Пример настройки перенаправления страницы регистрации контроллера беспроводной LAN

Содержание

Введение

Этот документ описывает способ настройки функции переадресации страницы-заставки на контроллерах беспроводных локальных сетей.

Предварительные условия

Требования

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

- Знание решений по обеспечению безопасности LWAPP
- Знание того, как настроить Cisco Secure ACS

Используемые компоненты

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

- Контроллер беспроводной локальной сети Cisco серии 4400 (WLC), который выполняет версию микропрограммы 5.0
- Cisco точка доступа легкого веса серии 1232 (LAP)
- Cisco Aironet 802.a/b/g адаптер беспроводного клиента, который выполняет версию микропрограммы 4.1
- Сервер Cisco Secure ACS, который выполняет версию 4.1
- Любой сторонний внешний веб-сервер

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

Веб-перенаправление Страницы-заставки является функцией, начатой с Версии 5.0 Контроллера беспроводной локальной сети. С этой функцией пользователь перенаправлен к определенной веб-странице после того, как аутентификация 802.1x завершила. Когда пользователь открывает браузер (настроенный с домашней страницей по умолчанию) или пытается обратиться к URL, перенаправление происходит. После того, как перенаправление к веб-странице завершено, у пользователя есть полный доступ к сети.

Можно задать страницу перенаправления на сервере Сервиса RADIUS. Сервер RADIUS должен быть настроен для возврата Cisco av-pair атрибут RADIUS перенаправления URL к Контроллеру беспроводной локальной сети на успешную аутентификацию 802.1x.

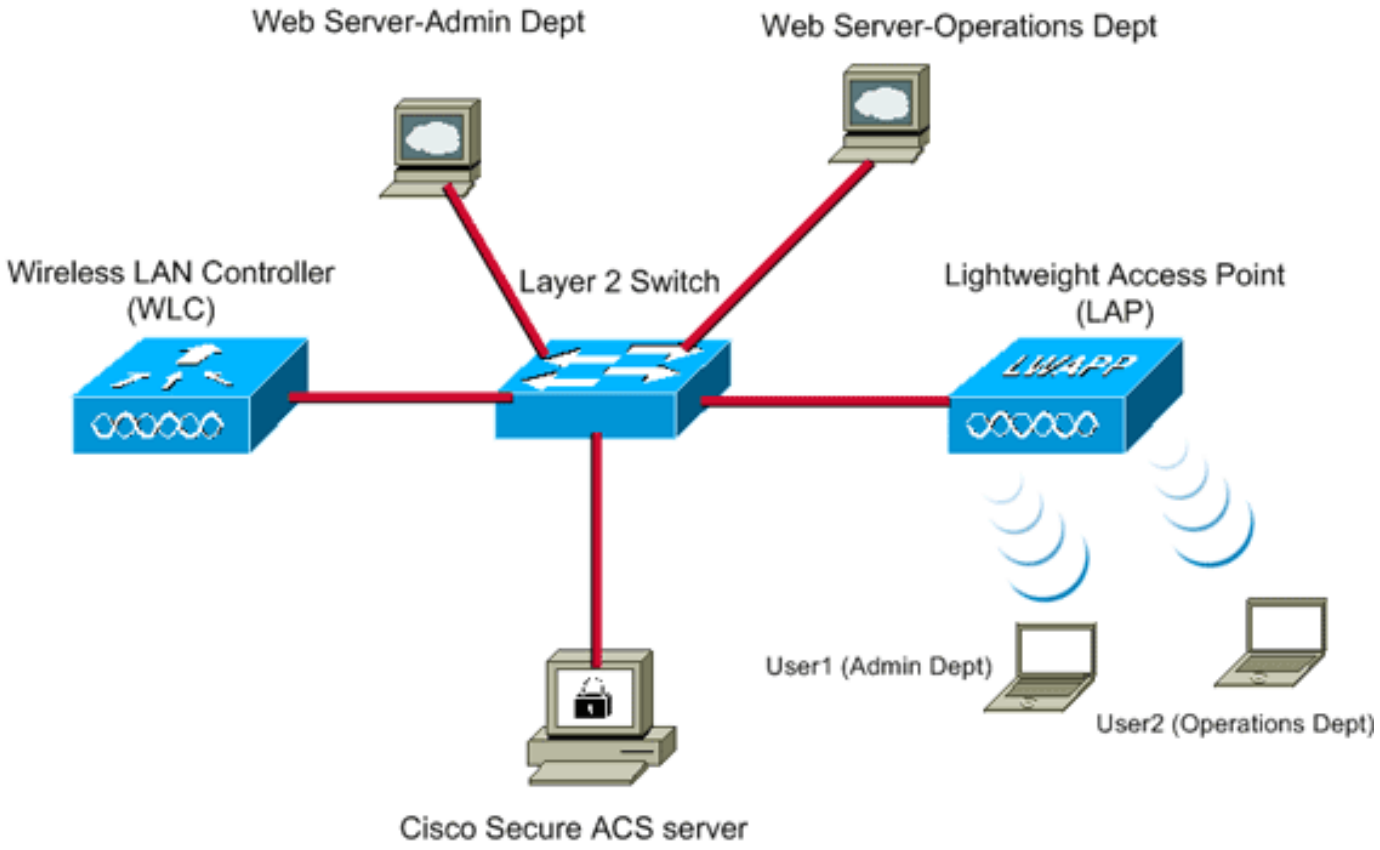
Веб-функция перенаправления Страницы-заставки доступна только для WLAN, настроенных для безопасности уровня 2 WPA/WPA2 или 802.1x.

Настройка сети

В данном примере, WLC Cisco 4404 и Cisco LAP серии 1232 связаны через Коммутатор уровня 2. Сервер Cisco Secure ACS (который действует как внешний сервер RADIUS) также связан с тем же коммутатором. Все устройства находятся в пределах одной подсети.

LAP первоначально зарегистрирован к контроллеру. Необходимо создать два WLAN: один для **Пользователей административного отдела** и другого для пользователей **Отдела Операций**. Оба WPA2 использования Беспроводных локальных сетей / AES (EAP-FAST используется для аутентификации). Оба WLAN используют функцию Перенаправления Страницы-заставки для перенаправления пользователей к соответствующим URL Домашней страницы (на внешних веб-серверах).

В настоящем документе используется следующая схема сети:



WLC Management IP address:	10.77.244.204
WLC AP Manager IP address:	10.77.244.205
Wireless Client IP address:	10.77.244.221
Cisco Secure ACS server IP address	10.77.244.196
Subnet Mask used in this example	255.255.255.224

Следующий раздел объясняет, как настроить устройства для этой настройки.

Настройка

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

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

Выполните эти шаги для настройки устройств для использования функции перенаправления страницы-заставки:

1. Настройте WLC для Проверки подлинности RADIUS через сервер Cisco Secure ACS.
2. Настройте WLAN для отделов Операций и Admin.
3. Настройте Cisco Secure ACS, чтобы поддерживать функцию перенаправления страницы-заставки.

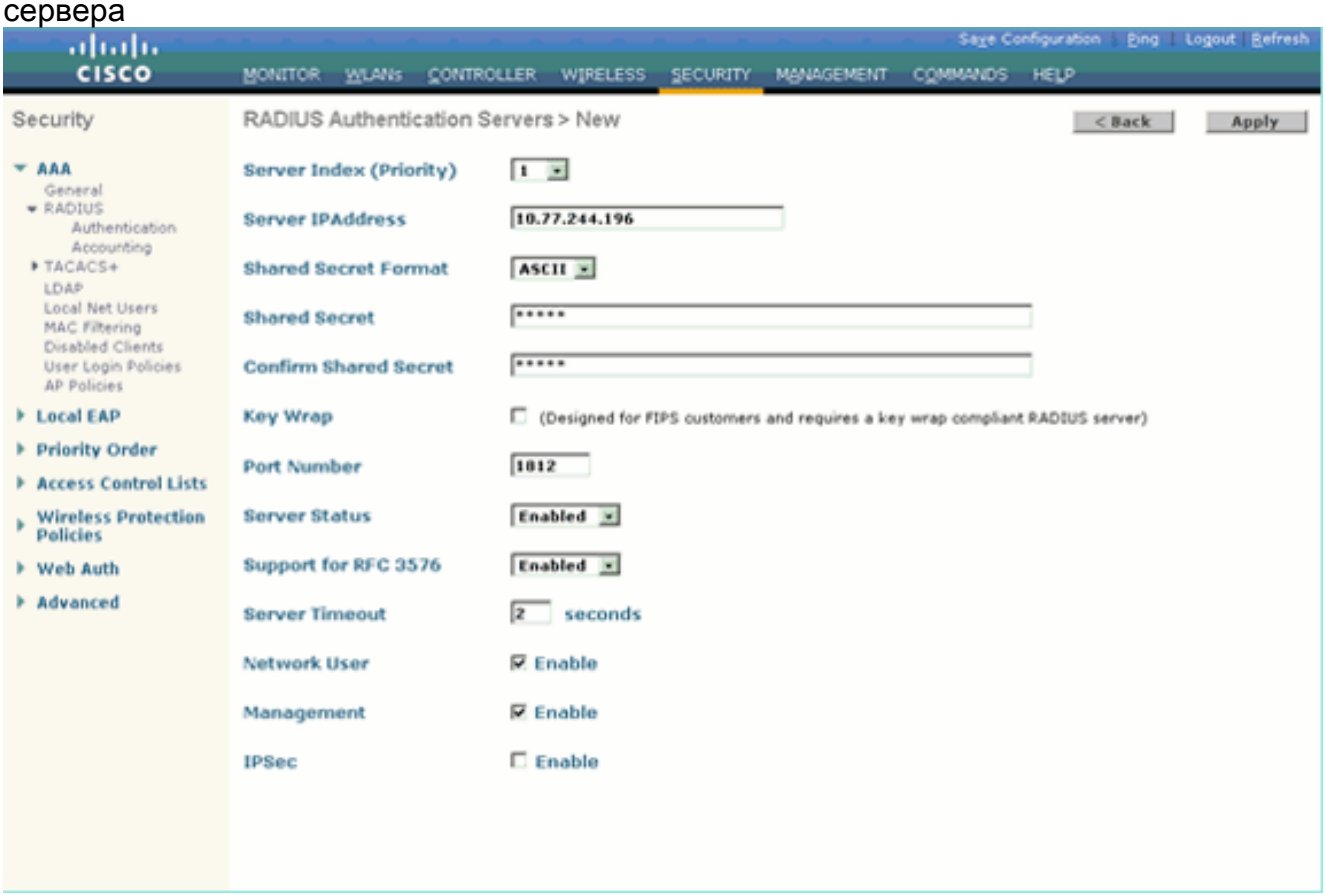
Шаг 1. Настройте WLC для Проверки подлинности RADIUS через сервер Cisco

