Пример настройки контроллера беспроводной сети с внешней веб-аутентификацией

Содержание

Введение

В этом документе поясняется использование внешнего web-сервера для настройки контроллера беспроводной локальной сети (WLC) в режиме web-аутентификации.

Предварительные условия

Требования

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

- Базовые знания о конфигурации Облегченных точек доступа (LAP) и WLC Cisco
- Базовые знания о Протоколе LWAPP и Контроле и Инициализации Точек беспроводного доступа (CAPWAP)

- Знание о том, как установить и настроить внешний веб-сервер
- Знание о том, как установить и настроить DHCP и серверы DNS

Используемые компоненты

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

- WLC Cisco 4400, который выполняет релиз микропрограммы 7.0.116.0
- LAP Cisco 1131AG Series
- Адаптер беспроводного клиента Cisco 802.11a/b/g, который выполняет релиз микропрограммы 3.6
- Внешний веб-сервер, который размещает страницу для входа в веб-аутентификацию
- DNS и Серверы DHCP для определения адресов и IP - адреса размещения беспроводным клиентам

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

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. Web-аутентификация является методом простой проверки подлинности без потребности в соискателе или служебной программе клиента.

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

Этот документ предоставляет пример конфигурации, чтобы объяснить, как настроить WLC для использования сценария регистрации от внешнего веб-сервера.

Процесс внешней веб-аутентификации

С внешней веб-аутентификацией страница входа, используемая для web-аутентификации, сохранена на внешнем веб-сервере. Это - последовательность событий, когда беспроводной клиент пытается обратиться к сети WLAN, которой включили внешнюю веб-аутентификацию:

1. Клиент (конечный пользователь) соединяется с WLAN и открывает web-браузер и вводит URL, такой как www. cisco . com.
2. Клиент передает запрос DNS к серверу DNS для решения www. cisco . com к IP-адресу.
3. WLC пересылает запрос на сервер DNS, который, в свою очередь, решает www. cisco . com к IP-адресу и передает ответ DNS. Контроллер вперед ответ клиенту.
4. Клиент пытается инициировать TCP - подключение с www. cisco . IP-адрес com путем передачи Пакета TCP SYN к www. cisco . IP-адрес com.
5. 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.
6. Клиент передает пакет GET HTTP, предназначенный к www.google.com. WLC перехватывает этот пакет, 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.
7. Клиент тогда запускает Подключение HTTPS к URL перенаправления, который передает его к 1.1.1.1. Это - виртуальный IP - адрес контроллера. Клиент должен проверить серверный сертификат или проигнорировать его для внедрения туннеля SSL.
8. Поскольку внешняя веб-аутентификация включена, WLC перенаправляет клиента к внешнему веб-серверу.
9. URL входа в систему аутентификации внешней web - страницы добавлен с параметрами, такими как AP_Mac_Address, client_url (www. cisco . com) и action_URL, что клиент должен связаться с Web-сервером контроллера.**Примечание:** action_URL говорит Web-серверу, что имя пользователя и пароль сохранено на контроллере. Учетные данные нужно передать обратно в контроллер, чтобы аутентифицироваться.
10. URL внешнего веб-сервера ведет пользователя к странице входа.
11. Страница входа берет ввод учетных данных пользователя и передает запрос обратно в action_URL, пример http://1.1.1.1/login.html, Веб-сервера WLC.
12. Веб-сервер WLC отправляет имя пользователя и пароль для аутентификации.
13. WLC инициирует запрос сервера RADIUS или использует локальную базу данных на WLC и аутентифицирует пользователя.
14. Если аутентификация успешна, Веб-сервер WLC или вперед пользователь к настроенному URL перенаправления или к URL, клиент запустил с, такие как www. cisco . com.
15. Если аутентификация отказывает, то Веб-сервер WLC перенаправляет пользователя назад к URL входа в систему клиента.

Примечание: Для настройки внешнего webauthentication для использования портов кроме HTTP и HTTPS, выполните эту команду:

```
(Cisco Controller) >config network web-auth-port <port> Configures an additional port to be
redirected for web authentication.
```

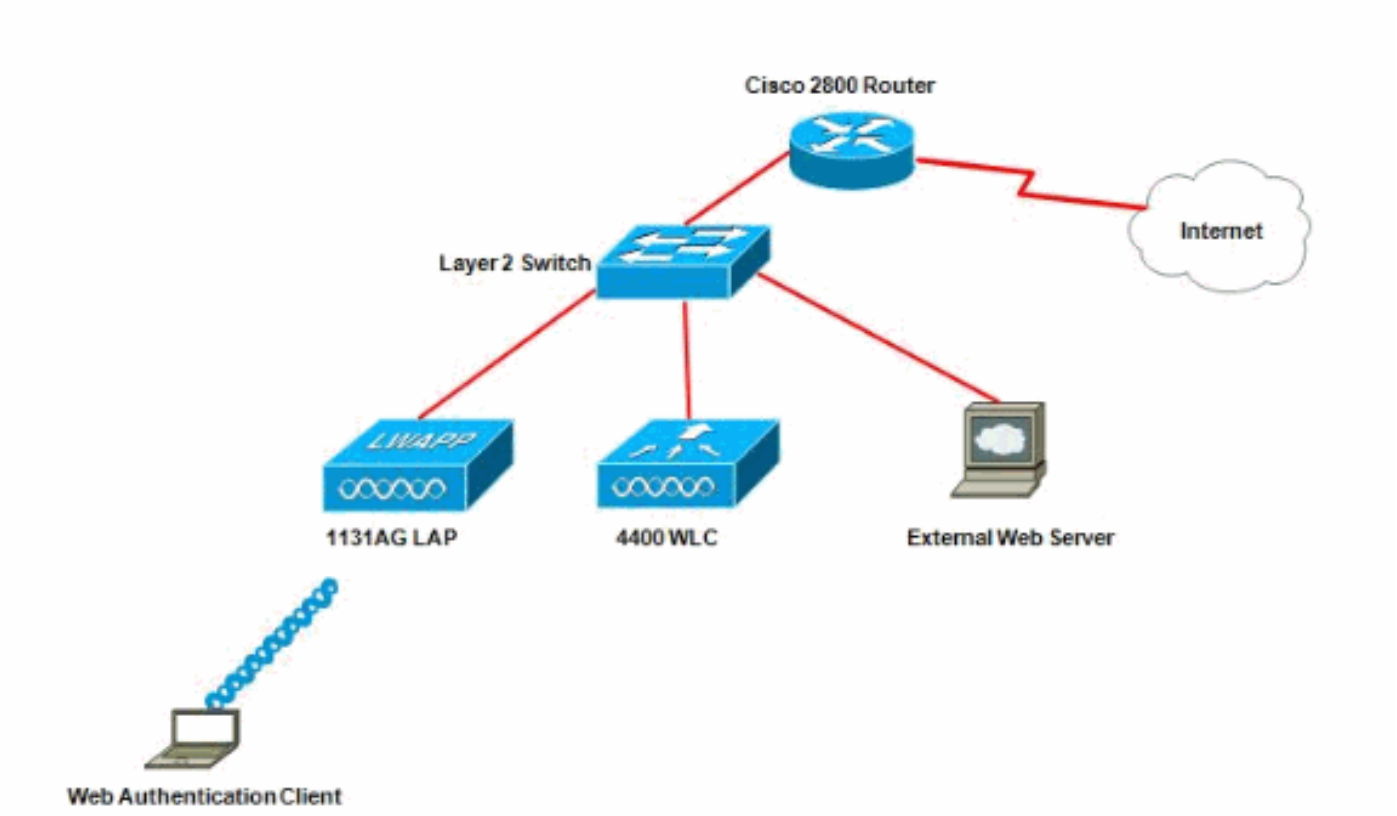
Настройка сети

Пример конфигурации использует эту настройку. LAP зарегистрирован к WLC. Необходимо настроить **гостя** WLAN для гостей и иметь для включения web-аутентификации для

пользователей. Также необходимо гарантировать, что контроллер перенаправляет пользователя к URL внешнего веб-сервера (для внешней веб-аутентификации). Внешний веб-сервер размещает веб-страницу для входа, которая используется для аутентификации.

Учетные данные пользователя должны быть проверены против локальной базы данных, поддержанной на контроллере. После успешной аутентификации пользователи должны быть предоставленным доступом гостю WLAN. Контроллер и другие устройства должны быть настроены для этой настройки.

Примечание: Можно использовать настроенную версию сценария регистрации, который будет использоваться для web-аутентификации. Можно загрузить типовой сценарий Web-аутентификации от страницы Cisco Software Downloads. Например, для этих 4400 контроллеров, перейдите к **продуктам> беспроводные сети> Контроллер беспроводной локальной сети> Автономные контроллеры> контроллеры беспроводной локальной сети Cisco серии 4400> Контроллер беспроводной локальной сети Cisco 4404> программное обеспечение на Шасси> Бандл Web-аутентификации Контроллера беспроводной локальной сети 1.0.1** и загрузите **webauth_bundle.zip** файл.



Примечание: Специализированная веб-подлинная связка (bundle) имеет предел до 30 символов для имен файлов. Гарантируйте, что никакие имена файлов в связке (bundle) не больше, чем 30 символов.

Примечание: Этот документ предполагает, что настроены DHCP, серверы DNS и внешние веб-серверы. См. соответствующую документацию для получения информации третьей стороны о том, как настроить DHCP, сервер DNS и внешний веб-сервер.

Настройка

Перед настройкой WLC для внешней веб-аутентификации необходимо настроить WLC для главной операции и зарегистрировать облегченные точки доступа на контроллере. Этот

документ предполагает, что WLC настроен для главной операции и что LAP зарегистрированы к WLC. См. регистрацию облегченных точек доступа к Контроллеру беспроводной локальной сети (WLC), если вы - новый пользователь, пытающийся устанавливать WLC для главной операции с LAP.

