Tecnología inalámbrica BYOD para el Guía de despliegue de FlexConnect

Contenido

Introducción

Los dispositivos móviles están llegando a ser más de cómputo potentes y populares entre los consumidores. Millones de estos dispositivos se venden a los consumidores con el Wi-Fi de alta velocidad así que los usuarios pueden comunicar y colaborar. Los consumidores ahora están acostumbrados a la mejora de la productividad que estos dispositivos móviles traen en sus vidas y están intentando traer su experiencia personal en el espacio de trabajo. Esto crea las necesidades de las funciones de una solución de Bring Your Own Device (BYOD) en el lugar de trabajo.

Este documento proporciona el despliegue de la bifurcación para la solución BYOD. Un empleado conecta con un Service Set Identifier (SSID) corporativo con su nuevo iPad y consigue reorientado a un portal del uno mismo-registro. El Cisco Identity Services Engine (ISE) autentica al usuario contra el Active Directory corporativo (AD) y descarga un certificado con una dirección MAC y un nombre de usuario integrados del iPad al iPad, junto con un perfil del supplicant que aplique el uso de la Seguridad de la capa del Protocolo-transporte de la autenticación ampliable (EAP-TLS) como método para la Conectividad del dot1x. De acuerdo con la directiva de la autorización en el ISE, el usuario puede después conectar con el uso del dot1x y acceder para apropiarse de los recursos.

Las funciones ISE en las versiones de software del controlador LAN de la tecnología inalámbrica de Cisco que 7.2.110.0 no apoyaron anterior a los clientes del Local Switching que se asocian con el (APS) de los Puntos de acceso de FlexConnect. La versión 7.2.110.0 soporta estas funciones ISE para FlexConnect AP para el Local Switching y los clientes centralmente autenticados. Además, la versión 7.2.110.0 integrado con ISE 1.1.1 proporciona (pero no se limita a) estas características de la solución BYOD para la Tecnología inalámbrica:

- Perfilado y postura del dispositivo
- Disposición del registro del dispositivo y del supplicant
- Onboarding de los dispositivos personales (IOS de la disposición o dispositivos de Android)

  Note: Aunque estén soportados, los otros dispositivos, tales como PC o laptopes inalámbricas y puestos de trabajo del mac, no se incluyan en esta guía.

Prerequisites

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Catalyst Switchs
- Reguladores de la tecnología inalámbrica de Cisco LAN (red inalámbrica (WLAN))
- Versión de software 7.2.110.0 del controlador de WLAN de Cisco (WLC) y posterior
- 802.11n AP en el modo de FlexConnect
- Software Release 1.1.1 y Posterior de Cisco ISE
- Windows 2008 AD con el Certificate Authority (CA)
- Servidor DHCP
- Servidor del Domain Name System (DNS)
- **Network Time Protocol** (NTP)
- Laptop, smartphone, y tablillas del cliente de red inalámbrica (IOS de Apple, Android, Windows, y mac)

Note: Refiera a los Release Note para los controladores LAN y los Puntos de acceso ligeros de la tecnología inalámbrica de Cisco para la versión 7.2.110.0 para la información importante sobre esta versión de software. Inicie sesión al sitio del cisco.com para los últimos Release Note antes de que usted cargue y pruebe el software.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Topología

Una configuración de la red mínima, tal y como se muestra en de este diagrama se requiere para implementar y probar correctamente estas características:

Para esta simulación, usted necesita una red con un FlexConnect AP, un local/sitio remoto con el DHCP local, DNS, el WLC, y el ISE. El FlexConnect AP está conectado con un trunk para probar el Local Switching con los VLAN múltiples.

Disposición del registro del dispositivo y del supplicant

Un dispositivo debe ser registrado de modo que su supplicant nativo pueda el aprovisionado para la autenticación del dot1x. De acuerdo con la política de autenticación correcta, reorientan a la página del invitado y son autenticado al usuario por las credenciales del empleado. El usuario ve la página del registro del dispositivo, que pide su información del dispositivo. El proceso de abastecimiento del dispositivo entonces comienza. Si el operating system (OS) no se soporta para disposición, reorientan al usuario al portal del registro del activo para marcar que dispositivo para el acceso de puente de la autenticación de MAC (MAB). Si se soporta el OS, el proceso de la inscripción comienza y configura el supplicant nativo del dispositivo para la autenticación del dot1x.

Portal del registro del activo

El portal del registro del activo es el elemento de la plataforma ISE que permite que los empleados inicien onboarding de los puntos finales con una autenticación y un proceso de inscripción.

Los administradores pueden borrar los activos de la página de las identidades de los puntos finales. Cada empleado puede editar, borrar, y poner los activos que se han registrado. Los puntos finales puestos se asignan a un grupo de la identidad de la lista negra, y una directiva de la autorización es creada para prevenir el acceso a la red por los puntos finales puestos.

