PEAP bajo redes inalámbricas unificadas con ACS 4.0 y Windows 2003

Contenido

Introducción

Este documento describe cómo configurar el acceso inalámbrico seguro mediante controladores LAN inalámbricos, el software Microsoft Windows 2003 y Cisco Secure Access Control Server (ACS) 4.0 a través de Protected Extensible Authentication Protocol (PEAP) con Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) versión 2.

Nota: Para la información sobre el despliegue de asegure la Tecnología inalámbrica, refiera al

modelo del sitio web del Wi-Fi de Microsoft y de la Tecnología inalámbrica del Cisco SAFE.

prerrequisitos

Requisitos

Hay una suposición que el instalador tiene la instalación de Windows 2003 del conocimietno básico y instalación del controlador de Cisco mientras que este documento cubre solamente las configuraciones específicas para facilitar las pruebas.

Para la instalación inicial y la información de la configuración para los reguladores de las Cisco 4400 Series, refiera a la guía de inicio rápido: Cisco Wireless LAN Controllers de la serie 4400. Para la instalación inicial y la información de la configuración para los reguladores de las Cisco 2000 Series, refiera a la guía de inicio rápido: Cisco Wireless LAN Controllers de la serie 2000.

Microsoft Windows 2003 guías de instalación y configuración se puede encontrar en instalar el r2 2003 del Servidor Windows .

Antes de que usted comience, instale el Microsoft Windows server 2003 con el sistema operativo SP1 en cada uno de los servidores en el laboratorio de prueba y ponga al día todo el Service Packs. Instale los reguladores y los Puntos de acceso ligeros (revestimientos) y asegúrese de que las actualizaciones de último software están configuradas.

Importante: A la hora de esta escritura, el SP1 es la última actualización del Microsoft Windows server 2003, y el SP2 con las correcciones de la actualización es el último software para el profesional del Microsoft Windows XP.

Utilizan al Servidor Windows 2003 con el SP1, Enterprise Edition, para poder configurar el autoenrollment de los Certificados del usuario y del puesto de trabajo para la autenticación PEAP. El autoenrollment del certificado y autorenewal hacen más fácil desplegar los Certificados y mejorar la Seguridad automáticamente la expiración y renovando los Certificados.

Componentes Utilizados

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

- Regulador de las Cisco o Series que ejecuta 3.2.116.21
- Cisco protocolo de 1131 Lightweight Access Point (LWAPP) AP
- Empresa de Windows 2003 con el Internet Information Server (IIS), el Certificate Authority (CA), el DHCP, y el Domain Name System (DNS) instalado
- Estándar de Windows 2003 con el Access Control Server (ACS) 4.0
- Profesional de Windows XP con el SP (y Service Packs actualizado) y Wireless Network Interface Card (NIC) (con CCX el soporte del v3) o supplicant del otro vendedor.
- Cisco 3560 Switch

Diagrama de la red

En este documento, se utiliza esta configuración de red:

Cisco asegura la Topología de laboratorio inalámbrica

El propósito primario de este documento es proporcionarle el procedimiento paso a paso para implementar el PEAP bajo redes inalámbricas unificadas con ACS 4.0 y el Servidor de Enterprise de Windows 2003. El énfasis principal está en el Autoregistro del cliente de modo que el cliente auto-aliste y tome el certificado del servidor.

Nota: Para agregar el Wi-Fi protegió el acceso (WPA)/WPA2 con la norma de encripción del Temporal Key Integrity Protocol (TKIP) /Advanced (AES) al profesional de Windows XP con el SP, refieren a la actualización del elemento de información de los servicios del aprovisionamiento WPA2/Wireless (WPS IE) para Windows XP con el Service Pack 2.