Secure ACS.

Необходимо настроить WLC для переадресации на внешний сервер RADIUS учетные данные пользователя.

Чтобы настроить WLC для внешнего сервера RADIUS, выполните следующие действия:

1. Выберите **Security** и **RADIUS Authentication** от графического интерфейса контроллера для отображения страницы RADIUS Authentication Servers.
2. Нажмите **New** для определения сервера RADIUS.
3. Определите параметры сервера RADIUS на странице RADIUS Authentication Servers> New.В их числе:IP-адрес сервера RADIUSОбщий secretPort numberСостояние сервера



Этот документ использует сервер ACS с IP-адресом 10.77.244.196.

4. **Щелкните "Применить".**

Шаг 2. Настройте WLAN для отдела Операций и Admin.

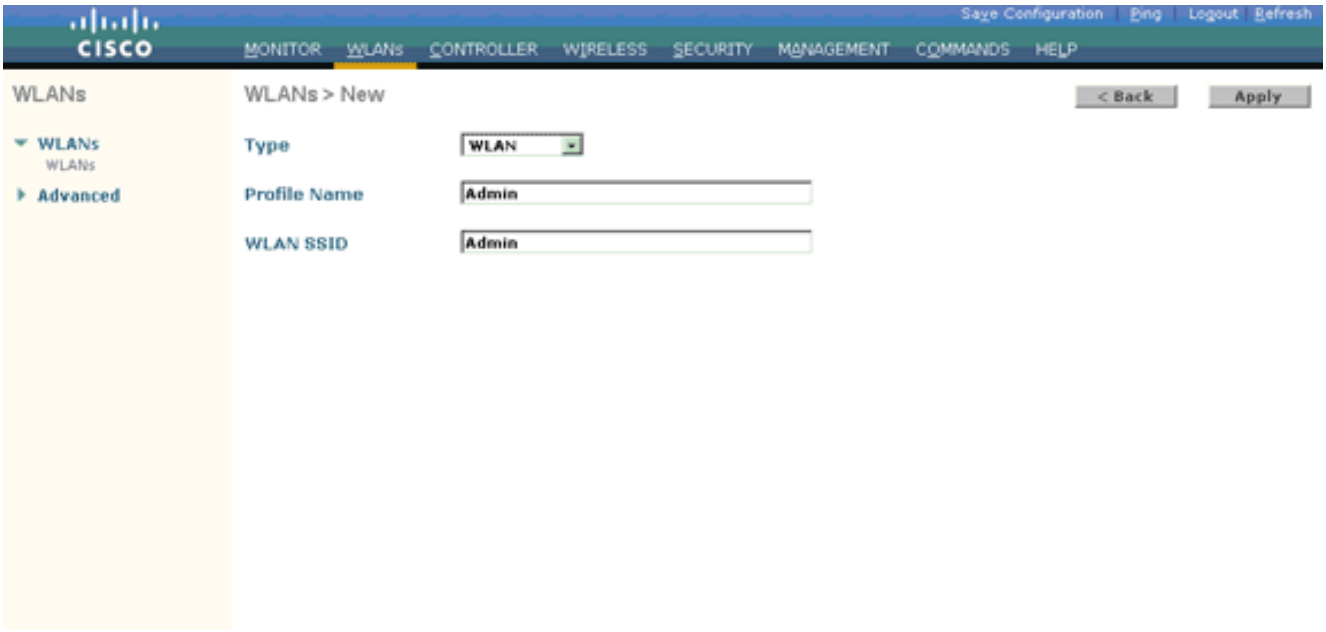
В этом шаге вы настраиваете эти два WLAN (один для Административного отдела и другого для отдела Операций), который клиенты будут использовать для соединения с беспроводной сетью.

SSID WLAN для Административного отдела будет *Admin*. SSID WLAN для отдела Операций будут Операции.

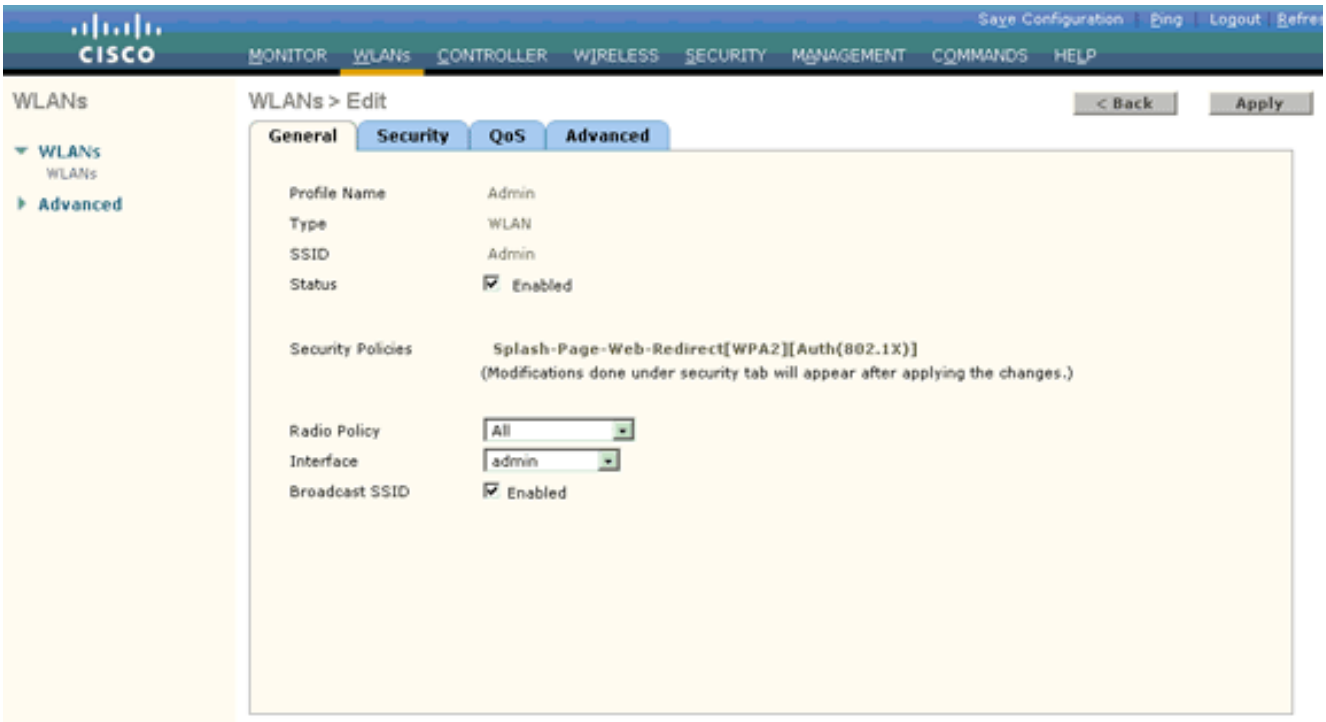
Используйте аутентификацию EAP-FAST для включения WPA2 как механизма безопасности уровня 2 на обоих WLAN и веб-политике - веб-функция Перенаправления Страницы-заставки как метод безопасности уровня 3.

