# Беспроводной BYOD для руководства по развертыванию FlexConnect

## Содержание



## Введение

Мобильные устройства становятся более в вычислительном отношении мощными и популярными среди потребителей. Миллионы этих устройств проданы потребителям с высокоскоростным Wi-Fi, таким образом, пользователи могут связаться и сотрудничать. Потребители теперь приучены к усовершенствованию производительности, которое эти мобильные устройства приносят в их жизни и стремятся принести свой личный опыт в рабочую область. Это создает потребности функциональности решения для BYOD на рабочем месте.

Этот документ предоставляет развертывания ответвления для решения BYOD. Сотрудник соединяется с корпоративным идентификатором набора сервисов (SSID) с его/ее новым iPad и перенаправлен к саморегистрационному порталу. Платформа Cisco Identity Services Engine (ISE) аутентифицирует пользователя против корпоративного Active Directory (AD) и загружает сертификат встроенным MAC-адресом iPad и именем пользователя к iPad, наряду с профилем соискателя, который принуждает использование Transport Layer Security расширяемого протокола аутентификации (EAP-TLS) как метод для подключения dot1x. На основе политики авторизации в ISE пользователь может тогда соединиться с использованием dot1x и получить доступ к соответствующим ресурсам.

Функциональность ISE в выпусках ПО контроллера беспроводной локальной сети Cisco ранее, чем 7.2.110.0 не поддерживала клиентов локального коммутатора, которые связываются через точки доступа FlexConnect (AP). Выпуск 7.2.110.0 поддерживает эту функциональность ISE для AP FlexConnect для локального коммутатора и централизованно аутентифицированных клиентов. Кроме того, Выпуск 7.2.110.0, интегрированный с ISE 1.1.1, предоставляет (но не ограничен), эти функции решения BYOD для радио:

- Профилирование устройства и положение
- Регистрация устройства и соискатель, настраивающий
- Onboarding персональных устройств (iOS условия или устройства на базе Android)

**Примечание:** Несмотря на то, что поддерживаемый, другие устройства, такие как ПК или портативные ПК радио Mac и рабочие станции, не включены в это руководство.

# Предварительные условия

## Требования

Для этого документа отсутствуют особые требования.

## Используемые компоненты

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

- Cisco Catalyst переключается
- Беспроводная сеть LAN Cisco (WLAN) контроллеры
- Контроллер беспроводной локальной сети Cisco (WLC) Выпуск ПО 7.2.110.0 и позже
- 802.11n AP в режиме FlexConnect
- Выпуск ПО Cisco ISE 1.1.1 и позже
- Windows 2008 AD с центром сертификации (CA)
- DHCP Server
- Сервер Системы доменных имен (DNS)
- Network Time Protocol (NTP)
- Портативный ПК беспроводного клиента, смартфон и планшеты (iOS Apple, Android, Windows и Mac)

**Примечание:** См. Комментарии к выпуску для контроллеров беспроводной локальной сети Cisco и Облегченные точки доступа для Выпуска 7.2.110.0 для важной информации об этом выпуске ПО. Войдите к узлу Cisco.com для последних Комментариев к выпуску, прежде чем вы загрузите и протестируете программное обеспечение.

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.

### Топология

Минимальная сетевая установка, как показано в этой схеме требуется, чтобы должным образом внедрить и протестировать эти функции:

Для этого моделирования вам нужны сеть с FlexConnect AP, локальный/удаленный узел с локальным DHCP, DNS, WLC и ISE. FlexConnect AP связан с транком для тестирования локального коммутатора с несколько интерфейсов VLAN.

## Регистрация устройства и соискатель, настраивающий

Устройство должно быть зарегистрировано так, чтобы его собственный соискатель мог настроенный для аутентификации dot1x. На основе правильной политики аутентификации пользователь перенаправляется к гостевой странице и аутентифицируется учетными данными сотрудника. Пользователь видит страницу регистрации устройства, которая просит их сведения об устройстве. Процесс инициализации устройства тогда начинается. Если операционная система (OS) не поддерживается для инициализации, пользователь перенаправлен к Регистрационному Порталу Актива для маркировки того устройства для доступа Обхода проверки подлинности MAC (MAB). Если ОС поддерживается, процесс регистрации начинает и настраивает собственного соискателя устройства для аутентификации dot1x.

## Регистрационный портал актива

Регистрационный Портал Актива является элементом платформы ISE, которая позволяет сотрудникам инициировать onboarding оконечных точек через аутентификацию и процесс регистрации.