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.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Empresa 2003 de Windows puesta con el IIS, Certificate Authority, DNS, DHCP (DC_CA)

DC_CA (wirelessdemoca)

DC_CA es un ordenador que funciona con al Servidor Windows 2003 con el SP1, Enterprise Edition, y realiza estos papeles:

- Un controlador de dominio para el **dominio wirelessdemo.local** que ejecuta el IIS
- Un servidor DNS para el **dominio DNS wirelessdemo.local**
- Un servidor DHCP
- Empresa raíz CA para el **dominio wirelessdemo.local**

Complete estos pasos para configurar DC_CA para estos servicios:

1. Realice una instalación básica y una configuración.
2. Configure el ordenador como controlador de dominio.
3. Aumente el nivel funcional del dominio.
4. Instale y configure el DHCP.
5. Instale los servicios de certificados.
6. Verifique los permisos del administrador para los Certificados.
7. Agregue los ordenadores al dominio.
8. Permita el acceso de red inalámbrica a los ordenadores.
9. Agregue a los usuarios al dominio.
10. Permita el acceso de red inalámbrica a los usuarios.
11. Agregue a los grupos al dominio.
12. Agregue a los usuarios al grupo de WirelessUsers.
13. Agregue las computadoras cliente al grupo de WirelessUsers.

Paso 1: Realice la instalación básica y la configuración

Complete estos pasos:

1. Instale al Servidor Windows 2003 con el SP1, Enterprise Edition, como servidor independiente.
2. Configure el protocolo TCP/IP con la dirección IP de **172.16.100.26** y la máscara de subred de **255.255.255.0**.

Paso 2: Configure la Computadora como controlador de dominio

Complete estos pasos:

1. Para comenzar al Asisitente de instalación de Active Directory, elija el **Start (Inicio) > Run (Ejecutar)**, teclee **dcpromo.exe, y** haga clic la AUTORIZACIÓN**.**
2. En la recepción a la página del Asisitente de instalación de Active Directory, haga clic **después**.
3. En la página de la compatibilidad del sistema operativo, haga clic **después**.
4. En la página de tipo del controlador de dominio, el **controlador de dominio** selecto **para un nuevo dominio** y el tecleo **después**.
5. En la nueva página del dominio del crear, el **dominio** selecto **en un nuevo bosque** y el tecleo **después**.
6. En la página del instalar o de la configuración DNS, seleccione **ningún, apenas instale y configure el DNS en este ordenador** y haga clic **después**.
7. En la nuevos página del Domain Name, tipo **wirelessdemo.local y** tecleo después**.**
8. En la página del Domain Name del NetBios, ingrese el nombre de NETBIOS del dominio como **wirelessdemo** y haga clic **después**.
9. En las carpetas de la base de datos y del registro que las ubicaciones paginan, que valide los directorios predeterminados de las carpetas de la base de datos y del registro y que haga clic **después**.
10. En System Volume (Volumen del sistema) la página compartida, verifique que la ubicación de la carpeta predeterminada está correcta y haga clic **después**.
11. En los permisos pagine, verifique que los **permisos compatibles solamente con los sistemas operativos del Windows 2000 o del Servidor Windows 2003** están seleccionados y tecleo **después**.
12. En la página de la contraseña de administración del modo del Restore de los servicios de directorio, deje el espacio en blanco de casillas de verificación de contraseña y haga clic **después**.
13. Revise la información sobre la página de resumen y haga clic **después**.
14. Cuando le hacen con la instalación de Active Directory, clic en Finalizar.
15. Cuando se le pregunte para recomenzar el ordenador, el tecleo **ahora recomienza**.

Paso 3: Aumente el nivel funcional del dominio

Complete estos pasos:

1. Abra los **dominios de Active Directory y las confianzas broche-**en de la carpeta de las **herramientas administrativas (Start (Inicio) > Programs (Programas) > Administrative Tools**

(Herramientas administrativas) > dominios de Active Directory y confianzas), y después haga clic con el botón derecho del ratón la computadora dominio **DC_CA.wirelessdemo.local.**
2. Haga clic el **nivel funcional del dominio del aumento**, y después seleccione al **Servidor Windows 2003** en la página del nivel funcional del dominio del aumento.
3. Haga clic el **aumento**, haga clic la **AUTORIZACIÓN**, y después haga clic la **AUTORIZACIÓN** otra vez.