Выполните эти шаги для настройки WLAN и его связанных параметров:

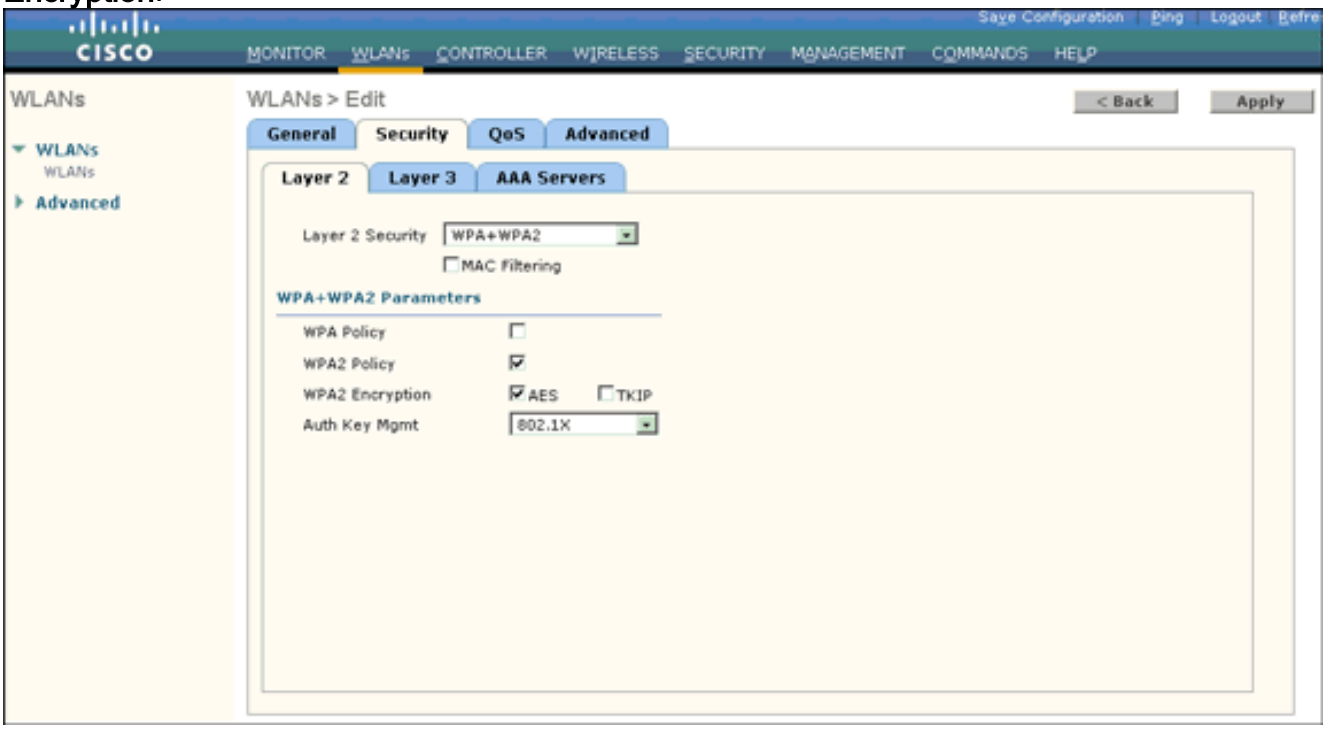
1. **Выберите WLANs в GUI контроллера, чтобы открыть страницу WLANs.**Эта страница перечисляет WLAN, которые существуют на контроллере.
2. Нажмите **New** для создания нового
   WLAN.



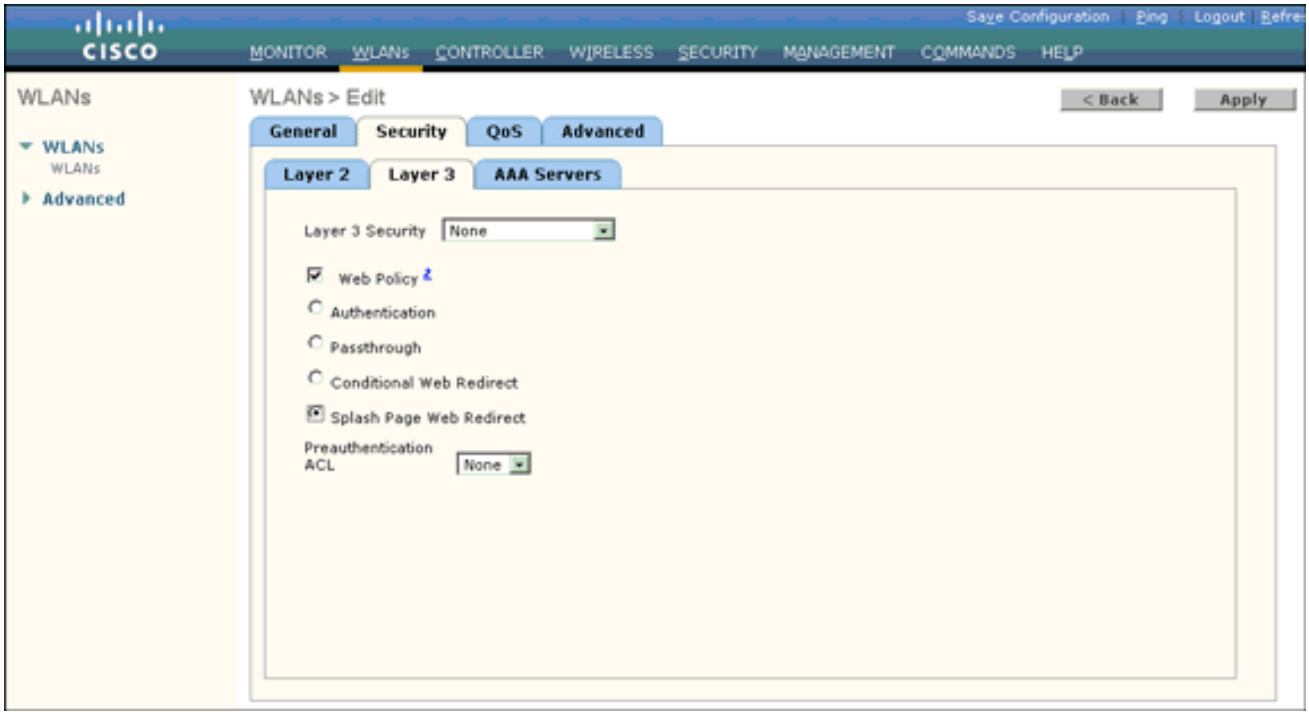
3. Введите имя SSID WLAN и Имя профиля на странице WLAN> New.
4. **Щелкните "Применить".**
5. Сначала давайте создадим WLAN для Административного отдела.После создания новой WLAN появляется страница WLAN > Edit для новой WLAN. На этой странице можно определить различные параметры, определенные для этого WLAN. Это включает Общую политику, Политику безопасности, политики QoS и Усовершенствованные параметры.
6. В соответствии с Общей политикой, установите флажок **Проверки состояния** для включения
   WLAN.



7. Нажмите **Вкладку Безопасность**, и затем нажмите **Таблицу уровня 2**.
8. Выберите **WPA+WPA2** из выпадающего списка безопасности уровня 2.Этот шаг включает аутентификацию WPA для WLAN.
9. Под Параметрами WPA+WPA2 проверьте флажки **WPA2 Policy и AES Encryption**.

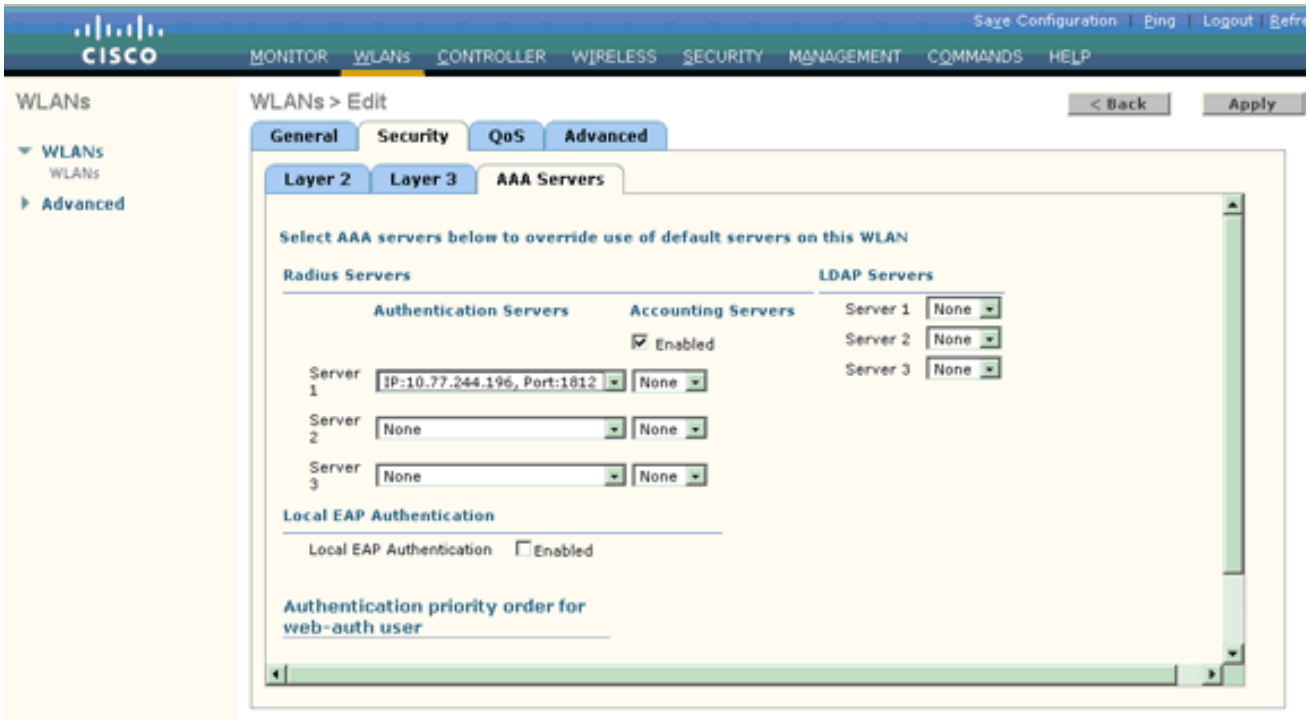


10. Выберите **802.1x** из Подлинного Ключевого выпадающего списка Mgmt. Эта опция включает WPA2 с 802.1X/АУТЕНТИФИКАЦИЕЙ EAP и шифрованием AES для WLAN.
11. Нажмите вкладку **безопасности уровня 3**.
12. Установите **веб-**флажок **Политики**, и затем нажмите кнопку с зависимой фиксацией **Splash Page Web Redirect**.Эта опция активирует веб-опцию Перенаправления страницы-
заставки.