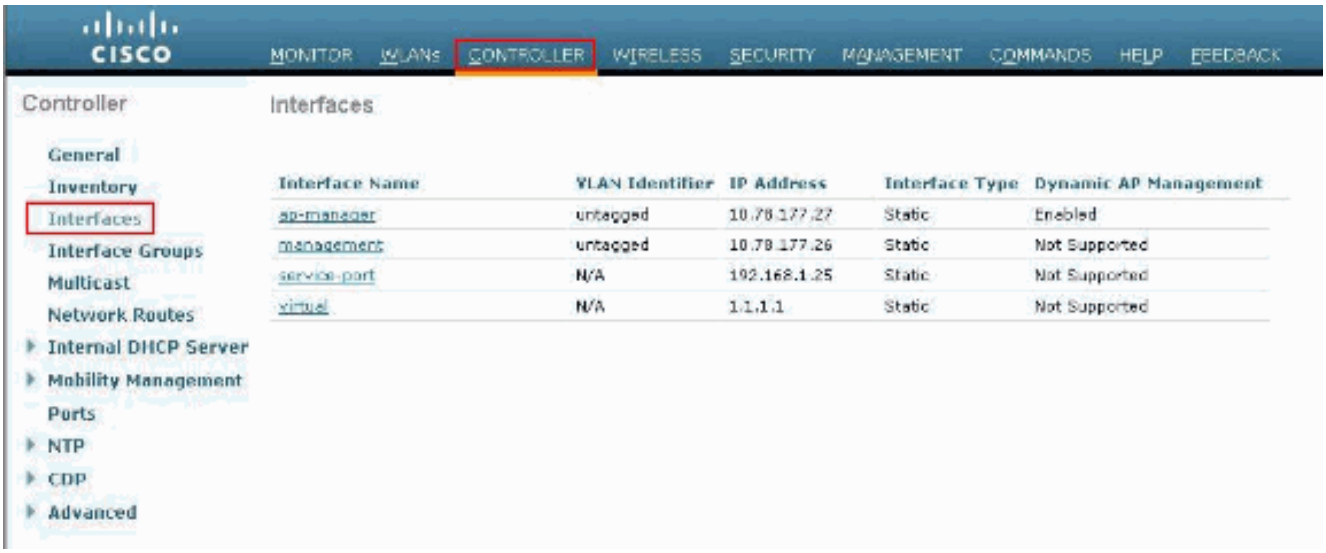
Выполните эти шаги для настройки LAP и WLC для этой настройки:

1. Создайте динамический интерфейс для гостей
2. Создайте ACL предварительной проверки подлинности
3. Создайте локальную базу данных на WLC для гостей
4. Настройте WLC для внешней веб-аутентификации
5. Настройте WLAN для гостей

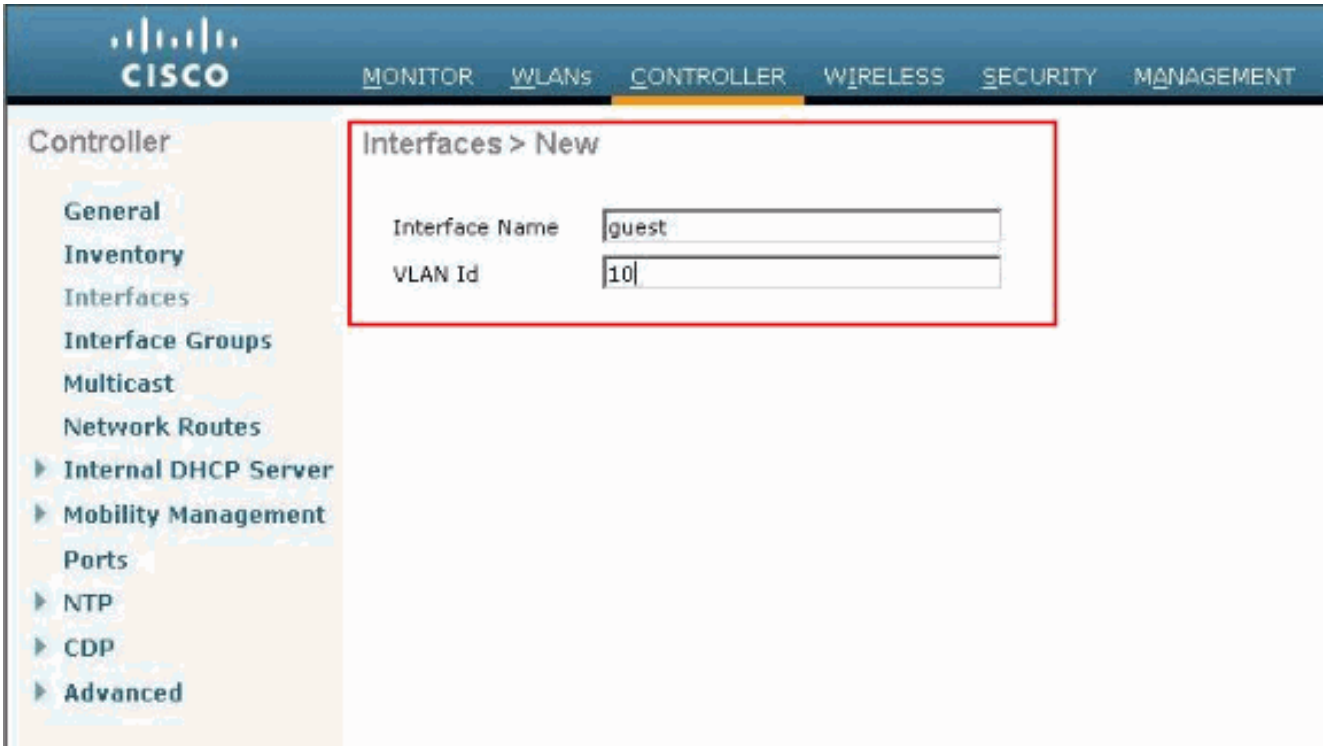
Создайте динамический интерфейс для гостей

Выполните эти шаги для создания динамического интерфейса для гостей:

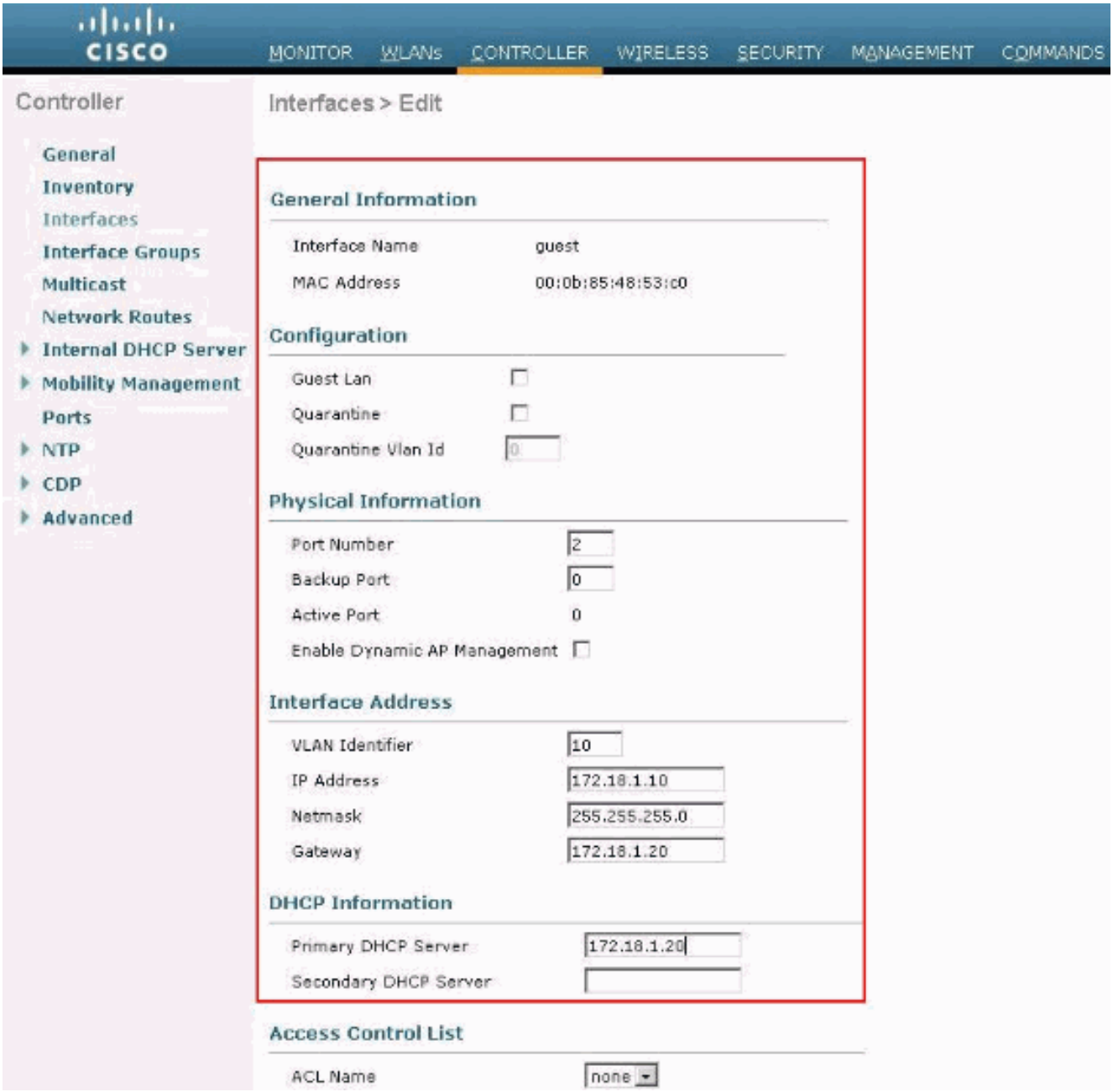
1. **В графическом интерфейсе пользователя (GUI) WLC, выберите Controllers > Interfaces.**Отобразится окно интерфейсов. В окне отобразится список интерфейсов, настроенных для этого контроллера. Список включает в себя интерфейсы по умолчанию, в которые входят интерфейс управления, интерфейс диспетчера точки доступа, виртуальный интерфейс и интерфейс сервисного порта, а также динамические интерфейсы, определенные пользователями.



2. **Нажмите New, чтобы создать новый динамический интерфейс.**
3. **В окне Interfaces > New введите имя интерфейса и идентификатор VLAN. Нажмите кнопку Apply.**В данном примере динамический интерфейс называют **гостем**, и ИДЕНТИФИКАТОР VLAN назначен **10**.



