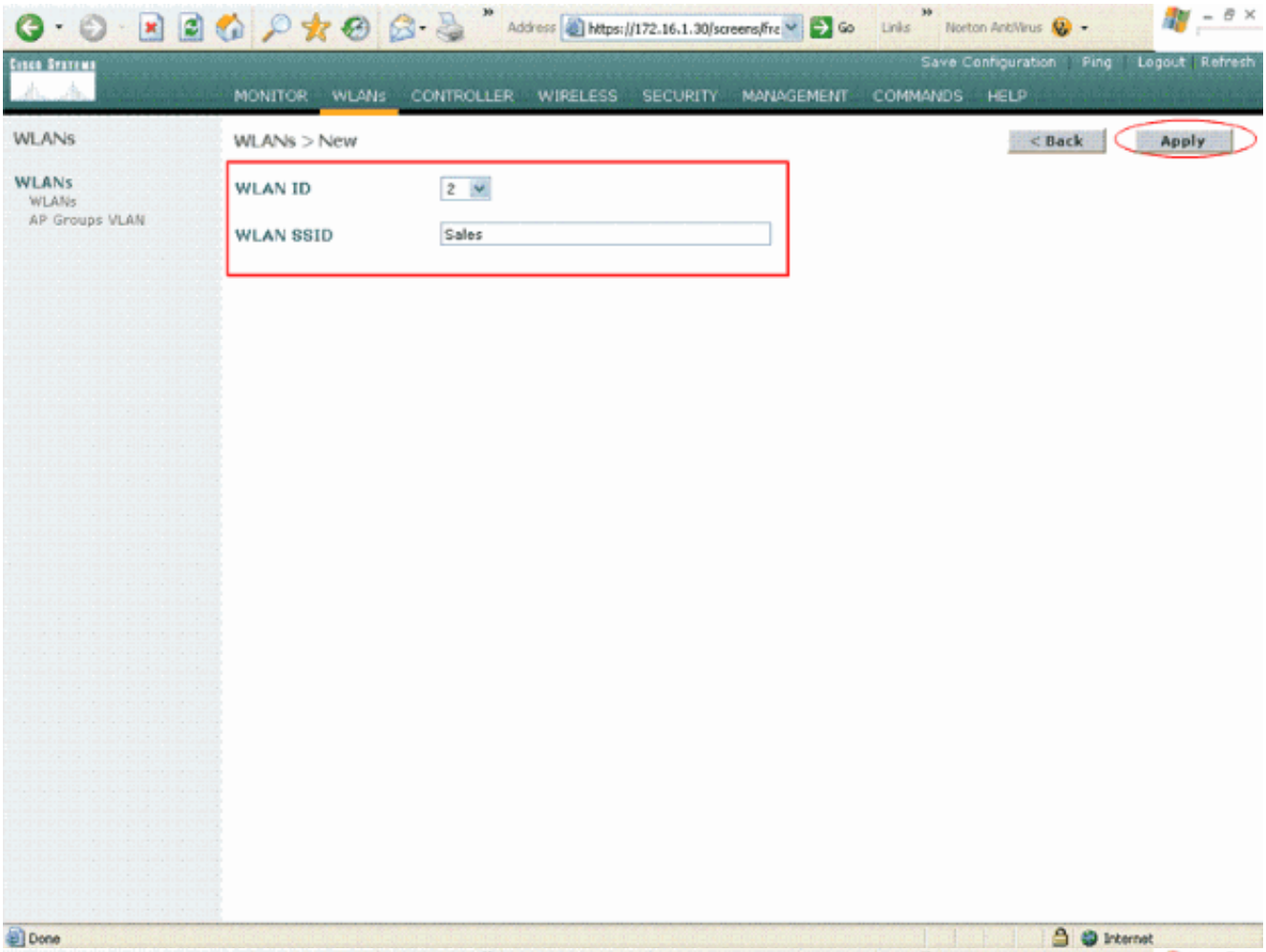
2. Настройте один WLAN для Административного отдела с **Admin** SSID и другой WLAN для Отдела продаж с **Продажами** SSID. Для этого выполните следующие действия:**Нажмите WLANs в графическом интерфейсе контроллера для создания WLAN.** Откроется окно WLAN. В данном окне находится список сетей WLAN, настроенных на контроллере.**Нажмите New для настройки новой WLAN.**Данный пример создает WLAN под названием **Admin** для Административного отдела, и ИДЕНТИФИКАТОР WLAN равняется **1**. **Щелкните "Применить".**

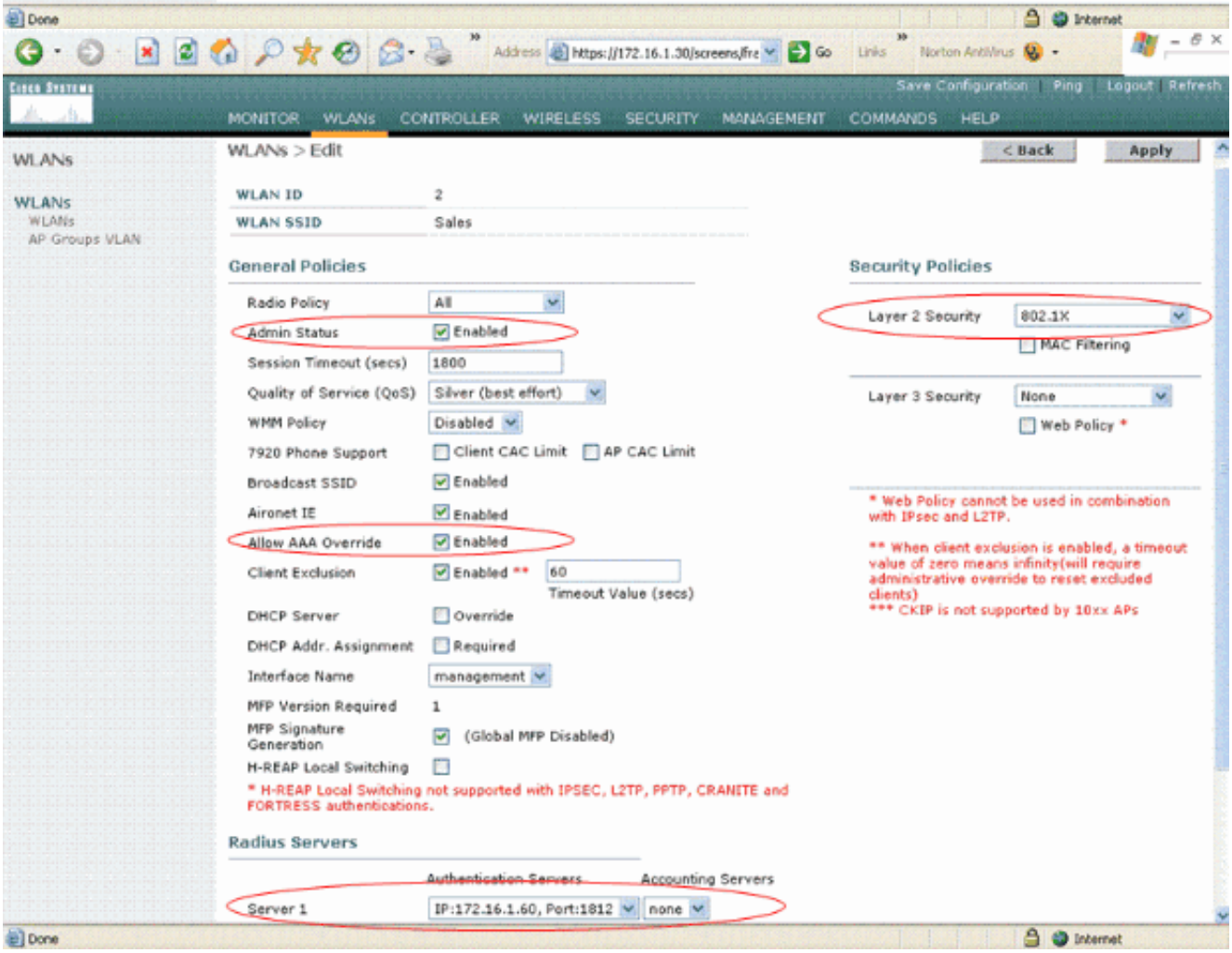


В окне WLAN > Edit укажите параметры сети:От ниспадающего меню безопасности уровня 2 выберите **802.1x**. Параметр обеспечения безопасности уровня 2 установлен на 802.1x по умолчанию. Это включает 802.1X/АУТЕНТИФИКАЦИЮ EAP для WLAN.В соответствии с общей политикой, установите флажок **замены AAA**. Когда Замена AAA включена, и у клиента есть конфликтный AAA и параметры аутентификации WLAN контроллера, аутентификация клиента выполнена AAA-сервером.Выберите соответствующий сервер RADIUS от ниспадающего меню под серверами RADIUS. Другие параметры могут быть изменены на основе требования сети WLAN. **Щелкните "Применить".**



Точно так же для создания WLAN для Отдела продаж, повторите шаги b и c. Вот снимки
экрана.