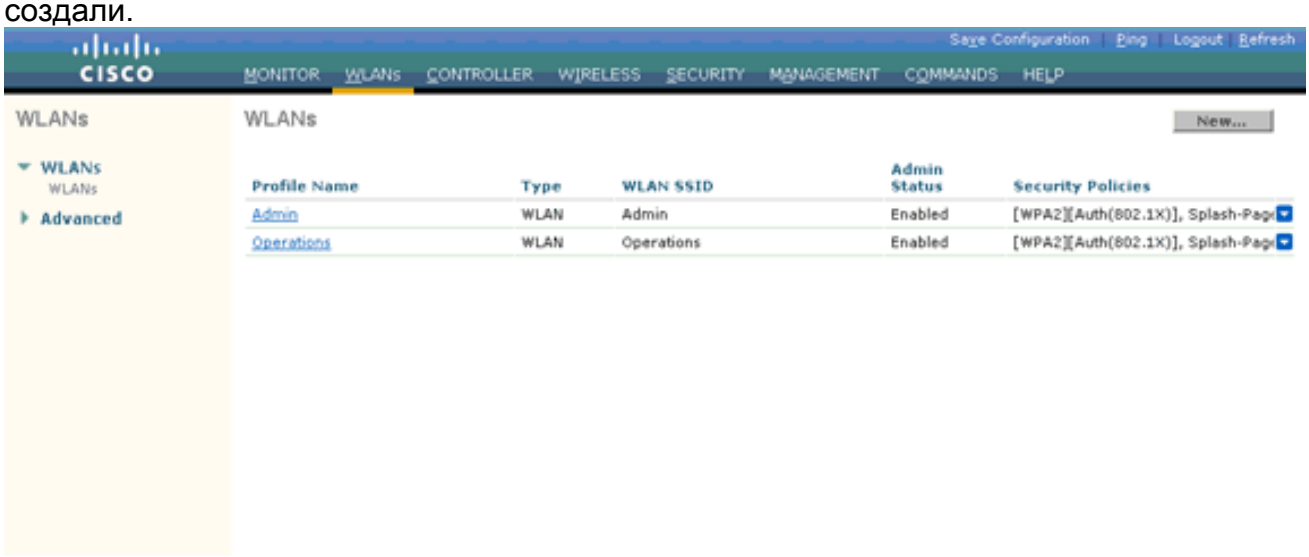
13. Нажмите вкладку **AAA Servers**.
14. Под Серверами проверки подлинности выберите соответствующий IP-адрес сервера

из Сервера 1 выпадающий
список.



В данном примере, 10.77.244.196 используется в качестве сервера RADIUS.

15. **Щелкните "Применить".**
16. Повторите шаги 2 - 15 для создания WLAN для отдела Операций.Страница WLANs перечисляет два WLAN, которые вы
создали.



Заметьте, что политика безопасности включает перенаправление страницы-заставки.

Шаг 3. Настройте Cisco Secure ACS, чтобы поддерживать функцию перенаправления Страницы-заставки.

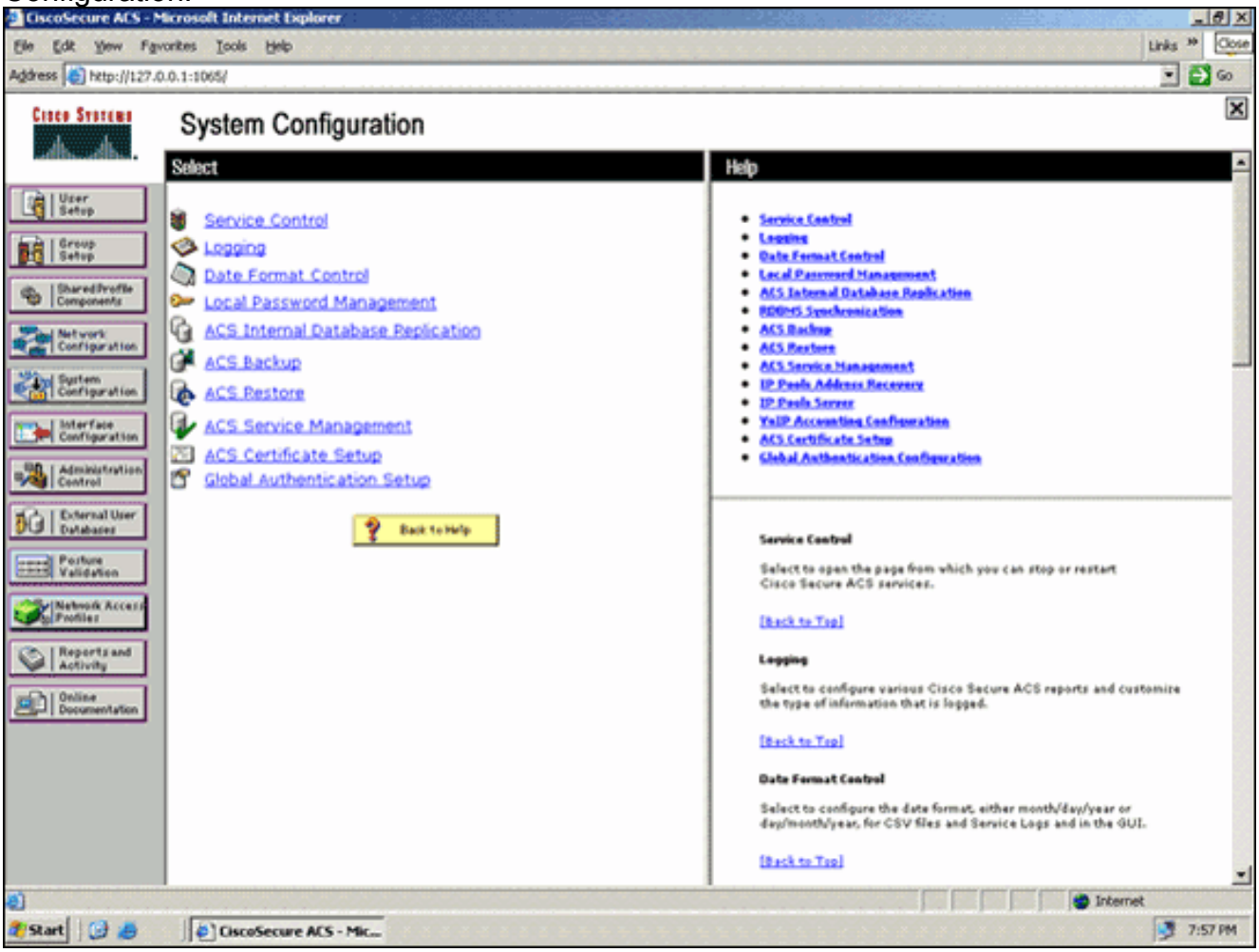
Следующий шаг должен настроить сервер RADIUS для этой функции. Сервер RADIUS должен выполнить аутентификацию EAP-FAST для проверки удостоверений клиента, и после успешной аутентификации, для перенаправления пользователя к URL (на внешнем веб-сервере) заданный у Cisco av-pair атрибут RADIUS ***перенаправления URL***.