Администраторы в состоянии удалить активы из идентификационной страницы оконечных точек. Каждый сотрудник в состоянии отредактировать, удалить, и поместить в черный список активы, которые они зарегистрировали. Помещенные в черный список оконечные точки назначены на идентификационную группу черного списка, и политика авторизации создана для предотвращения доступа к сети помещенными в черный список оконечными точками.

## Саморегистрационный портал

В потоке Центральной веб-аутентификации (CWA) сотрудники перенаправлены к порталу, который позволяет им вводить свои учетные данные, аутентифицироваться и вводить специфические особенности определенного актива, который они хотят зарегистрировать. Этот портал вызывают Сам Инициализация Портала и подобен Порталу Регистрации устройства. Это позволяет сотрудникам вводить MAC-адрес, а также значимый escription оконечной точки.

## Аутентификация и инициализация

Как только сотрудники выбирают Self-Registration Portal, им бросают вызов предоставить ряд допустимых учетных данных сотрудника для перехода к фазе инициализации. После успешной аутентификации оконечная точка может быть настроена в базу данных оконечных точек, и сертификат генерируется для оконечной точки. Ссылка на странице позволяет сотруднику загружать Пилота соискателя мастера (SPW).

> **Примечание:** См. статью FlexConnect Feature Matrix Cisco для просмотра последней матрицы функций FlexConnect для BYOD.

## Инициализация для iOS (iPhone/iPad/iPod)

Для конфигурации EAP-TLS ISE придерживается Apple Беспроводной (OTA) процесс регистрации:

- После успешной аутентификации механизм оценки оценивает настраивающую клиента политику, который приводит к профилю соискателя.
- Если профиль соискателя для значения EAP-TLS, процесс ОТЫ определяет, использует ли ISE самоподписанный или со знаком неизвестным CA., Если одно из условий истинно, пользователя просят загрузить сертификат или ISE или CA прежде чем сможет начаться процесс регистрации.
- Для других методов EAP ISE выдвигает заключительный профиль после успешной аутентификации.

## Инициализация для Android

Из-за учитываемых факторов безопасности агент Android должен быть загружен от узла рынка Android и не может быть настроен от ISE. Cisco загружает версию предвыпускной версии мастера в рынок Android через учетную запись издателя рынка Android Cisco.

Это - процесс инициализации Android:

1. Cisco использует Software Development Kit (SDK) для создания пакета Android с .apk расширением.
2. Cisco загружает пакет в рынок Android.

3. Пользователь настраивает политику в клиенте, настраивающем с соответствующими параметрами.
4. Когда аутентификация dot1x отказывает, после регистрации устройства конечный пользователь перенаправлен клиенту, настраивающему сервис.
5. Страница портала инициализации предоставляет кнопку, которая перенаправляет пользователя к порталу рынка Android, где они могут загрузить SPW.
6. Cisco SPW запущен и выполняет инициализацию соискателя: SPW обнаруживает ISE и загружает профиль от ISE.SPW создает свидетельство/пару ключей для EAP-TLS.SPW выполняет вызов запроса прокси Протокола SCEP (SCEP) к ISE и получает сертификат.SPW применяет беспроводные профили.Если профили применены успешно, SPW инициирует повторную проверку подлинности.Выходы SPW.

## Двойные беспроводные сети SSID саморегистрация BYOD

Это - процесс для двойного радио SSID саморегистрация BYOD:

1. Пользователь связывается к Гостевому SSID.
2. Пользователь открывает браузер и перенаправлен к ISE Гостевой Портал CWA.
3. Пользователь вводит имя пользователя и пароль сотрудника в Гостевой Портал.
4. ISE аутентифицирует пользователя, и, на основе факта, что они - сотрудник и не гость, перенаправляет пользователя к гостевой странице Регистрации устройства Сотрудника.
5. MAC-адрес предварительно заполнен на гостевой странице Регистрации устройства для DeviceID. Пользователь вводит описание и принимает политику допустимого использования (AUP) при необходимости.
6. Пользователь выбирает **Accept** и начинает загружать и устанавливать SPW.
7. Соискатель, для которого устройство пользователя настроено наряду с любыми сертификатами.
8. CoA происходит, и устройство повторно связывается к корпоративному SSID (CORP) и аутентифицируется с EAP-TLS (или другой метод авторизации в использовании для того соискателя).

## Одиночные беспроводные сети SSID саморегистрация BYOD

В этом сценарии существует одиночный SSID для корпоративного доступа (CORP), который поддерживает и Защищенный расширяемый протокол аутентификации (PEAP) и EAP-TLS. Нет никакого Гостевого SSID.