Address https://172.16.1.30/screens/fra
Go
Links
Norton AntiVirus
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
AP Groups VLAN
WLANs > New
< Back
Apply
WLAN ID
2
WLAN SSID
Sales


Done
Internet
Address https://172.16.1.30/screens/fra
Go
Links
Norton AntiVirus
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANs
WLANs
WLANs
AP Groups VLAN
WLANs > Edit
< Back
Apply
WLAN ID 2
WLAN SSID Sales
General Policies
Radio Policy All
Admin Status Enabled
Session Timeout (secs) 1800
Quality of Service (QoS) Silver (best effort)
WMM Policy Disabled
7920 Phone Support Client CAC Limit AP CAC Limit
Broadcast SSID Enabled
Aironet IE Enabled
Allow AAA Override Enabled
Client Exclusion Enabled ** 60
Timeout Value (secs)
DHCP Server Override
DHCP Addr. Assignment Required
Interface Name management
MFP Version Required 1
MFP Signature Generation (Global MFP Disabled)
H-REAP Local Switching
* H-REAP Local Switching not supported with IPSEC, L2TP, PPTP, CRANITE and FORTRESS authentications.
Security Policies
Layer 2 Security 802.1X
MAC Filtering
Layer 3 Security None
Web Policy *
* Web Policy cannot be used in combination with IPsec and L2TP.
** When client exclusion is enabled, a timeout value of zero means infinity(will require administrative override to reset excluded clients)
*** CKIP is not supported by 10xx APs
Radius Servers
Authentication Servers
Accounting Servers
Server 1 IP:172.16.1.60, Port:1812 none
Done
Internet

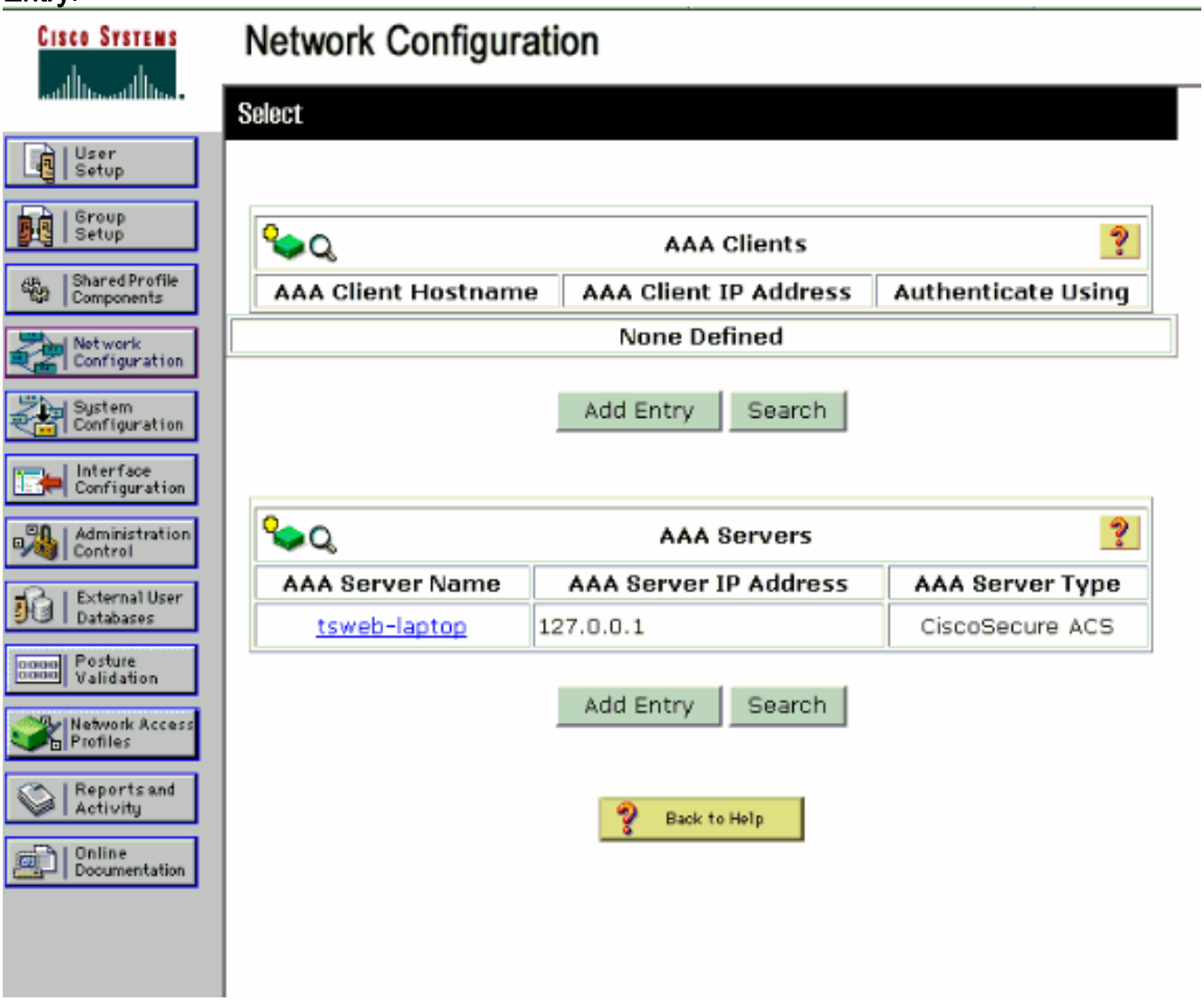
Настройте Cisco Secure ACS

На сервере Cisco Secure ACS вы должны:

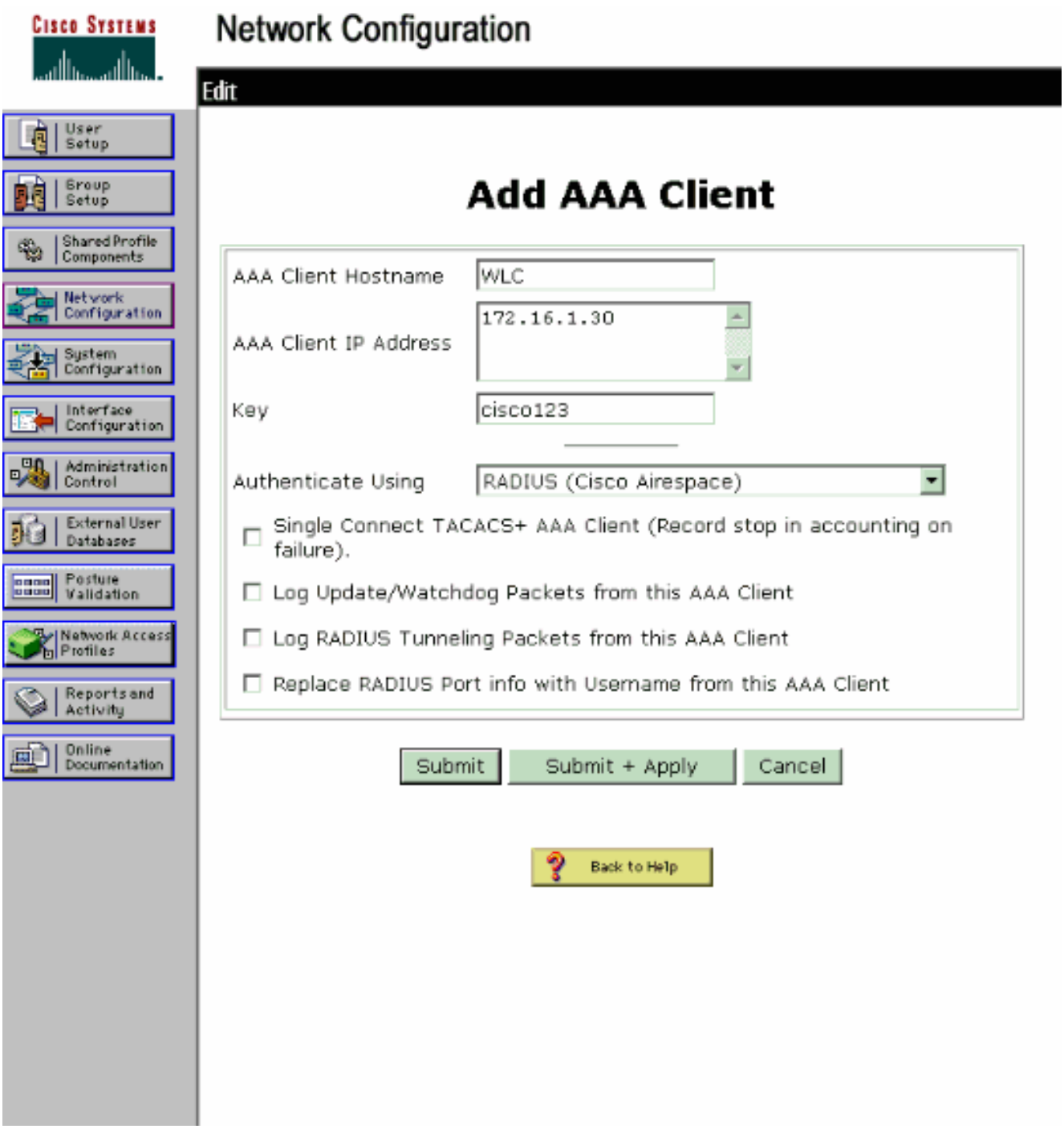
1. Настройте WLC как клиента AAA.
2. Создайте Базу данных пользователей и определите NAR для основанной на SSID аутентификации.
3. Включите Аутентификацию eap.