Настройте Cisco Secure ACS для аутентификации EAP-FAST

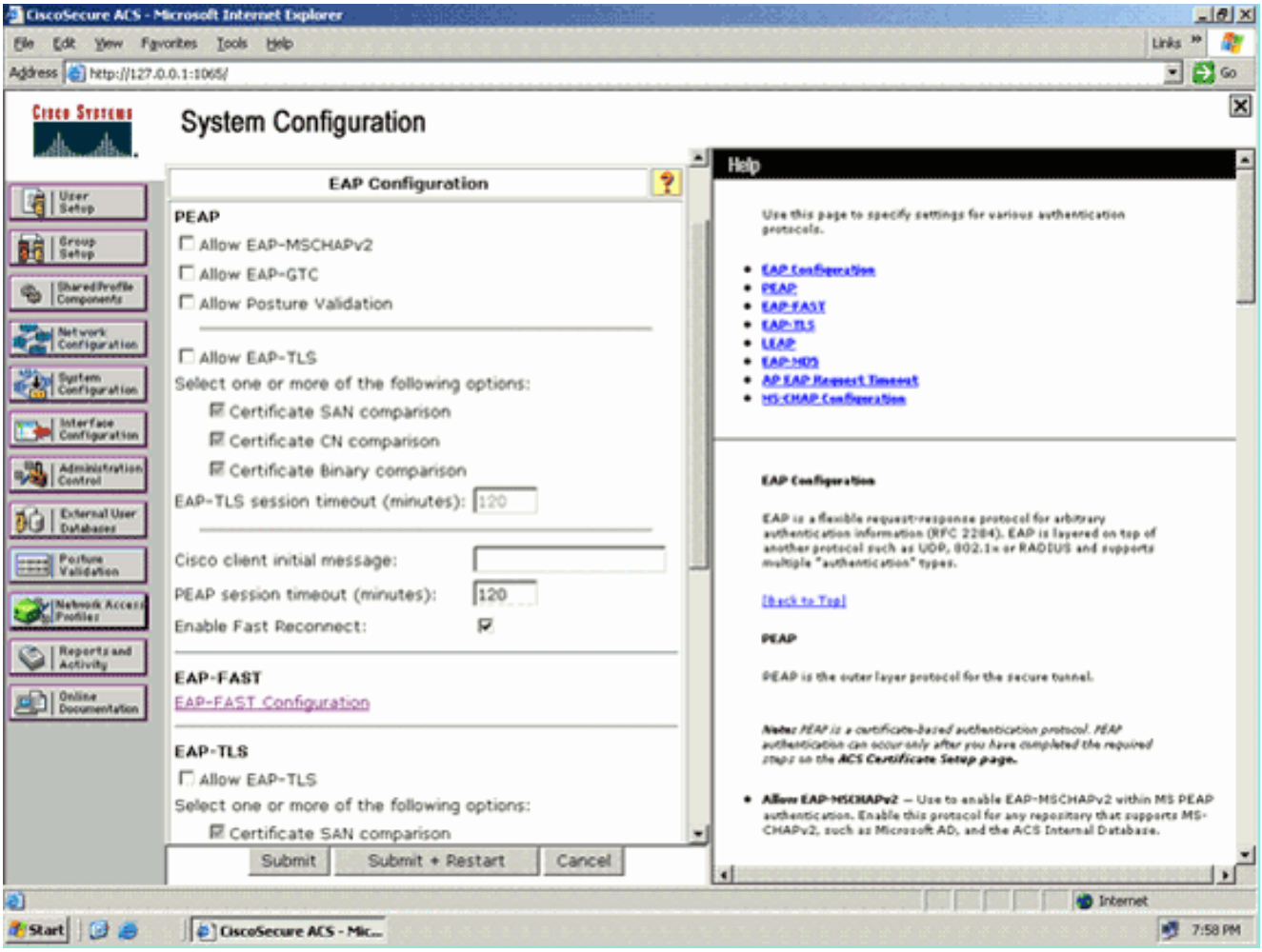
Примечание: Этот документ предполагает, что Контроллер беспроводной локальной сети добавлен к Cisco Secure ACS как клиент AAA.

Выполните эти шаги для настройки аутентификации EAP-FAST в сервере RADIUS:

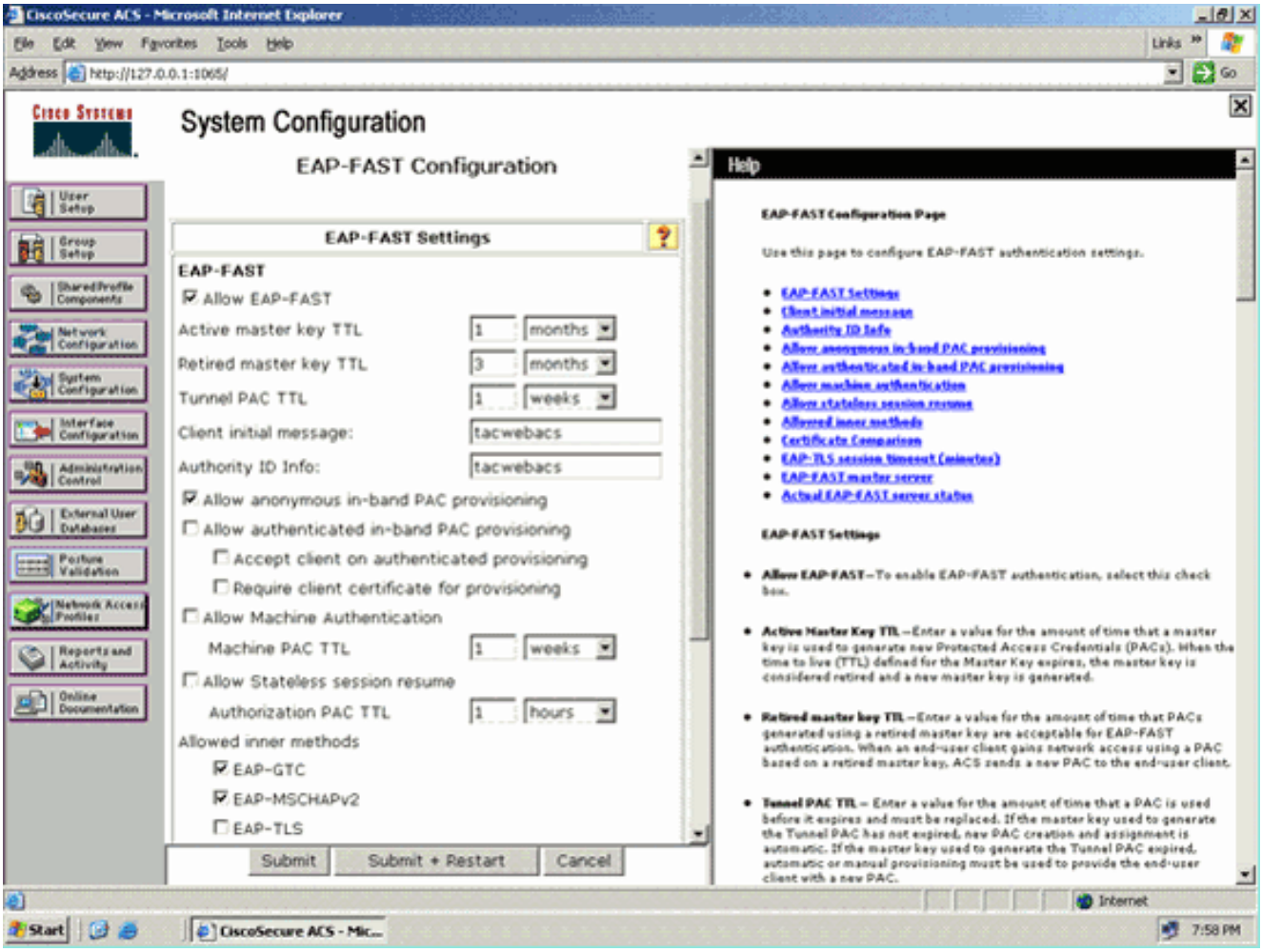
1. Нажмите **System Configuration** от GUI сервера RADIUS, и затем выберите, выбирают **Global Authentication Setup** из страницы System Configuration.



2. От страницы настройки Глобальной аутентификации нажмите **EAP-FAST Configuration**, чтобы перейти к странице настроек EAP-FAST.



3. От Страницы настроек EAP-FAST проверьте флажок **Allow EAP-FAST** для включения EAP-FAST в сервере
RADIUS.



4. Настройте Активный/Исключенный TTL главного ключа (Время существования) значения, как желаемый или установите его в значение по умолчанию как показано в данном примере.Поле Authority ID Info представляет текстовую идентичность этого сервера ACS, который конечный пользователь может использовать для определения который сервер ACS аутентифицироваться против. Заполнение этого поля является обязательным.Клиентская начальная буква отображается, поле сообщения задает сообщение, которое будет передаваться пользователям, которые аутентифицируются с клиентом EAP-FAST. Максимальная длина составляет 40 символов. Пользователь будет видеть начальное сообщение только если поддержки клиентов конечного пользователя показ.
5. Если вы хотите, чтобы ACS выполнил анонимную внутриполосную инициализацию PAC, проверьте **Позволение анонимного внутриполосного** флажка **инициализации PAC**.
6. *Позволенная внутренняя* опция *методов* определяет, какие внутренние методы EAP могут работать в туннеле TLS EAP-FAST. Для анонимной внутриполосной инициализации необходимо включить EAP-GTC и MS-CHAP EAP для обратной совместимости. При выборе Allow анонимная внутриполосная инициализация PAC необходимо выбрать EAP-MS-CHAP (фазовый нуль) и EAP-GTC (фаза два).
7. **Нажмите кнопку Submit (Отправить).Примечание:** Для получения дальнейшей информации и примеры о том, как настроить FAST EAP с Анонимной Внутриполосной Инициализацией PAC и Аутентифицируемой Внутриполосной Инициализацией, обратитесь к Аутентификации EAP-FAST с Примером конфигурации Внешнего сервера RADIUS и Контроллерами беспроводной локальной сети.