4. **В окне Interfaces > Edit динамического интерфейса введите IP-адрес, маску подсети и шлюз по умолчанию.** Назначьте его для физического порта контроллера беспроводной сети и укажите IP-адрес сервера DHCP. **Затем нажмите Apply.**



Создайте ACL предварительной проверки подлинности

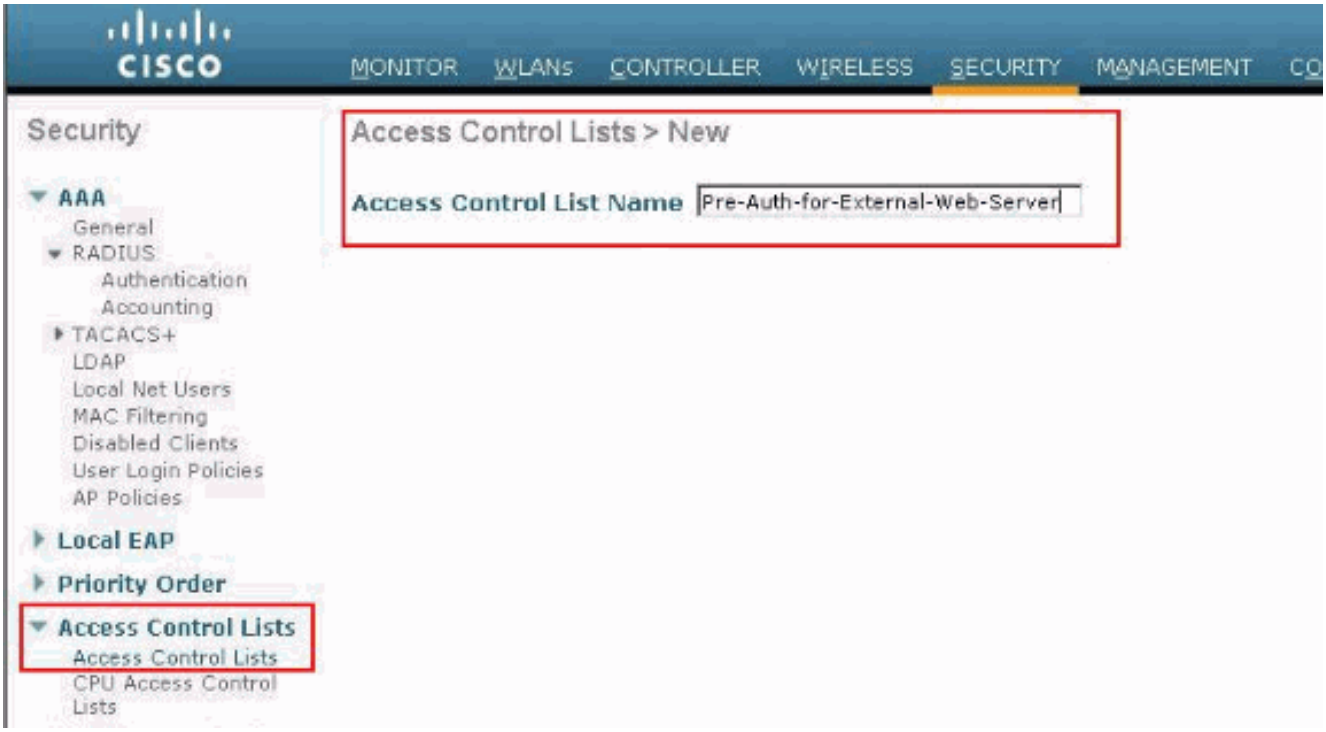
При использовании внешнего веб-сервера для web-аутентификации некоторым платформам WLC нужен ACL процедур, предшествующих аутентификации для внешнего веб-сервера (Контроллер серии 5500 Cisco, Cisco Контроллер серии 2100, серия Cisco 2000 и модуль контроллерной сети). Для других платформ WLC ACL процедур, предшествующих аутентификации не является обязательным.

Однако это - полезный прием для настройки ACL процедур, предшествующих аутентификации для внешнего веб-сервера при использовании внешней веб-аутентификации.

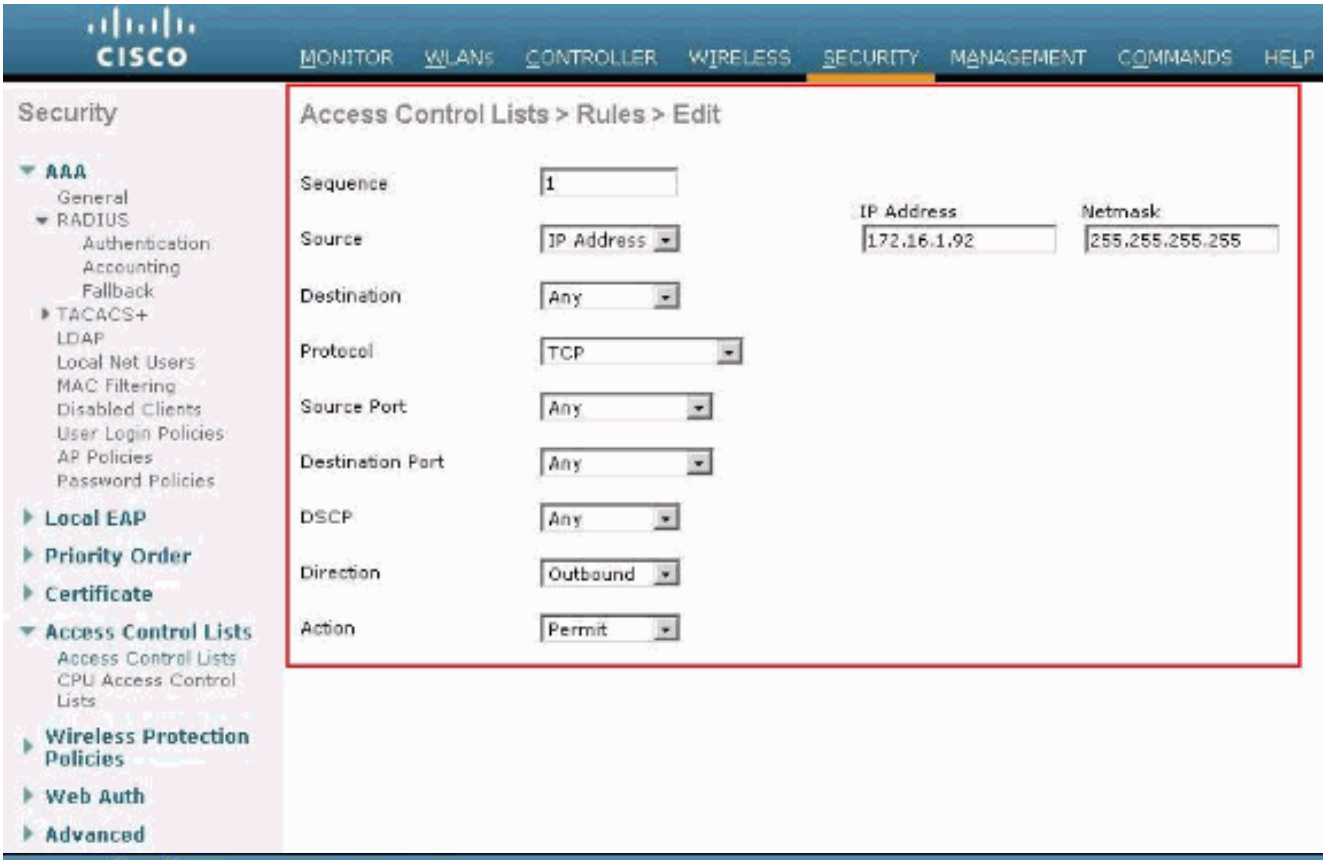
Выполните эти шаги для настройки ACL процедур, предшествующих аутентификации для WLAN:

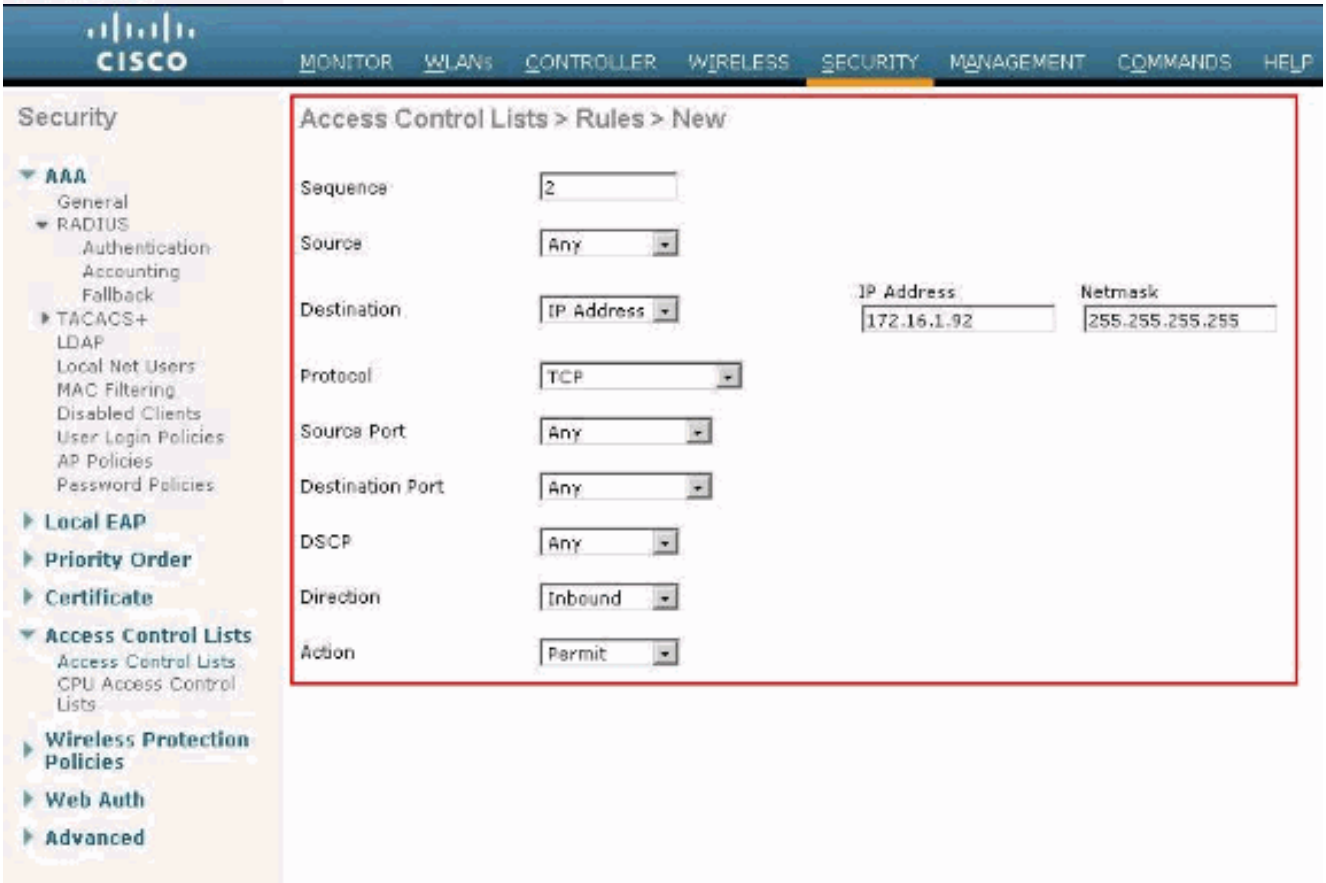
1. От GUI WLC выберите **Security> Access Control Lists**.Это окно позволяет вам просматривать текущие ACL, которые подобны стандартным ACL межсетевого экрана.
2. Нажмите **New** для создания нового ACL.