Выполните эти шаги на Cisco Secure ACS:

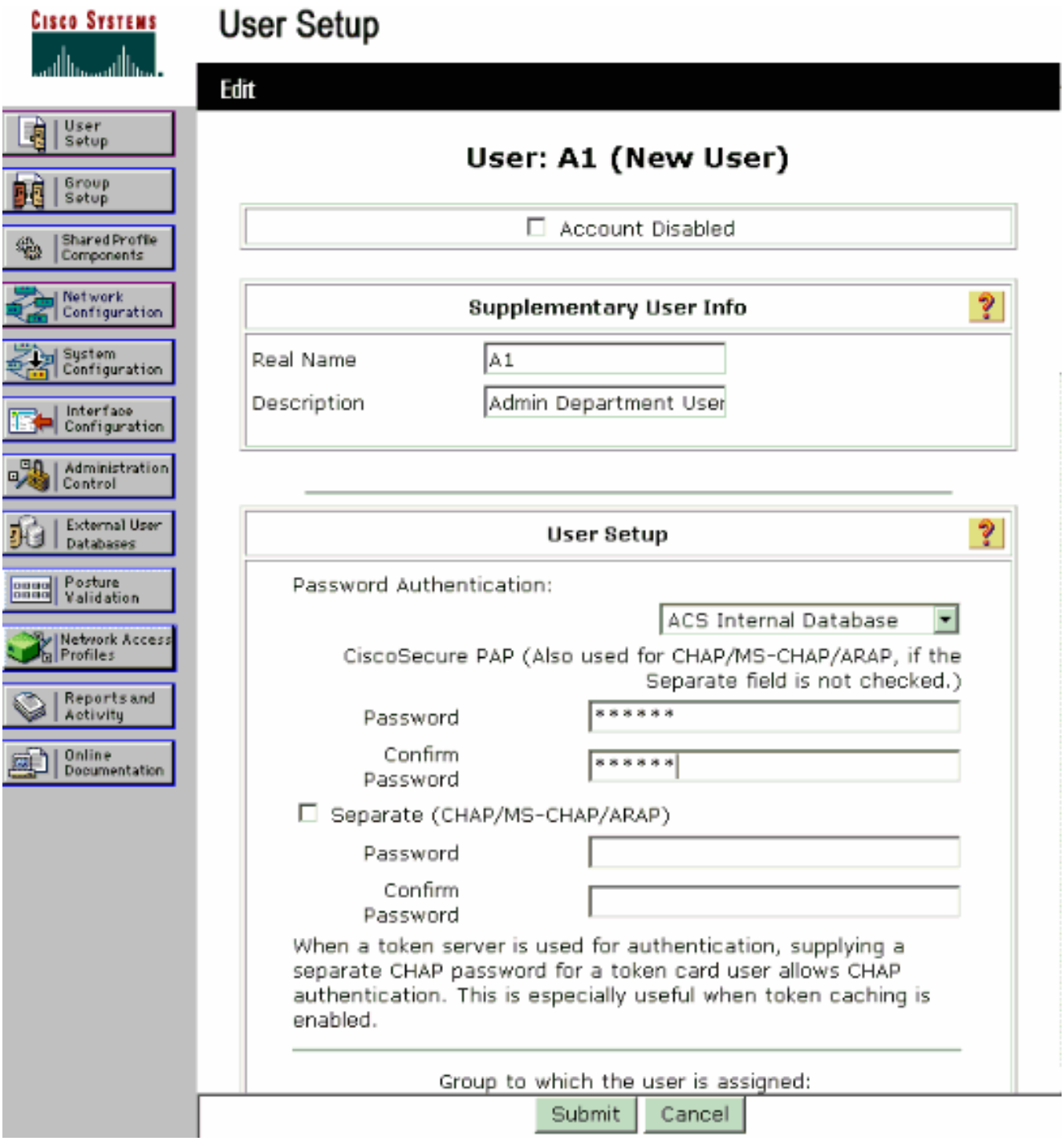
1. Для определения контроллера как клиент AAA на сервере ACS нажмите **Network Configuration** от GUI ACS. При клиентах AAA щелкают **по Add Entry**.



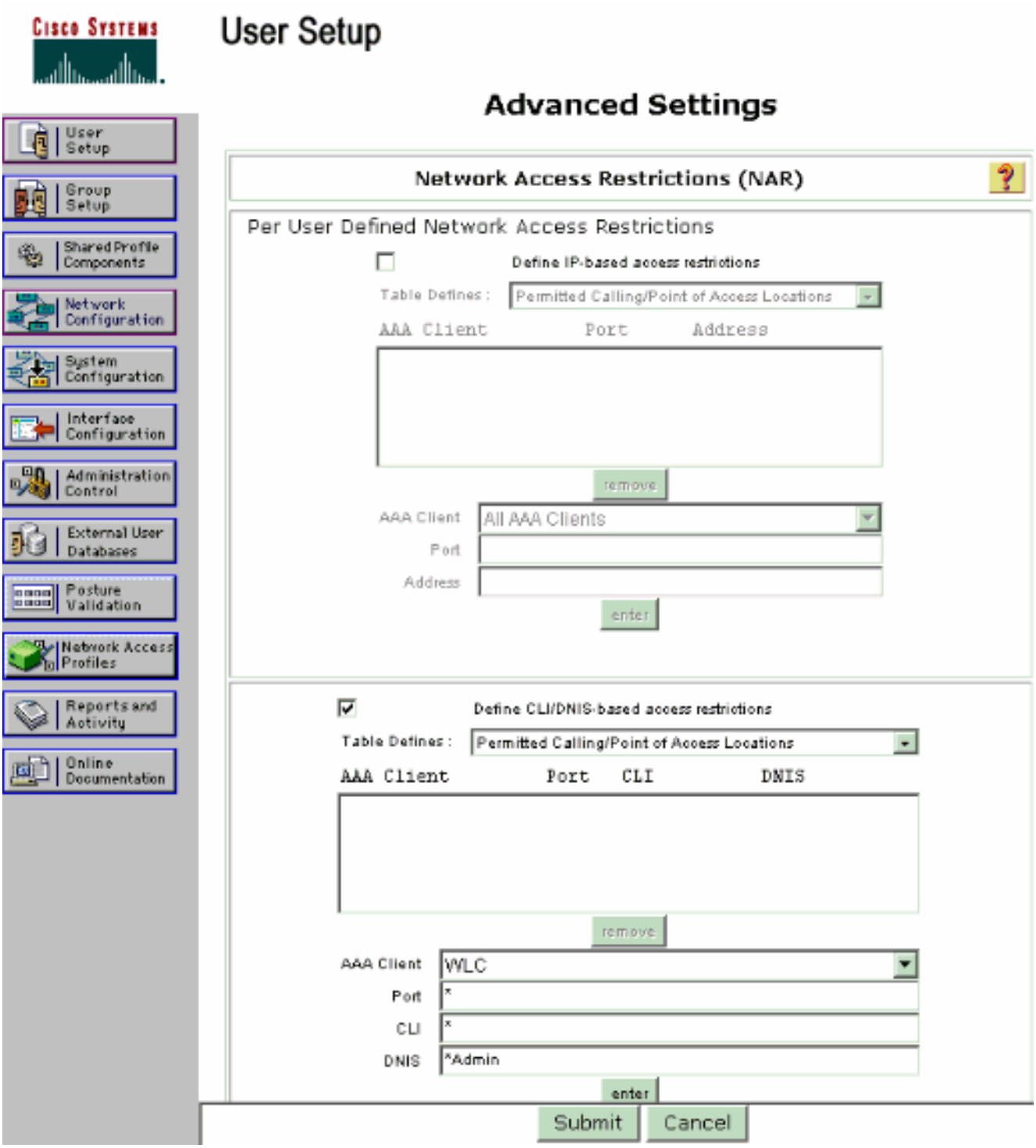
2. Когда страница Network Configuration появится, определите название WLC, IP-адреса, общего секретного ключа и метода аутентификации (RADIUS Airespace Cisco).