Это - процесс для одиночного радио SSID саморегистрация BYOD:

1. Пользователь связывается к CORP.
2. Пользователь вводит имя пользователя и пароль сотрудника в соискателя для аутентификации PEAP.
3. ISE аутентифицирует пользователя, и, на основе метода PEAP, предоставляет политику авторизации, принимают с перенаправлением к гостевой странице Регистрации устройства Сотрудника.
4. Пользователь открывает браузер и перенаправлен к гостевой странице Регистрации

устройства Сотрудника.
5. MAC-адрес предварительно заполнен на гостевой странице Регистрации устройства для DeviceID. Пользователь вводит описание и принимает AUP.
6. Пользователь выбирает **Accept** и начинает загружать и устанавливать SPW.
7. Соискатель, для которого устройство пользователя настроено наряду с любыми сертификатами.
8. CoA происходит, и устройство повторно связывается к SSID CORP и аутентифицируется с EAP-TLS.

# Конфигурация функции

Выполните эти шаги для начала конфигурации:

1. Для этого руководства гарантируйте, что версия WLC 7.2.110.0 или позже.

2. Перейдите к **Безопасности> RADIUS> Аутентификация** и добавьте сервер RADIUS к WLC.

3. Добавьте ISE 1.1.1 к WLC:

   Введите общий секретный ключ.Поддержка набора RFC 3576 к **включенному**.

4. Добавьте тот же сервер ISE как учетный сервер RADIUS.

5. Создайте ACL Предаутентификации WLC для использования в политике ISE позже. Перейдите к**> Security WLC> Списки контроля доступа> ACL FlexConnect** и создайте новый **REDIRECT именованного списка управления доступом (ACL) FlexConnect ACL** (в данном примере).

6. В правилах списка прав доступа (ACL) разрешите всему к/оту трафика ISE и разрешите трафик клиента во время соискателя, настраивающего.

   Для первого правила (последовательность 1):

   Источник набора **любому**.IP Набора (адрес ISE) / маска подсети **255.255.255.255**.Действие набора для **разрешения**.

Для второго правила (последовательность 2), source IP набора (адрес ISE) / маска 255.255.255.255 **Любому** и Действию для **Разрешения**.

7. Создайте новую FlexConnect Group по имени Flex1 (в данном примере):

   Перейдите к вкладке **FlexConnect Group> WebPolicies**.Под полем WebPolicy ACL **нажмите Add** и выберите **ACL-REDIRECT** или FlexConnect ACL, созданный ранее.Подтвердите, что это заполняет поле **WebPolicy Access Control Lists**.

8. Нажмите **Apply** и **Save Configuration**.

## WLAN Configuration

Выполните эти шаги для настройки WLAN:

1. Создайте Открытый SSID WLAN для двойного примера SSID:

   Введите имя WLAN: **DemoCWA** (в данном примере).Выберите опцию **Enabled** для Статуса.

2. Перейдите к **Вкладке Безопасность> Таблица уровня 2** и установите эти атрибуты:

   Безопасность уровня 2: **Нет**Фильтрация по MAC-адресам: **Включенный** (флажок установлен),Быстрый Переход: **Отключенный** (флажок не установлен),

3. Перейдите к вкладке **AAA Servers** и установите эти атрибуты:

   Аутентификация и серверы учетной записи: **включенный**Сервер 1: *<IP-адрес ISE>*

4. Прокрутите вниз от вкладки **AAA Servers**. В соответствии с заказом Приоритета аутентификации относительно веб-подлинного пользователя, удостоверьтесь, что **RADIUS** используется для аутентификации, и другие не используются.

5. Перейдите **к Вкладке Дополнительно** и установите эти атрибуты:

   Позвольте замену AAA: **включенный**Состояние NAC: **NAC радиуса**
   **Примечание:** Когда FlexConnect AP находится в разъединенном режиме, Network Admission Control (NAC) RADIUS не поддерживается. Таким образом, если FlexConnect

AP находится в автономном режиме и теряет соединение с WLC, все клиенты разъединены, и SSID больше не объявляется.

6. Прокрутите вниз во Вкладке Дополнительно и установите Локальный коммутатор FlexConnect во **Включенный**.

7. Нажмите **Apply** и **Save Configuration**.

8. Создайте SSID WLAN 802.1X по имени **Demo1x** (в данном примере) для одиночных и двойных сценариев SSID.