3. Введите имя ACL и нажмите **Apply**.В данном примере ACL называют **Pre-Auth-for-External-Web-Server**.

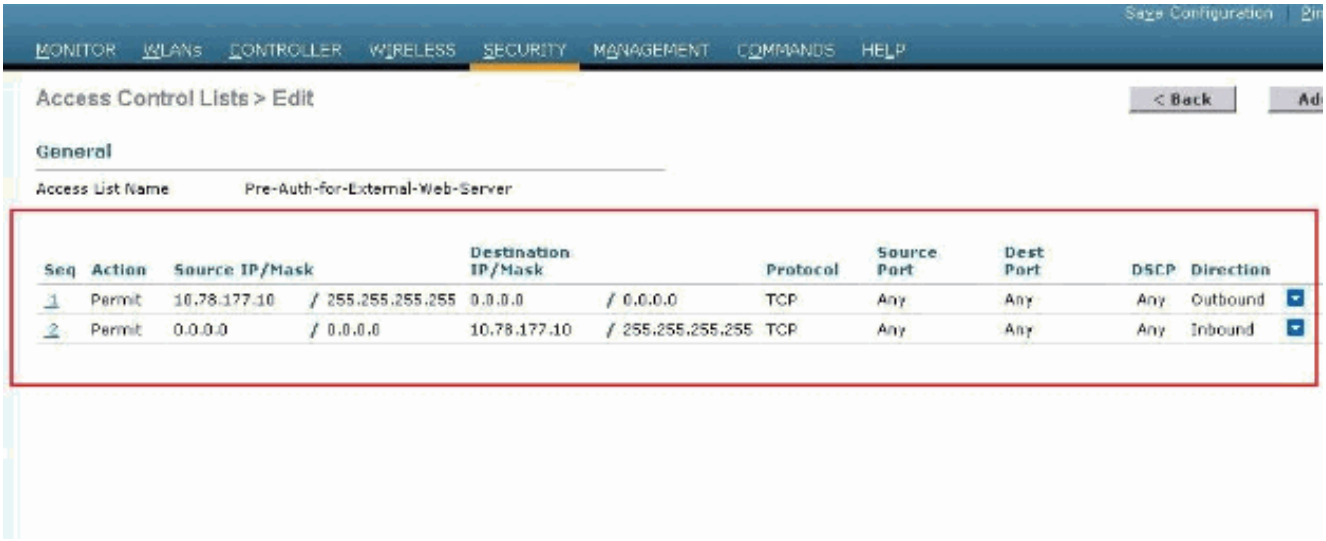


4. Для нового созданного ACL нажмите **Edit**.ACL> Окно редактирования появляется. Это окно позволяет пользователю определить новые правила или модифицировать правила ACL, которые существуют.
5. **Нажать add new rule**.
6. Определите правило списка прав доступа (ACL), которое предоставляет доступ для клиентов к внешнему веб-серверу.В данном примере, 172.16.1.92 IP-адрес внешнего веб-
сервера.





7. Нажмите **Apply** для фиксации изменений.

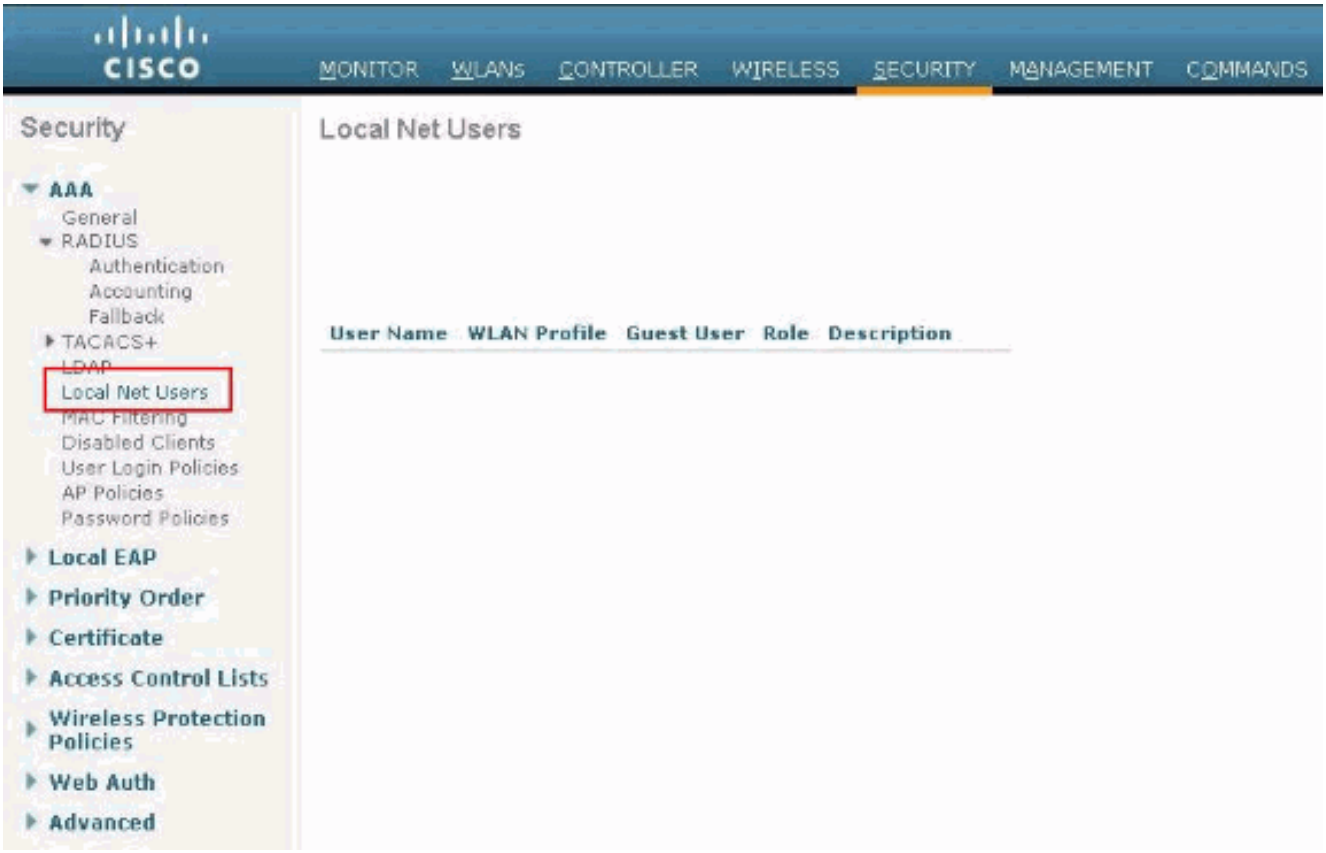


Создайте локальную базу данных на WLC для гостей

База данных пользователей для гостей может или быть сохранена на локальной базе данных Контроллера беспроводной локальной сети или могла бы быть сохранена внешняя из контроллера.

В этом документе локальная база данных на контроллере используется для аутентификации пользователей. Необходимо создать Локального сетевого пользователя и определить пароль для входа в систему клиента web-аутентификации. Выполните эти шаги для создания базы данных пользователей на WLC:

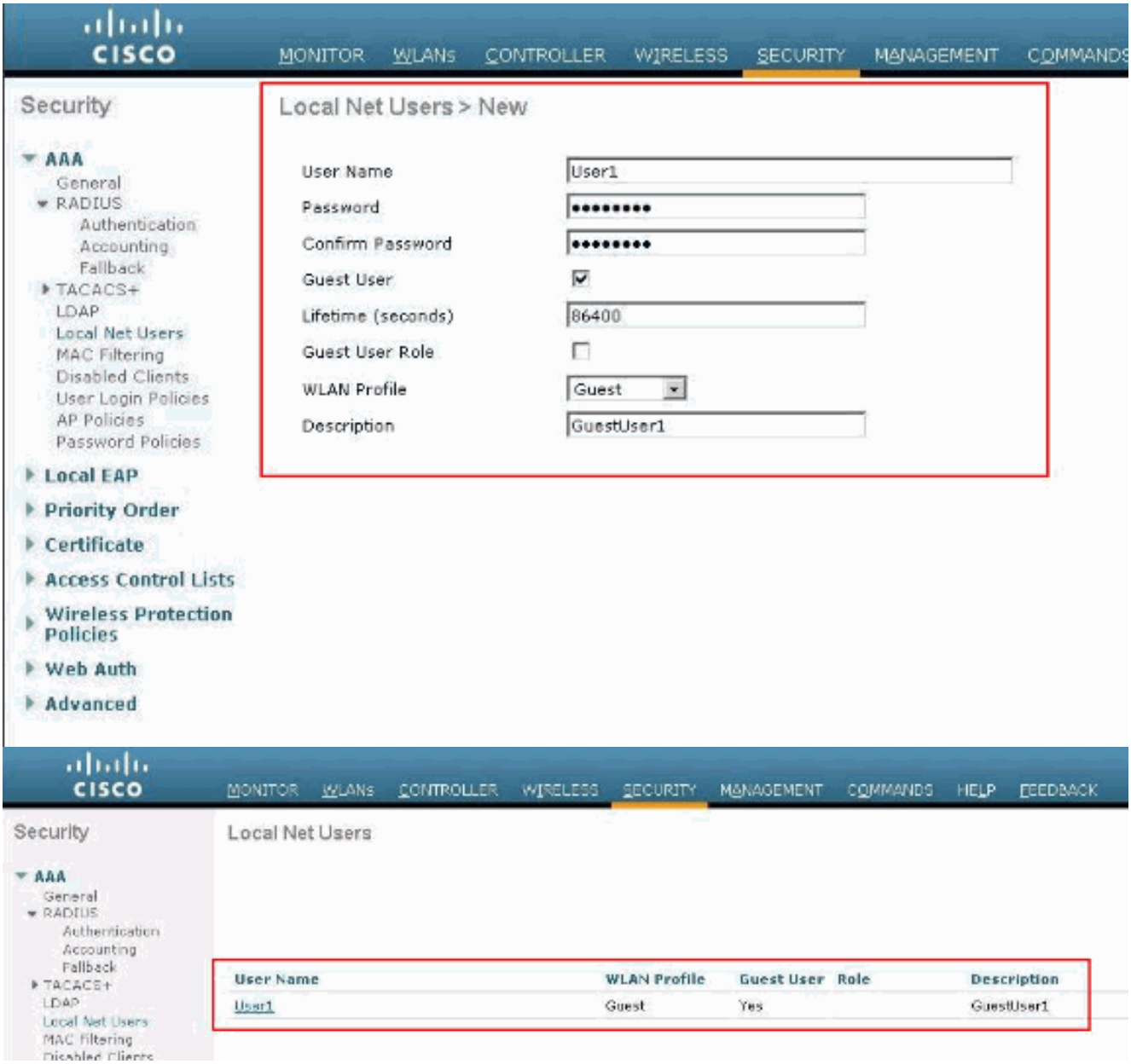
1. От GUI WLC выберите **Security**.
2. Нажмите **Local Net Users** из меню AAA слева.



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.



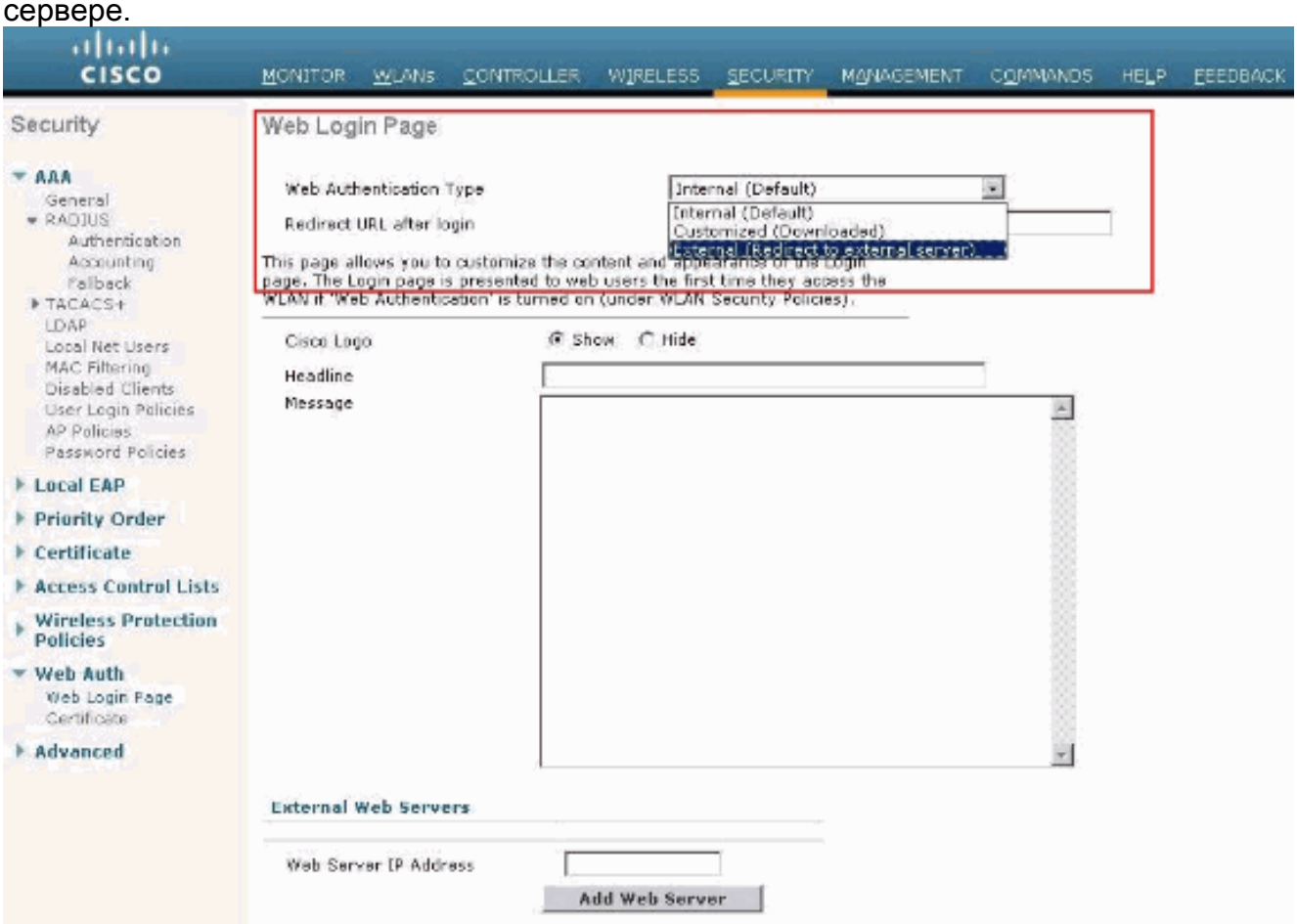
7. Повторите шаги 3-6 для добавления большего количества пользователей к базе данных.

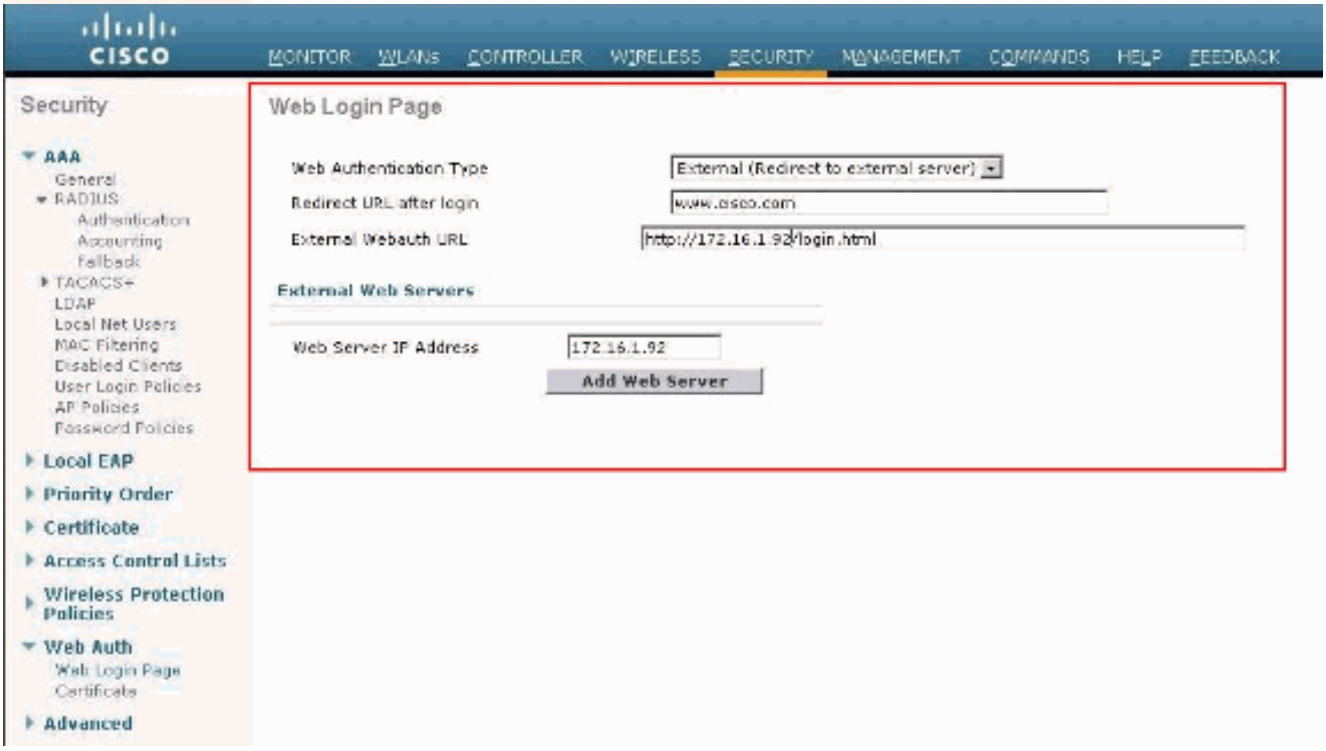
Настройте WLC для внешней веб-аутентификации

Следующий шаг должен настроить WLC для внешней веб-аутентификации. Выполните следующие действия:

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 **External (Redirect к внешнему серверу)**.

3. В разделе **Внешнего веб-сервера** добавьте новый внешний веб-сервер.
4. В **URL Перенаправления после** поля **входа в систему** введите URL страницы, к которой конечный пользователь будет перенаправлен к после успешной аутентификации. В поле **External Web Auth URL** введите URL, где страница входа сохранена на внешнем веб-
сервере.