Portal del Uno mismo-registro

En el flujo central de la autenticación Web (CWA), reorientan a los empleados a un portal que permita que ingresen sus credenciales, que autentiquen, y que ingresen los específicos del activo

determinado que desean registrarse. Este portal se llama el aprovisionamiento del uno mismo porta y es similar al portal del registro del dispositivo. Permite que los empleados ingresen el MAC address así como un escription significativo del punto final.

Autenticación y aprovisionamiento

Una vez que los empleados seleccionan el portal del Uno mismo-registro, los desafían a proporcionar un conjunto de las credenciales válidas del empleado para proceder a la fase del aprovisionamiento. Después de la autenticación satisfactoria, el punto final puede ser aprovisionado en la base de datos de los puntos finales, y un certificado se genera para el punto final. Un link en la página permite que el empleado descargue al Asisitente del piloto del supplicant (SPW).

> **Note**: Refiera al artículo de Cisco de la Matriz de la función de FlexConnect para ver la última Matriz de la función de FlexConnect para BYOD.

Disposición para IOS (iPhone/iPad/iPod)

Para la configuración del EAP-TLS, el ISE sigue Apple sobre - ventile el proceso de la inscripción (OTA):

- Después de la autenticación satisfactoria, el motor de la evaluación evalúa las directivas del cliente-aprovisionamiento, que da lugar a un perfil del supplicant.
- Si el perfil del supplicant está para la configuración del EAP-TLS, el proceso OTA determina si el ISE es el usar uno mismo-firmado o firmado por un CA desconocido. Si una de las condiciones es verdad, piden el usuario descargar el certificado de ISE o de CA antes de que el proceso de la inscripción pueda comenzar.
- Para otros métodos EAP, el ISE avanza el perfil final sobre la autenticación satisfactoria.

Disposición para Android

Debido a las observaciones de seguridad, el agente de Android se debe descargar del sitio del mercado de Android y no puede ser aprovisionado del ISE. Cisco carga una versión del candidato de la versión del Asisitente en el mercado de Android con la cuenta del editor del mercado de Cisco Android.

Éste es el proceso de abastecimiento de Android:

1. Cisco utiliza el Software Development Kit (SDK) para crear el paquete de Android con una extensión .apk.
2. Cisco carga un paquete en el mercado de Android.
3. El usuario configura la directiva en el aprovisionamiento del cliente con los parámetros apropiados.
4. Después del registro del dispositivo, reorientan al usuario final al servicio del aprovisionamiento del cliente cuando la autenticación del dot1x falla.
5. La página porta del aprovisionamiento proporciona un botón que reoriente al usuario al

portal del mercado de Android en donde pueden descargar el SPW.
6. Cisco SPW se inicia y realiza el aprovisionamiento del supplicant: SPW descubre el ISE y descarga el perfil del ISE.SPW crea un CERT/un par clave para el EAP-TLS.SPW hace una llamada de la petición del proxy del protocolo simple certificate enrollment (SCEP) al ISE y consigue el certificado.SPW aplica los perfiles inalámbricos.SPW acciona la reautentificación si los perfiles se aplican con éxito.Salidas SPW.

Uno mismo-registro inalámbrico dual SSID BYOD

Éste es el proceso para el uno mismo-registro inalámbrico dual SSID BYOD:

1. Los socios del usuario al invitado SSID.
2. El usuario abre a un navegador y se reorienta al portal del invitado ISE CWA.
3. El usuario ingresa un nombre de usuario y contraseña del empleado en el portal del invitado.
4. El ISE autentica al usuario, y, sobre la base del hecho de que son empleado y no un invitado, reorienta al usuario a la página del invitado del registro del dispositivo del empleado.
5. La dirección MAC PRE-se puebla en la página del invitado del registro del dispositivo para el DeviceID. El usuario ingresa una descripción y valida el Acceptable Use Policy (AUP) si procede.
6. El usuario selecciona **valida** y comienza a descargar y a instalar el SPW.
7. El supplicant para el dispositivo de ese usuario es aprovisionado junto con cualquier Certificados.
8. El CoA ocurre, y el dispositivo reasocia al SSID corporativo (CORP) y autentica con el EAP-TLS (o el otro método de autorización funcionando para ese supplicant).

Solo Uno mismo-registro inalámbrico SSID BYOD

En este escenario, hay un solo SSID para el acceso corporativo (CORP) ese protocolo extensible authentication protegido de los soportes (PEAP) y EAP-TLS. No hay invitado SSID.