Paso 4: Instale y configure el DHCP

Complete estos pasos:

1. Instale el **Protocolo de configuración dinámica de host (DHCP)** como componente de **servicio de red** usando **agregan o quitan los programas** en el panel de control.
2. Abra el **DHCP broche-**en de la carpeta de las **herramientas administrativas (Start (Inicio) > Programs (Programas) > Administrative Tools (Herramientas administrativas) > DHCP)**, y después resalte al servidor DHCP, **DC_CA.wirelessdemo.local.**
3. Haga clic la **acción**, y después haga clic **autorizan** para autorizar el servicio del DHCP.
4. En el árbol de la consola, haga clic con el botón derecho del ratón **DC_CA.wirelessdemo.local, y después haga clic el nuevo** alcance.
5. En la página de Bienvenida del nuevo asistente de alcance, haga clic **después**.
6. En la página del nombre del alcance, teclee **CorpNet** en el campo de nombre.
7. Haga clic **después** y complete estos parámetros:Comience a la dirección IP 172.16.100.1Termine a la dirección IP 172.16.100.254Longitud **— 24**Máscara de subred **— 255.255.255.0**
8. Haga clic **después** y ingrese **172.16.100.1** para el IP Address del comienzo y **172.16.100.100** para que el IP Address del extremo sea excluido. Luego haga clic en Next (Siguiente). Esto reserva los IP Addresses en el rango de 172.16.100.1 a 172.16.100.100. Éstos reservan los IP Addresses no son asignados por el servidor DHCP.
9. En la página del tiempo de validez, haga clic **después**.
10. En la configuración las opciones DHCP paginan, eligen **sí, quiero ahora configurar estas opciones** y hacer clic **después**.
11. En la página del router (default gateway) agregue a la dirección del router predeterminada de **172.16.100.1** y haga clic **después**.
12. En el Domain Name y los servidores DNS pagine, teclee **wirelessdemo.local en el** campo del dominio del padre, teclee 172.16.100.26 **en el** campo de la dirección IP, y después haga clic el tecleo de Addand después**.**
13. En los TRIUNFOS que los servidores paginan, que haga clic **después**.
14. En la página del alcance del activar, elija **sí, quiero ahora activar este alcance** y hacer clic **después**.
15. Cuando usted acaba con la nueva página del asistente de alcance, clic en Finalizar.

Paso 5: Instale los servicios de certificados

Complete estos pasos:

Nota: El IIS debe ser instalado antes de que usted instale los servicios de certificados y el usuario debe ser parte de la empresa Admin OU.

1. En el panel de control, abierto **agregue o quite los programas**, y después haga clic **agregan/quitan a los componentes de Windows**.
2. En la página del Asistente de componentes de Windows, elija los **servicios de certificados**, y después haga clic **después**.
3. En la página de tipo de CA, elija la **empresa raíz CA** y haga clic **después**.
4. En CA que identifica la página de información, teclee el **wirelessdemoca** en el Common Name para este cuadro de CA. Usted puede también ingresar los otros detalles opcionales. Entonces haga clic **después** y valide los valores por defecto en la página de las configuraciones de la base de datos del certificado.
5. Haga clic en Next (Siguiente). Al completar la instalación, clic en Finalizar.
6. Haga Click en OK después de que usted leyera el mensaje de advertencia sobre instalar el IIS.

Paso 6: Verifique los permisos del administrador para los Certificados

Complete estos pasos:

1. Elija el **Start (Inicio) > Administrative Tools (Herramientas administrativas) > las autoridades de certificación**.
2. Haga clic con el botón derecho del ratón el **wirelessdemoca CA** y después haga clic las **propiedades**.
3. En la ficha de seguridad, haga clic a los **administradores** en la lista del **grupo o de Nombres de usuario**.
4. En los permisos o los administradores enumere, verifique que estas opciones están fijadas **para permitir**:Publique y maneje los CertificadosManeje CAPida los CertificadosSi ninguno de estos se fijan para negar o no se seleccionan, fije el permiso **para permitir**.
5. Haga Click en OK para cerrar el cuadro de diálogo Propiedades de CA del wirelessdemoca, y después para cerrar las autoridades de certificación.