9. Перейдите к **Вкладке Безопасность> Таблица уровня 2** и установите эти атрибуты:

   Безопасность уровня 2: **WPA+WPA2**Быстрый Переход: **Отключенный** (флажок не установлен),Менеджмент ключа проверки подлинности: 802.IX: **включить**

10. Перейдите **к Вкладке Дополнительно** и установите эти атрибуты:

    Позвольте замену AAA: **включенный**Состояние NAC: **NAC радиуса**

11. Прокрутите вниз во **Вкладке Дополнительно** и установите Локальный коммутатор FlexConnect во **Включенный**.

12. Нажмите **Apply** и **Save Configuration**.

13. Подтвердите, что были созданы оба из новых WLAN.

## Конфигурация точки доступа FlexConnect

Выполните эти шаги для настройки FlexConnect AP:

1. Перейдите к **WLC> беспроводные сети** и нажмите целевой FlexConnect AP.

2. Нажмите вкладку **FlexConnect**.

3. Включите Поддержку VLAN (флажок установлен), установите ID Собственного VLAN и нажмите **VLAN Mappings**.

4. Установите ИДЕНТИФИКАТОР VLAN в **21** (в данном примере) для SSID для локального коммутатора.

5. Нажмите **Apply** и **Save Configuration**.

## Конфигурация ISE

Выполните эти шаги для настройки ISE:

1. Войдите к серверу ISE: <*https://ise*>.

2. Перейдите к **администрированию> Управление идентификацией> Внешние Идентификационные Источники**.

3. Нажмите **Active Directory**.

4. Во вкладке Connection:

   Добавьте Доменное имя **corp.rf-demo.com** (в данном примере) и измените Идентификационный по умолчанию Названия магазина на **AD1**.Нажмите **Save Configuration**.Нажмите **Join** и предоставьте AD имя пользователя и пароль Учетной записи администратора, требуемое присоединиться.Статус должен быть зеленым. Включите **Связанный к:** (флажок установлен).

5. Выполните тест основного подключения к AD с пользователем текущего домена.

6. Если соединение с AD успешно, диалоговое окно подтверждает, что пароль корректен.

7. Перейдите к **администрированию> Управление идентификацией> Внешние Идентификационные Источники**:

   Нажмите **Certificate Authentication Profile**.**Нажмите Add** для нового Профиля проверки подлинности сертификата (CAP).

8. Введите имя **CertAuth** (в данном примере) для CAP; для Основного Атрибута X509 Имени пользователя выберите **Common Name**; **затем щелкните Submit (Отправить).**

9. Подтвердите, что добавлен новый CAP.

10. Перейдите к **администрированию> Управление идентификацией> Идентификационные Исходные Последовательности** и **нажмите Add**.

11. Дайте последовательности название **TestSequence** (в данном примере).

12. Прокрутите вниз для **Сертификации Базирующейся Аутентификации**:

    Включите **Выбирают Certificate Authentication Profile** (флажок установлен).Выберите **CertAuth** (или другой профиль CAP создал ранее).

13. Прокрутите вниз к **Опознавательному Поисковому Списку**:

    Переместите AD1 от доступного до выбранного.Нажмите кнопка для перемещения AD1 в высший приоритет.

14. Нажмите **Submit** для сохранения.

15. Подтвердите, что добавлена новая Идентификационная Исходная Последовательность.

16. Используйте AD для аутентификации Портала «мои устройства». Перейдите к **ISE>**

администрирование> Управление идентификацией> Идентификационная Исходная Последовательность и отредактируйте MyDevices_Portal_Sequence.

17. Добавьте AD1 к Выбранному списку и нажмите кнопка для перемещения AD1 в высший приоритет.

18. Нажмите Save.

19. Подтвердите, что Последовательность хранилища идентификаторов для MyDevices_Portal_Sequence содержит AD1.

20. Повторите шаги 16-19, чтобы добавить AD1 для Guest_Portal_Sequence и нажать Save.

21. Подтвердите, что Guest_Portal_Sequence содержит AD1.

22. Для добавления WLC к Устройству Доступа к сети (WLC) перейдите к администрированию> Сетевые ресурсы> Сетевые устройства и нажмите Add.

23. Добавьте название WLC, IP-адрес, Маску подсети, и т.д.

24. Прокрутите вниз к параметрам аутентификации и введите Общий секретный ключ. Это должно совпасть с общим секретным ключом RADIUS WLC.

25. Нажмите кнопку Submit (Отправить).

26. Перейдите к ISE> Политика> Элементы Политики> Результаты.

27. Разверните **Результаты** и **Авторизацию**, нажмите **Authorization Profiles** и **нажмите Add** для нового профиля.