Éste es el proceso para el solo uno mismo-registro inalámbrico SSID BYOD:

1. Los socios del usuario a la corporación.
2. El usuario ingresa un nombre de usuario y contraseña del empleado en el supplicant para la autenticación PEAP.
3. El ISE autentica al usuario, y, sobre la base del método PEAP, proporciona una directiva de la autorización de valida con reorienta a la página del invitado del registro del dispositivo del empleado.
4. El usuario abre a un navegador y se reorienta a la página del invitado del registro del dispositivo del empleado.
5. La dirección MAC PRE-se puebla en la página del invitado del registro del dispositivo para el DeviceID. El usuario ingresa una descripción y valida el AUP.
6. El usuario selecciona **valida** y comienza a descargar y a instalar el SPW.
7. El supplicant para el dispositivo de ese usuario es aprovisionado junto con cualquier Certificados.
8. El CoA ocurre, y el dispositivo reasocia al CORP SSID y autentica con el EAP-TLS.

Configuración de la característica

Complete estos pasos para comenzar la configuración:

1. Para esta guía, asegúrese de que la versión del WLC sea 7.2.110.0 o más adelante.

2. Navegue a la **Seguridad** > al **RADIUS** > a la **autenticación**, y agregue al servidor de RADIUS al WLC.

3. Agregue el ISE 1.1.1 al WLC:

   Ingrese un secreto compartido.Fije el soporte para el RFC 3576 a **habilitado**.

4. Agregue el mismo servidor ISE que un servidor de contabilidad RADIUS.

5. Cree un PRE-auth ACL del WLC para utilizar en la directiva ISE más adelante. Navegue al > Security (Seguridad) > a las **listas de control de acceso** > a **FlexConnect ACL del WLC**, y cree un nuevo FlexConnect ACL nombrado **ACL-REDIRECT** (en este ejemplo).

6. En las reglas ACL, permita todo el tráfico a/desde el ISE, y permita el tráfico del cliente durante la disposición del supplicant.

   Para la primera regla (secuencia 1):

   Fije la fuente a **ningunos**.Fija IP ()/netmask **255.255.255.255 del** direccionamiento ISE.Fije la acción **para permitir**.

   Para segundo regla (secuencia 2), fija fuente IP ()/máscara 255.255.255.255 a **ningunos** y acción del direccionamiento ISE **a permitir**.

7. Cree un nuevo grupo de FlexConnect nombrado Flex1 (en este ejemplo):

   Navegue a la lengueta del **grupo** > de **WebPolicies de FlexConnect**.Bajo campo de WebPolicy ACL, el tecleo **agrega**, y **ACL-REDIRECT** selecto o el FlexConnect ACL creado

previamente.Confirme que puebla el campo de las **listas de control de acceso de WebPolicy**.

8. El tecleo **aplica** y **salva la configuración**.

Configuración de la red inalámbrica (WLAN)

Complete estos pasos para configurar la red inalámbrica (WLAN):

1. Cree una red inalámbrica (WLAN) abierta SSID por el ejemplo dual SSID:

   Ingrese un nombre WLAN: **DemoCWA** (en este ejemplo).Seleccione la opción **habilitada** para el estatus.

2. Navegue a la lengueta de la **ficha de seguridad >** de la **capa 2**, y fije estos atributos:

   Seguridad de la capa 2: **Ninguno**Filtración MAC: **Habilitado** (se marca el cuadro)Transición rápida: **Discapacitado** (el cuadro no se marca)

3. Vaya a la lengueta de los **servidores de AAA**, y fije estos atributos:

   Servidores de la autenticación y de la cuenta: **Habilitado**Server1: *Dirección IP <ISE >*

4. Navegue hacia abajo de la lengueta de los **servidores de AAA**. Bajo pedido de la prioridad de la autenticación para el usuario del red-auth, aseegurese que el **RADIUS** está utilizado para la autenticación y los otros no están utilizados.

5. Vaya a la **ficha Avanzadas**, y fije estos atributos:

   Permita la invalidación AAA: **Habilitado**Estado del NAC: **NAC del radio**
   Note: El Network Admission Control (NAC) RADIUS no se soporta cuando el FlexConnect AP está en el modo disconnected. Así, si el FlexConnect AP está en el modo autónomo y pierde la conexión al WLC, todos los clientes son disconnected, y el SSID se hace publicidad no más.
6. Navegue hacia abajo en la ficha de opciones avanzadas, y fije el Local Switching de FlexConnect a **habilitado**.

7. El tecleo **aplica** y **salva la configuración**.

8. Cree una red inalámbrica (WLAN) SSID del 802.1x nombrada **Demo1x** (en este ejemplo) para los escenarios solos y duales SSID.

9. Navegue a la lengueta de la **ficha de seguridad >** de la **capa 2**, y fije estos atributos:

   Seguridad de la capa 2: **WPA+WPA2**Transición rápida: **Discapacitado** (el cuadro no se marca)Administración de clave de autenticación: 802.IX: **Habilitar**

10. Vaya a la **ficha Avanzadas**, y fije estos atributos:

    Permita la invalidación AAA: **Habilitado**Estado del NAC: **NAC del radio**

11. Navegue hacia abajo en la **ficha de opciones avanzadas**, y fije el Local Switching de FlexConnect a **habilitado**.