Paso 7: Agregue las Computadoras al dominio

Complete estos pasos:

Nota: Si el ordenador se agrega ya al dominio, proceda a agregar a los usuarios al dominio.

1. Abra a los **usuarios de directorio activo y computadora broche-**en.
2. En el árbol de la consola, amplíe **wirelessdemo.local.**
3. Haga clic con el botón derecho del ratón a los **usuarios**, haga clic **nuevo**, y después haga clic la **Computadora**.
4. En el nuevo objeto – El cuadro de diálogo de la Computadora, teclea el nombre del ordenador en el campo de nombre de la computadora y hace clic **después**. Este ejemplo utiliza al **cliente del** nombre de computadora.
5. En el cuadro de diálogo manejado, haga clic **después**.
6. En el nuevo objeto – Cuadro de diálogo de la Computadora, clic en Finalizar.
7. Relance los pasos 3 a 6 para crear las cuentas de la computadora adicional.

Paso 8: Permita el acceso de red inalámbrica a las Computadoras

Complete estos pasos:

1. En el árbol de la consola de los usuarios de directorio activo y computadora, haga clic la carpeta de las **Computadoras** y haga clic con el botón derecho del ratón en el ordenador para el cual usted quiere asignar el acceso de red inalámbrica. Este ejemplo muestra el procedimiento con la computadora cliente cuál usted agregó en las **propiedades del** tecleo del paso 7., y después va al **dial-in tab**.
2. Elija **permiten el acceso** y hacen clic la **AUTORIZACIÓN**.

Paso 9: Agregue a los usuarios al dominio

Complete estos pasos:

1. En el árbol de la consola de los usuarios de directorio activo y computadora, haga clic con el botón derecho del ratón a los **usuarios**, haga clic **nuevo**, y después haga clic al **usuario**.
2. En el nuevo objeto – El cuadro de diálogo del usuario, teclea el nombre del usuario de red inalámbrica. Este ejemplo utiliza el nombre **WirelessUser** en el campo de primer nombre, y **WirelessUser** en el campo de nombre de inicio de usuario. Haga clic en Next (Siguiente).
3. En el nuevo objeto – El cuadro de diálogo del usuario, teclea una contraseña de su opción en la contraseña y confirma los campos de contraseña. Borre al **usuario debe cambiar la contraseña en la** casilla de verificación **siguiente del inicio**, y hace clic **después**.
4. En el nuevo objeto – Cuadro de diálogo del usuario, clic en Finalizar.
5. Relance los pasos 2 a 4 para crear las cuentas de usuario adicionales.

Paso 10: Permita el acceso de red inalámbrica a los usuarios

Complete estos pasos:

1. En el árbol de la consola de los **usuarios de directorio activo y computadora**, haga clic la **carpeta del usuario**, haga clic con el botón derecho del ratón **WirelessUser**, haga clic las **propiedades**, y después vaya al dial-in tab.
2. Elija **permiten el acceso** y hacen clic la **AUTORIZACIÓN**.

Paso 11: Agregue a los grupos al dominio

Complete estos pasos:

1. En el árbol de la consola de los **usuarios de directorio activo y computadora**, haga clic con el botón derecho del ratón a los **usuarios**, haga clic **nuevo**, y después haga clic al **grupo**.
2. En el nuevo objeto – Agrupe el cuadro de diálogo, teclee el nombre del grupo en el campo de nombre del grupo y haga clic la **AUTORIZACIÓN**. Este documento utiliza el nombre del grupo **WirelessUsers**.

Paso 12: Agregue a los usuarios al grupo de WirelessUsers

Complete estos pasos:

1. En el panel de detalles de los usuarios de directorio activo y computadora, haga doble clic

en el grupo **WirelessUsers**.
2. Vaya a la lengueta y al haga click en Add de los miembros
3. En los usuarios selectos, los contactos, cuadro de diálogo de las Computadoras, o de los grupos, teclean el nombre de los usuarios que usted quiere agregar al grupo. Este ejemplo muestra cómo agregar el **wirelessuser del** usuario al grupo. Haga clic en OK.
4. En el múltiplo los nombres encontraron el cuadro de diálogo, **AUTORIZACIÓN del** tecleo. La cuenta de usuario de WirelessUser se agrega al grupo de WirelessUsers.
5. Haga Click en OK para salvar los cambios al grupo de WirelessUsers.
6. Relance este procedimiento para agregar a más usuarios al grupo.

