Пример настройки веб-аутентификации контроллера беспроводной LAN

Содержание

Введение

Этот документ объясняет, как Cisco внедряет web-аутентификацию и показывает, как настроить Cisco Беспроводная локальная сеть серии 4400 (WLAN) Контроллер (WLC) для поддержки Внутренней веб-аутентификации.

Предварительные условия

Требования

Этот документ предполагает, что у вас уже есть начальная конфигурация на 4400 WLC.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного

обеспечения и оборудования:

- WLC серии 4400, который выполняет версию 7.0.116.0
- Сервер Cisco Secure Access Control Server (ACS) версия 4.2 установлен на Microsoft® Windows 2003 Server
- Cisco Aironet точка доступа легкого веса серии 1131AG
- Беспроводной адаптер a/b/g CardBus 802.11 Cisco Aironet, который выполняет версию 4.0

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

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

Web-аутентификация

Web-аутентификация является функцией безопасности уровня 3, которая заставляет контроллер не позволять IP - трафик (кроме DHCP и DNS связанные пакеты) от конкретного клиента, пока тот клиент правильно не предоставил допустимое имя пользователя и пароль. Это - метод простой проверки подлинности без потребности в соискателе или служебной программе клиента. Web-аутентификация, как правило, используется клиентами, которые хотят развернуть сеть гостевого доступа. Типичные развертывания могут включать местоположения "оперативной точки", такие как T-Mobile или Starbucks.

Следует иметь в виду, что web-аутентификация не предоставляет шифрование данных. Веб-проверка подлинности обычно используется в качестве простого гостевого доступа для так называемых "горячих точек" (точек общего доступа) или кампусов, где важна сама возможность подключения.

Web-аутентификация может быть выполнена с помощью:

- Окно входа в систему по умолчанию на WLC
- Измененная версия окна входа в систему по умолчанию на WLC
- Специализированное окно входа в систему, которое вы настраиваете на внешнем веб-сервере (Внешняя веб-аутентификация)
- Специализированное окно входа в систему, которое вы загружаете к контроллеру

В этом документе настроен Контроллер беспроводной локальной сети для Внутренней веб-аутентификации.

Процесс веб-аутентификации

Это - то, что происходит, когда пользователь соединяется с WLAN, настроенным для web-аутентификации:

- Пользователь открывает web-браузер и вводит URL, например, http://www. cisco . com.

Клиент отсылает запрос DNS для этого URL для получения IP для назначения. WLC обходит запрос DNS к серверу DNS, и сервер DNS отвечает назад ответом DNS, который содержит IP-адрес целевого www. cisco . com. Это, в свою очередь, передано беспроводным клиентам.

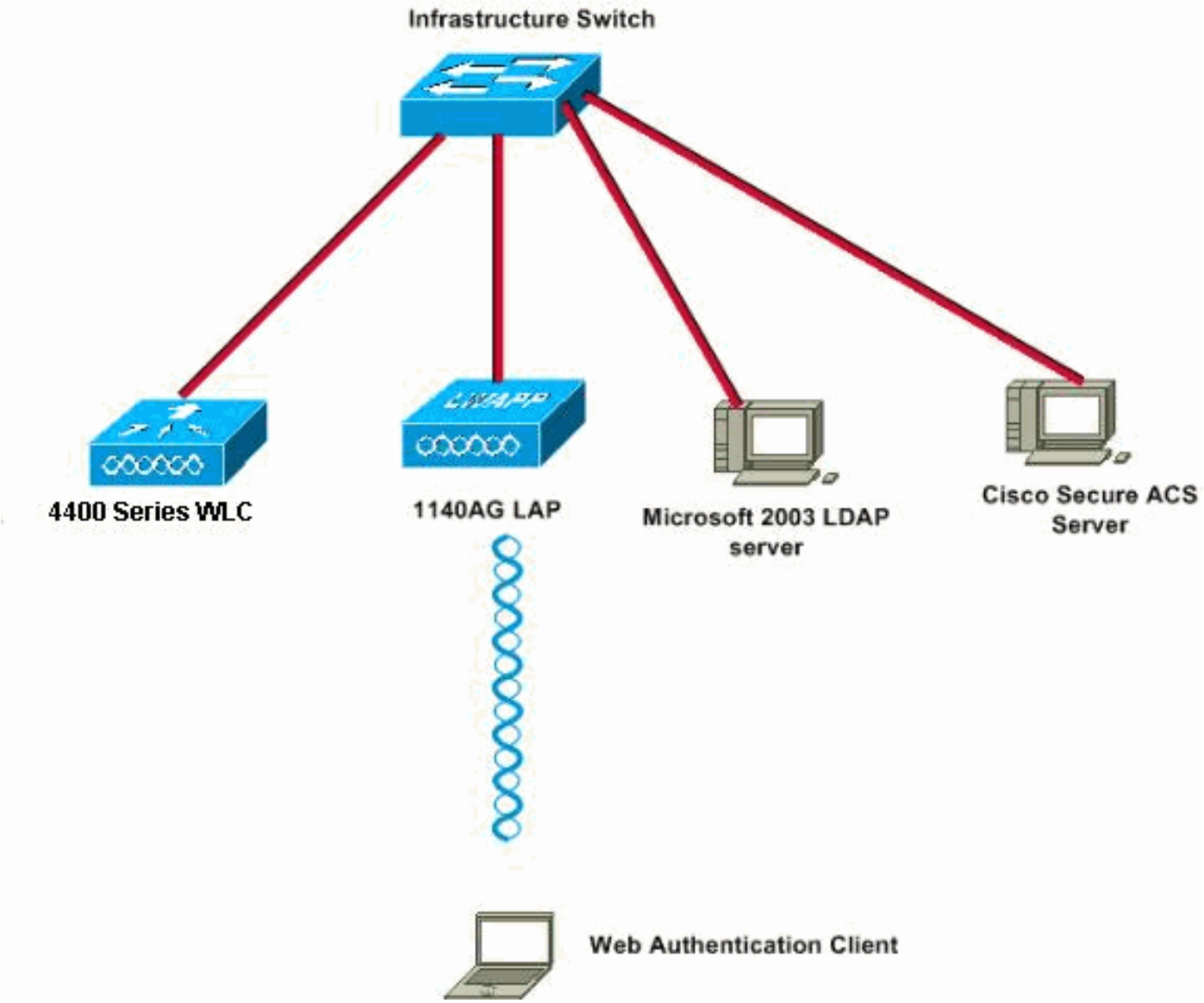
- Клиент тогда пытается открыть TCP - подключение с IP - адресом назначения. Это отсылает Пакет TCP SYN, предназначенный в IP-адрес www. cisco . com.
- WLC имеет правила, настроенные для клиента, и следовательно может действовать как прокси для www. cisco . com. Это передает пакет SYN-ACK TCP обратно клиенту с источником как IP-адрес www. cisco . com. Клиент передает пакет ACK TCP обратно для завершения трех способов, которыми полностью установлены квитирование TCP - подключения и TCP - подключение.
- Клиент передает пакет GET HTTP, предназначенный к www. cisco . com. WLC перехватывает этот пакет и передает его за обработкой перенаправления. Шлюз приложений HTTP готовит "тело" HTML и передает его обратно как ответ на GET HTTP, который запрашивает клиент. Этот HTML заставляет клиента перейти к URL веб-страницы по умолчанию WLC, например, http://<Действительный IP - сервер>/login.html.
- Клиент закрывает TCP - подключение с IP-адресом, например, www. cisco . com.
- Теперь клиент хочет перейти к http://1.1.1.1/login.html. Поэтому клиент пытается открыть TCP - подключение с виртуальным IP - адресом WLC. Это передает Пакет TCP SYN за 1.1.1.1 к WLC.
- WLC отвечает назад SYN-ACK TCP, и клиент передает ACK TCP обратно в WLC для завершения квитирования.
- Клиент передает GET HTTP за/login.html, предназначенным к 1.1.1.1 для запроса на страницу входа.
- Этот запрос позволен до Web-сервера WLC, и сервер отвечает назад страницей для входа по умолчанию. Клиент получает страницу входа на окне браузера, где пользователь может идти вперед и войти.

Вот ссылка на видео на Сообществе Cisco Support, которое объясняет Процесс веб-аутентификации:

Web-аутентификация на контроллерах беспроводной локальной сети Cisco (WLC)

Настройка сети

В настоящем документе используется следующая схема сети:



Настройте контроллер для web-аутентификации

В этом документе WLAN настроен для web-аутентификации и сопоставлен с выделенной сетью VLAN. Это шаги, включенные для настройки WLAN для web-аутентификации:

- Создайте интерфейс виртуальной локальной сети (VLAN)
- Настройте WLC для внутренней веб-аутентификации
- Добавьте экземпляр WLAN
- Настройте тип проверки подлинности (Три способа аутентифицировать пользователей в web-аутентификации)

В этом разделе вам предоставляют информацию по настройке контроллер для web-аутентификации.

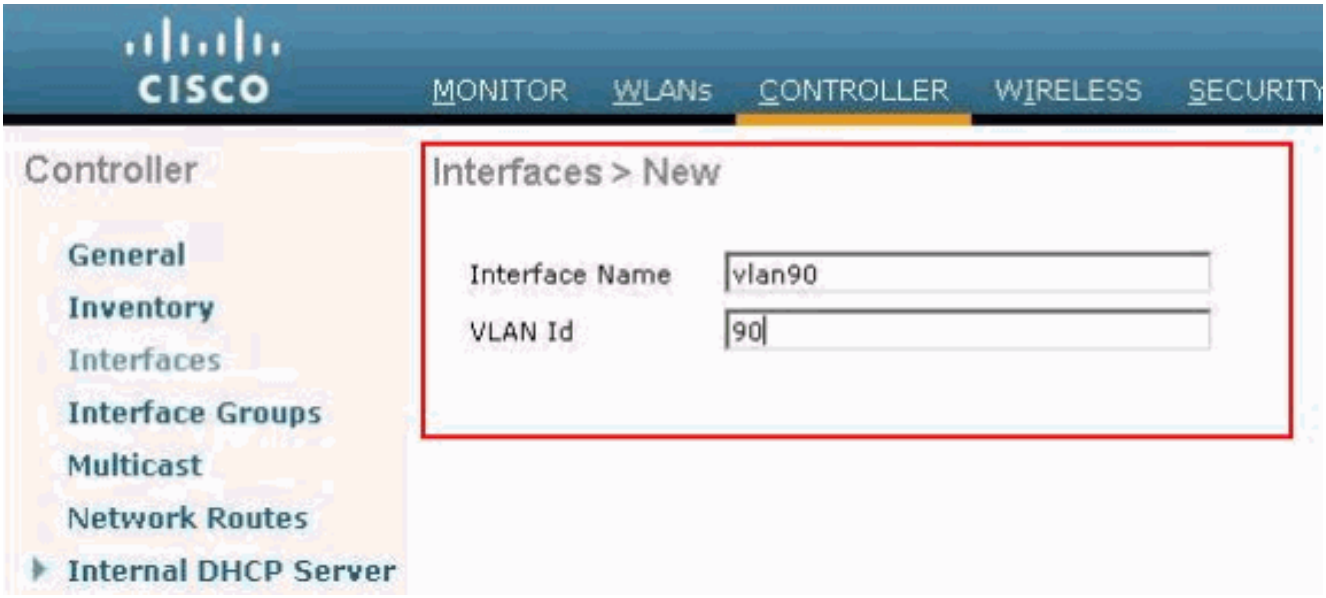
Это IP-адреса, используемые в этом документе:

- IP-адрес WLC 10.77.244.204.
- IP-адрес сервера ACS 10.77.244.196.