12. El tecleo **aplica** y **salva la configuración**.

13. Confirme que ambos nuevos WLAN fueron creados.

Configuración de FlexConnect AP

Complete estos pasos para configurar el FlexConnect AP:

1. Navegue al **WLC >** a la **Tecnología inalámbrica**, y haga clic la blanco FlexConnect AP.

2. Haga clic la lengueta de **FlexConnect**.

3. Habilite el soporte a VLAN (se marca el cuadro), fije el VLAN nativo ID, y haga clic las **asignaciones del VLA N**.

4. Fije el VLAN ID a **21** (en este ejemplo) para el SSID para el Local Switching.

5. El tecleo **aplica** y **salva la configuración**.

Configuración ISE

Complete estos pasos para configurar el ISE:

1. Inicie sesión al servidor ISE: < *https://ise* >.

2. Navegue a la **administración** > a la **Administración de la identidad** > las **fuentes externas de la identidad**.

3. Haga clic el **Active Directory**.

4. En la lengueta de la conexión:

   Agregue el Domain Name de **corp.rf-demo.com** (en este ejemplo), y cambie el valor por defecto del nombre del almacén de la identidad a **AD1**.Haga clic la **configuración de la salvaguardia**.El tecleo **se une a**, y proporciona el nombre de usuario y contraseña de la cuenta del administrador AD requerido para unirse a.El estatus debe ser verde. Permiso **conectado con:** (se marca el cuadro).

5. Realice una prueba de la conexión básica al AD con un usuario del dominio actual.

6. Si la conexión al AD es acertada, un diálogo confirma que la contraseña está correcta.

7. Navegue a la **administración** > a la **Administración de la identidad** > las **fuentes externas de la identidad**:

   Haga clic el **perfil de la autenticación certificada**.El tecleo **agrega** para un nuevo perfil de la autenticación certificada (CASQUILLO).

8. Ingrese un nombre de **CertAuth** (en este ejemplo) para el CASQUILLO; para el atributo principal del nombre de usuario X509, seleccione el **Common Name**; entonces, el tecleo **somete**.

9. Confirme que el nuevo CASQUILLO está agregado.

10. Navegue a las **secuencias de la fuente de la administración >** de la **Administración de la identidad >** de la **identidad**, y el haga click en Add

11. Dé a secuencia un nombre de **TestSequence** (en este ejemplo).

12. Navegue hacia abajo **para certificar la autenticación basada**:

    Habilite el **perfil selecto de la autenticación certificada** (se marca el cuadro).Seleccione **CertAuth** (u otro perfil del CASQUILLO creado anterior).

13. Navegue hacia abajo a la **lista de la búsqueda de la autenticación**:

    Muévase AD1 desde disponible a seleccionado.Haga clic el botón ascendente para moverse AD1 a la prioridad máxima.

14. El tecleo **somete** para salvar.

15. Confirme que la nueva secuencia de la fuente de la identidad está agregada.

16. Utilice el AD para autenticar los mis dispositivos porta. Navegue a **ISE > secuencia de la fuente de la administración >** de la **Administración de la identidad >** de la **identidad**, y edite **MyDevices_Portal_Sequence**.

17. Agregue **AD1 a la** lista seleccionada, y haga clic el botón ascendente para moverse AD1 a la prioridad máxima.

18. Click **Save**.

19. Confirme que la secuencia del almacén de la identidad para MyDevices_Portal_Sequence contiene **AD1**.

20. Relance los pasos 16-19 para agregar AD1 para Guest_Portal_Sequence, y haga clic la **salvaguardia**.

21. Confirme que Guest_Portal_Sequence contiene **AD1**.

22. Para agregar el WLC al dispositivo de acceso a la red (WLC), navegue a la **administración** > a los **recursos de red** > a los **dispositivos de red**, y el haga click en Add

23. Agregue el nombre del WLC, dirección IP, máscara de subred, y así sucesivamente.

24. Navegue hacia abajo a las configuraciones de la autenticación, y ingrese el secreto compartido. Esto debe hacer juego el secreto compartido del WLC RADIUS.

25. Haga clic en Submit (Enviar).

26. Navegue a **ISE > directiva** > los **elementos** > los **resultados de la directiva**.

27. Amplíe los **resultados** y la **autorización**, haga clic los **perfiles de la autorización**, y el tecleo **agrega** para un nuevo perfil.