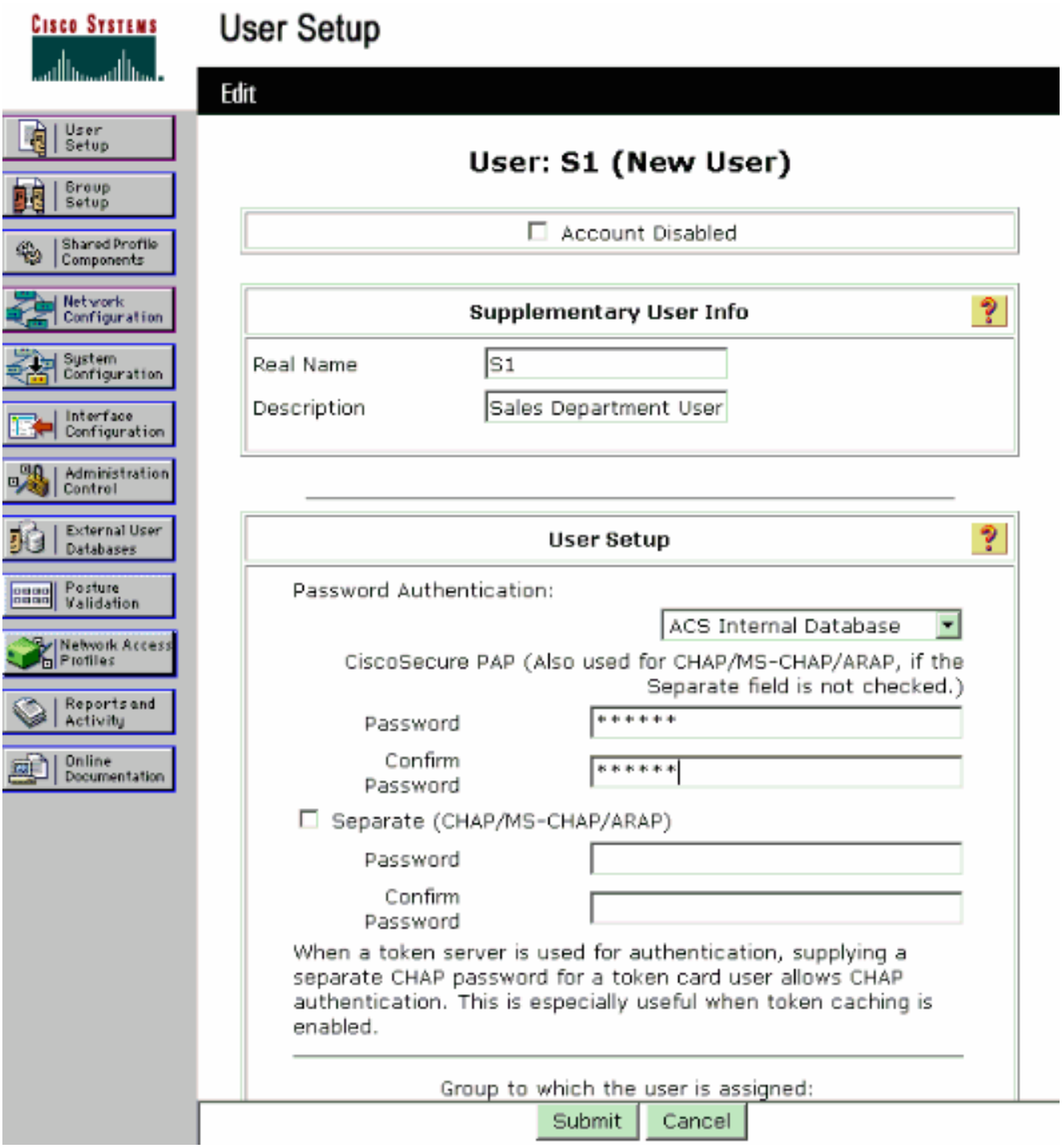
3. Нажмите **User Setup** от GUI ACS, введите имя пользователя и нажмите **Add/Edit**. В данном примере пользователь является A1.
4. Когда откроется страница User Setup, определите все параметры, которые относятся к данному пользователю. В данном примере настроены имя пользователя, пароль и Дополнительные Сведения о пользователе, потому что вам нужны эти параметры для Аутентификации
   LEAP.

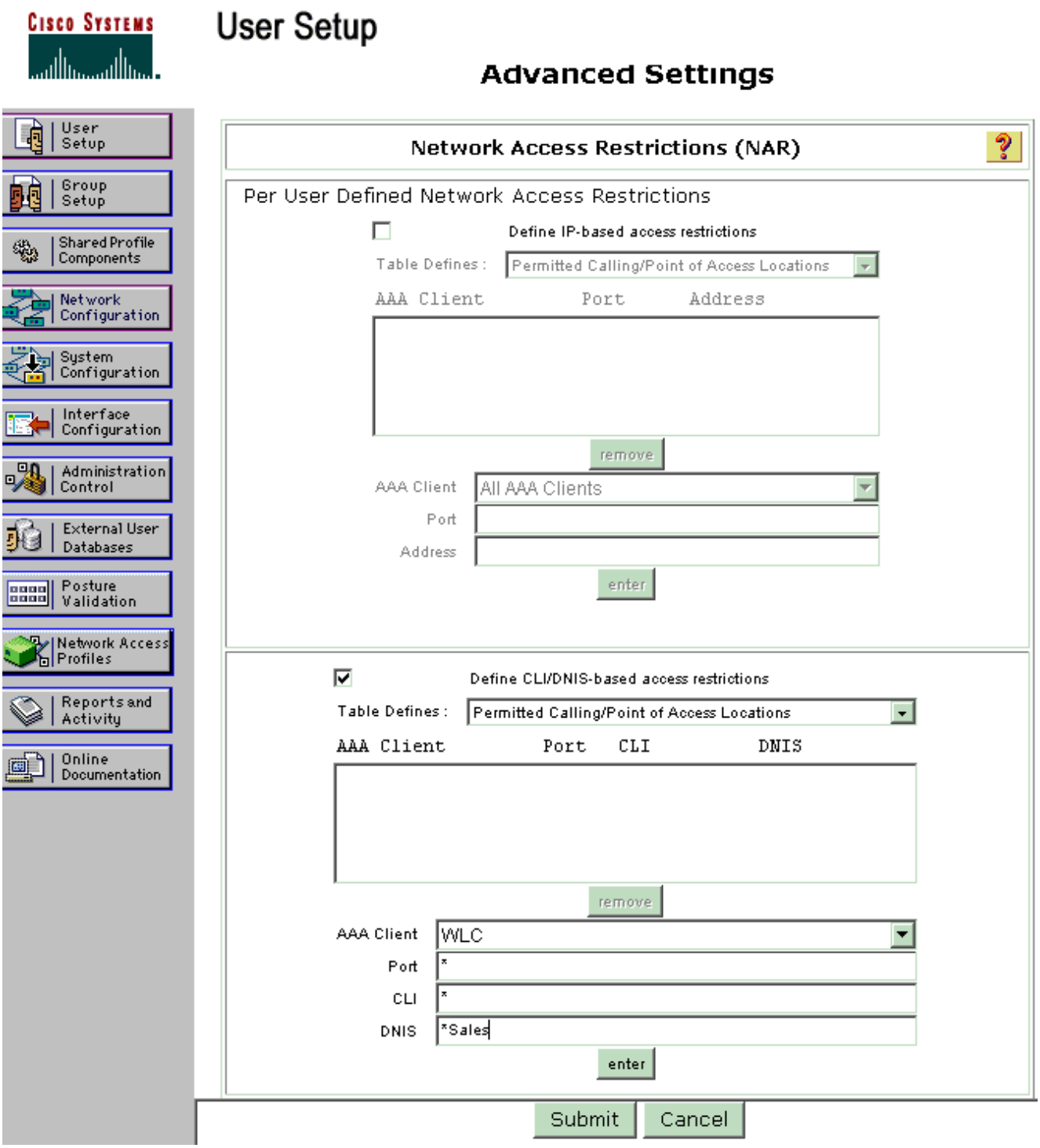


5. Прокрутите страницу User Setup вниз, пока вы не будете видеть раздел Ограничений доступа к сети. Под Интерфейсом пользователя Ограничения DNIS/ДОСТУПА CLI выберите **Permitted Calling / Точка Местоположений Доступа** и определите эти параметры:**Клиент AAA** — IP-адрес WLC (172.16.1.30 в нашем примере)**Порт** —***CLI** —***DNIS** — *ssidname
6. Атрибут DNIS определяет SSID, к которому пользователю разрешают обратиться. WLC передает SSID в атрибуте DNIS к серверу RADIUS.Если пользователь должен обратиться только к WLAN под названием Admin, войдите ***Admin** для поля DNIS. Это гарантирует, что у пользователя есть доступ только к WLAN под названием Admin. Нажмите **Enter**.**Примечание:** SSID нужно всегда предшествовать с *. Это является обязательным.