28. Дайте этому профилю эти значения:

    Name: **CWA**

    Включите Web-аутентификацию (флажок установлен):

    Web-аутентификация: **централизованный**ACL: **REDIRECT ACL** (Это должно совпасть с названием ACL предаутентификации WLC.)Перенаправление: **По умолчанию**

29. Нажмите **Submit** и подтвердите, что был добавлен профиль авторизации CWA.

30. **Нажмите Add** для создания нового профиля авторизации.

31. Дайте этому профилю эти значения:

    Name: **Условие**

    Включите Web-аутентификацию (флажок установлен):

    Значение web-аутентификации: **соискатель, настраивающий**

    ACL: **REDIRECT ACL** (Это должно совпасть с названием ACL предаутентификации WLC.)

32. Нажмите **Submit** и подтвердите, что был добавлен профиль авторизации Условия.

33. Прокрутите вниз в Результатах, разверните **Клиентскую Инициализацию** и нажмите

**Resources**.

34. Выберите **Native Supplicant Profile**.

35. Дайте Профилю название **WirelessSP** (в данном примере).

36. Введите эти значения:

    Тип соединения: **беспроводные сети**SSID: **Demo1x** (это значение от конфигурации WLAN 802.1x WLC),Разрешенный протокол: **TLS**Размер ключа: **1024**

37. **Нажмите кнопку Submit (Отправить).**

38. **Нажмите Save.**

39. Подтвердите, что был добавлен новый профиль.

40. Перейдите к **Политике> Клиентская Инициализация**.

41. Введите эти значения для правила инициализации устройств на iOS:

    Имя правила: **iOS**Identity Groups: **любой**

    Операционные системы: **IOS Mac Все**

    Результаты: **WirelessSP** (это - Собственный Профиль Соискателя, создал ранее),

    Перейдите к **Результатам> Профиль Мастера** (выпадающий список)> **WirelessSP**.

42. Подтвердите, что была добавлена iOS Provisioning Profile.

43. На правой части первого правила найдите выпадающий список Действий и выберите **Duplicate ниже** (или выше).

44. Поменяйте Имя нового правила к **Android**.

45. Измените операционные системы на **Android**.

46. Оставьте другие значения неизменными.

47. Нажмите **Save** (нижний левый экран).

48. Перейдите к **ISE> Политика> Аутентификация**.

49. Модифицируйте условие включать Wireless_MAB и развернуть **Wired_MAB**.

50. Нажмите выпадающий список **Названия Условия**.

51. Выберите **Dictionaries> Compound Condition**.

52. Выберите **Wireless_MAB**.

53. Направо от правила выберите стрелку для расширения.

54. Выберите эти значения от выпадающего списка:

    Идентификационный Источник: **TestSequence** (это - значение, создал ранее),Если отказала аутентификация: **Отклонение**Если пользователь, не найденный: **Продолжить**Если отказал процесс: **Отбрасывание**

55. Перейдите к правилу **Dot1X** и измените эти значения:

    Условие: **Wireless_802.1X**

    Идентификационный источник: **TestSequence**

56. **Нажмите Save.**

57. Перейдите к **ISE> Политика> Авторизация**.

58. Стандартные правила (такие как По умолчанию Черного списка, Представленный, и По умолчанию), уже настроены от установки; первые два могут быть проигнорированы; Стандартное правило будет отредактировано позже.

59. Направо от второго правила (Представленные Cisco IP Phone), нажмите стрелку вниз рядом с Редактированием и выберите **Insert New Rule Below**.

    Добавлено новое Стандартное Правило #.

60. Измените Имя правила из Стандартного Правила # к **OpenCWA**. Это правило инициирует процесс регистрации на открытом WLAN (двойной SSID) для пользователей, которые приезжают в гостевую сеть для настраивания устройств.

61. Нажмите знак "плюс" **(+)** для Условия (условий) и нажмите **Select Existing Condition**

from Library.

62. Выберите Compound Conditions> Wireless_MAB.

63. В Профиле AuthZ нажмите знак "плюс" (+) и выберите Standard.

64. Выберите стандартный CWA (это - Профиль Авторизации, созданный ранее).

65. Подтвердите, что правило добавлено с корректными Условиями и Авторизацией.

66. Нажмите Done (на правой части правила).

67. Направо от того же правила нажмите стрелку вниз рядом с Редактированием и выберите Insert New Rule Below.

68. Измените Имя правила из Стандартного Правила # к PEAPrule (в данном примере). Это правило для PEAP (также используется для одиночного сценария SSID), чтобы проверить, что аутентификация 802.1X без Transport Layer Security (TLS) и что сетевой соискатель, настраивающий, инициируется с профилем авторизации Условия, созданным ранее.