28. Dé a este perfil estos valores:

    Nombre: **CWA**

Autenticación Web del permiso (se marca el cuadro):

Autenticación Web: **Centralizado**ACL: **ACL-REDIRECT** (esto debe hacer juego el nombre del PRE-auth ACL del WLC.)Redirigir: **Predeterminado**

29. Haga clic **someten**, y confirman que se ha agregado el perfil de la autorización CWA.

30. El tecleo **agrega** para crear un nuevo perfil de la autorización.

31. Dé a este perfil estos valores:

    Nombre: **Disposición**

    Autenticación Web del permiso (se marca el cuadro):

    Valor de la autenticación Web: **Disposición del supplicant**

    ACL: **ACL-REDIRECT** (esto debe hacer juego el nombre del PRE-auth ACL del WLC.)

32. Haga clic **someten**, y confirman que el perfil de la autorización de la disposición fue agregado.

33. Navegue hacia abajo en los resultados, amplíe el **aprovisionamiento del cliente**, y haga clic los **recursos**.

34. Seleccione el **perfil nativo del supplicant**.

35. Dé a perfil un nombre de **WirelessSP** (en este ejemplo).

36. Ingrese estos valores:

    Tipo de conexión: **Tecnología inalámbrica**SSID: **Demo1x** (este valor es de la configuración de la red inalámbrica (WLAN) del 802.1x del WLC)Protocolo permitido: **TLS**Tamaño de clave: **1024**

37. Haga clic en Submit (Enviar).

38. Click **Save**.

39. Confirme que se ha agregado el nuevo perfil.

40. Navegue a la **directiva >** al **aprovisionamiento del cliente**.

41. Ingrese estos valores para la regla del aprovisionamiento de dispositivos IOS:

    'Nombre de la regla **IOS**Grupos de la identidad: **Ningunos**

    Sistemas operativos: **IOS todo del mac**

    Resultados: **WirelessSP** (éste es el perfil nativo del supplicant creado anterior)

    Navegue a los **resultados >** al **perfil del Asisitente** (lista desplegable) **> WirelessSP**.

42. Confirme que el perfil del aprovisionamiento IOS fue agregado.

43. A la derecha de la primera regla, localice la lista desplegable de las acciones, y seleccione el **duplicado abajo** (o arriba).

44. Cambie el nombre de la nueva regla a **Android**.

45. Cambie los sistemas operativos a **Android**.

46. Deje otros valores sin cambios.

47. Haga clic la **salvaguardia** (pantalla de la izquierda inferior).

48. Navegue a **ISE > directiva > autenticación**.

49. Modifique la condición para incluir Wireless_MAB, y amplíe **Wired_MAB**.

50. Haga clic la lista desplegable del **nombre de condición**.

51. Seleccione los **diccionarios > condición compuesta**.

52. Seleccione **Wireless_MAB**.

53. A la derecha de la regla, seleccione la flecha para ampliarse.

54. Seleccione estos valores de la lista desplegable:

    Fuente de la identidad: **TestSequence** (éste es el valor creado anterior)Si la autenticación falló: **Rechazo**Si usuario no encontrado: **Continúe**Si el proceso falló: **Descenso**

55. Vaya a la regla del **dot1x**, y cambie estos valores:

Condición: **Wireless_802.1X**

Fuente de la identidad: **TestSequence**

56. Click **Save**.

57. Navegue a **ISE > directiva > autorización**.

58. Las reglas predeterminadas (tales como valor por defecto negro de la lista, perfilado, y valor por defecto) se configuran ya de la instalación; los primeros dos pueden ser ignorados; la regla predeterminada será editada más adelante.

59. A la derecha de la segunda regla (Teléfonos IP perfilados de Cisco), haga clic la flecha hacia abajo al lado de editan, y seleccionan la **nueva regla del separador de millares abajo**.

    Se agrega una nueva regla estándar #.

60. Cambie el nombre de la regla de la regla estándar # a **OpenCWA**. Esta regla inicia el proceso de inscripción en la red inalámbrica (WLAN) abierta (SSID dual) para los usuarios que vienen a la red del invitado para tener aprovisionado de los dispositivos.

61. Haga clic el signo más (**+**) para las condiciones, y haga clic la **condición existente selecta de la biblioteca**.

62. Seleccione las **condiciones compuestas > Wireless_MAB**.

63. En el perfil de AuthZ, haga clic el signo más (**+**), y seleccione el **estándar**.

64. Seleccione el **CWA** estándar (éste es el perfil de la autorización creado anterior).

65. Confirme que la regla está agregada con las condiciones y la autorización correctas.

66. Haga clic **hecho** (a la derecha de la regla).

67. A la derecha de la misma regla, haga clic la flecha hacia abajo al lado de editan, y seleccionan la **nueva regla del separador de millares abajo**.

68. Cambie el nombre de la regla de la regla estándar # a **PEAPrule** (en este ejemplo). Esta regla está para el PEAP (también usado para el solo escenario SSID) para marcar esa autenticación del 802.1x sin Transport Layer Security (TLS) y esa disposición del supplicant de la red se inicia con el perfil de la autorización de la disposición creado previamente.