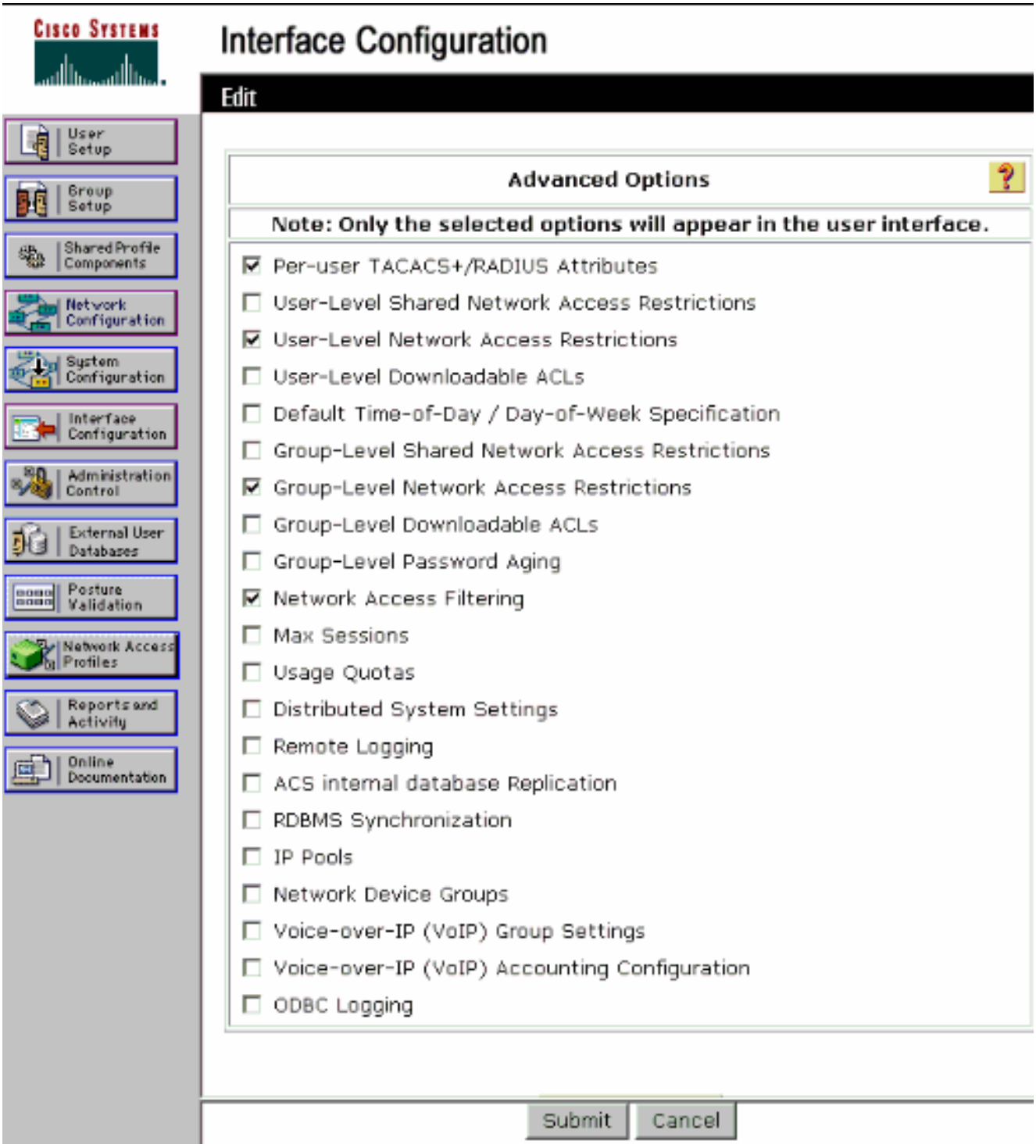


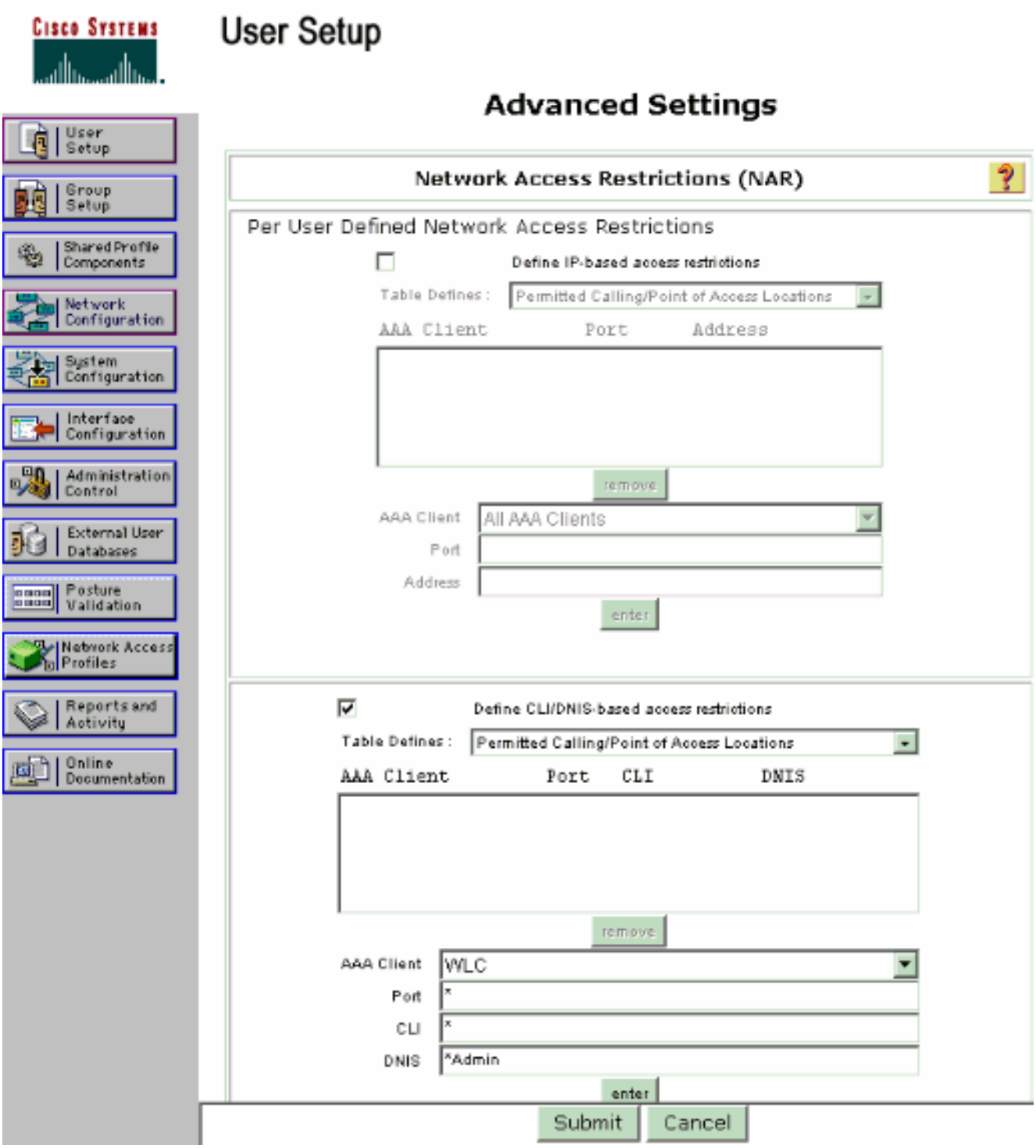
7. **Нажмите кнопку Submit (Отправить).**
8. Точно так же создайте пользователя для пользователя Отдела продаж. Вот снимки экрана.