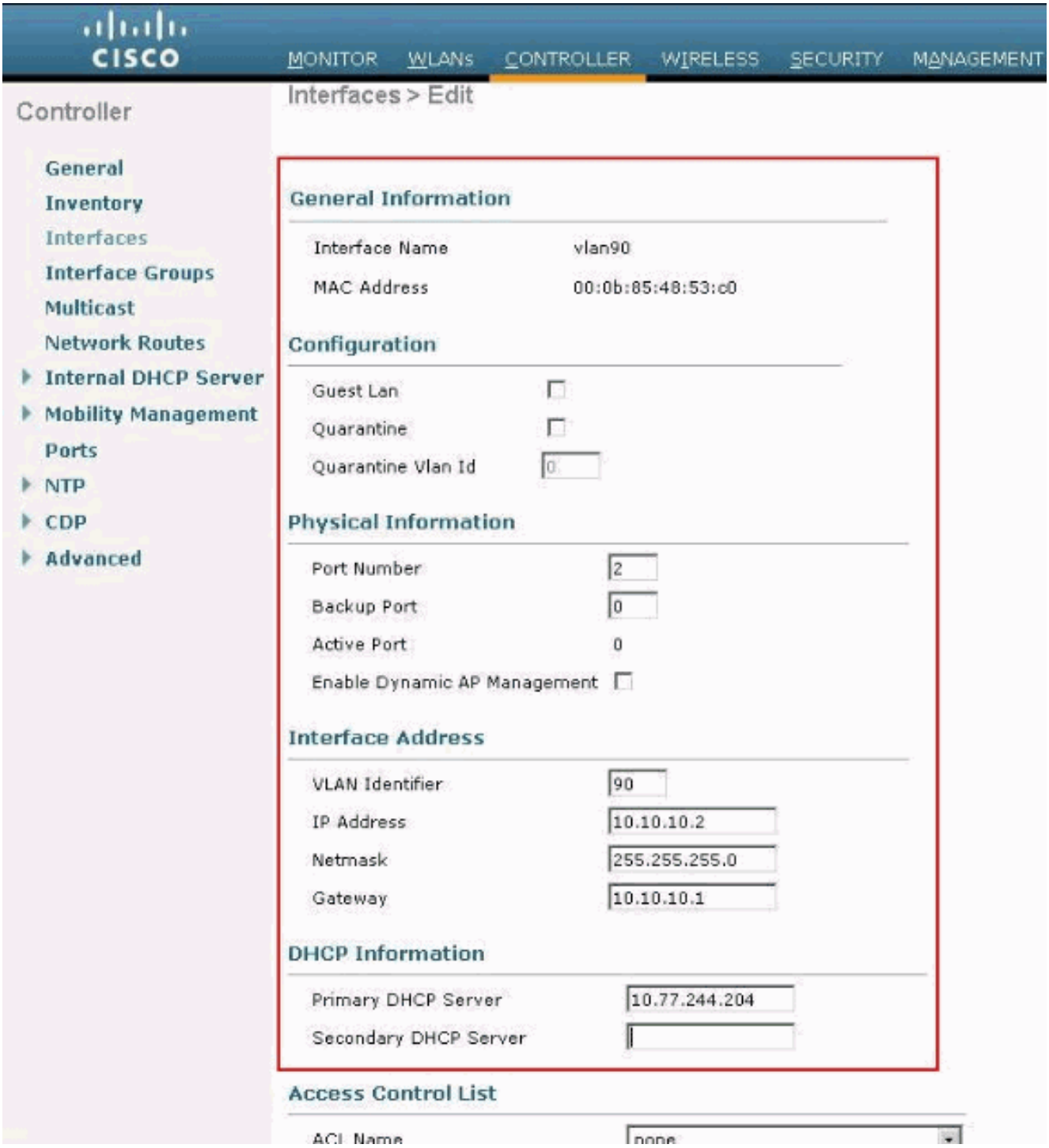
Создайте интерфейс виртуальной локальной сети (VLAN)

Выполните следующие действия:

1. От GUI Контроллера беспроводной локальной сети выберите **Controller** из меню наверху, выберите **Interfaces** из меню слева и нажмите **New** на верхней правой стороне окна для создания нового динамического интерфейса.**Интерфейсы> Новое окно** появляются. Данный пример использует Имя интерфейса *vlan90* с ИДЕНТИФИКАТОРОМ VLAN *90*:



2. Нажмите **Apply** для создания интерфейса виртуальной локальной сети (VLAN).**Интерфейсы> Окно редактирования** появляется, который просит, чтобы вы заполнили интерфейсную определенную информацию.
3. Этот документ использует эти параметры:IP-адресМаска подсети — 255.255.255.0 (24 бита)Шлюз — 10.10.10.1Номер порта — 2Основной сервер DHCP — 10.77.244.204**Примечание:** Этим параметром должен быть IP-адрес вашего RADIUS или сервера DHCP. В данном примере адрес управления WLC используется в качестве сервера DHCP, потому что Внутренняя область DHCP настроена на WLC.Вторичный сервер DHCP — 0.0.0.0**Примечание:** В данном примере нет дополнительного DHCP-сервера, поэтому используется значение 0.0.0.0. Если ваша конфигурация имеет вторичный сервер DHCP, добавьте IP-адрес сервера в этом поле.Название ACL — ни один



4. Нажмите **Apply** для сохранения изменений.

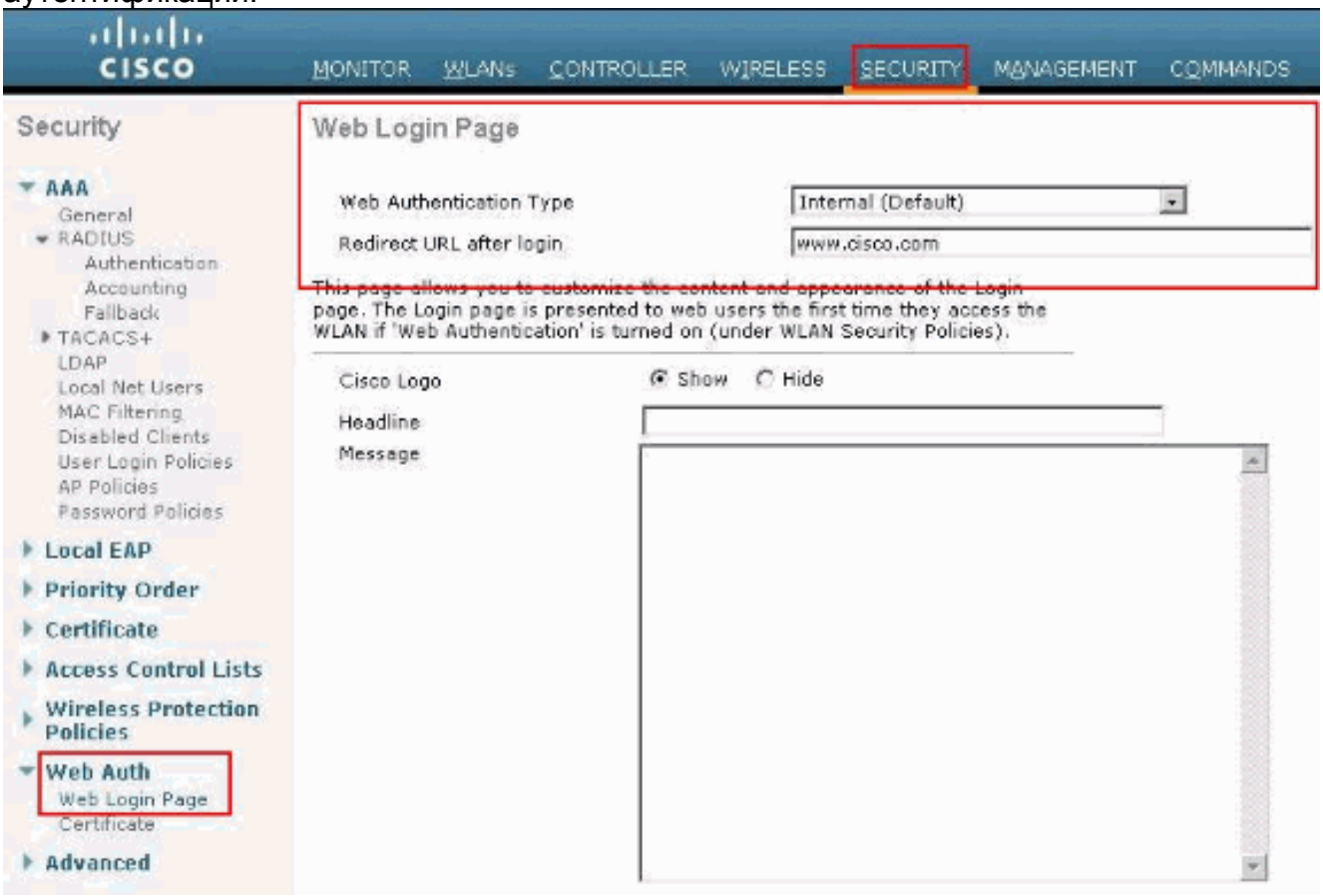
Настройте WLC для внутренней веб-аутентификации

Следующий шаг должен настроить WLC для Внутренней веб-аутентификации. Внутренняя веб-аутентификация является типом проверки подлинности веб-страницы по умолчанию на WLC. Если этот параметр не был изменен, никакая конфигурация не требуется, чтобы включать Внутреннюю веб-аутентификацию. Если параметр web-аутентификации был изменен ранее, выполните эти шаги для настройки WLC для Внутренней веб-аутентификации:

1. От графического интерфейса контроллера выберите **Security> Web Auth> Web Login Page** для доступа к Веб-странице для входа.
2. От раскрывающегося окна Типа Web-аутентификации выберите **Internal Web**

Authentication.

3. В **URL Перенаправления после** поля **входа в систему** введите URL страницы, к которой конечный пользователь будет перенаправлен к после успешной аутентификации.



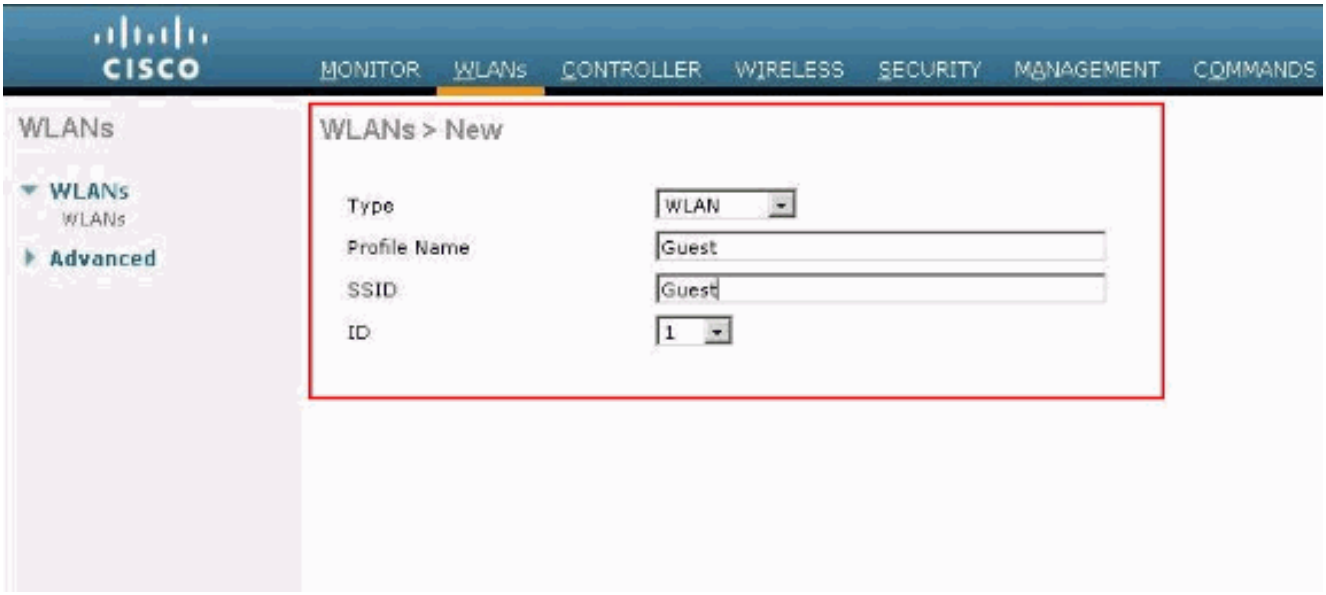
Примечание: В версиях WLC 5.0 и позже, может также быть настроена страница выхода из системы для web-аутентификации. См. Назначать Вход в систему, Ошибку регистрации в системе и страницы Logout на раздел WLAN *Руководства по конфигурации Контроллера беспроводной локальной сети, 5.2* для получения дополнительной информации о том, как настроить его.