69. Cambie la condición a **Wireless_802.1X**.

70. Haga clic el icono del engranaje a la derecha de la condición, y selecto **agregue el atributo/el valor**. Éste es “y” condición, no “o” condición.

71. Localice y seleccione el **acceso a la red**.

72. Seleccione **AuthenticationMethod**, y ingrese estos valores:

    AuthenticationMethod: **Iguales**

    Seleccione el **MSCHAPV2**.

Éste es un ejemplo de la regla; esté seguro de confirmar que la condición es Y.

73. En el perfil de AuthZ, **estándar > disposición** selectos (éste es el perfil de la autorización creado anterior).

74. Haga clic en Done (Listo).

75. A la derecha del PEAPrule, haga clic la flecha hacia abajo al lado de editan, y seleccionan la **nueva regla del separador de millares abajo**.

76. Cambie el nombre de la regla de la regla estándar # a **AllowRule** (en este ejemplo). Esta regla será utilizada para permitir el acceso a los dispositivos registrados con los Certificados instalados.

77. Bajo condiciones, seleccione las **condiciones compuestas**.

78. Seleccione **Wireless_802.1X**.

79. Agregue Y atribúyalo.

80. Haga clic el icono del engranaje a la derecha de la condición, y selecto **agregue el atributo/el valor**.

81. Localice y seleccione el **radio**.

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

83. Seleccione los **iguales**.

84. Vaya al **CERTIFICADO**, y haga clic la flecha correcta.

85. Seleccione el **nombre alternativo sujeto**.

86. Para el perfil de AuthZ, seleccione el **estándar**.

87. Seleccione el **acceso del permiso**.

88. Haga clic en Done (Listo).

Éste es un ejemplo de la regla:

89. Localice la regla predeterminada para cambiar PermitAccess a DenyAccess.

90. El tecleo **edita** para editar la regla predeterminada.

91. Vaya al perfil existente de AuthZ de PermitAccess.

92. Seleccione el **estándar**.

93. Seleccione **DenyAccess**.

94. Confirme que la regla predeterminada tiene DenyAccess si no se encuentra ningunas coincidencias.

95. Haga clic en Done (Listo).

    Éste es un ejemplo de las reglas principales requeridas para esta prueba; son aplicables para un solo SSID o el escenario dual SSID.

96. Click **Save**.

97. Navegue a **ISE** > la **administración** > **sistema** > los **Certificados** para configurar el servidor ISE con un perfil SCEP.

98. En las operaciones del certificado, haga clic los **perfiles SCEP CA**.

99. Haga clic en Add (Agregar).

100. Ingrese estos valores para este perfil:

     Nombre: **mySCEP** (en este ejemplo)URL: *<ca-server>* **/CertSrv/mscep/ de https://** (marque su Configuración del servidor de CA para la dirección correcta.)

101. Haga clic la **Conectividad de la prueba** para probar la Conectividad de la conexión SCEP.

102. Esta respuesta muestra que la conectividad de servidor es acertada.

103. Haga clic en Submit (Enviar).

104. El servidor responde que el perfil de CA fue creado con éxito.

105. Confirme que el perfil SCEP CA está agregado.

Experiencia del usuario - IOS de disposición

SSID dual

Esta sección cubre el SSID dual y describe cómo conectar con el invitado para ser aprovisionado y cómo conectar con el 802.1x una red inalámbrica (WLAN).

Complete estos pasos para provision el IOS en el escenario dual SSID:

1. En el dispositivo IOS, vaya a las **redes del Wi-Fi**, y a **DemoCWA** selecto (red inalámbrica (WLAN) abierta configurada en el WLC).

2. Abra al navegador del safari en el dispositivo IOS, y visite un URL accesible (por ejemplo, web server interno y externo). El ISE le reorienta al portal. Haga clic en **Continue** (Continuar).

3. Le reorientan al portal del invitado para el login.

4. Login con una cuenta de usuario y la contraseña AD. Instale el perfil de CA cuando está indicado.

5. El tecleo **instala el** certificado confiable del servidor de CA.

6. Haga clic **hecho** una vez que el perfil está instalado totalmente.

7. Vuelva al navegador, y haga clic el **registro**. Anote el ID del dispositivo que contiene la dirección MAC del dispositivo.

8. El tecleo **instala** para instalar el perfil verificado.

9. El tecleo **ahora instala**.

10. Después de que se complete el proceso, el perfil de WirelessSP confirma que el perfil está instalado. Haga clic en Done (Listo).