Paso 13: Agregue las computadoras cliente al grupo de WirelessUsers

Complete estos pasos:

1. Relance los pasos 1 y 2 en los usuarios del agregar a la sección de grupo de WirelessUsers de este documento
2. En los usuarios selectos, el cuadro de diálogo de los contactos, o de las Computadoras, teclea el nombre del ordenador que usted quiere agregar al grupo. Este ejemplo muestra cómo agregar el ordenador nombrado **Client al** grupo.
3. Haga clic los **tipos de objeto**, borre la casilla de verificación de los **usuarios**, y después marque las **Computadoras**.
4. Haga clic en OK dos veces. La cuenta de la computadora cliente se agrega al grupo de WirelessUsers.
5. Relance el procedimiento para agregar más ordenadores al grupo.

Estándar 2003 de Windows puesto con el Cisco Secure ACS 4.0

El Cisco Secure ACS es un ordenador que funciona con al Servidor Windows 2003 con el SP1, la edición estándar, que proporciona la autenticación de RADIUS y la autorización para el regulador. Complete los procedimientos en esta sección para configurar el ACS como servidor de RADIUS:

Instalación básica y configuración

Complete estos pasos:

1. Instale al Servidor Windows 2003 con el SP1, edición estándar, como **servidor miembro** nombrado **ACS** en el **dominio wirelessdemo.local**.**Nota:** El nombre de servidor ACS aparece como cisco_w2003 en las Configuraciones restantes. ACS o cisco_w2003 substituto en la configuración de laboratorio restante.
2. Para la conexión de área local, configure el protocolo TCP/IP con la dirección IP de **172.16.100.26**, la máscara de subred de **255.255.255.0**, y la dirección IP del servidor DNS de **127.0.0.1**.

Instalación del Cisco Secure ACS 4.0

Nota: Refiera a la guía de instalación para el Cisco Secure ACS 4.0 para Windows para más información sobre cómo configurar el Cisco Secure ACS 4.0 para Windows.

Complete estos pasos:

1. Utilice una cuenta del administrador de dominio para iniciar sesión al ordenador nombrado ACS para instalar el Cisco Secure ACS.**Nota:** Solamente las instalaciones realizadas en el ordenador donde usted instala el Cisco Secure ACS se soportan. Las instalaciones remotas realizadas usando el Windows Terminal Services o los Productos tales como Virtual Network Computing (VNC) no se prueban, y no se soportan.
2. Inserte el CD del Cisco Secure ACS en un unidad de Cd-ROM en el ordenador.
3. Si el unidad de Cd-ROM soporta la característica del autorun de Windows, el cuadro de diálogo del servidor del Cisco Secure ACS for Windows aparece.**Nota:** Si el ordenador no tiene un paquete de servicio solicitado instalado, un cuadro de diálogo aparece. Los paquetes de servicios de Windows pueden ser aplicados cualquiera antes o después de que usted instala el Cisco Secure ACS. Usted puede continuar con la instalación, pero el paquete de servicio solicitado debe ser aplicado después de que la instalación sea completa. Si no, el Cisco Secure ACS no pudo funcionar confiablemente.
4. Realice una de estas tareas:Si aparece el cuadro de diálogo del servidor del Cisco Secure ACS for Windows, el tecleo **instala**.Si no aparece el cuadro de diálogo del servidor del Cisco Secure ACS for Windows, ejecute el **setup.exe, situado** en el directorio raíz del CD del Cisco Secure ACS.
5. El Cisco Secure ACS puso el cuadro de diálogo visualiza el acuerdo de licencia de software.
6. Lea el acuerdo de licencia de software. Si usted valida el acuerdo de licencia de software, el tecleo **valida**.El cuadro de diálogo agradable visualiza la información básica sobre el programa de configuración.
7. Después de que usted haya leído la información en el cuadro de diálogo agradable, haga clic **después**.
8. Antes de que usted comience los elementos de las listas del cuadro de diálogo que usted debe completar antes de que usted continúe con la instalación. Si usted ha completado todos los elementos enumerados en antes de que usted comience el cuadro de diálogo, marque el cuadro correspondiente para cada elemento y haga clic **después**.**Nota:** Si usted no ha completado todos los elementos enumerados en antes de que usted comience el cuadro de diálogo, haga clic la **cancelación** y después haga clic la **configuración de la salida**. Después de que usted complete todos los elementos enumerados en antes de que usted comience el cuadro de diálogo, recomience la instalación.
9. El cuadro de diálogo de la Ubicación de destino del elegir aparece. Bajo la carpeta de destino, la ubicación de la instalación aparece. Ésta es la unidad y la trayectoria en donde el programa de configuración instala el Cisco Secure ACS.
10. Si usted quiere cambiar la ubicación de la instalación, complete estos pasos:El tecleo **hojea**. El cuadro de diálogo de la carpeta del elegir aparece. El cuadro de la trayectoria contiene la ubicación de la instalación.Cambie la ubicación de la instalación. Usted puede teclear la nueva ubicación en el cuadro de la trayectoria o utilizar las listas de las unidades y de los directorios para seleccionar una nuevos unidad y directorio. La ubicación de la instalación debe estar en una unidad local al ordenador.**Nota:** No especifique una trayectoria que contenga un carácter del por ciento, “%”. Si usted lo hace así pues, la instalación pudo aparecer continuar correctamente pero falla antes de que complete.Haga clic en OK.**Nota:** Si usted especificó una carpeta que no existe, el programa de configuración visualiza un cuadro de diálogo para confirmar la creación de la carpeta. Para continuar, haga clic en **Sí**.
11. En el cuadro de diálogo de la Ubicación de destino del elegir, la nueva ubicación de la

instalación aparece bajo la carpeta de destino.
12. Haga clic en Next (Siguiente).
13. El cuadro del diálogo de configuración de la base de datos de autenticación enumera las opciones para los usuarios de autenticidad. Usted puede autenticar con la base de datos de Usuario usuario seguro de Cisco solamente, o también con una base de datos de usuario de Windows.**Nota:** Después de que usted instale el Cisco Secure ACS, usted puede configurar el soporte de la autenticación para todos los tipos de la Base de datos de usuarios externa además de las bases de datos de usuario de Windows.
14. Si usted quiere autenticar a los usuarios con la base de datos de Usuario usuario seguro de Cisco solamente, elija el **control la** opción de la **base de datos del Cisco Secure ACS solamente**.
15. Si usted quiere autenticar a los usuarios con una base de datos de usuarios del administrador del acceso a la seguridad de Windows (SAM) o la base de datos de usuarios del Active Directory además de la base de datos de Usuario usuario seguro de Cisco, complete estos pasos:Elija **también el marcar la opción de base de datos del usuario de Windows**.**El sí, refiere "Grant que el permiso de marcado a la** casilla de verificación de la **configuración al usuario"** está disponible.**Nota:** El sí, refiere "Grant que el permiso de marcado a la casilla de verificación de la configuración al usuario" se aplica a todas las formas de acceso controladas por el Cisco Secure ACS, no apenas acceso dial in. Por ejemplo, un usuario que accede la red a través de un túnel VPN no marca en un servidor de acceso a la red. Sin embargo, si el **sí, refiera "Grant que** se marca el **permiso de marcado al** rectángulo de la configuración al **usuario"**, Cisco Secure ACS aplica los permisos de dial in del usuario de Windows para determinar si conceder el acceso del usuario a la red.Si usted quiere permitir el acceso a los usuarios que son autenticados por una base de datos de usuarios del Dominio de Windows solamente cuando tienen permiso de dial in en su cuenta de Windows, marque el **sí, refieren "permiso de marcado de Grant al** cuadro de la **configuración al usuario"**.
16. Haga clic en Next (Siguiente).
17. El programa de configuración instala el Cisco Secure ACS y pone al día el registro de Windows.
18. El cuadro anticipado del diálogo de opciones enumera varias características del Cisco Secure ACS que no se habiliten por abandono. Para más información sobre estas características, refiera al guía del usuario para el servidor del Cisco Secure ACS for Windows, versión 4.0.**Nota:** Las características mencionadas aparecen en la interfaz de HTML del Cisco Secure ACS solamente si usted las habilita. Después de la instalación, usted puede habilitarlas o inhabilitar en la página opciones avanzada en la sección de configuración de la interfaz.
19. Para cada característica que usted quiere habilitar, marque el cuadro correspondiente.
20. Haga clic en Next (Siguiente).
21. El cuadro de diálogo de la supervisión del servicio activo aparece.**Nota:** Después de la instalación, usted puede configurar las características de la supervisión del servicio activo en la página de la Administración del servicio activo en la sección de configuración del sistema.
22. Si usted quisiera que el Cisco Secure ACS monitoreara los servicios de autenticación de usuario, marque el cuadro de la **supervisión del login del permiso**. Del script para ejecutar la lista, elija la opción que usted quiere aplicado en caso de error del servicio de autenticación:**Ninguna acción reparadora** — El Cisco Secure ACS no ejecuta un script.**Nota:** Esta opción es útil si usted habilita las notificaciones del correo del