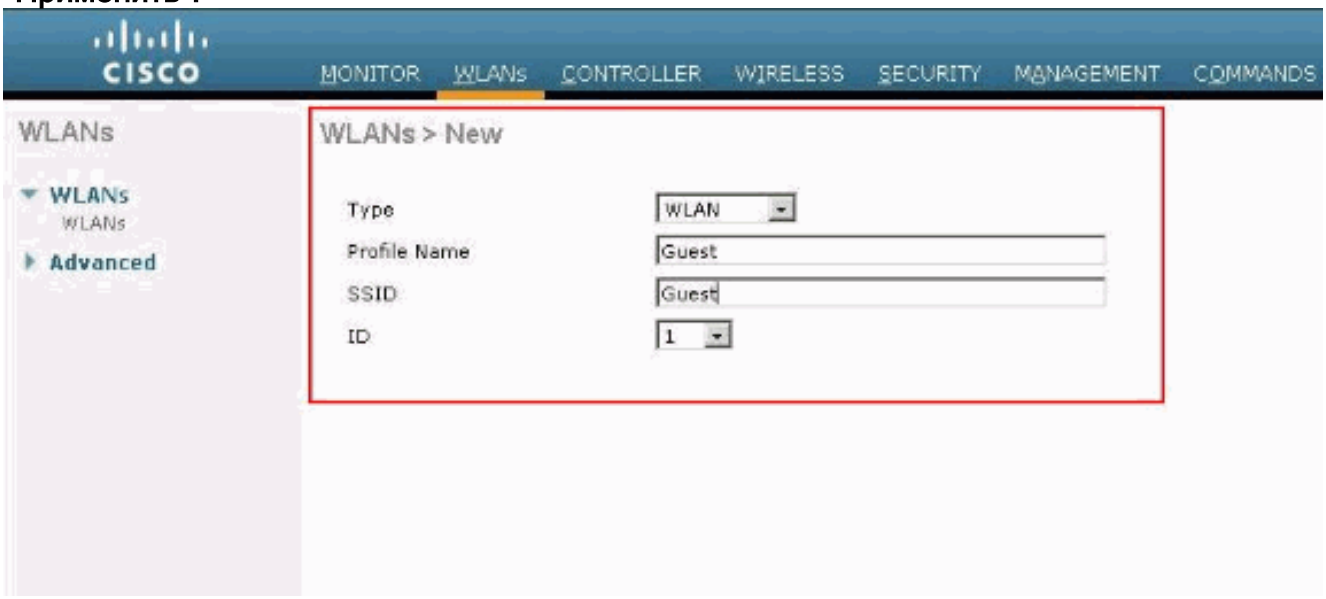
Примечание: В версиях WLC 5.0 и позже, может также быть настроена страница выхода из системы для web-аутентификации. См. Назначать Вход в систему, Ошибку регистрации в системе и страницы Logout на раздел WLAN *Руководства по*

конфигурации Контроллера беспроводной локальной сети, 5.2 для получения дополнительной информации о том, как настроить его.

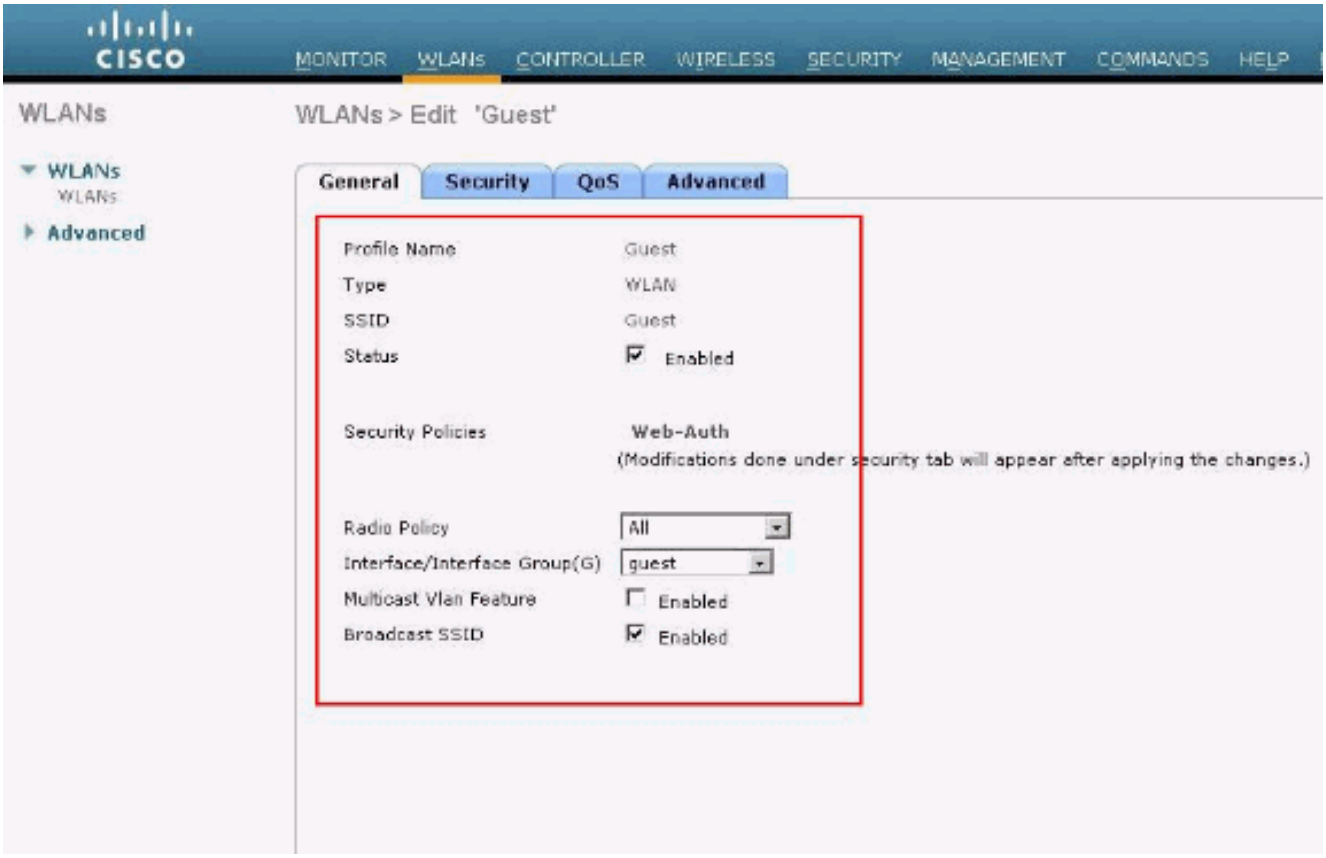
Настройте WLAN для гостей

Заключительный шаг должен создать WLAN для гостей. Выполните следующие действия:

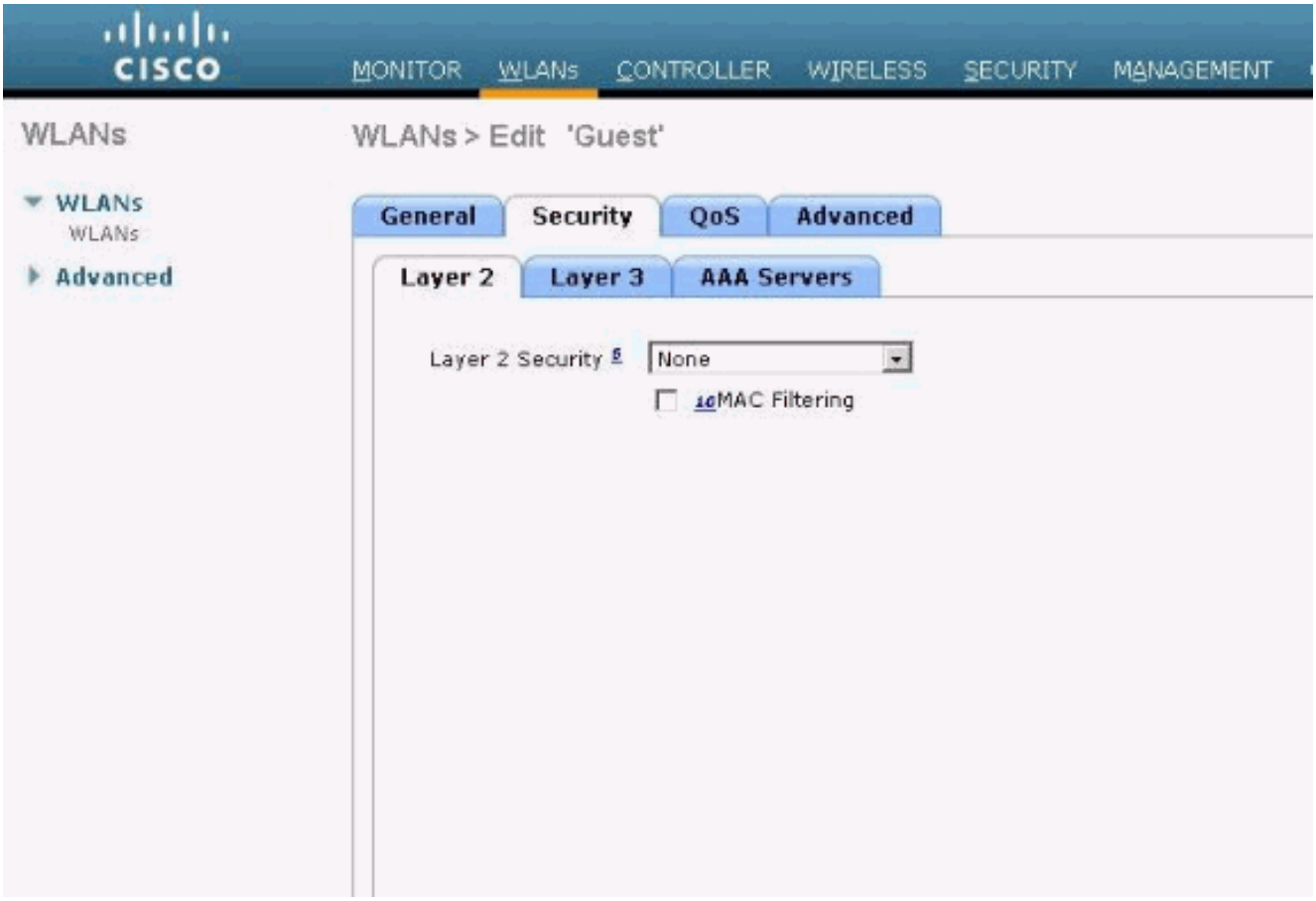
1. **Нажмите WLANs в графическом интерфейсе контроллера для создания WLAN.**Откроется окно WLAN. В данном окне находится список сетей WLAN, настроенных на контроллере.
2. **Нажмите New для настройки новой WLAN.**В данном примере WLAN называют **Гостем**, и ИДЕНТИФИКАТОР WLAN равняется **1**.
3. **Щелкните "Применить".**