11. Vaya a las **redes del Wi-Fi**, y cambie la red a **Demo1x**. Su dispositivo ahora está conectado y utiliza TLS.

12. En el ISE, navegue a las **operaciones >** a las **autenticaciones**. Los eventos muestran el proceso en el cual el dispositivo está conectado con la red del invitado abierta, entra con el proceso de inscripción con el supplicant provisioning, y no se prohibe el acceso del permiso después del registro.

13. Navegue a **ISE >** la **administración > Administración de la identidad >** Groups **>** los **grupos > RegisteredDevices de la identidad del punto final**. La dirección MAC se ha agregado a la base de datos.

Solo SSID

Esta sección cubre el solo SSID y describe cómo conectar directamente con una red inalámbrica (WLAN) del 802.1x, proporcionar el nombre de usuario AD/la contraseña para la autenticación PEAP, provision con una cuenta de invitado, y volver a conectar con TLS.

Complete estos pasos para provision el IOS en el solo escenario SSID:

1. Si usted está utilizando el mismo dispositivo IOS, quite el punto final de los dispositivos registrados.

2. En el dispositivo IOS, navegue a las **configuraciones** > a los **generales** > a los **perfiles**. Quite los perfiles instalados en este ejemplo.

3. El tecleo **quita** para quitar los perfiles anteriores.

4. Conecte directamente con el 802.1x con el dispositivo (borrado) existente o con un nuevo dispositivo IOS.

5. Conecte con el **dot1x**, ingrese un nombre de usuario y contraseña, y el tecleo **se une a**.

6. Relance los pasos 90 y encendido de la sección de configuración ISE hasta que los perfiles apropiados estén instalados totalmente.

7. Navegue a **ISE** > las **operaciones** > las **autenticaciones** para monitorear el proceso. Este ejemplo muestra al cliente que está conectado directamente con la red inalámbrica (WLAN) del 802.1x pues es aprovisionado, desconecta, y vuelve a conectar a la misma red inalámbrica (WLAN) con el uso de TLS.

8. Navegue al **WLC** > al **monitor** > al **[Client MAC]**. En el detalle del cliente, observe que el cliente está en el estado de FUNCIONAMIENTO, su transferencia de los datos se fija al local, y la autenticación es central. Esto es verdad para los clientes que conectan con FlexConnect AP.

Experiencia del usuario - Android de disposición

SSID dual

Esta sección cubre el SSID dual y describe cómo conectar con el invitado para ser aprovisionado y cómo conectar con el 802.1x una red inalámbrica (WLAN).

El proceso de la conexión para el dispositivo de Android es muy similar a ése para un dispositivo IOS (SSID solo o dual). Sin embargo, una diferencia importante es que el dispositivo de Android requiere el acceso a Internet para acceder el mercado de Google (ahora Google Play) y descargar el agente del supplicant.

Complete estos pasos para provision un dispositivo de Android (tal como el Samsung Galaxy en

este ejemplo) en el escenario dual SSID:

1. En el dispositivo de Android, utilice el Wi-Fi para conectar con **DemoCWA**, y abrir la red inalámbrica (WLAN) del invitado.

2. Valide cualquier certificado para conectar con el ISE.

3. Ingrese un nombre de usuario y contraseña en el portal del invitado para iniciar sesión.

4. Haga clic el **registro**. El dispositivo intenta alcanzar Internet para acceder el mercado de Google. Agregue cualquier regla adicional al PRE-auth ACL (tal como ACL-REDIRECT) en el regulador para permitir el acceso a Internet.

5. Google enumera la red de Cisco puesta como App de Android. El tecleo **INSTALA**.

6. Ingrese a Google, y el tecleo **INSTALA**.

7. Click OK.

8. En el dispositivo de Android, encuentre el app instalado de **Cisco SPW**, y ábralo.

9. Aseegurese que le todavía abren una sesión al portal del invitado de su dispositivo de Android.

10. Haga clic el **comienzo** para comenzar al ayudante de la configuración del Wi-Fi.

11. Cisco SPW comienza a instalar los Certificados.

12. Cuando se le pregunte, fije una contraseña para el almacenamiento de credenciales.

13. Cisco SPW vuelve con un nombre del certificado, que contiene la clave y el Certificado de usuario del usuario. Haga clic en Aceptar para confirmar.

14. Cisco SPW continúa y indica para otro nombre del certificado, que contiene el certificado de CA. Ingrese el **iseca del** nombre (en este ejemplo), después haga clic la **AUTORIZACIÓN** para continuar.

15. El dispositivo de Android ahora está conectado.

Mis dispositivos porta

Mi portal de los dispositivos permite que los usuarios pongan previamente los dispositivos registrados en el evento que se pierde o que se roba un dispositivo. También permite que los usuarios alisten de nuevo si es necesario.

Complete estos pasos para poner un dispositivo:

1. Para iniciar sesión a mi portal de los dispositivos, abra a un navegador, conectan con https://ise-server:8443/mydevices (observe el número del puerto 8443), y inician sesión con una cuenta AD.