69. Измените условие на Wireless_802.1X.

70. Нажмите значок механизма на правой части условия и выберите Add Attribute/Value. Это 'и' условие, не 'или' условие.

71. Найдите и выберите Network Access.

72. Выберите **AuthenticationMethod** и введите эти значения:

    Authentication method: **Равняется**

    Выберите **MSCHAPV2**.

    Это - пример правила; обязательно подтвердите, что Условием является AND.

73. В Профиле AuthZ выберите **Standard> Provision** (это - Профиль Авторизации, созданный ранее).

74. **Нажмите "Готово".**

75. Направо от PEAPrule нажмите стрелку вниз рядом с Редактированием и выберите **Insert New Rule Below**.

76. Измените Имя правила из Стандартного Правила # к **AllowRule** (в данном примере). Это правило будет использоваться для разрешения доступа к зарегистрированным устройствам с установленными сертификатами.

77. При Условии (условиях) выберите **Compound Conditions**.

78. Выберите **Wireless_802.1X**.

79. Добавьте атрибут AND.

80. Нажмите значок механизма на правой части условия и выберите **Add Attribute/Value**.

81. Найдите и выберите **Radius**.

82. Выберите **Calling-Station-ID - [31]**.

83. Выберите **Equals**.

84. Перейдите **к СЕРТИФИКАТУ** и нажмите правую стрелку.

85. Выберите **Subject Alternative Name**.

86. Для Профиля AuthZ выберите **Standard**.

87. Выберите **Permit Access**.

88. **Нажмите "Готово".**

Это - пример правила:

89. Найдите Стандартное правило для изменения PermitAccess на DenyAccess.

90. Нажмите **Edit** для редактирования Стандартного правила.

91. Перейдите к существующему профилю AuthZ PermitAccess.

92. Выберите **Standard**.

93. Выберите **DenyAccess**.

94. Подтвердите, что Стандартное правило имеет DenyAccess, если не найдены никакие соответствия.

95. **Нажмите "Готово".**

    Это - пример основных правил, требуемых для этого теста; они применимы или для одиночного SSID или для двойного сценария SSID.

96. **Нажмите Save.**

97. Перейдите к **ISE> администрирование> Система> Сертификаты** для настройки сервера ISE с профилем SCEP.

98. В Операциях Сертификата нажмите **SCEP CA Profiles**.

99. **Нажмите Add.**

100. Введите эти значения для этого профиля:

    Name: **mySCEP** (в данном примере)Url : **https://***<server> CA/certsrv/mscep/*(Проверяют вашу конфигурацию сервера CA для верного адреса.)

101. Нажмите **Test Connectivity** для тестирования подключения соединения SCEP.

102. Этот ответ показывает, что возможность подключения сервера успешна.

103. **Нажмите кнопку Submit (Отправить).**

104. Сервер отвечает, что Профиль CA был создан успешно.

105. Подтвердите, что добавлен SCEP CA Профиль.

# IOS User Experience - Provisioning

## Двойной SSID

Этот раздел покрывает двойной SSID и описывает, как соединиться с гостем, чтобы быть настроенным и как соединиться с WLAN 802.1x.

Выполните эти шаги для инициализации iOS в двойном сценарии SSID:

1. На устройстве на iOS перейдите **к сетям Wi-Fi** и выберите **DemoCWA** (настроенный открытый WLAN на WLC).

2. Откройте браузер Safari на устройстве на iOS и посетите достижимый URL (например, внутренний/внешний веб-сервер). ISE перенаправляет вас к порталу. **Нажмите кнопку Continue.**

3. Вы перенаправлены к Гостевому Порталу для входа в систему.

4. Войдите с AD учетной записью пользователя и паролем. Установите Профиль CA, когда предложено.

5. Нажмите надежный сертификат **Install** сервера CA.

6. Нажмите **Done**, как только полностью установлен профиль.

7. Возвратитесь к браузеру и нажмите **Register**. Обратите внимание на Идентификатор устройства, который содержит MAC-адрес устройства.

8. Нажмите **Install** для установки проверенного профиля.

9. Нажмите **Install Now**.

10. После того, как процесс завершен, профиль WirelessSP подтверждает, что установлен профиль. **Нажмите "Готово".**

11. Перейдите **к сетям Wi-Fi** и измените сеть на **Demo1x**. Ваше устройство теперь связано и использует TLS.

12. На ISE перейдите к **Операциям> Аутентификации**. События показывают процесс, в котором устройство связано с открытой гостевой сетью, проходит процесс регистрации с соискателем, настраивающим, и предоставлено доступ разрешения после регистрации.