Cisco Systems
User Setup
Edit
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
User: S1 (New User)
Account Disabled
Supplementary User Info
Real Name
S1
Description
Sales Department User
User Setup
Password Authentication:
ACS Internal Database
CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)
Password
******
Confirm Password
******
Separate (CHAP/MS-CHAP/ARAP)
Password
Confirm Password
When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.
Group to which the user is assigned:
Submit
Cancel

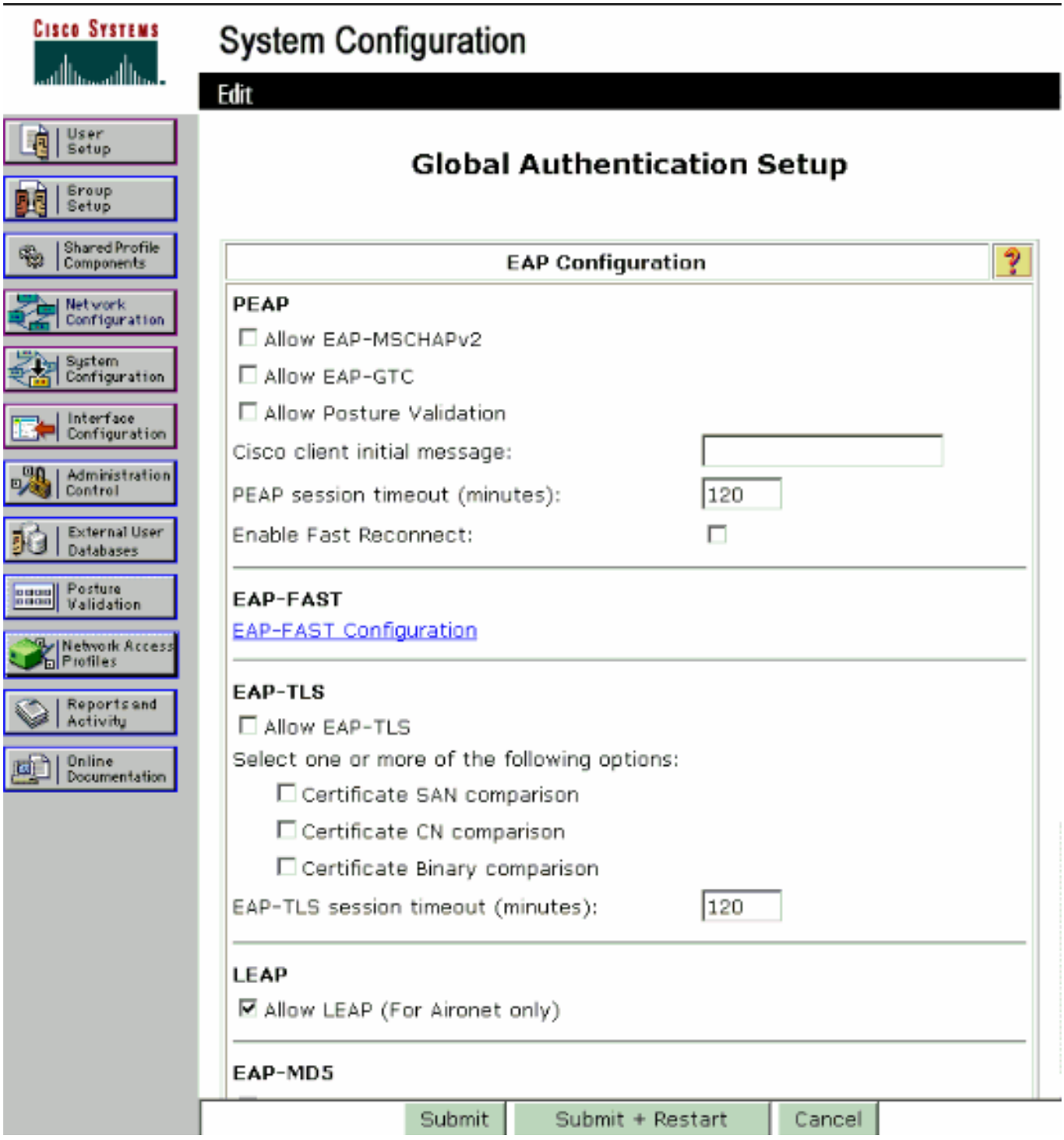


9. Повторите тот же процесс для добавления большего количества пользователей к базе данных.**Примечание:** По умолчанию все пользователи объединяются в группу по умолчанию. Если вы хотите назначить определенных пользователей на различные группы, обратитесь к Разделу управления Группы пользователей Руководства пользователя для Cisco Secure ACS для Windows Server 3.2.**Примечание:** Если вы не видите раздел Ограничений доступа к сети в окне User Setup, это могло бы быть, потому что это не включено. Для включения Ограничений доступа к сети для пользователей выберите **Interfaces> Advanced Options** от GUI ACS, выберите **User-Level Network Access Restrictions** и нажмите **Submit**. Это включает NAR и появляется в окне User
Setup.


Cisco Systems
Interface Configuration
Edit
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
Advanced Options
Note: Only the selected options will appear in the user interface.
Per-user TACACS+/RADIUS Attributes
User-Level Shared Network Access Restrictions
User-Level Network Access Restrictions
User-Level Downloadable ACLs
Default Time-of-Day / Day-of-Week Specification
Group-Level Shared Network Access Restrictions
Group-Level Network Access Restrictions
Group-Level Downloadable ACLs
Group-Level Password Aging
Network Access Filtering
Max Sessions
Usage Quotas
Distributed System Settings
Remote Logging
ACS internal database Replication
RDBMS Synchronization
IP Pools
Network Device Groups
Voice-over-IP (VoIP) Group Settings
Voice-over-IP (VoIP) Accounting Configuration
ODBC Logging
Submit
Cancel



10. Для включения Аутентификации eap нажмите **System Configuration** и **Global Authentication Setup**, чтобы гарантировать, что сервер проверки подлинности настроен для выполнения желаемого метода аутентификации EAP.Под EAP параметры конфигурации выбирают соответствующий метод EAP. В данном примере используется аутентификация LEAP. **По завершении нажмите Submit.**