2. **¿**Localice el dispositivo bajo ID del dispositivo, y haga clic **perdido?** para iniciar poner de un dispositivo.

3. Cuando el ISE indica una advertencia, haga clic **sí** para proceder.

4. El ISE confirma que el dispositivo está marcado como **perdido**.

5. Cualquier tentativa de conectar con la red con el dispositivo registrado ahora se bloquea previamente, incluso si hay un certificado válido instalado. Éste es un ejemplo de un dispositivo puesto que falle la autenticación:

6. Un administrador puede navegar a **ISE >** la **administración > Administración de la identidad >** Groups, los **grupos de la identidad del punto final del** tecleo **> lista negra**, y ve que el dispositivo está puesto.

Complete estos pasos para reinstalar un dispositivo puesto:

1. Del mi portal de los dispositivos, el tecleo **reinstala** para ese dispositivo.

2. Cuando el ISE indica una advertencia, haga clic **sí** para proceder.

3. El ISE confirma que el dispositivo se ha reinstalado con éxito. Conecte el dispositivo reinstalado con la red para probar que el dispositivo ahora será permitido.

Referencia - Certificados

El ISE no sólo requiere un certificado raíz válido de CA, pero también necesita un certificado válido firmado por CA.

Complete estos pasos para agregar, atar, e importar el nuevo certificado de CA de confianza:

1. Navegue a **ISE >** la **administración > sistema >** los **Certificados**, los **Certificados locales del** tecleo, y haga click en Add

2. Selecto **genere el pedido de firma de certificado** (CSR).

3. Ingrese el tema **CN=<ISE-SERVER** *hostname.FQDN> del* certificado. Para los otros campos, usted puede utilizar el valor por defecto o los valores requeridos por su configuración de CA. Haga clic en Submit (Enviar).

4. El ISE verifica que el CSR fuera generado.

5. Para acceder el CSR, haga clic las operaciones de los **pedidos de firma de certificado**.

6. Seleccione el CSR creado recientemente, después haga clic la **exportación**.

7. El ISE exporta el CSR a un archivo del .pem. **El archivo de la salvaguardia del** tecleo, entonces hace clic la **AUTORIZACIÓN** para salvar el archivo a la máquina local.

8. Localice y abra el archivo de certificado ISE con un editor de textos.

9. Copie el contenido entero del certificado.

10. Conecte con CA el servidor, y el login con una cuenta del administrador. El servidor es Microsoft 2008 CA en https://10.10.10.10/certsrv (en este ejemplo).

11. **Petición del** tecleo un **certificado**.

12. **Pedido de certificado avanzado del** tecleo.

13. Haga clic la segunda opción para **presentar un pedido de certificado usando un base-64-encoded CMC o…**.

14. Pegue el contenido del archivo de certificado ISE (.pem) en el campo del Saved Request, asegúrese que el Certificate Template plantilla de certificado es **servidor Web**, y el tecleo **somete**.

15. Haga clic el **certificado de la descarga**.

16. Salve el archivo de certnew.cer; será utilizado más adelante para atar con el ISE.

17. **De los Certificados** ISE, navegue a los **Certificados locales**, y el tecleo **agrega > certificado de CA del lazo**.

18. Hojee al certificado que fue guardado a la máquina local en el paso anterior, habilitan los protocolos **EAP** y de la **interfaz de administración** (se marcan los cuadros), y el tecleo **somete**. El ISE puede tomar varios minutos o más para recomenzar los servicios.

19. Vuelva a la página del aterrizaje de CA (https://CA/certsrv/), y hace clic la **descarga un certificado de CA, una Cadena de certificados, o un CRL**.

20. Haga clic el **certificado de CA de la descarga**.

21. **Salve el** archivo a la máquina local.

22. Con el servidor ISE en línea, vaya a los **Certificados**, y haga clic los **Certificados del Certificate Authority**.

23. Haga clic la **importación**.

24. Hojee para el certificado de CA, habilite la **confianza para la autenticación de cliente** (se marca el cuadro), y el tecleo **somete**.

25. Confirme que el nuevo certificado de CA de confianza está agregado.

Información Relacionada

- Guía de instalación del hardware del Cisco Identity Services Engine, versión 1.0.4
- Controladores LAN inalámbricos Cisco de la serie 2000
- Controladores LAN inalámbricos Cisco de la serie 4400
- Cisco Aironet de la serie 3500
- Guía de despliegue del regulador de bifurcación de la Tecnología inalámbrica de la flexión 7500
- Bring Your Own Device - Autenticación del dispositivo unificada y experiencia constante del acceso
- Tecnología inalámbrica BYOD con el Identity Services Engine
- Soporte Técnico y Documentación - Cisco Systems