Добавьте экземпляр WLAN

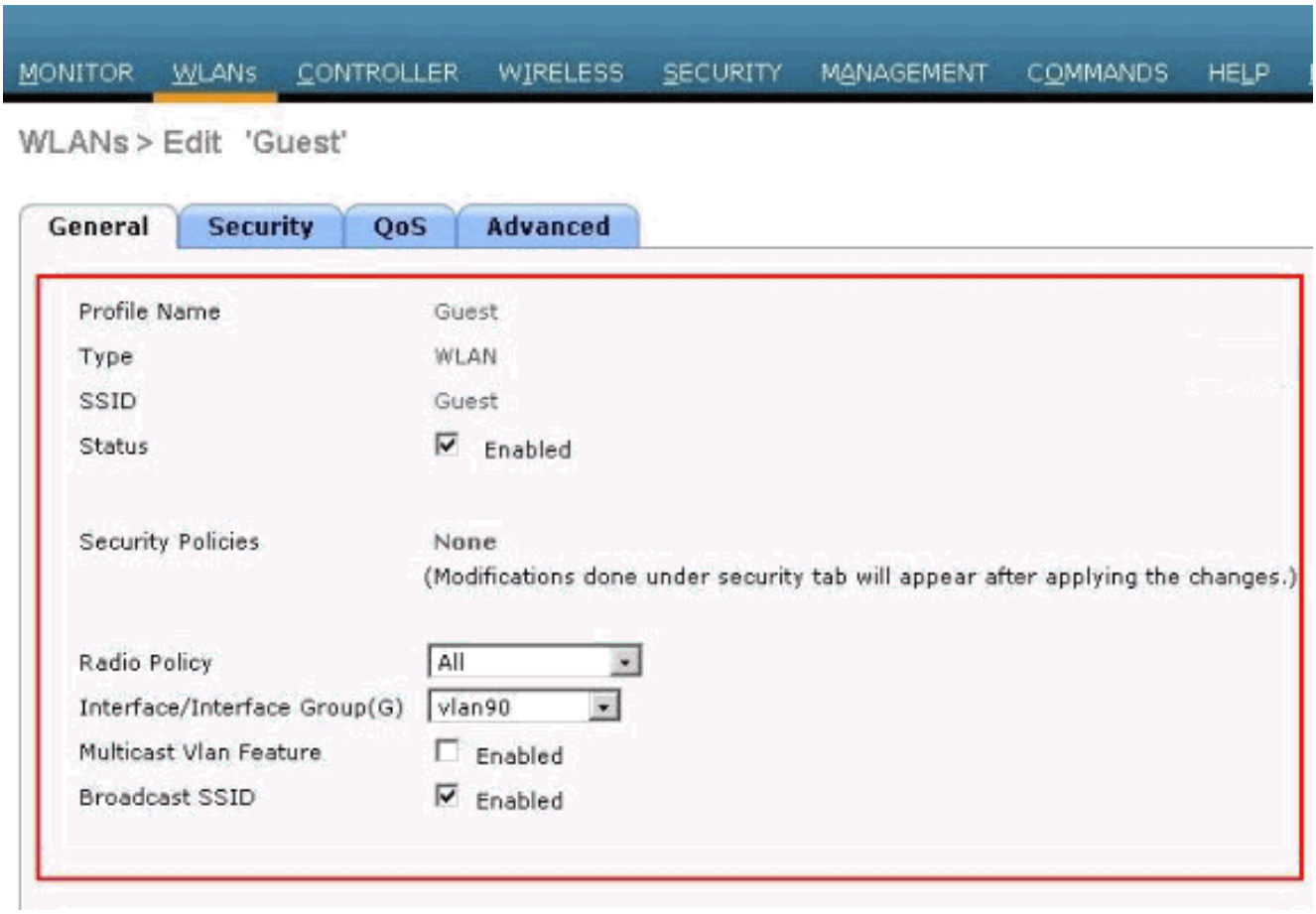
Теперь, когда Внутренняя веб-аутентификация была включена и существует интерфейс виртуальной локальной сети (VLAN), выделенный для web-аутентификации, необходимо предоставить новый WLAN/SSID для поддержки пользователей web-аутентификации.

Выполните эти шаги для создания нового WLAN/SSID:

1. От GUI WLC нажмите **WLAN** в меню наверху и нажмите **New** на верхней правой стороне.Выберите **WLAN** в качестве Типа. Выберите имя профиля и SSID WLAN для Web-аутентификации. Данный пример использует **Гостя** и для Имени профиля и для SSID
WLAN.

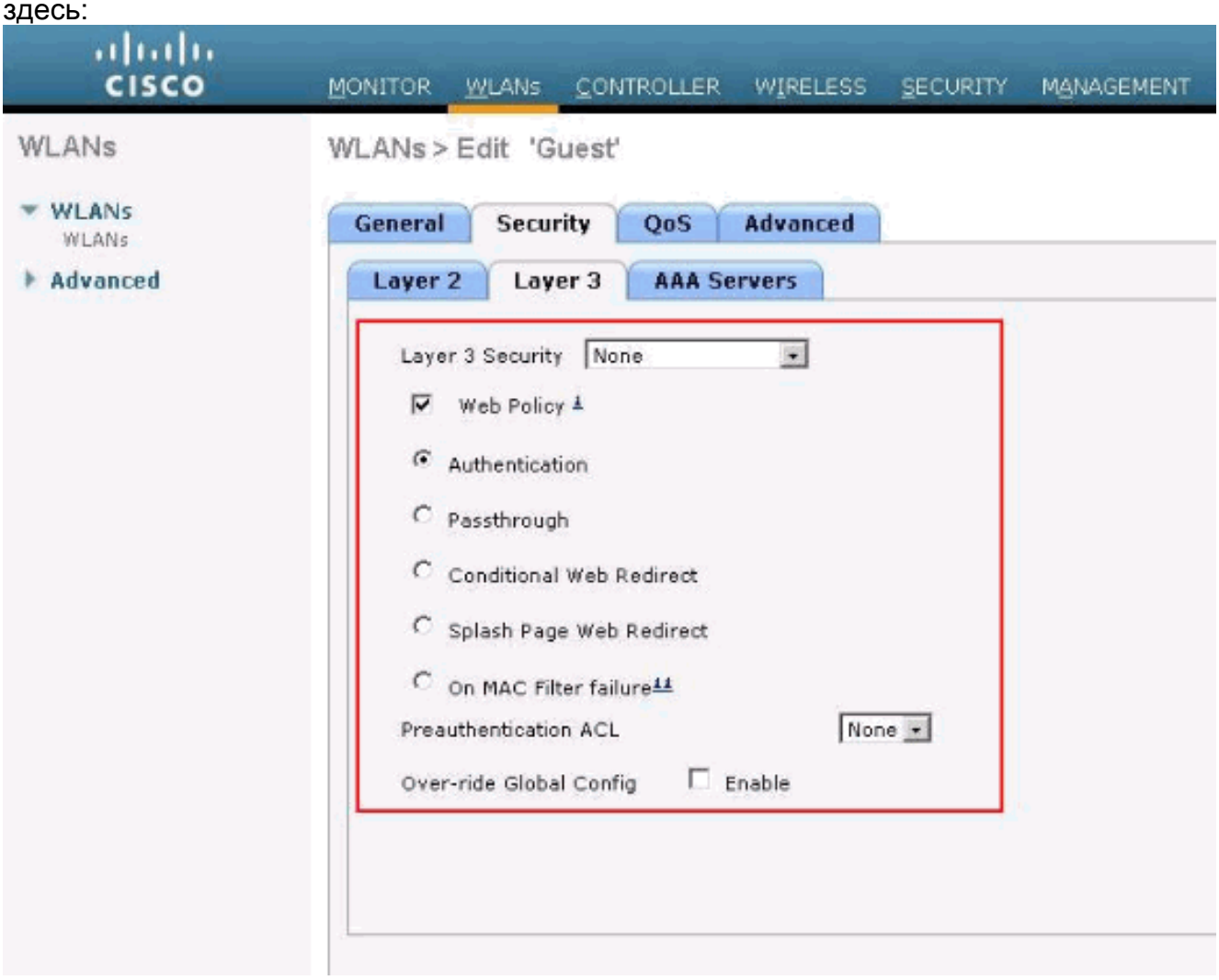


2. **Щелкните "Применить".**Новые WLAN> Окно редактирования появляется.



3. Установите флажок статуса WLAN для включения WLAN. Из меню Interface выберите название интерфейса виртуальной локальной сети (VLAN), который вы создали ранее. В данном примере Имя интерфейса является *vlan90*.**Примечание:** Оставьте значение по умолчанию для других параметров на этом экране.
4. **Щелкните вкладку Безопасность.**Выполните эти шаги для настройки web-аутентификации:Нажмите **Таблицу уровня 2** и установите безопасность ни в ***Один***.**Примечание:** Вы не можете настроить веб-passthrough как безопасность уровня 3 с 802.1x или WPA/WPA2 как безопасность уровня 2 для WLAN. См. Матрицу совместимости безопасности уровня 3 Уровня 2 Контроллера беспроводной локальной сети для получения дополнительной информации об Уровне 2 Контроллера

беспроводной локальной сети и совместимости безопасности уровня 3.Нажмите вкладку **Уровня 3**. Установите **веб-**флажок **Политики** и выберите ***Параметр проверки подлинности***, как показано
здесь:



Нажмите **Apply** для сохранения WLAN.Вы возвращены к окну сводки WLAN. Удостоверьтесь, что Веб-Аутентификация включена под столбцом Security Policies таблицы WLAN для Гостевого SSID.

Три способа аутентифицировать пользователей в web-аутентификации

Существует три способа аутентифицировать пользователей при использовании web-аутентификации. Локальная проверка подлинности позволяет вам аутентифицировать пользователя в WLC Cisco. Можно также использовать внешний сервер RADIUS или Сервер LDAP как база данных бэкэнда для аутентификации пользователей.

Этот документ предоставляет пример конфигурации для всех трех методов.

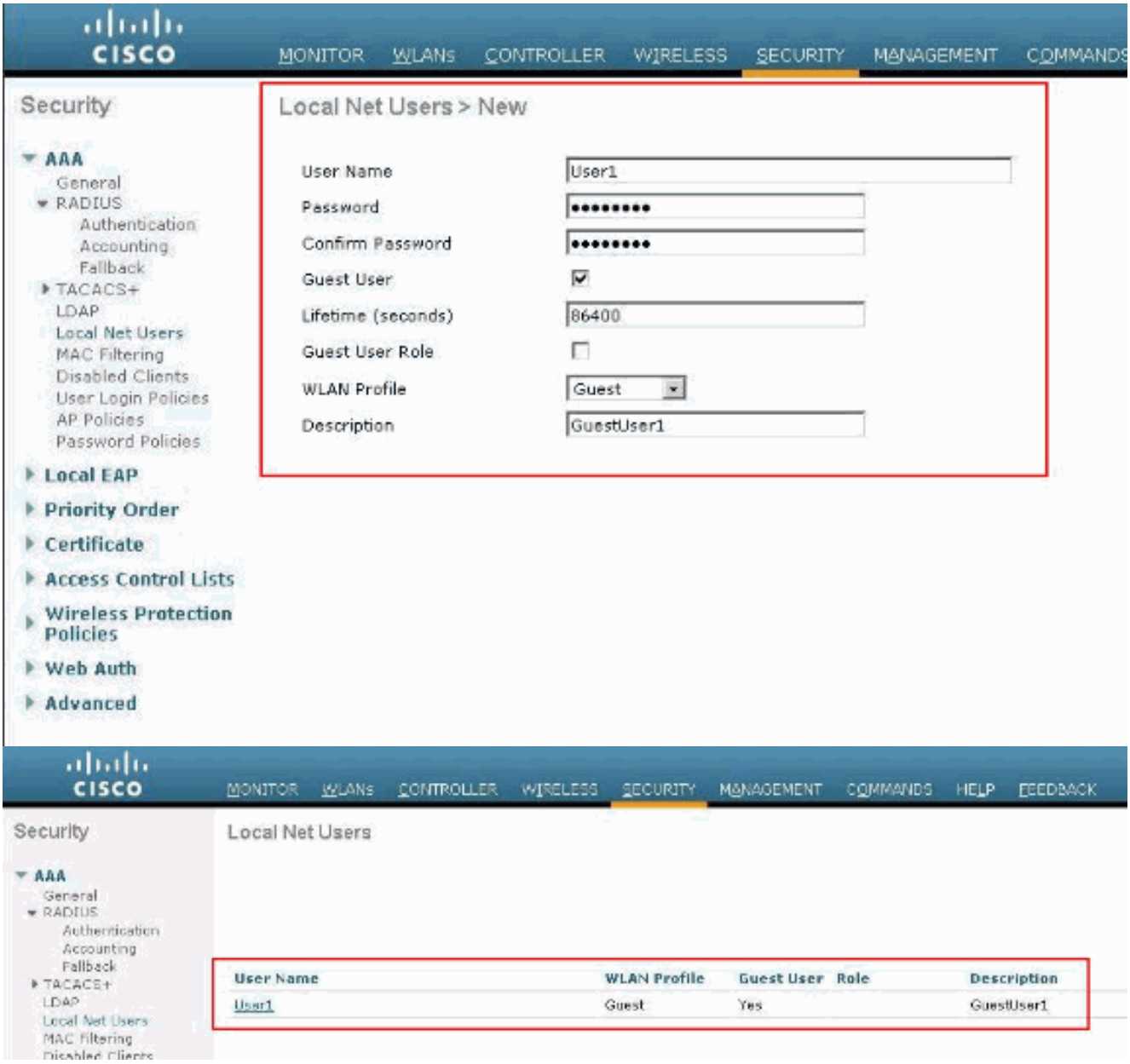
Локальная проверка подлинности

База данных пользователей для гостей сохранена на локальной базе данных WLC. Пользователи аутентифицируются WLC против этой базы данных.