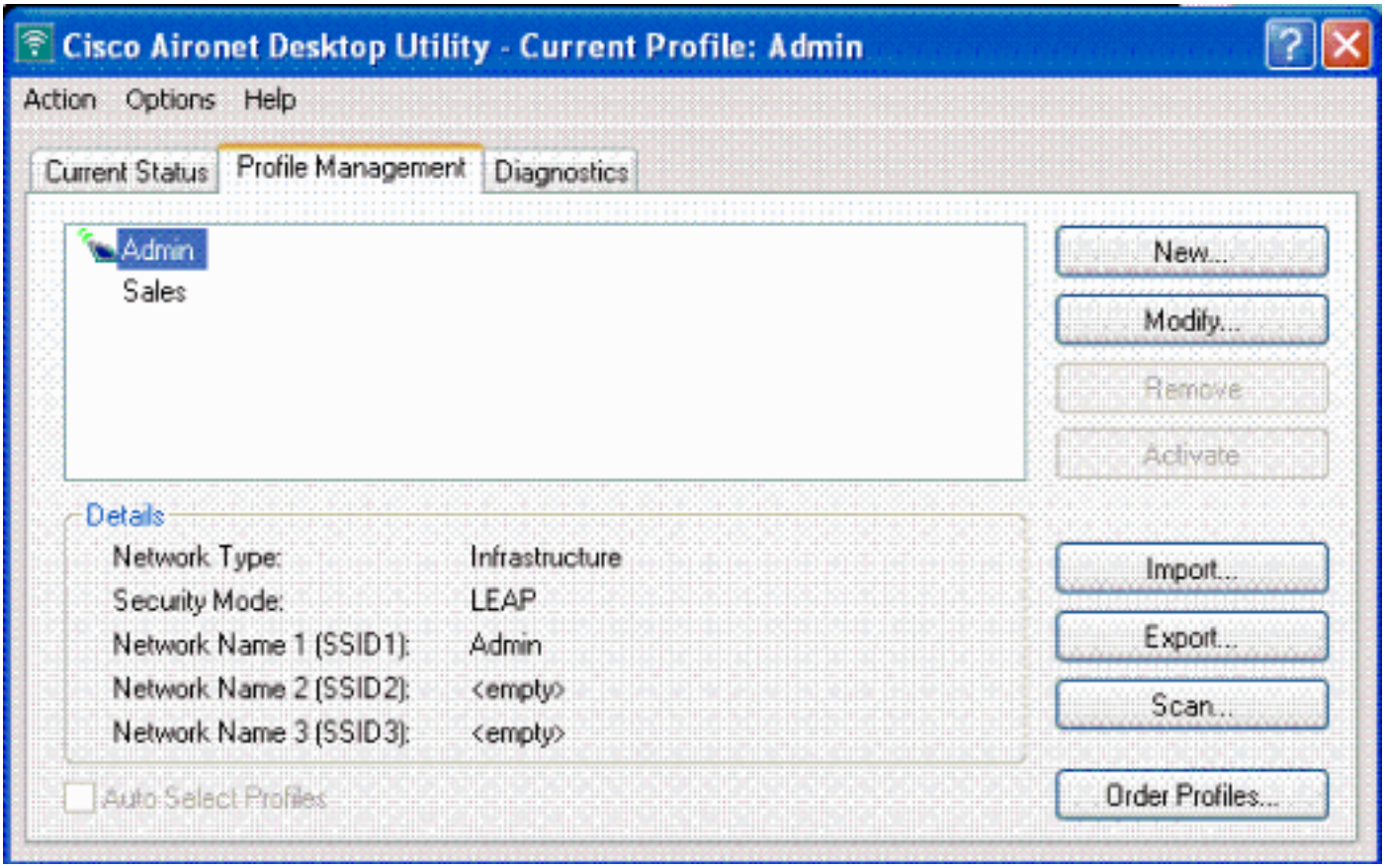


Настройте беспроводного клиента и проверьте

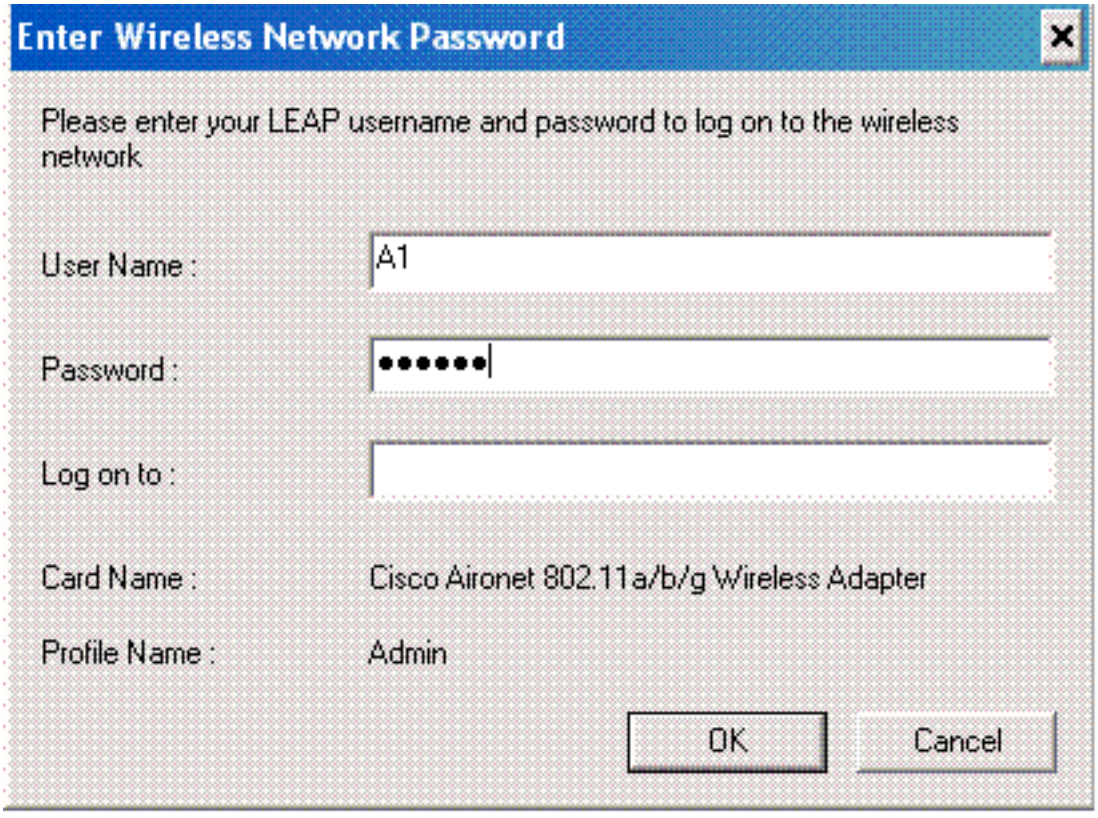
Этот раздел позволяет убедиться, что конфигурация работает правильно. Попытайтесь привязать беспроводного клиента к LAP с помощью Аутентификации LEAP, чтобы проверить, работает ли конфигурация как ожидалось.

Примечание: В данном документе предполагается, что профиль клиента настроен для аутентификации LEAP. См. Использование Аутентификации eap для получения информации о том, как настроить адаптер беспроводного клиента a/b/g 802.11 для Аутентификации LEAP.

Примечание: От ADU вы видите настройку двух клиентских профилей. Один для Пользователей административного отдела с **Admin** SSID и другим профилем для пользователей Отдела продаж с **Продажами** SSID. Оба профиля настроены для Аутентификации LEAP.



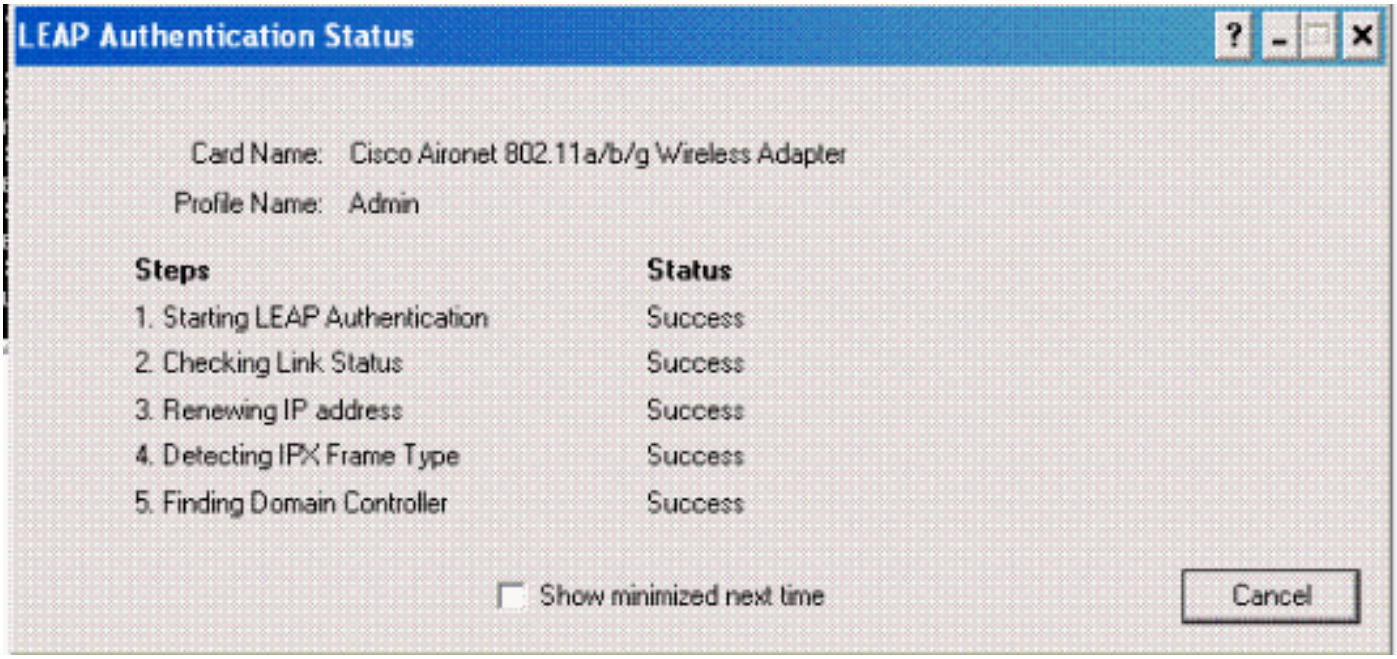
Когда профиль для пользователя беспроводной связи от Административного отдела активирован, пользователя просят ввести имя пользователя для Аутентификации LEAP. Например:



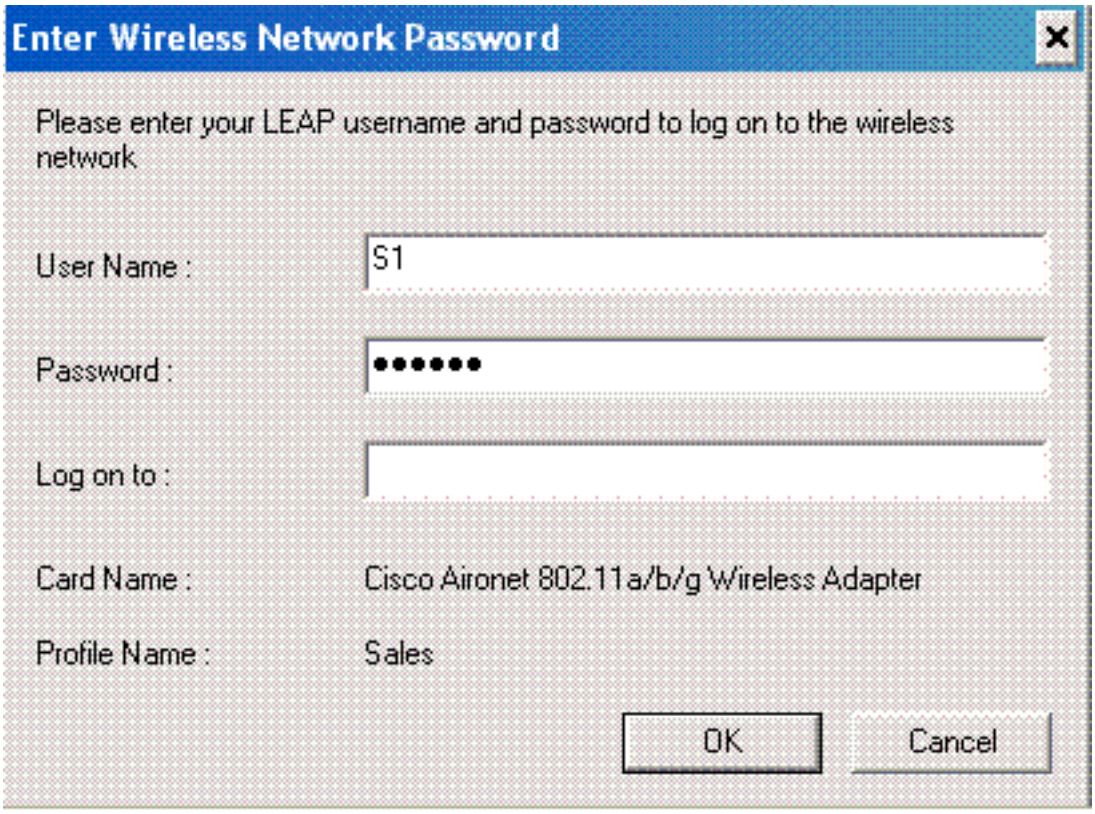
LAP и затем WLC передают учетные данные пользователя внешнему серверу RADIUS (Cisco Secure ACS) для проверки учетных данных. WLC передает учетные данные включая атрибут DNIS (название SSID) к серверу RADIUS для проверки.