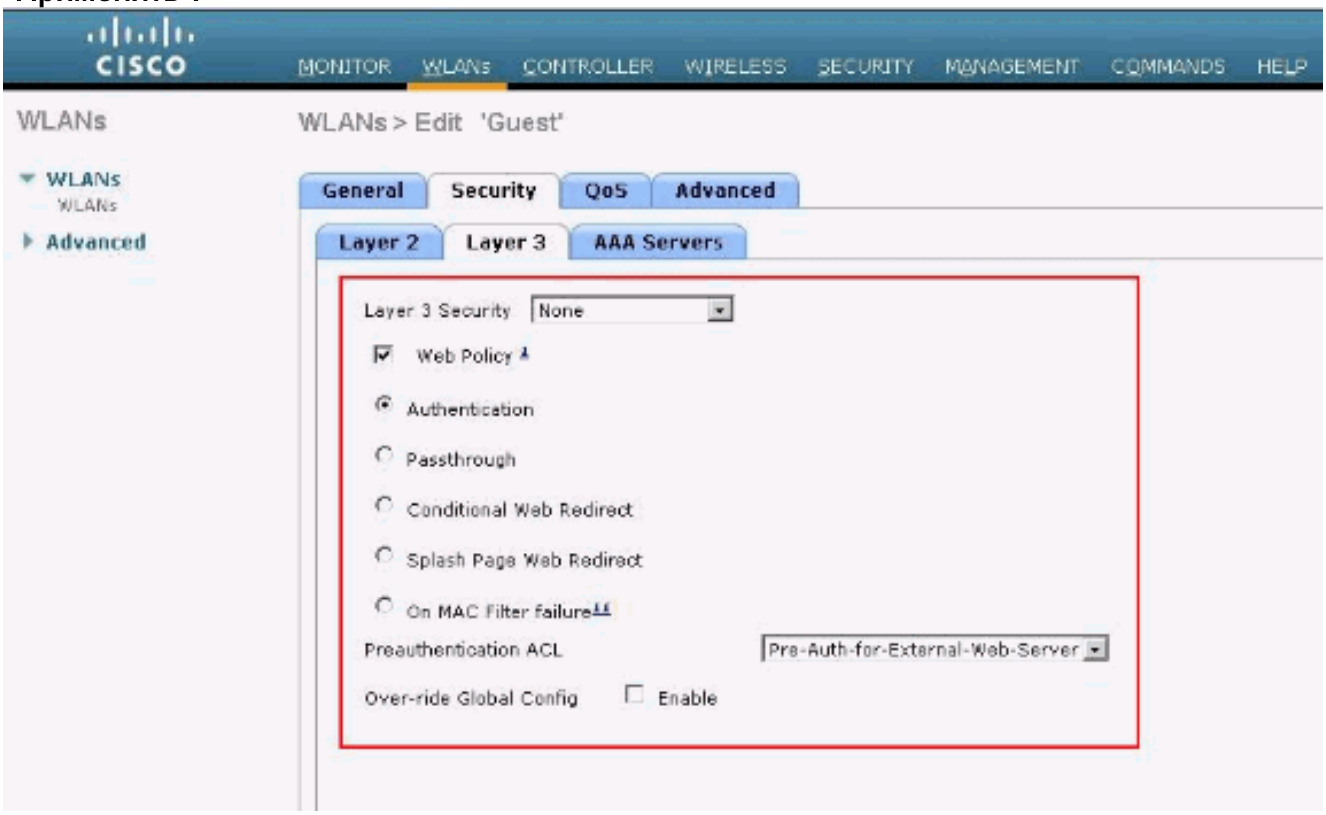
4. В окне WLAN > Edit укажите параметры сети.Для гостевого WLAN, во Вкладке Общие, выбирают соответствующий интерфейс из поля Interface Name.Данный пример сопоставляет **гостя** динамического интерфейса, который был создан на предыдущем этапе гостю
WLAN.



Перейдите на вкладку Безопасность. Под безопасностью уровня 2 **Ни один** не выбран в данном примере.**Примечание:** Web-аутентификация не поддерживается с аутентификацией 802.1x. Это означает, что вы не можете выбрать 802.1x или WPA/WPA2 с 802.1x как безопасность уровня 2 при использовании web-аутентификации. Web-аутентификация поддерживается со всеми другими параметрами безопасности уровня
2.



В поле безопасности уровня 3 проверьте **веб-флажок Policy** и выберите **Параметр проверки подлинности**.Выбор данного параметра осуществляется из-за того, что веб-аутентификация используется для аутентификации гостевых беспроводных клиентов.Выберите соответствующий ACL предварительной проверки подлинности из раскрывающегося меню.В данном примере ранее используется ACL процедур, предшествующих аутентификации, который был создан.**Щелкните "Применить".**