1. От GUI WLC выберите **Security**.
2. Нажмите **Local Net Users** из меню AAA

слева.

3. Нажмите **New** для создания нового пользователя.Новое окно отображается, который запрашивает информацию имени пользователя и пароля.
4. Введите Имя пользователя и пароль для создания нового пользователя, затем подтвердите пароль, который вы хотите использовать.Данный пример создает пользователя под названием **User1**.
5. Добавьте описание, если вы выбираете.Данный пример использует **Гостевой User1**.
6. Нажмите **Apply** для сохранения конфигурации нового пользователя.



7. Повторите шаги 3-6 для добавления большего количества пользователей к базе данных.

Сервер RADIUS для web-аутентификации

Этот документ использует беспроводной ACS на Windows 2003 Server как сервер RADIUS. Можно использовать любой доступный RADIUS-сервер, развернутый в сети в данный момент.

Примечание: ACS может быть установлен или на Windows NT или на Сервере Windows 2000. Для загрузки ACS от Cisco.com обратитесь к Центру программного обеспечения (Загрузки) - Программное обеспечение Cisco Secure (только зарегистрированные клиенты). Вам нужна веб-учетная запись Cisco для загружения программного обеспечения.

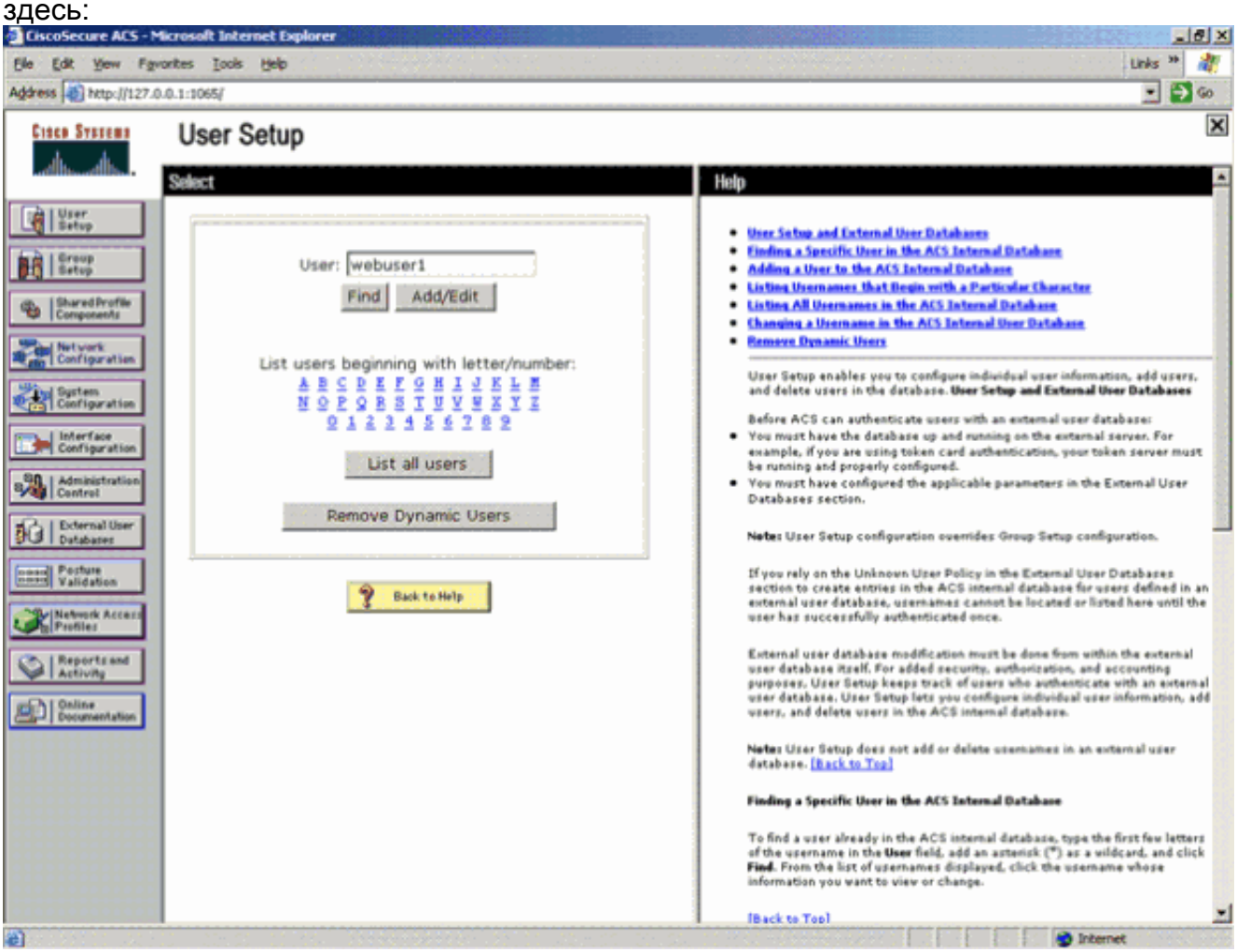
Установленный раздел ACS показывает вам, как настроить ACS для RADIUS. Требуются полностью функциональная сеть со службами DNS и RADIUS-сервер.

Установите ACS

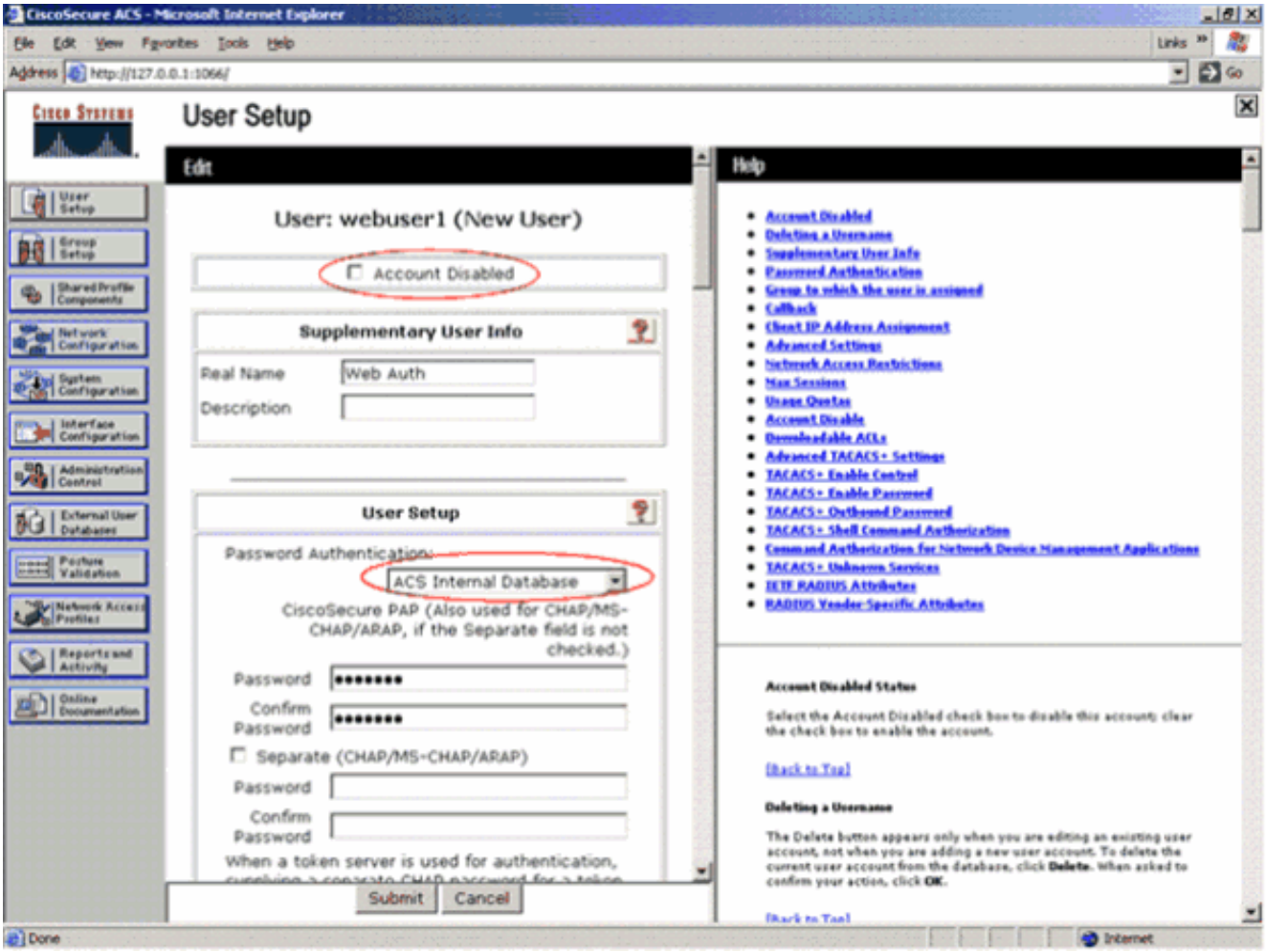
В этом разделе вам предоставляют информацию для устанавливания ACS для RADIUS.

Установите ACS на своем сервере и затем выполните эти шаги для создания пользователя для аутентификации:

1. Когда ACS спрашивает, хотите ли вы открыть ACS в окне браузера для настройки, нажмите **да**.**Примечание:** После того, как вы установите ACS, у вас также есть значок на вашем рабочем столе.
2. В меню слева, нажмите **User Setup**.Это действие берет вас к Экрану настройки пользователя как показано
здесь:



3. Введите пользователя, которого вы хотите использовать для web-аутентификации и нажать **Add/Edit**.После того, как пользователь создан, второе окно открывается как показано
здесь:

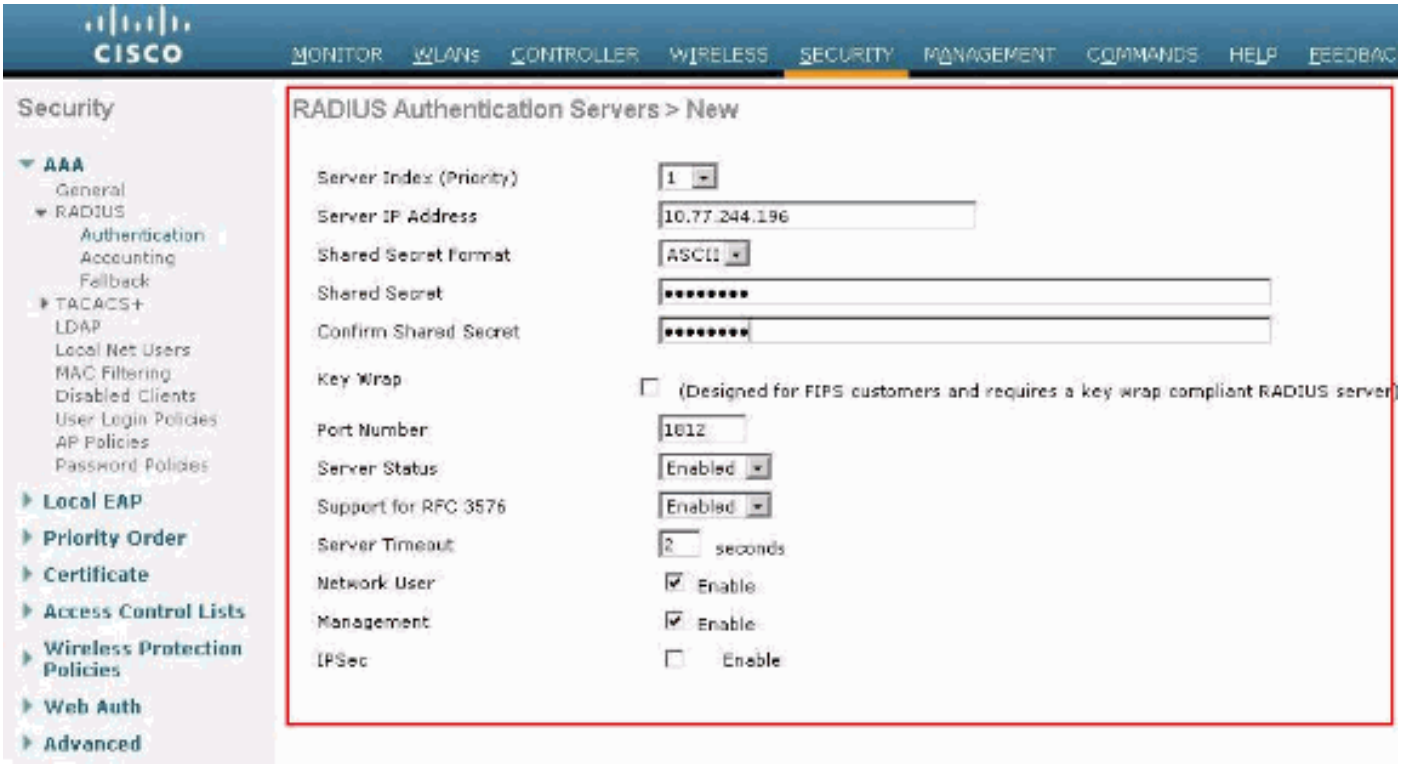


4. Гарантируйте, что наверху не проверена **Учетная запись Отключенная** Коробка.
5. Выберите **ACS Internal Database** для опции Password Authentication.
6. Ввести пароль. У Admin есть опция для настройки PAP/CHAP или АУТЕНТИФИКАЦИИ CHAP MD5 при добавлении пользователя во Внутренней базе данных ACS. PAP является типом проверки подлинности по умолчанию для веб-подлинных пользователей на контроллерах. У admin есть гибкость для изменения метода аутентификации на chap/md5-chap использование этой команды CLI:`config custom-web radiusauth <auth method>`
7. **Нажмите кнопку Submit (Отправить).**