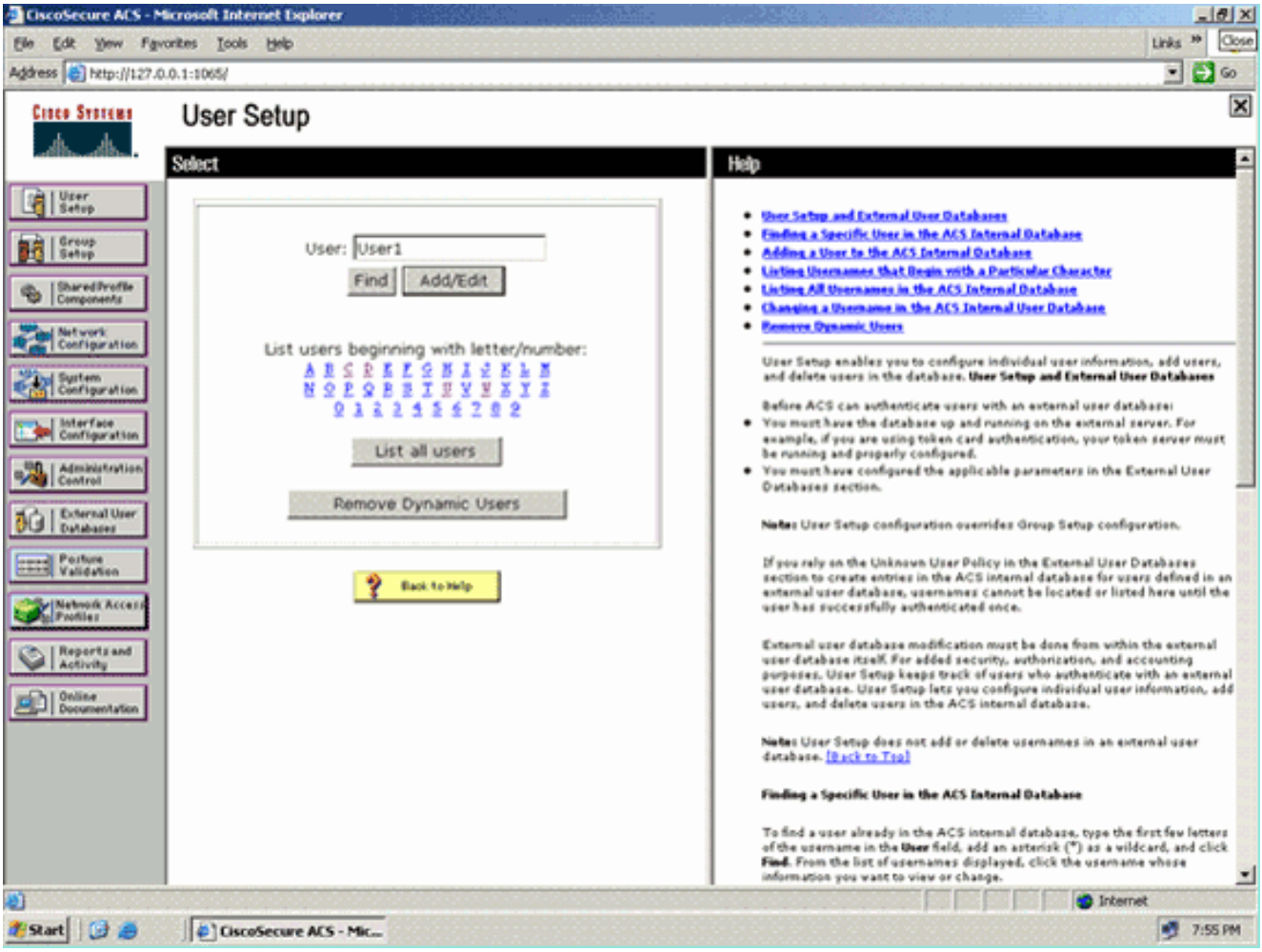
Настройте Базу данных пользователей и определите атрибут RADIUS *перенаправления*

URL

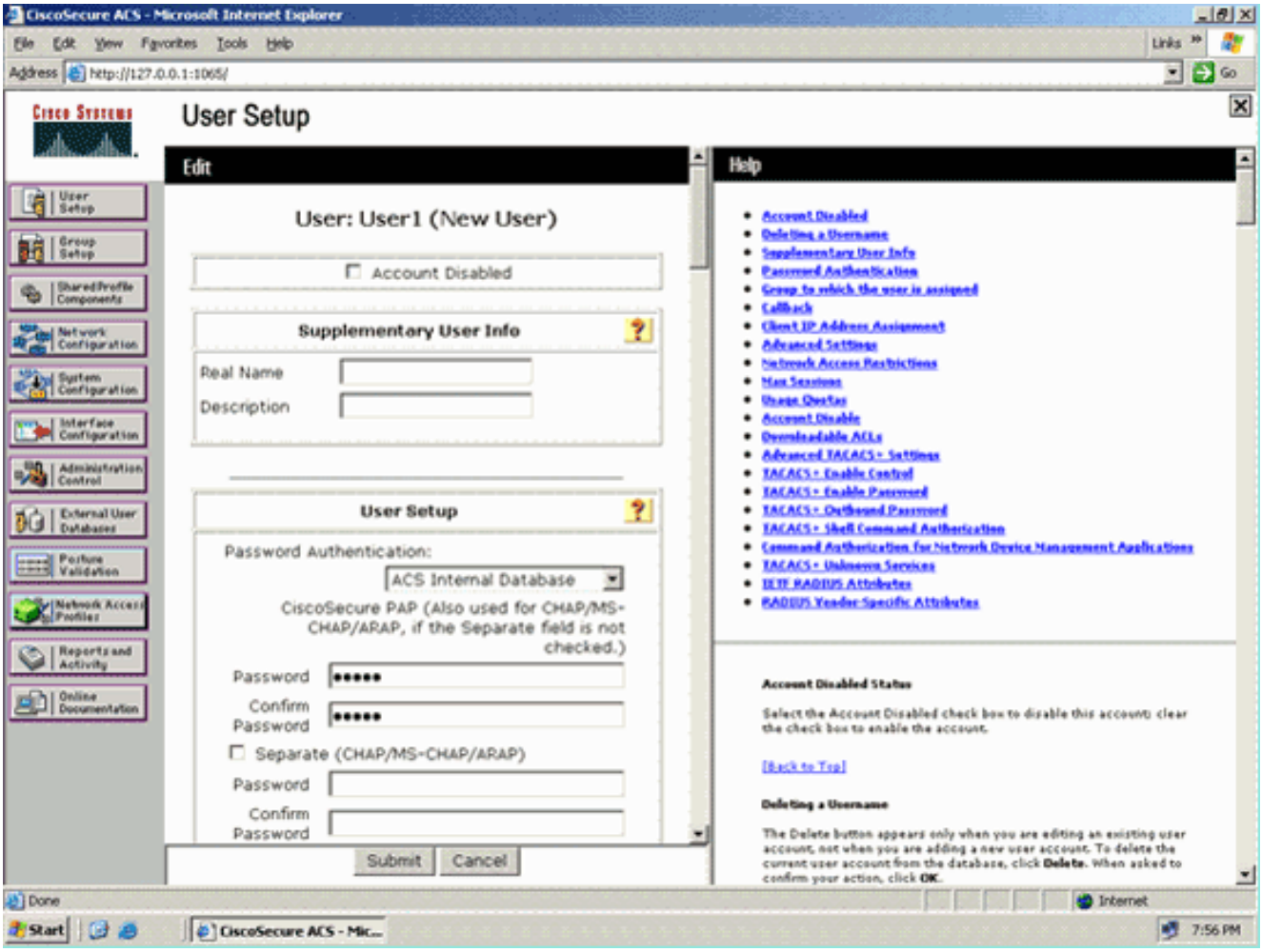
Данный пример настраивает имя пользователя и пароль беспроводного клиента как User1 и User1, соответственно.

Выполните эти шаги для создания базы данных пользователей:

1. От GUI ACS в панели навигации выберите **User Setup**.
2. Создайте радио нового пользователя, и затем нажмите **Add/Edit**, чтобы перейти к странице Edit этого пользователя.



3. От страницы Edit Настройки пользователя настройте Настоящее имя и Описание, а также Вводы пароля, как показано в данном примере.Этот документ использует Внутреннюю базу данных ACS для Проверки подлинности с помощью пароля.



4. Прокрутите страницу вниз для изменения атрибутов RADIUS.
5. Проверьте **[009\001]** флажок **Cisco-av-pair**.
6. Введите этот Cisco av-пары в [009\001] окно редактирования Cisco-av-pair для определения URL, к которому перенаправлен пользователь:url-redirect=http://10.77.244.196/Admin-Login.html