13. Перейдите к **ISE> администрирование> Управление идентификацией> Группы> Endpoint Identity Groups> RegisteredDevices**. MAC-адрес был добавлен к базе данных.

## Одиночный SSID

Этот раздел покрывает одиночный SSID и описывает, как соединиться непосредственно с

WLAN 802.1x, ввести AD имя пользователя для аутентификации PEAP, условия через гостевую учетную запись, и воссоединяется с TLS.

Выполните эти шаги для инициализации iOS в одиночном сценарии SSID:

1. При использовании то же устройство на iOS, удаляете оконечную точку из Зарегистрированных устройств.

2. На устройстве на iOS перейдите к **Параметрам настройки> общие сведения> Профили**. Удалите профили, установленные в данном примере.

3. Нажмите **Remove** для удаления предыдущих профилей.

4. Соединитесь непосредственно с 802.1x с существующим (очищенным) устройством или с новым устройством на iOS.

5. Соединитесь с **Dot1x**, введите Имя пользователя и пароль и нажмите **Join**.

6. Повторите Шаги 90 и на от Раздела конфигурации ISE, пока не будут полностью установлены соответствующие профили.

7. Перейдите к **ISE> Операции> Аутентификации** для мониторинга процесса. Данный пример показывает клиенту, который связан непосредственно с WLAN 802.1X, поскольку это настроено, разъединяет и повторно соединяется с тем же WLAN с использованием TLS.

8. Перейдите к **WLC> Монитор> [MAC - адрес клиента]**. В клиентской подробности обратите внимание, что клиент находится в состоянии ВЫПОЛНЕНИЯ, его Коммутация данных установлена в локальную переменную, и Аутентификация является Центральной. Это истинно для клиентов то подключение к FlexConnect AP.

# Пользовательский опыт - инициализация Android

## Двойной SSID

Этот раздел покрывает двойной SSID и описывает, как соединиться с гостем, чтобы быть настроенным и как соединиться с WLAN 802.1x.

Процесс соединения для устройства на базе Android подобен этому для устройства на iOS (одиночный или двойной SSID). Однако важное различие - то, что устройство на базе Android требует доступа к Интернету, чтобы обратиться к Google Marketplace (теперь Google Play) и загрузить агента соискателя.

Выполните эти шаги для инициализации устройства на базе Android (такого как Samsung Galaxy в данном примере) в двойном сценарии SSID:

1. В устройстве на базе Android используйте Wi-Fi, чтобы соединиться с **DemoCWA** и открыть гостевой WLAN.

2. Примите любой сертификат для соединения с ISE.

3. Введите Имя пользователя и пароль в Гостевой Портал для регистрации.

4. Нажмите **Register**. Устройство пытается достигнуть Интернета для доступа к Google Marketplace. Добавьте любые дополнительные правила к Предподлинному ACL (такие как REDIRECT ACL) в контроллере для предоставления доступа к Интернету.

5. Google перечисляет Настройку Сети Cisco как приложение для Android. **Нажмите кнопку Install (Установить).**

6. Регистрируйтесь к Google и нажмите **INSTALL**.

7. **Нажмите кнопку OK.**

8. На устройстве на базе Android посчитайте установленную **Cisco** приложением **SPW** и откройте его.

9. Удостоверьтесь, что в вас все еще входят к Гостевому Порталу от вашего устройства

на базе Android.

10. Нажмите **Start** для начала Помощника Настройки Wi-Fi.

11. Cisco SPW начинает устанавливать сертификаты.

12. Когда предложено, устанавливает пароль для учетного хранилища.

13. SPW Cisco возвращается с названием сертификата, которое содержит пользовательский ключ и сертификат пользователя. Нажмите **OK** для подтверждения.

14. Cisco SPW продолжает и вызывает для другого названия сертификата, которое содержит сертификат CA. Введите имя **iseca** (в данном примере), затем нажмите **OK** для продолжения.

15. Устройство на базе Android теперь связано.

## Портал «мои устройства»

Портал «мои устройства» позволяет пользователям помещать в черный список ранее зарегистрированные устройства в конечном счете, устройство потеряно или украдено. Это также позволяет пользователям повторно поступать на службу в случае необходимости.

Выполните эти шаги для помещения в черный список устройства:

1. Для регистрации к Порталу «мои устройства» откройте браузер, соединитесь с https://ise-server:8443/mydevices (обратите внимание на номер порта 8443), и войдите с AD учетной записью.