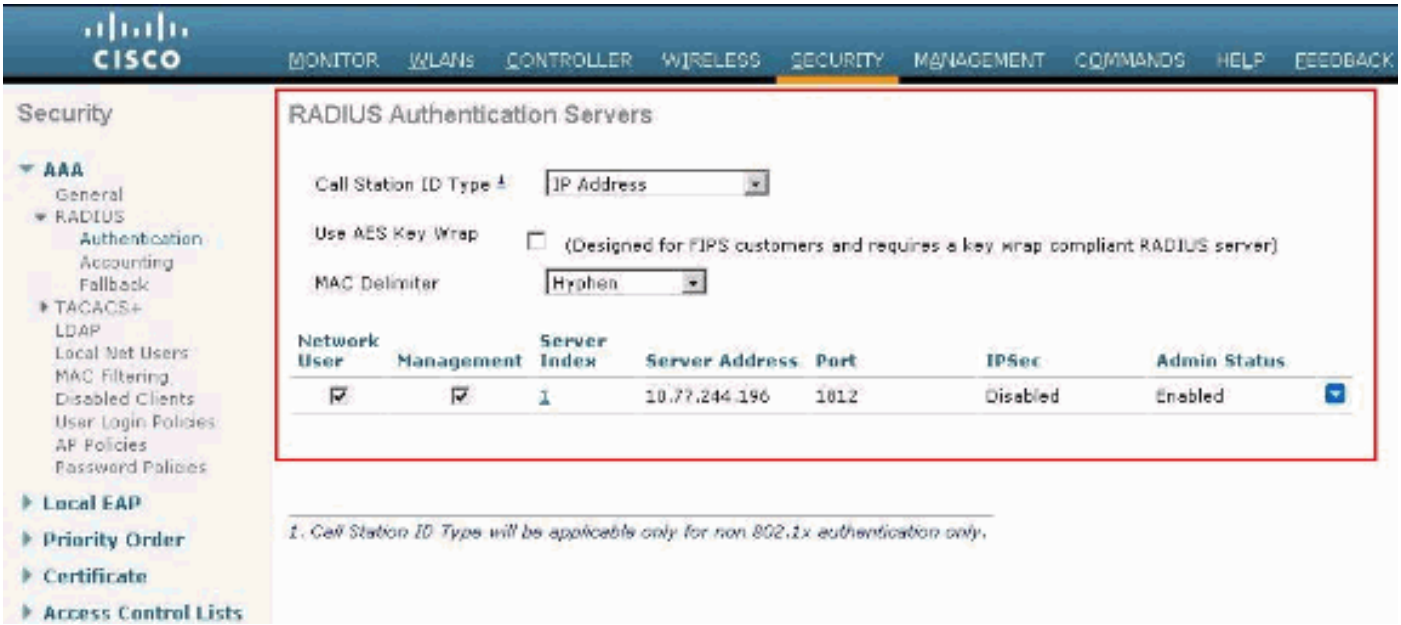
Введите свою информацию о сервере RADIUS в WLC Cisco

Выполните следующие действия:

1. **Выберите Security (Безопасность) в меню в верхней части окна.**
2. Нажмите **RADIUS Authentication** в меню слева.
3. Нажмите **New** и введите IP-адрес своего ACS/СЕРВЕРА RADIUS. В данном примере IP-адрес сервера ACS **10.77.244.196**.
4. Введите общий секретный ключ для сервера RADIUS. Удостоверьтесь, что этот секретный ключ совпадает с тем, который вы ввели в сервер RADIUS для WLC.
5. Оставьте Номер порта в по умолчанию, 1812.
6. Гарантируйте, что Включена опция **Server Status**.
7. Проверьте**, что Пользователь сети Включает** коробку так, чтобы этот сервер RADIUS использовался для аутентификации пользователей вашей беспроводной сети.
8. **Щелкните "Применить".**



Удостоверьтесь, что флажок *Пользователя сети* установлен, и *Административный статус* Включен.

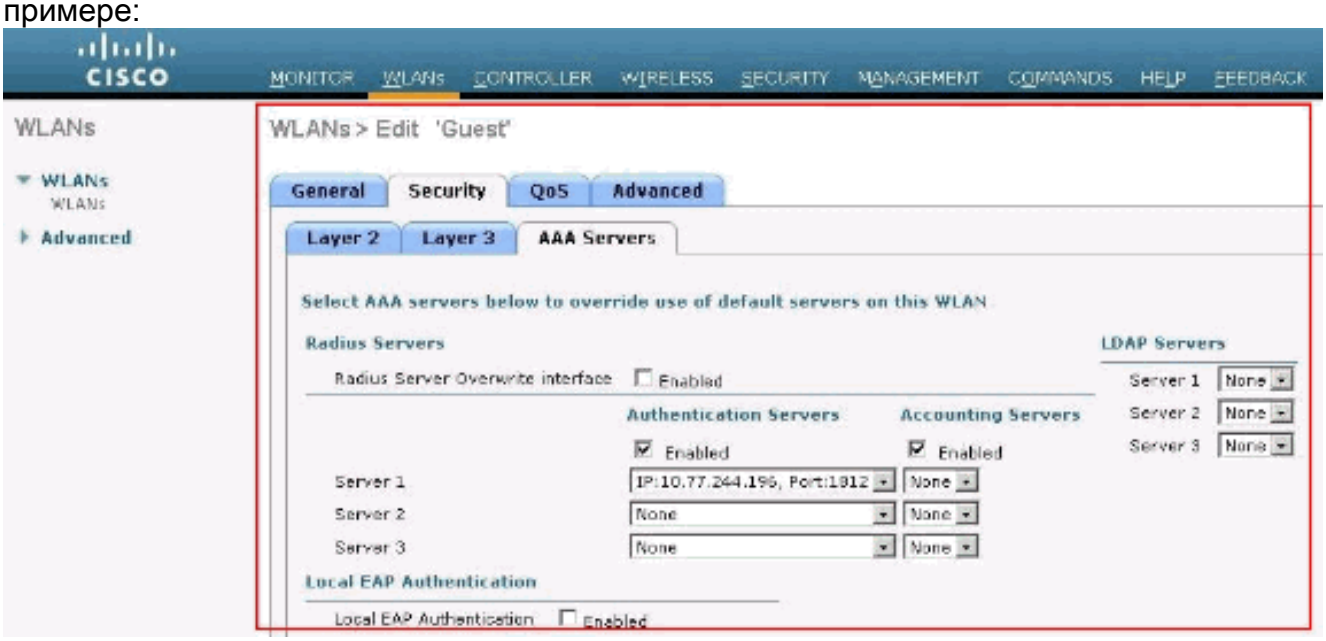


WLAN Настройки с сервером RADIUS

Теперь, когда сервер RADIUS настроен на WLC, необходимо настроить WLAN для использования этого сервера RADIUS для web-аутентификации. Выполните эти шаги для настройки WLAN с сервером RADIUS.

1. Откройте своего обозревателя WLC и нажмите **WLAN**. Это отображает список WLAN, настроенных на WLC. Нажмите **WLAN Guest**, который был создан для web-аутентификации.
2. На **WLAN> страница Edit** нажимают **Security Menu**. Нажмите вкладку **AAA Servers** под Безопасностью. Затем выберите сервер RADIUS, который является 10.77.244.196 в

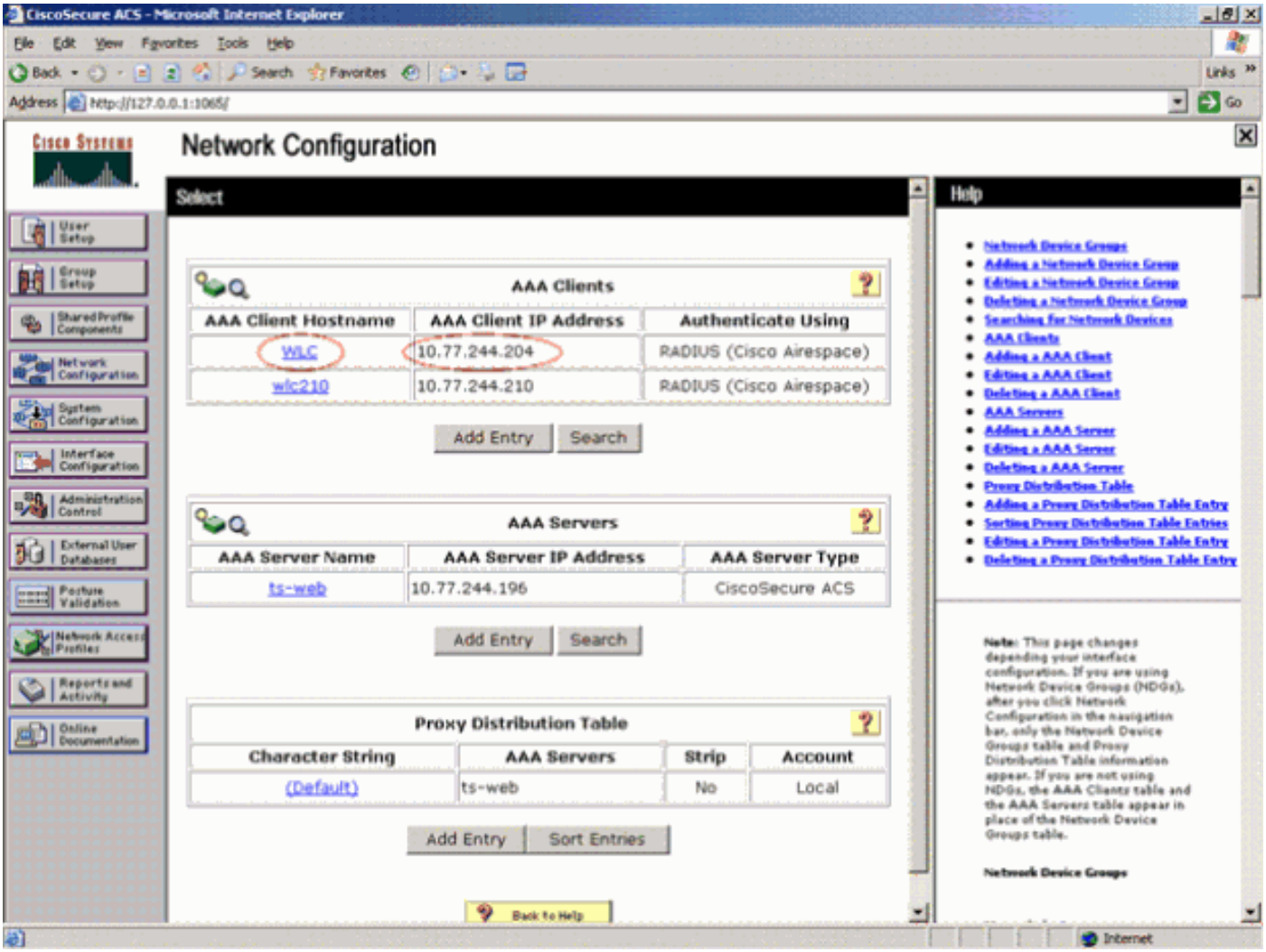
данном
примере:



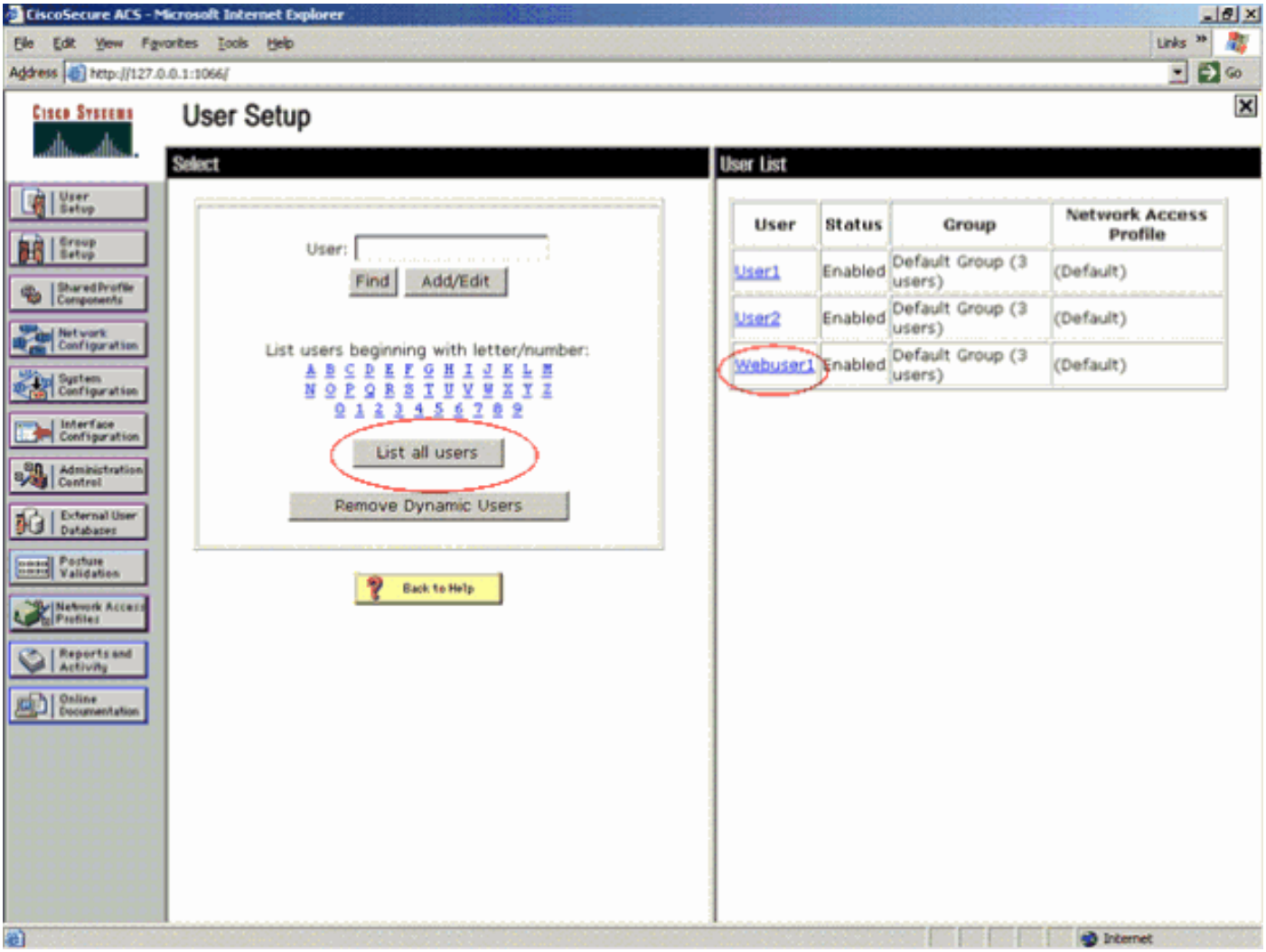
3. **Щелкните "Применить".**

Проверьте ACS

Когда вы установите ACS, не забудьте загружать все текущие исправления и последний код. Это должно решить нависшие проблемы. В случае, если вы используете Проверку подлинности RADIUS, удостоверяются, что ваш WLC перечислен как один из Клиентов AAA. Нажмите меню **Network Configuration** на левой стороне для проверки этого. Нажмите клиента AAA, затем проверьте пароль и настроенный тип проверки подлинности. См. раздел Клиентов AAA Настройки Руководства пользователя для сервера Cisco Secure Access Control Server 4.2 для получения дополнительной информации о том, как настроить клиента AAA.



Когда вы выбираете User Setup, проверяете снова, что фактически существуют ваши пользователи. Нажмите **List All Users**. Окно как показано появляется. Удостоверьтесь пользователь, который был создан, существует в списке.

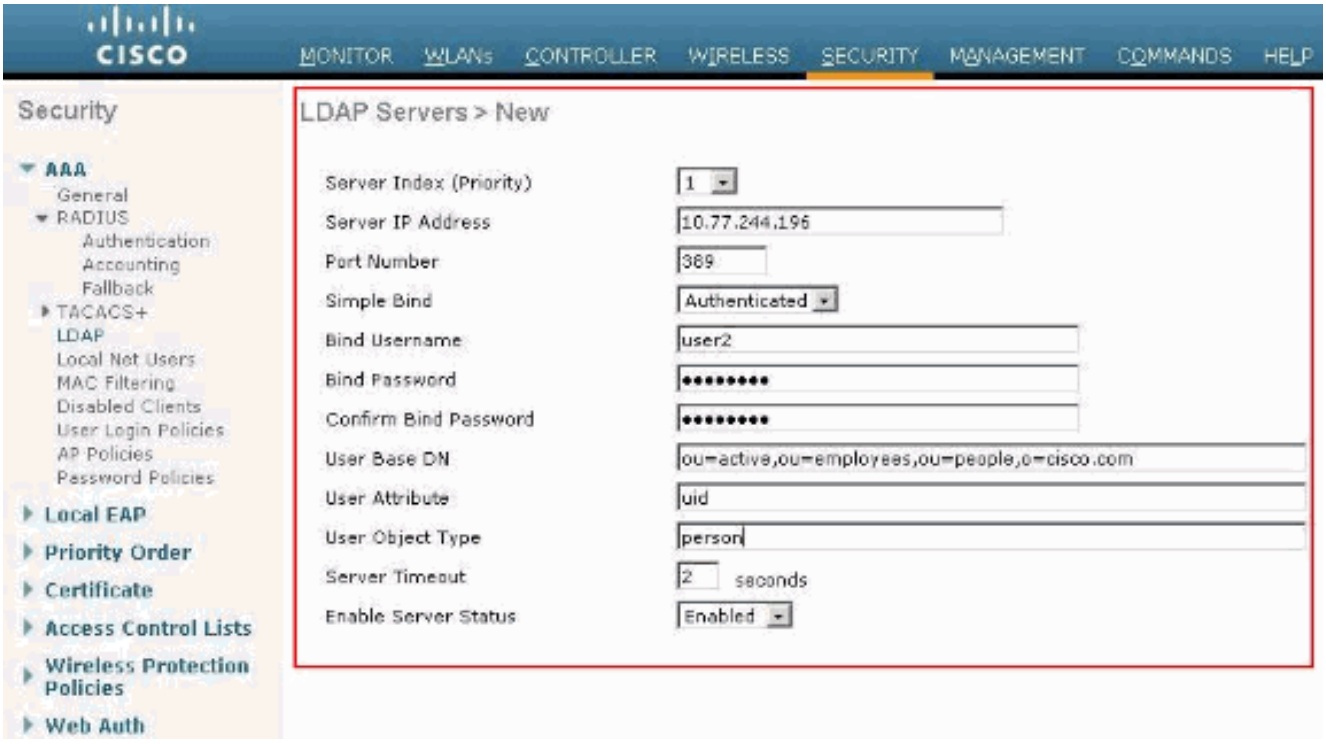


Сервер LDAP

Этот раздел объясняет, как настроить сервер Протокола LDAP как базу данных бэкэнда, подобную RADIUS или базе локальных пользователей. База данных бэкэнда LDAP позволяет контроллеру сделать запрос Сервера LDAP для учетных данных (имя пользователя и пароль) индивидуального пользователя. Эти учетные данные тогда используются для аутентификации пользователя.

Выполните эти шаги для настройки LDAP с помощью графического интерфейса контроллера:

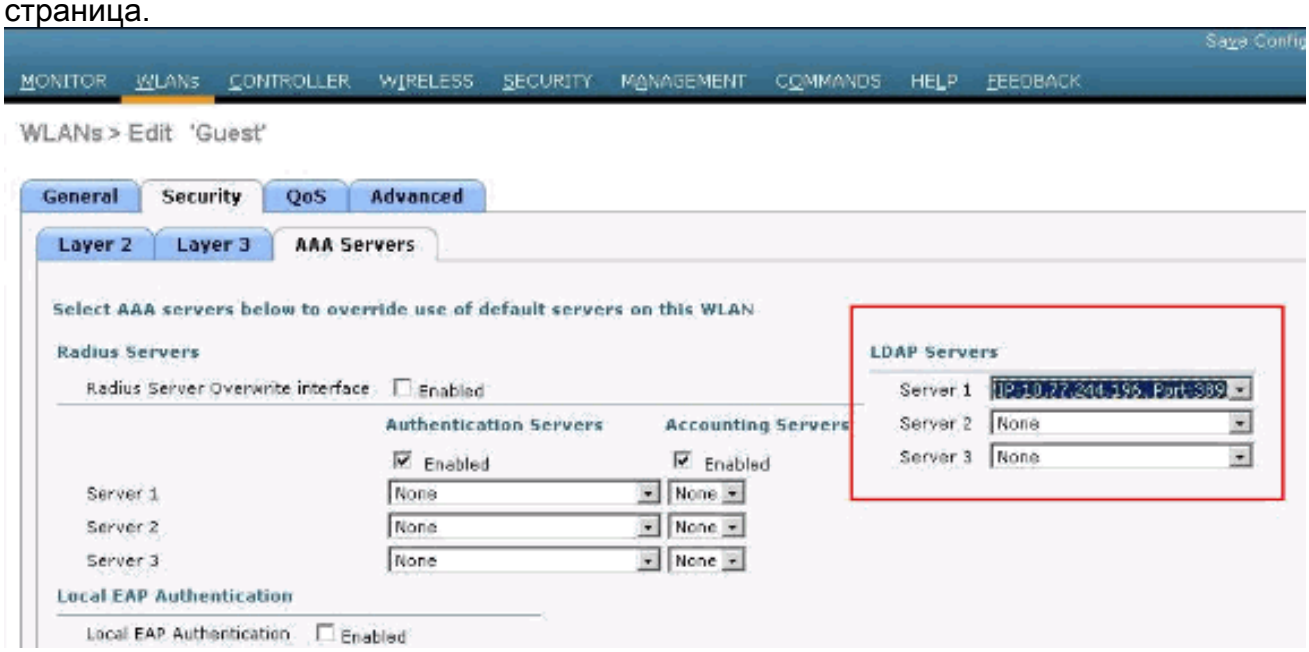
1. Нажмите **Security> AAA> LDAP** для открытия Серверов LDAP.Эта страница перечисляет любые Серверы LDAP, которые были уже настроены.Если вы хотите удалить существующий Сервер LDAP, переместить ваш курсор через синюю стрелку выпадающего списка для того сервера и выбрать **Remove**.Если вы хотите удостовериться, что контроллер может достигнуть индивидуального сервера, парение ваш курсор по синей стрелке выпадающего списка для того сервера и выбрать **Ping**.
2. Выполните одно из придерживающегося:Для редактирования существующего Сервера LDAP нажмите номер индекса для того сервера. Серверы LDAP> страница Edit появляются.Для добавления Сервера LDAP нажмите **New**. Страница LDAP Servers> New
появляется.