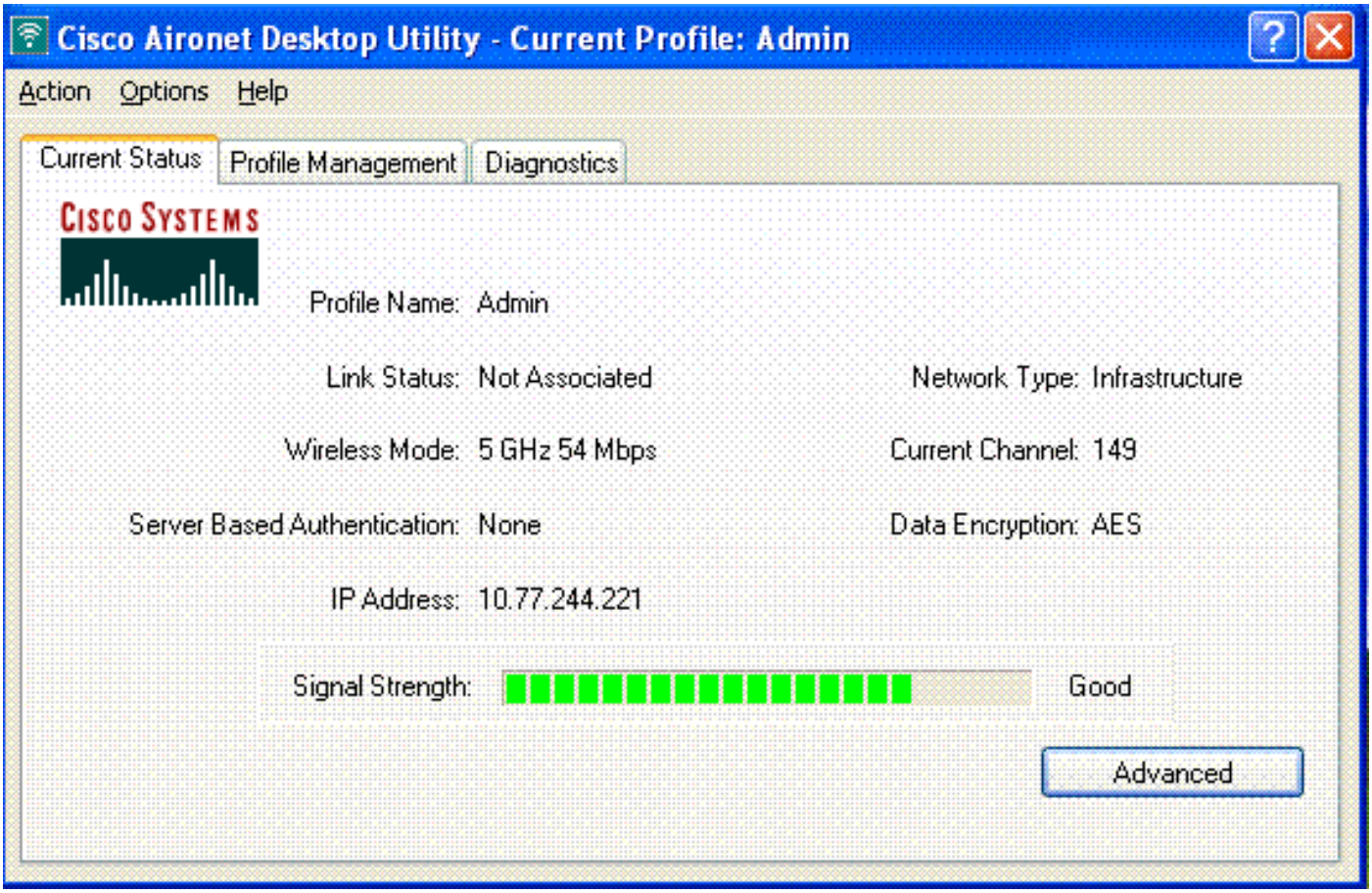
Это - домашняя страница Пользователей административного отдела.

7. **Нажмите кнопку Submit (Отправить).**
8. Повторите эту процедуру для добавления User2 (Пользователь отдела операций).
9. Повторите шаги 1 - 6 для добавления большего количества Пользователей административного отдела и пользователей отдела Операций к базе данных.**Примечание:** Атрибуты RADIUS могут быть настроены в пользовательском уровне или уровне группы на Cisco Secure ACS.

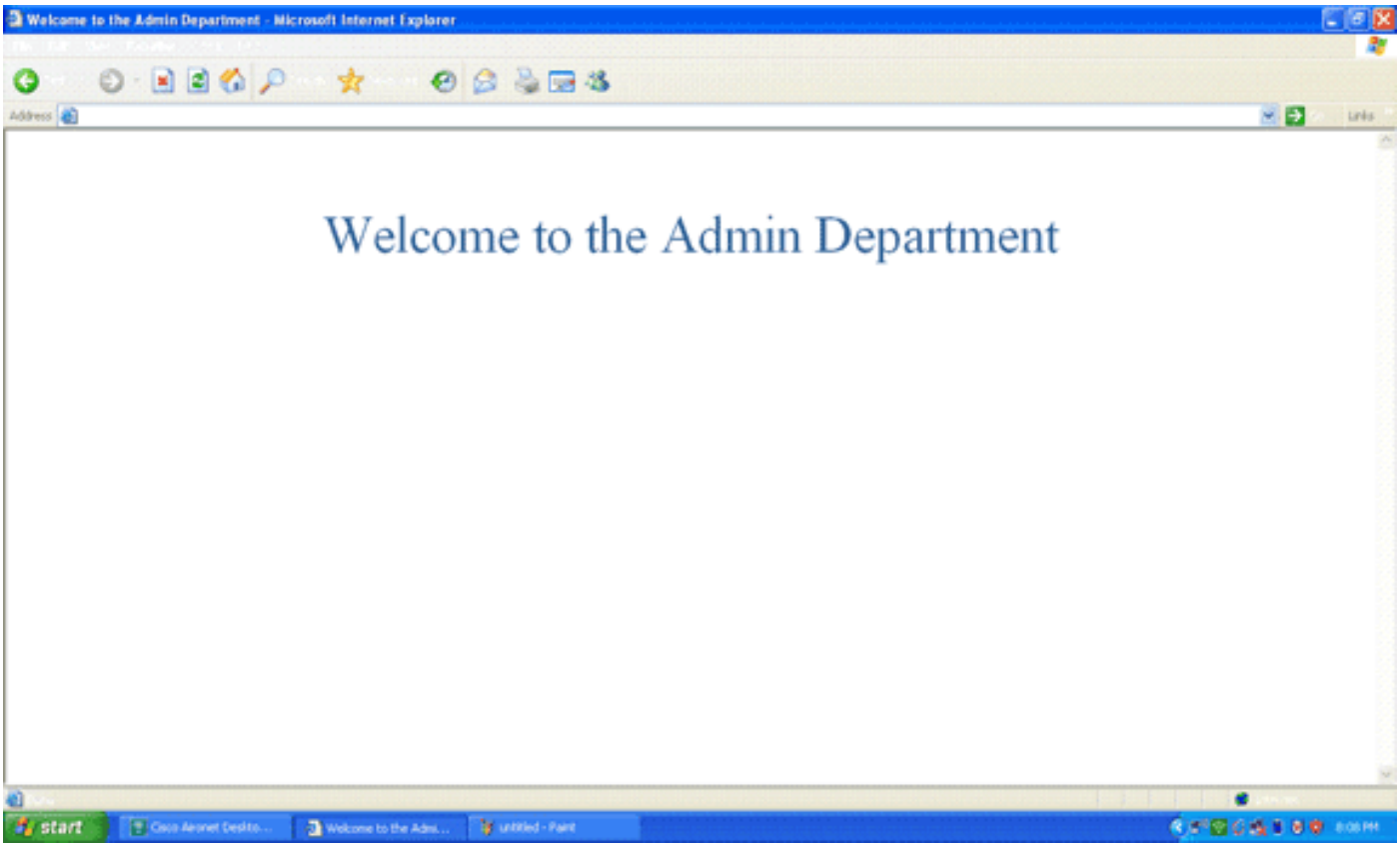
Проверка

Для проверки конфигурации привяжите клиента сетей WLAN от Административного отдела и отдела Операций к их соответствующим WLAN.

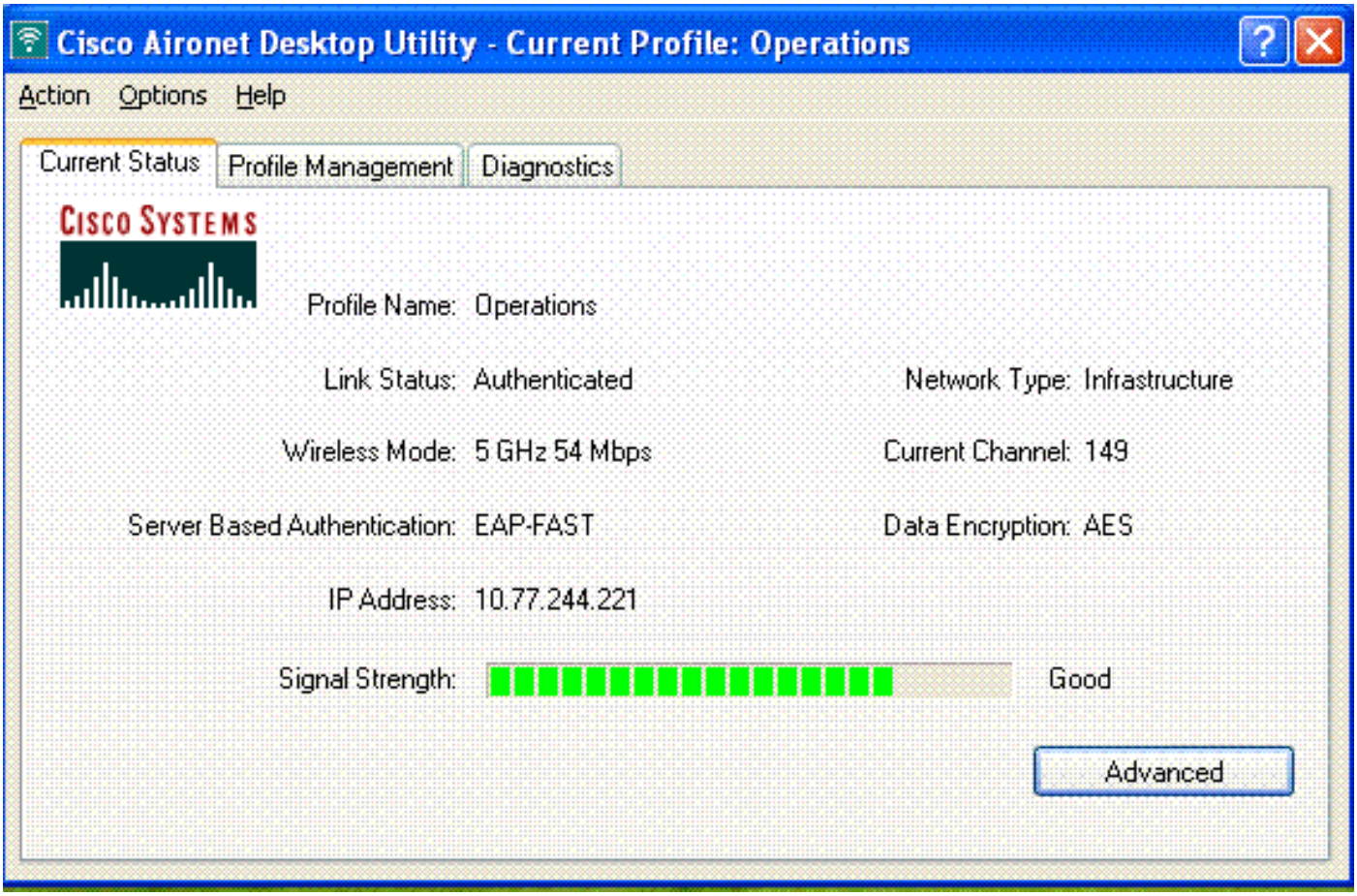
Когда пользователь от подключений Административного отдела до Admin Беспроводной локальной сети, пользователю предлагают для учетных данных 802.1x (учетные данные EAP-FAST в нашем случае). Как только пользователь предоставляет учетные данные, WLC передает те учетные данные к серверу Cisco Secure ACS. Сервер Cisco Secure ACS проверяет учетные данные пользователя против базы данных, и после успешной аутентификации, возвращает атрибут перенаправления URL к Контроллеру беспроводной локальной сети. Аутентификация завершена на данном этапе.