Сервер RADIUS проверяет учетные данные пользователя путем сравнения данных с базой данных пользователей (и NAR) и предоставляет доступ к беспроводному клиенту каждый раз, когда учетные данные пользователя допустимы.

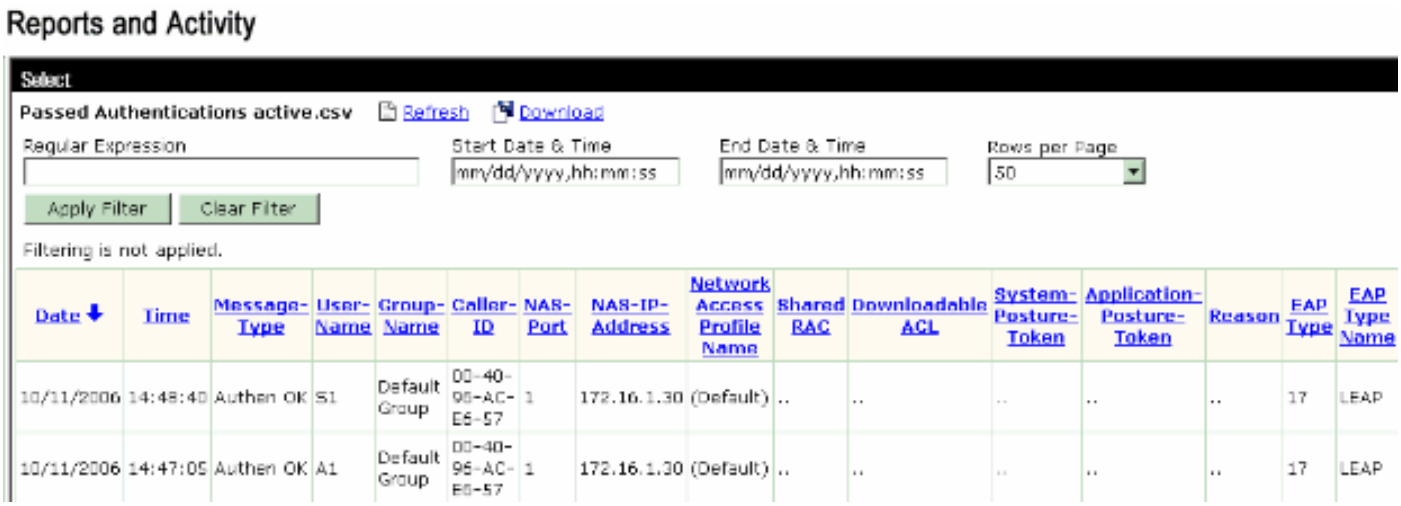
После успешной Проверки подлинности RADIUS беспроводной клиент связывается с LAP.



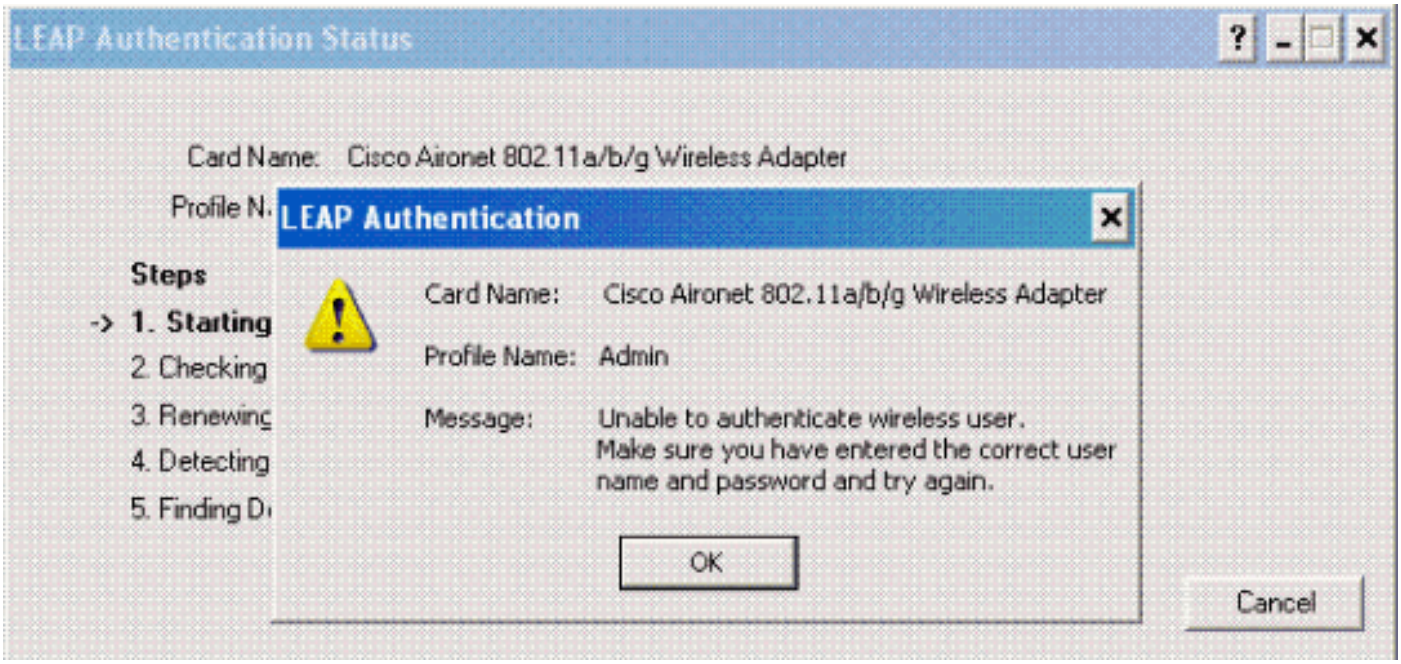
Так же, когда пользователь от Отдела продаж активирует профиль Продаж, пользователь аутентифицируется сервером RADIUS на основе имени пользователя/пароля LEAP и SSID.



Переданный Опознавательный отчёт относительно сервера ACS показывает, что клиент передал Проверку подлинности RADIUS (Аутентификация eap и аутентификация SSID). Например:



Теперь, если Пользователь Продаж пытается обратиться к SSID **Admin**, сервер RADIUS запрещает пользовательский доступ к WLAN. Например:



Таким образом, пользователи могут быть ограниченным доступом на основе SSID. В среде предприятия все пользователи, которые попадают в определенный отдел, могут быть сгруппированы в одиночную группу, и доступ к WLAN может быть предоставлен на основе SSID, который они используют, как объяснено в этом документе.

Устранение неполадок

Команды для устранения неполадок

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

Примечание: Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки".

- **aaa debug dot1x включает** — Включает отладку взаимодействий AAA 802.1x.

- **debug dot1x packet enable – активирует отладку всех пакетов dot1x.**
- **debug aaa all enable – настраивает отладку сообщений AAA.**

Можно также использовать Переданный Опознавательный отчёт и отчёт об Ошибке проверки подлинности относительно сервера Cisco Secure ACS для устранения проблем конфигурации. Эти отчёты находятся под **Отчётами и Окном активности** на GUI ACS.

Дополнительные сведения

- Пример конфигурации аутентификации EAP в контроллерах WLAN (WLC)
- Пример настройки веб-аутентификации контроллера беспроводной LAN
- Пример настройки виртуальных локальных сетей VLAN AP Group с беспроводными сетевыми картами
- Страница поддержки беспроводных технологий
- Cisco Systems – техническая поддержка и документация