3. Если вы добавляете новый сервер, выбираете номер из Индекса Сервера (Приоритетное) раскрывающееся окно для определения порядка приоритетов этого сервера относительно каких-либо других настроенных Серверов LDAP. Можно настроить до семнадцати серверов. Если контроллер не может достигнуть первого сервера, то это пробует второй из списка и так далее.
4. Если вы добавляете новый сервер, введите IP-адрес Сервера LDAP в поле Server IP Address.
5. Если вы добавляете новый сервер, введите номер порта TCP Сервера LDAP в поле Port Number. Допустимый диапазон 1 - 65535, и значение по умолчанию 389.
6. Проверьте флажок **Enable Server Status**, чтобы включить этот Сервер LDAP или снять флажок с ним для отключения его. Значение по умолчанию отключено.
7. От Простого Связывают раскрывающееся окно, выбирают **Anonymous** или **Authenticated**, чтобы указать, что локальная проверка подлинности связывает метод для Сервера LDAP. Анонимный метод предоставляет анонимный доступ к Серверу LDAP, тогда как Аутентифицируемый метод требует, чтобы имя пользователя и пароль было введено в безопасный доступ. Значение по умолчанию является Анонимным.
8. При выборе Authenticated in Step 7 выполните эти шаги:В Связывать Поле имени пользователя введите имя пользователя, которое будет использоваться для локальной проверки подлинности к Серверу LDAP.В Связывать Пароле и Подтверждают, Связывают Поля Password, вводят пароль, который будет использоваться для локальной проверки подлинности к Серверу LDAP.
9. В поле User Base DN введите составное имя (DN) поддерева в Сервере LDAP, который содержит список всех пользователей. Например, ou=organizational модуль, .ou=next подразделение и o=corporation.com. Если дерево, содержащее пользователей, является основным DN, введите o=corporation.com или dc=corporation, dc=com.
10. В поле User Attribute введите имя атрибута в записи пользователя, которая содержит имя пользователя. Можно получить этот атрибут из сервера каталогов.
11. В поле User Object Type введите значение атрибута LDAP objectType, который определяет запись как пользователя. Часто, записи пользователя имеют несколько значений для атрибута objectType, некоторые из которых уникальны для

пользователя и некоторые из которых разделены с другими типами объекта.

12. В поле Server Timeout введите кол-во секунд между повторными передачами. Допустимый диапазон составляет 2 - 30 секунд, и значение по умолчанию составляет 2 секунды.
13. Нажмите **Apply** для фиксации изменений.
14. Нажмите **Save Configuration** для сохранения изменений.
15. Выполните эти шаги, если вы хотите назначить определенные Серверы LDAP на WLAN:Нажмите **WLAN** для открытия страницы WLANs.Нажмите Номер ID желаемого WLAN.Когда WLAN> страница Edit появляется, нажмите вкладки **Security> AAA Servers** для открытия, WLAN> Редактируют (Безопасность> AAA-серверы) страница.



От раскрывающихся окон Серверов LDAP выберите Сервер (серверы) LDAP, который вы хотите использовать с этим WLAN. Можно разделиться на команды к трем Серверам LDAP, которые пробуют в порядке приоритетов.Нажмите **Apply** для фиксации изменений.Нажмите **Save Configuration** для сохранения изменений.

Настройте своего клиента WLAN для Использования web-аутентификации

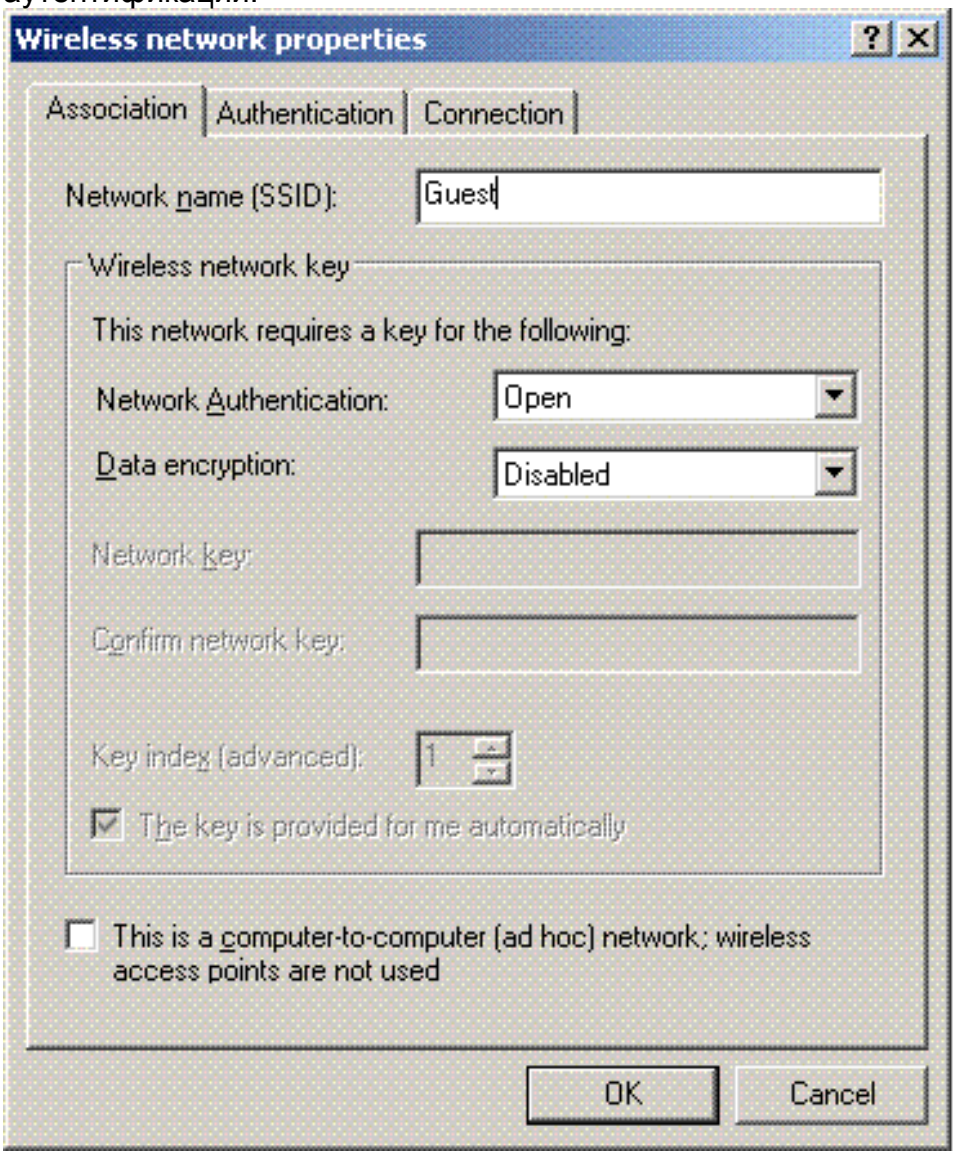
Как только WLC настроен, клиент должен быть настроен соответственно для web-аутентификации. В этом разделе вам предоставляют информацию по настройке ваша Система Windows для web-аутентификации.

Конфигурация клиента

Конфигурация беспроводного клиента Microsoft остается главным образом неизменной для этого абонента. Только необходимо добавить соответствующие сведения о конфигурации WLAN/SSID. Выполните следующие действия:

1. Из **меню Пуск Windows** выберите **Settings> Control Panel> Network и Internet Connections**.
2. Нажмите значок **Сетевых подключений**.
3. Щелкните правой кнопкой мыши значок **Подключения LAN** и выберите **Disable**.

4. Щелкните правой кнопкой мыши значок **Беспроводного соединения** и выберите **Enable**.
5. Щелкните правой кнопкой мыши значок **Беспроводного соединения** снова и выберите **Properties**.
6. От Окна настроек беспроводного сетевого соединения нажмите вкладку **Wireless Networks**.
7. Под предпочтительными сетями область **нажмите Add** для настройки SSID Web-аутентификации.
8. Под вкладкой Association введите Сетевое имя (WLAN/SSID) значение, которое вы хотите использовать для web-аутентификации.



Примечание: Шифрованием данных является Протокол WEP по умолчанию. Отключите Шифрование данных для web-аутентификации для работы.

9. **Нажмите кнопку ОК в нижней части окна, чтобы сохранить конфигурацию.**Когда вы связываетесь с WLAN, вы видите значок маяка в Предпочтительной Сетевой коробке.

Это показывает успешное беспроводное соединение web-аутентификации. WLC предоставил вашему клиенту беспроводных клиентов Windows IP-адрес.

Примечание: Если ваш беспроводной клиент является также оконечная точкой VPN, и вам настроили web-аутентификацию как характеристику безопасности для WLAN, то VPN-туннель не установлен, пока вы не проходите процесс веб-аутентификации, объясненный здесь. Для установления VPN-туннеля клиент должен сначала пройти процесс web-аутентификации с успехом. Только тогда делает VPN, туннелирующую, становятся успешными.

Примечание: После успешной регистрации в системе, если беспроводные клиенты являются простаивающими и не связываются ни с одним из других устройств, клиент является de-authenticated после периода времени простоя. Период ожидания составляет 300 секунд по умолчанию и может быть изменен с помощью этой команды CLI: `<seconds> config network usertimeout`. Когда это происходит, запись клиента удалена из контроллера. Если клиент свяжется снова, то это попятится к состоянию Webauth_Reqd.

Примечание: Если клиенты будут активны после успешной регистрации в системе, то они получат de-authenticated, и запись может все еще быть удалена из контроллера после периода превышения времени ожидания сеанса, настроенного на том WLAN (например, 1800 секунд по умолчанию, и может быть изменен с помощью этой команды CLI: `wlan session-timeout < WLAN> <seconds>`). Когда это происходит, запись клиента удалена из контроллера. Если клиент свяжется снова, то это попятится в состоянии Webauth_Reqd.

Если клиенты будут в состоянии Webauth_Reqd, независимо от того если они будут активными или простаивающими, то клиенты получат de-authenticated после того, как **веб-аутентификация потребовала периода ожидания** (например, 300 секунд, и на этот раз конфигурируемое лицо, не использующее своего права). Весь трафик от клиента (позволенный через Предподлинный ACL) будет разрушен. Если клиент свяжется снова, то это попятится к состоянию Webauth_Reqd.

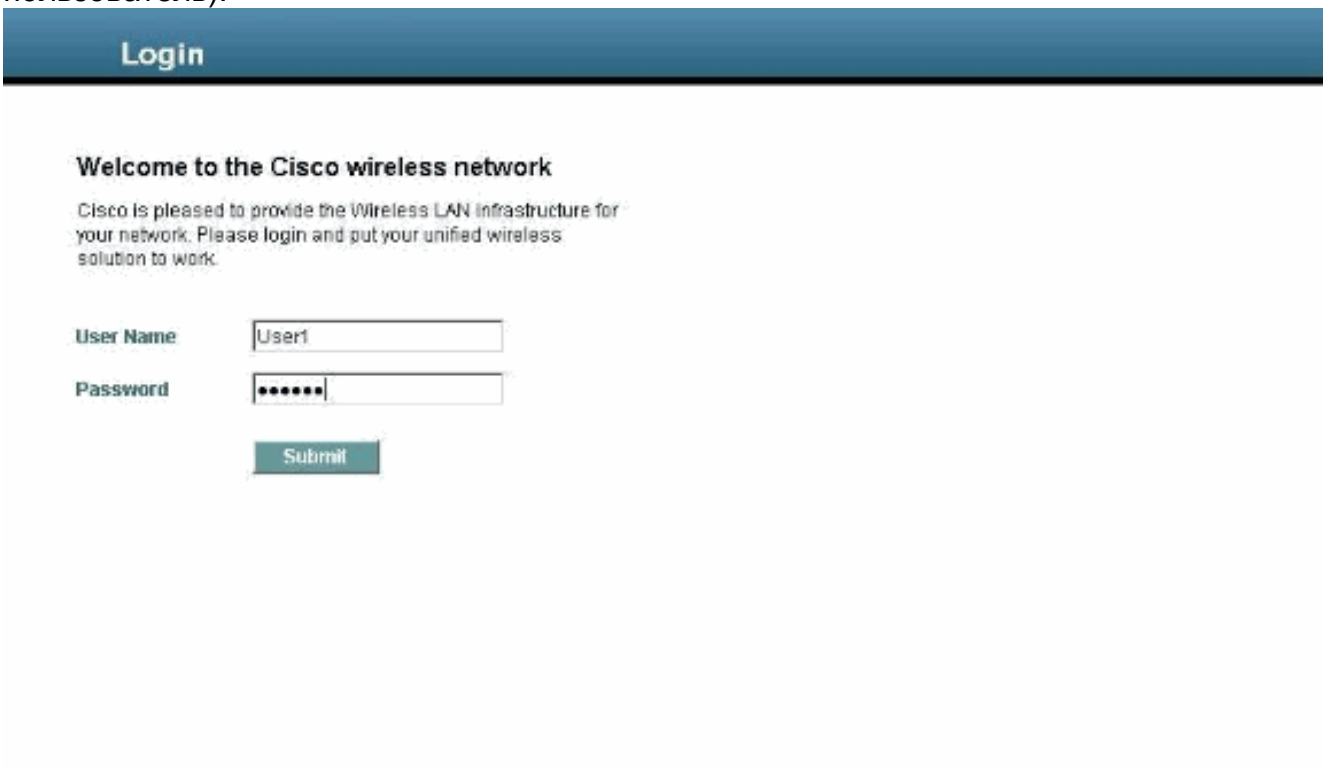
Вход в систему клиента

Выполните следующие действия:

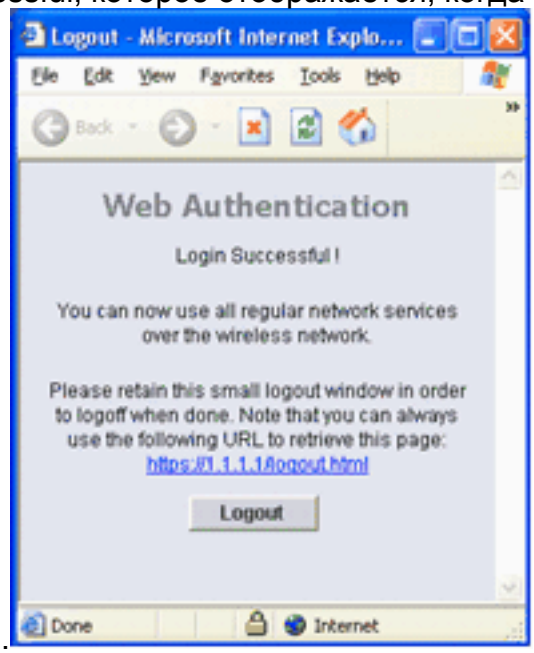
1. Откройте окно браузера и введите любой URL или IP-адрес. Это приносит страницу веб-аутентификации клиенту.Если контроллер выполняет какой-либо выпуск ранее, чем 3.0, пользователь должен ввести https://1.1.1.1/login.html для внедрения страницы

веб-аутентификации.Окно сигнала о нарушении безопасности отображается.

2. **Для продолжения нажмите кнопку Yes (Да).**
3. При отображении окна "Login" (Вход в систему) введите имя пользователя и пароль созданного пользователя Local Net User (Локальный сетевой пользователь).



Если ваш вход в систему успешен, вы видите два окна браузера. Большее окно указывает на успешную регистрацию в системе, и вы можете это окно для просмотра Интернета. Используйте меньшее окно, чтобы выйти из системы, когда ваше использование гостевой сети завершено.Снимок экрана показывает успешное перенаправление для web-аутентификации.Следующий снимок экрана показывает окно Login Successful, которое отображается, когда произошла аутентификация.



Контроллеры Cisco 4404/WiSM могут поддержать 125 одновременных веб-Подлинных Пользовательских входов в систему и увеличиться 5000 веб-подлинных клиентов.

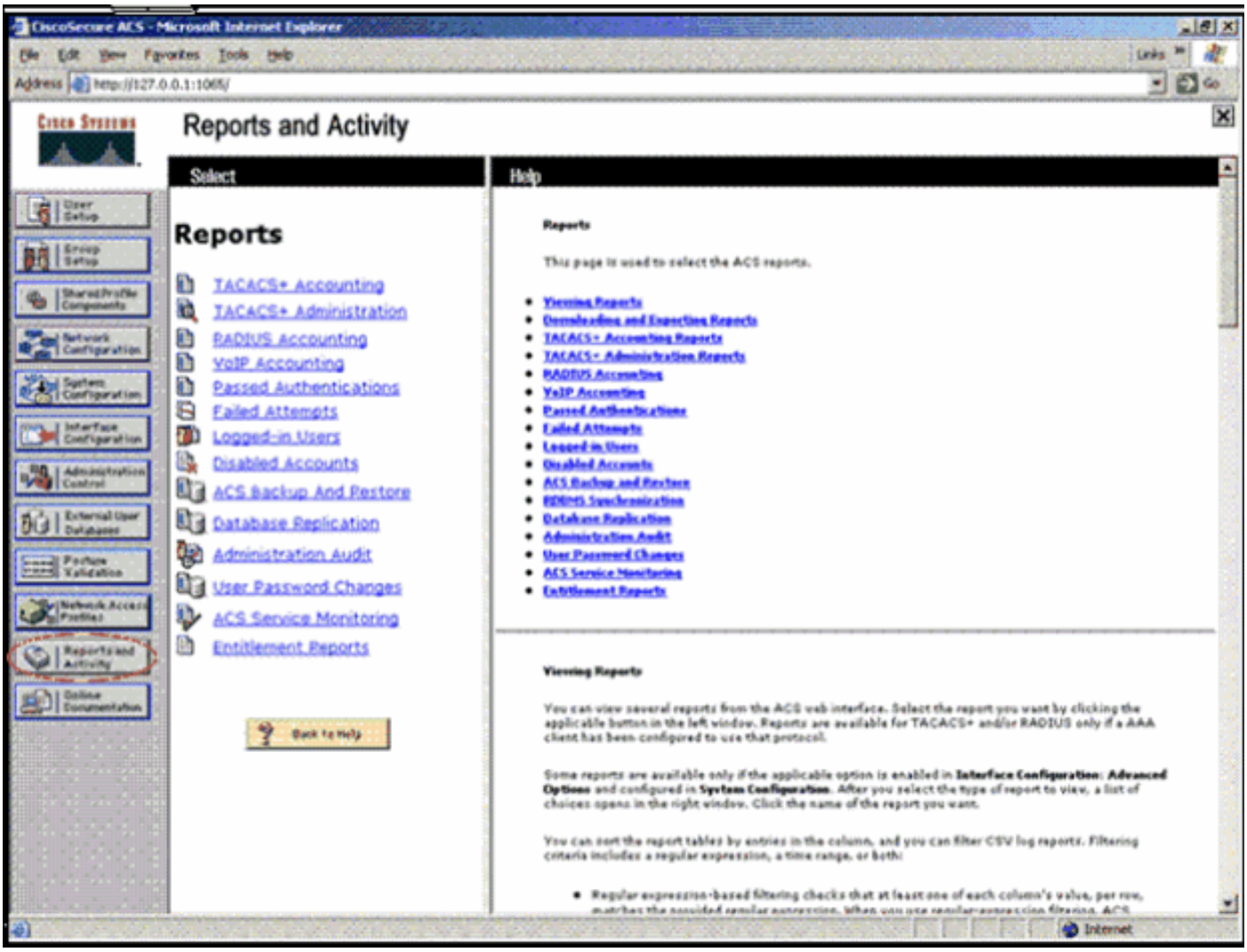
Контроллеры Cisco 5500 могут поддержать 150 одновременных веб-Подлинных

Пользовательских входов в систему.

Web-аутентификация устранения неполадок

ACS устранения неполадок

Если у вас есть проблемы с проверкой подлинности с помощью пароля, нажмите **Reports и Activity** на нижней левый стороне ACS для открытия всех доступных отчётов. После открытия окна отчётов у вас есть опция для открытия RADIUS Accounting, Неудачных попыток для входа в систему, Передал Аутентификации, Вошедшии в систему пользователь и другие отчёты. Эти отчёты являются файлами .csv, и можно открыть файлы локально на машине. Отчеты помогают обнаруживать проблемы с проверкой подлинности, например неправильное имя пользователя и/или пароль. ACS также идет с онлайн-документацией. Если вы не связаны с действующей сетью и не определили сервисный порт, ACS использует IP-адрес вашего Порта Ethernet для вашего сервисного порта. Если нет подключения к сети, скорее всего, будет использован IP-адрес Windows по умолчанию 169.254.x.x.



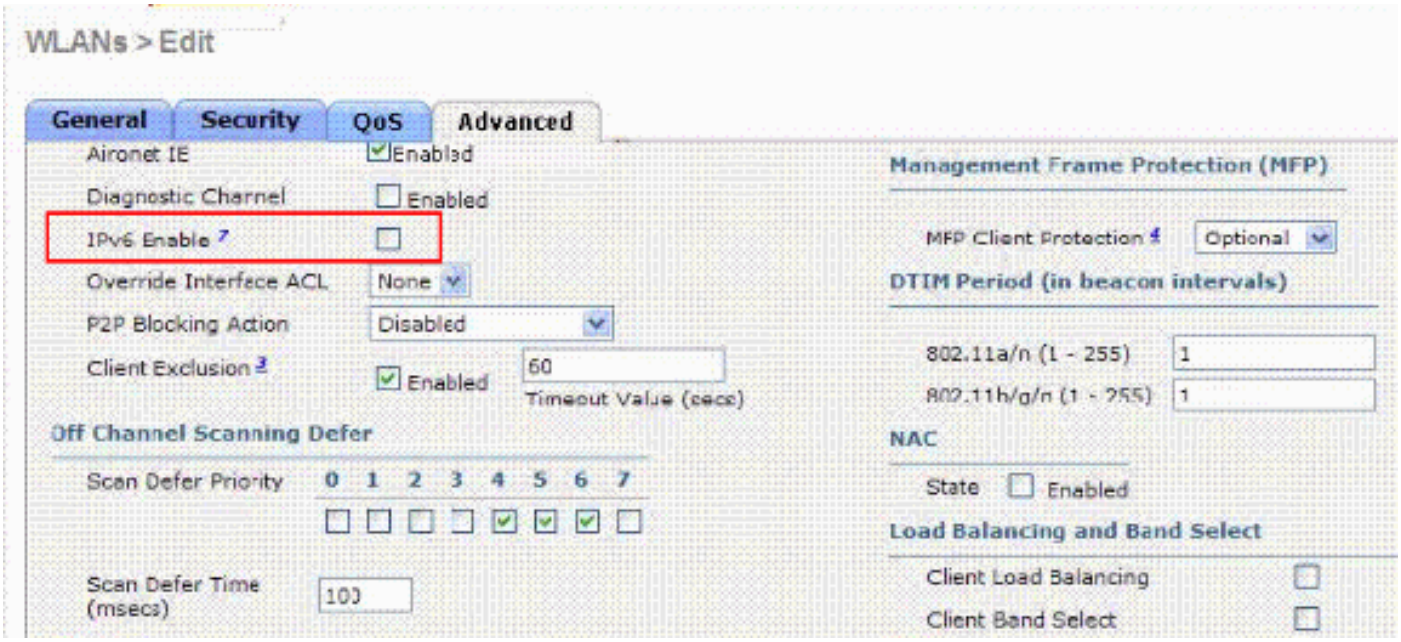
Примечание: Если вы вводите в каком-либо внешнем URL, WLC автоматически подключает вас со страницей внутренней веб-аутентификации. Если автоматическое подключение не работает, можно ввести управление IP-адресами WLC в панели URL для устранения проблем. Посмотрите наверху браузера для сообщения, которое говорит для перенаправления для web-аутентификации.

См. Устранение проблем Web-аутентификации на Контроллере беспроводной локальной сети (WLC) для получения дополнительной информации об устранении проблем web-аутентификации.

Веб-аутентификация с мостовым соединением IPv6

Для настройки WLAN для мостового соединения IPv6, от графического интерфейса контроллера, перейдите к **WLAN**. Затем выберите желаемый WLAN и выберите **Advanced** из **WLAN> страница Edit**.

Выберите **флажок IPv6 Enable**, если вы хотите включить клиентам, которые соединяются с этим WLAN для принятия пакетов IPv6. В противном случае оставьте флажок отменявшим, который является значением по умолчанию. При отключении (или снятие) флажка IPv6 IPv6 будет только позволен после аутентификации. Включение IPv6 означает, что контроллер может передать трафик IPv6 без аутентификации клиента.



Для более подробной информации о мостовом соединении IPv6 и **рекомендациях для того, чтобы использовать эту функцию**, обратитесь к разделу Мостового соединения IPv6 Настройки руководства по конфигурированию контроллера Cisco Wireless LAN, Выпуска 7.0.

Дополнительные сведения

- Пример настройки контроллера беспроводной сети с внешней веб-аутентификацией
- Устранение проблем web-аутентификации на контроллере беспроводной локальной сети (WLC)
- Беспроводная сеть LAN Cisco
- Пример конфигурации гостевого доступа к проводной сети с использованием контроллеров WLAN Cisco
- Руководство по конфигурированию контроллера Cisco Wireless LAN, выпуск 7.0 - управляющие учетные записи пользователя
- Проверка подлинности "администратора подъезда" контроллера беспроводной сети с помощью сервера RADIUS

- Cisco Systems – техническая поддержка и документация