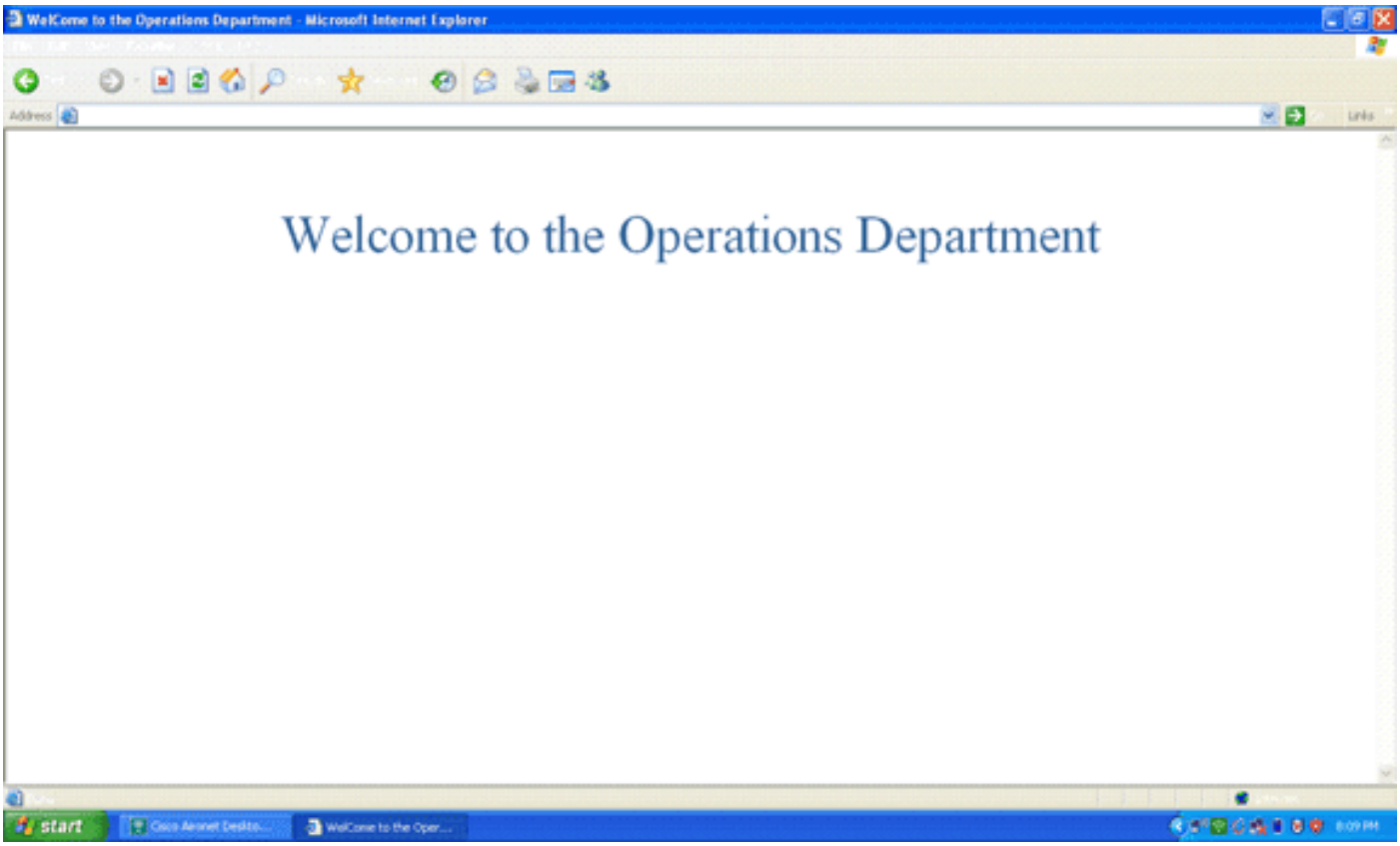


Когда пользователь открывает web-браузер, пользователь перенаправлен к URL домашней страницы Административного отдела. (Этот URL возвращен к WLC через атрибут Cisco-av-pair). После перенаправления у пользователя есть полный доступ к сети. Вот снимки экрана:



Когда пользователь от отдела Операций соединяется с Операциями WLAN, те же последовательности событий происходят.





Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Примечание: Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с

документом "Важные сведения о командах отладки".

Можно использовать следующие команды для устранения проблем конфигурации.

- **show wlan wlan_id** — Отображает статус веб-функций перенаправления определенного WLAN.Например:
```
WLAN Identifier.................................. 1
Profile Name..................................... Admin
Network Name (SSID).............................. Admin
...
Web Based Authentication......................... Disabled
Web-Passthrough.................................. Disabled
Conditional Web Redirect......................... Disabled
Splash-Page Web Redirect......................... Enabled
```
- **debug dot1x events enable** — Включает отладку пакетных сообщений 802.1x.Например:
```
Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Sending EAP Request from AAA to mobile 00:40:96:ac:dd:05 (EAP Id 16) Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Received EAPOL EAPPKT from mobile 00:40:96:ac:dd:05 Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Received EAP Response from mobile 00:40:96:ac:dd:05 (EAP Id 16, EAP Type 43) Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Processing Access-Challenge for mobile 00:40:96:ac:dd:05 Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Setting re-auth timeout to 1800 seconds, got from WLAN config. Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Station 00:40:96:ac:dd:05 setting dot1x reauth timeout = 1800 Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Creating a new PMK Cache Entry for station 00:40:96:ac:dd:05 (RSN 2) Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Adding BSSID 00:1c:58:05:e9:cf to PMKID cache for station 00:40:96:ac:dd:05 Fri Feb 29 10:27:16 2008: New PMKID: (16) Fri Feb 29 10:27:16 2008: [0000] 79 ee 88 78 9c 71 41 f0 10 7d 31 ca fb fa 8e 3c Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Disabling re-auth since PMK lifetime can take care of same. Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Sending EAP-Success to mobile 00:40:96:ac:dd:05 (EAP Id 17) Fri Feb 29 10:27:16 2008: Including PMKID in M1 (16) Fri Feb 29 10:27:16 2008: [0000] 79 ee 88 78 9c 71 41 f0 10 7d 31 ca fb fa 8e 3c Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Sending EAPOL-Key Message to mobile 00:40:96:ac:dd:05 state INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00 Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Received Auth Success while in Authenticating state for mobile 00:40:96:ac:dd:05
```
- **debug aaa events enable** — Включает выходные данные отладки всех событий aaa.Например:
```
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Successful transmission of Authentication Packet (id 103) to 10.77.244.196:1812, proxy state 00:40:96:ac:dd:05-00:00 Thu Feb 28 07:55:18 2008: ****Enter processIncomingMessages: response code=11 Thu Feb 28 07:55:18 2008: ****Enter processRadiusResponse: response code=11 Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Access-Challenge received from RADIUS server 10.77.244.196 for mobile 00:40:96:ac:dd:05 receiveId = 3 Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Successful transmission of Authentication Packet (id 104) to 10.77.244.196:1812, proxy state 00:40:96:ac:dd:05-00:00 Thu Feb 28 07:55:18 2008: ****Enter processIncomingMessages: response code=2 Thu Feb 28 07:55:18 2008: ****Enter processRadiusResponse: response code=2 Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Access-Accept received from RADIUS server 10.77.244.196 for mobile 00:40:96:ac:dd:05 receiveId = 3 Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 AAA Override Url-Redirect 'http://10.77.244.196/Admin-login.html' set Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Applying new AAA override for station 00:40:96:ac:dd:05 Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Override values for station 00:40:96:ac:dd:05 source: 4, valid bits: 0x0 qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1 dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1 vlanIfName: '', aclName: '
```

Дополнительные сведения

- Руководство по конфигурированию контроллера Cisco Wireless LAN, выпуск 5.0
- Пример настройки веб-аутентификации контроллера беспроводной LAN
- Пример настройки контроллера беспроводной сети с внешней веб-аутентификацией
- Страница поддержки беспроводных технологий

- Cisco Systems – техническая поддержка и документация