2. Определить местоположение устройства под Идентификатором устройства и нажать **Lost?** для инициирования помещения в черный список устройства.

3. Когда ISE вызывает предупреждение, нажмите **Yes** для перехода.

4. ISE подтверждает, что устройство отмечено, как **потеряно**.

5. Даже если существует установленный подтвержденный сертификат, любая попытка соединиться с сетью с ранее зарегистрированное устройство теперь заблокировано. Это - пример помещенного в черный список устройства, которое отказывает аутентификацию:

6. Администратор может перейти к **ISE> администрирование> Управление идентификацией> Группы**, нажать **Endpoint Identity Groups> Blacklist** и видеть, что устройство помещено в черный список.

Выполните эти шаги для восстановления помещенного в черный список устройства:

1. От Портала «мои устройства» нажмите **Reinstate** для того устройства.

2. Когда ISE вызывает предупреждение, нажмите **Yes** для перехода.

3. ISE подтверждает, что было успешно восстановлено устройство. Подключите восстановленное устройство с сетью для тестирования этого, устройство будет теперь разрешено.

## Ссылка - сертификаты

ISE не только требует допустимого корневого сертификата CA, но также и нуждается в подтвержденном сертификате, подписанном CA.

Выполните эти шаги, чтобы добавить, связать, и импортировать новый доверяемый сертификат CA:

1. Перейдите к **ISE> администрирование> Система> Сертификаты**, нажмите **Local Certificates** и **нажмите Add**.

2. Выберите **Generate Certificate Signing Request (CSR)**.

3. Введите **CN** Предмета Сертификата **=** *<имя хоста СЕРВЕРА ISE. FQDN>*. Для других полей можно использовать по умолчанию или значения, требуемые настройкой CA. **Нажмите кнопку Submit (Отправить).**

4. ISE проверяет, что генерировался CSR.

5. Для доступа к CSR нажмите операции **Запросов подписи сертификата**.

6. Выберите CSR, недавно созданный, затем нажмите **Export**.

7. ISE экспортирует CSR в файл .pem. Нажмите **Save File**, затем нажмите **OK**, чтобы сохранить файл к локальному компьютеру.

8. Найдите и откройте файл сертификата ISE с текстовым редактором.

9. Скопируйте все содержание сертификата.

10. Соединитесь с сервером CA и войдите с учетной записью администратора. Сервером является Microsoft 2008 CA в https://10.10.10.10/certsrv (в данном примере).

11. Нажмите **Request сертификат**.

12. Нажмите **усовершенствованный запрос сертификата**.

13. Нажмите вторую опцию для **Отправки запроса сертификата при помощи base-64-encoded CMC или...**.

14. Вставьте содержание от файла сертификата ISE (.pem) в поле Saved Request, гарантируйте, что Шаблоном сертификата является **Web-сервер**, и нажмите **Submit**.

15. Нажмите **сертификат Download**.

16. Сохраните certnew.cer файл; это будет использоваться позже для привязки с ISE.

17. От **Сертификатов** ISE перейдите к **Локальным Сертификатам** и **нажмите Add>, Связывают Сертификат CA**.

18. Перейдите к сертификату, который был сохранен к локальному компьютеру в предыдущем шаге, включите и **EAP** и протоколы **Интерфейса управления** (флажки установлены), и нажмите **Submit**. ISE может занять несколько минут или больше для перезапуска сервисов.

19. Возвратитесь к целевой странице CA (https://CA/certsrv/) и нажмите **Download a CA certificate, цепочку сертификатов или CRL**.

20. Нажмите **Download CA certificate**.

21. **Сохраните** файл к локальному компьютеру.

22. С сервером ISE онлайн, перейдите **к Сертификатам** и нажмите **Certificate Authority Certificates**.

23. **Нажмите кнопку Import (Импортировать).**

24. Ищите сертификат CA, включите **Доверие для аутентификации клиента** (флажок установлен), и нажмите **Submit**.

25. Подтвердите, что добавлен новый доверяемый сертификат CA.

## Дополнительные сведения

- Руководство по установке оборудования платформы Cisco Identity Services Engine, выпуск 1.0.4
- Контроллеры беспроводных LAN серии Cisco 2000
- Контроллеры беспроводных LAN серии Cisco 4400
- Cisco Aironet серии 3500
- Руководство по развертыванию контроллера ответвления беспроводных сетей Flex 7500
- Принесите свое собственное устройство - унифицированное Устройство аутентификации и последовательный опыт доступа
- Беспроводной BYOD с платформой Identity Services Engine
- Cisco Systems – техническая поддержка и документация