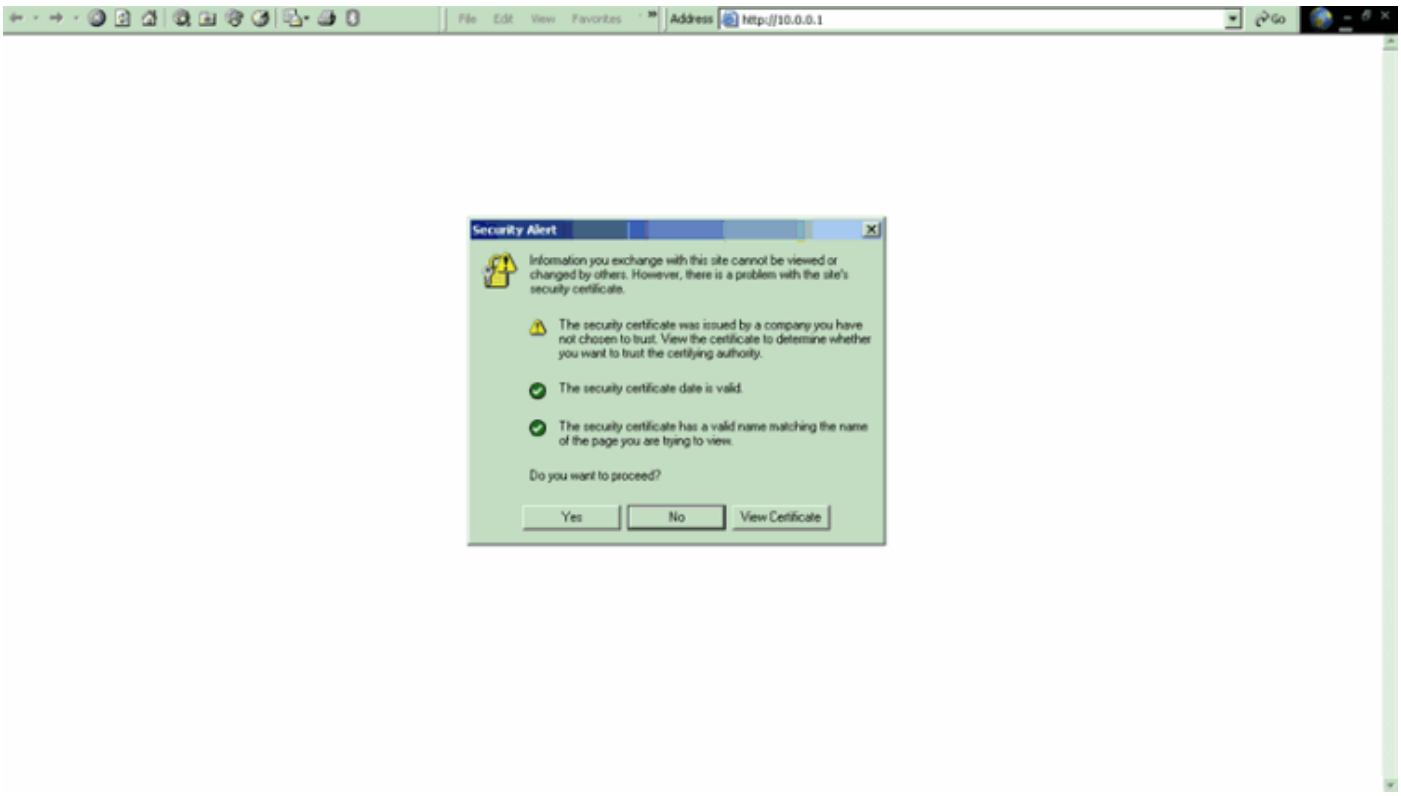


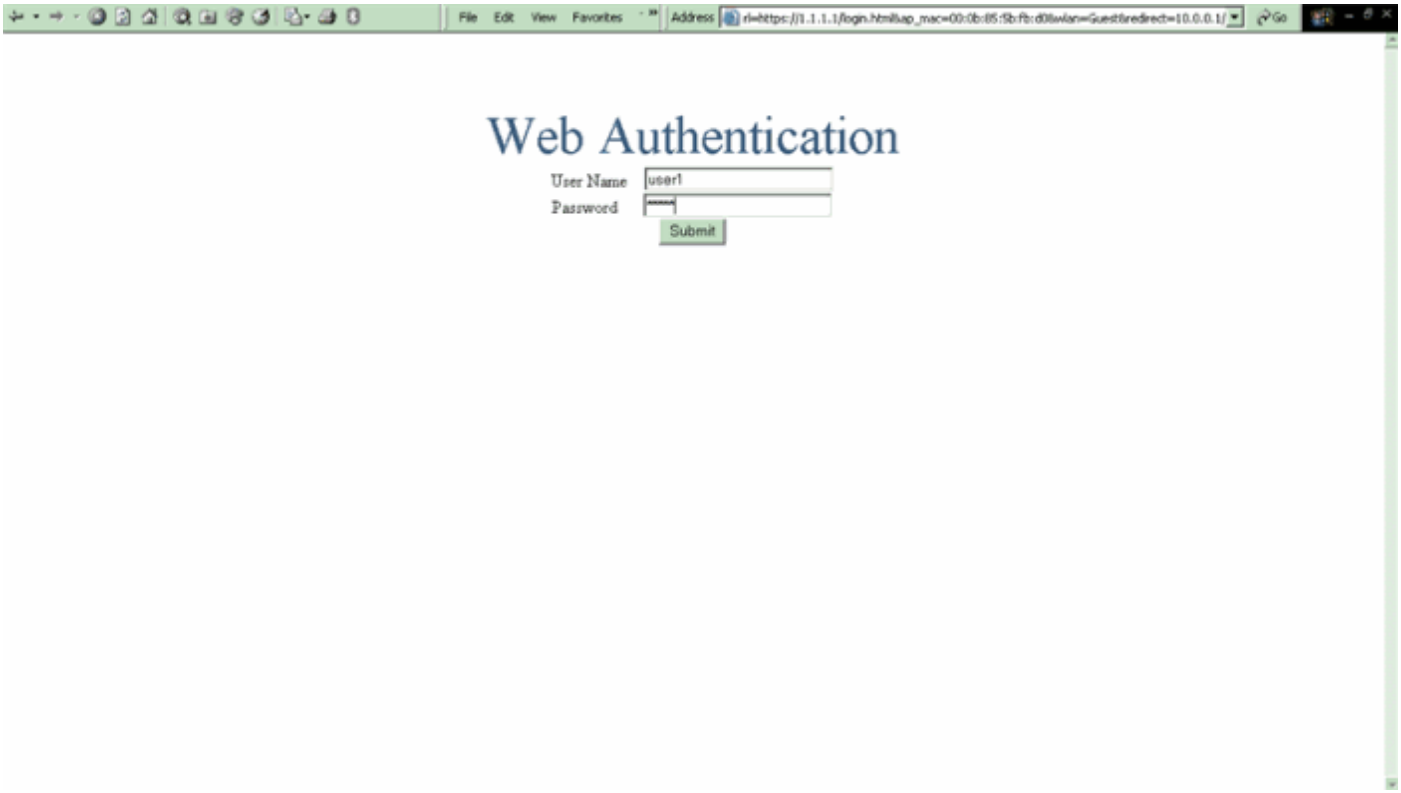
Проверка

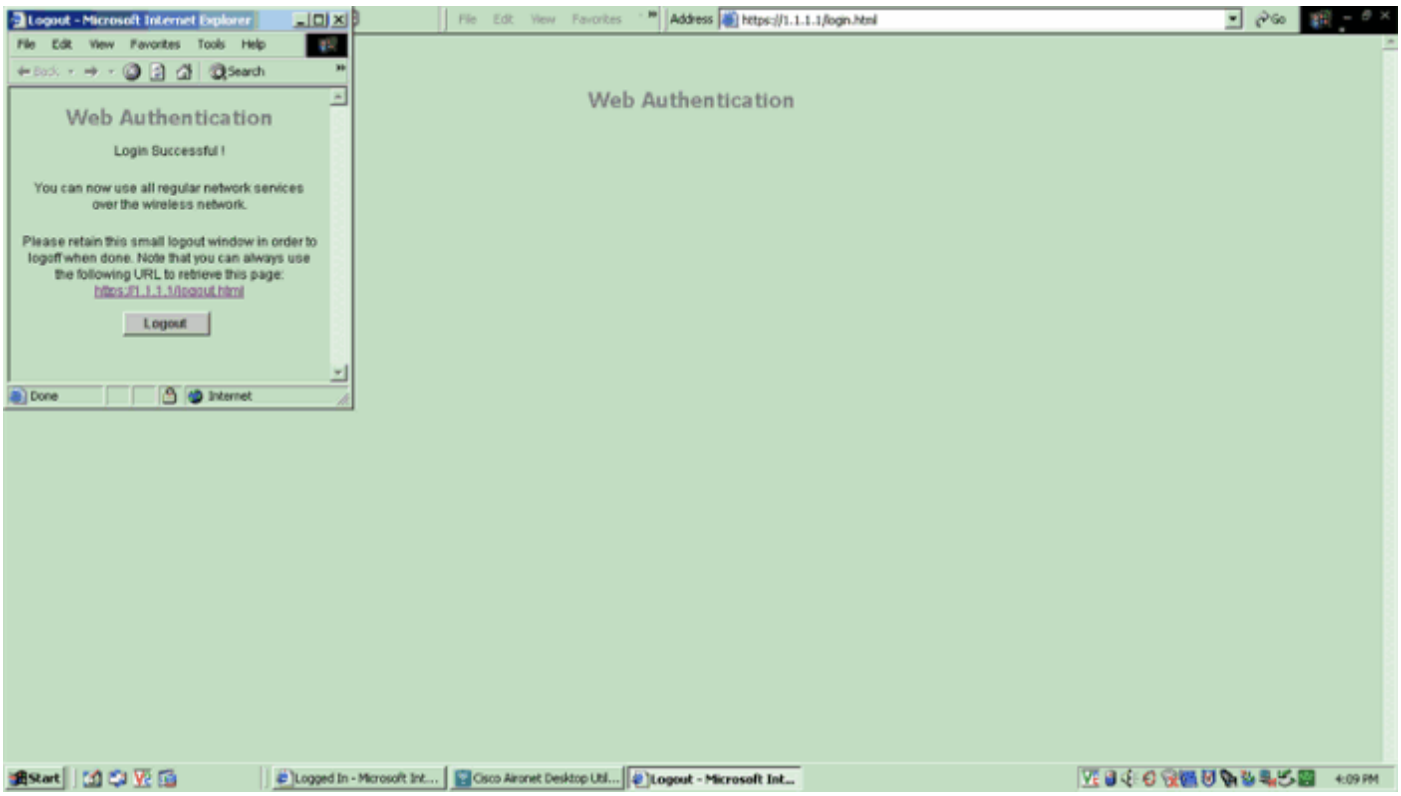
Беспроводной клиент подходит, и пользователь вводит URL, такой как www. cisco . com, в web-браузере. Поскольку пользователь не аутентифицировался, WLC перенаправляет пользователя к URL входа в систему внешней web - страницы.

Пользователю предлагают для учетных данных пользователя. Как только пользователь отправляет имя пользователя и пароль, страница входа берет ввод учетных данных пользователя, и на подвергаются, передает запрос обратно в action_URL пример, http://1.1.1.1/login.html, Веб-сервера WLC. Это предоставлено как параметр ввода URL перенаправления клиента, где 1.1.1.1 Адрес Виртуального интерфейса на коммутаторе.

WLC аутентифицирует пользователя против локальной базы данных, настроенной на WLC. После успешной аутентификации Веб-сервер WLC или вперед пользователь к настроенному URL перенаправления или к URL клиент запустил с, такие как www. cisco . com.







Устранение неполадок

Используйте эти команды отладки для устранения проблем конфигурации.

- адрес debug mac <MAC - адрес клиента xx:xx:xx:xx:xx:xx>
- debug aaa all enable
- состояние debug pem включает
- debug pem events enable
- сообщение debug dhcp включает

- debug dhcp packet enable
- ssh-appgw debug pm включает
- tcp ssh debug pm включает

Используйте этот раздел для устранения неполадок своей конфигурации.

Клиенты, перенаправленные к серверу внешней веб-аутентификации, получают предупреждение сертификата

Проблема: Когда клиенты перенаправлены к серверу внешней веб-аутентификации Cisco, они получают предупреждение сертификата. Существует подтвержденный сертификат на сервере, и если вы соединяетесь с сервером внешней веб-аутентификации непосредственно, сертификат, предупреждающий, не получен. Это то, потому что виртуальный IP - адрес (1.1.1.1) из WLC представлен клиенту вместо фактического IP-адреса сервера внешней веб-аутентификации, который привязан к сертификату?

Решение: Да. Выполняете ли вы локальную проверку подлинности или внешнюю веб-аутентификацию, вы все еще поражаете внутренний веб-сервер в контроллер. Когда вы перенаправляете к внешнему веб-серверу, вы все еще получаете предупреждение сертификата от контроллера, пока у вас нет подтвержденного сертификата на самом контроллере. Если перенаправление передается https, вы получаете предупреждение сертификата от контроллера и от внешнего веб-сервера, пока у обоих нет подтвержденного сертификата.

Для избавлений от предупреждений сертификата всех вместе, у вас должен быть корневой сертификат уровня, выполненный и загруженный на ваш контроллер. Сертификат выполнен для имени хоста, и вы помещаете то имя хоста в поле имени хоста DNS под виртуальным интерфейсом на контроллере. Также необходимо добавить имя хоста к локальному DNS - серверу и указать его к виртуальному IP - адресу (1.1.1.1) из WLC.

См. Генерацию Запроса подписи сертификата (CSR) для Стороннего Сертификата на Контроллере беспроводной локальной сети (WLC) для получения дополнительной информации.

Ошибка: "страница не может быть отображена"

Проблема: После того, как контроллер обновлен к 4.2.61.0, "страница не может быть отображена" сообщение об ошибках, появляется, когда вы используете загруженную веб-страницу для web-аутентификации. Это работало хорошо до обновления. Страница внутренней сети по умолчанию загружается без любой проблемы.

Решение: От версии 4.2 WLC и позже новая характеристика представлена в чем, у вас могут быть множественные cutomized страницы входа для Web-аутентификации.

Для имения загрузки веб-страницы должным образом, не достаточно установить тип web-аутентификации, как **настроено** глобально в **Безопасности> веб-Аутентификация> Веб-страница для входа**. Это должно также быть настроено на определенном WLAN. Для этого выполните следующие действия:

1. Войдите в GUI WLC.
2. Щелкните по вкладке **WLAN** и обратитесь к профилю WLAN, настроенного для Web-аутентификации.

3. На WLAN> страница Edit, нажмите **Вкладку Безопасность**. Затем выберите **Layer 3.**
4. На этой странице выберите **None** в качестве безопасности уровня 3.
5. Установите **веб-**флажок **Политики** и выберите **Параметр проверки подлинности**.
6. Проверьте, что глобальный Config Замены **Включает** коробку, выбирает **Customized (Downloaded)** в качестве веб-Подлинного Типа и выбирает желаемую страницу входа от **Входа в систему Pagepull** вниз меню. **Щелкните "Применить".**

Дополнительные сведения

- Пример настройки веб-аутентификации контроллера беспроводной LAN
- Видео: web-аутентификация на контроллерах беспроводной локальной сети Cisco (WLC)
- Пример конфигурации сетей VLAN на контроллерах беспроводной LAN
- Пример базовой конфигурации контроллера беспроводной локальной сети и "облегченной" точки доступа
- Cisco Systems – техническая поддержка и документация