evento.**Reinicialización** — El Cisco Secure ACS ejecuta un script que reinicia el ordenador que ejecuta el Cisco Secure ACS.**Recomience todos** — El Cisco Secure ACS recomienza todos los servicios del Cisco Secure ACS.**Reinicio RADIUS/TACACS+** — El Cisco Secure ACS recomienza los servicios solamente RADIUS y TACACS+.

23. Si usted quisiera que el Cisco Secure ACS enviara un correo electrónico cuando la supervisión del servicio detecta un evento, marque el cuadro de la **notificación del correo**.
24. Haga clic en Next (Siguiente).
25. El cuadro de diálogo de contraseña del cifrado de la base de datos aparece.**Nota:** La contraseña del cifrado de la base de datos se cifra y se salva en el registro ACS. Usted puede ser que necesite reutilizar esta contraseña cuando se presentan los problemas críticos y la base de datos necesita ser accedida manualmente. Mantenga esta contraseña a mano de modo que el Soporte técnico pueda acceder a la base de datos. La contraseña se puede cambiar cada período de la expiración.
26. Ingrese una contraseña para el cifrado de la base de datos. La contraseña necesita ser por lo menos ocho caracteres de largo y necesita contener los caracteres y los dígitos. No hay caracteres no válidos.
27. Haga clic en Next (Siguiente).
28. El programa de configuración acaba y el cuadro de diálogo del lanzamiento del servicio del Cisco Secure ACS aparece.
29. Para cada Cisco Secure ACS mantiene la opción del lanzamiento que usted quiere, que marca el cuadro correspondiente. Las acciones asociadas a las opciones ocurren después de que el programa de configuración acabe.**Sí, quiero ahora comenzar el servicio del Cisco Secure ACS** — comienza los servicios de Windows que componen el Cisco Secure ACS. Si usted no selecciona esta opción, la interfaz de HTML del Cisco Secure ACS no está disponible a menos que usted reinicie el ordenador o comience el servicio de CSAdmin.**Sí, quisiera que la configuración iniciara al administrador del Cisco Secure ACS de mi instalación de siguiente del navegador** — abre la interfaz de HTML del Cisco Secure ACS en el buscador Web predeterminado para la cuenta de usuario de las ventanas actuales.**Sí, quiero ver el archivo Léame** — abre el archivo leame.txt en el Bloc de notas de Windows.
30. Haga clic en Next (Siguiente).
31. Si usted seleccionó una opción, los servicios del Cisco Secure ACS comienzan. El cuadro de diálogo completo de la configuración visualiza la información sobre la interfaz de HTML del Cisco Secure ACS.
32. Haga clic en Finish (Finalizar).**Nota:** El resto de la configuración se documenta bajo sección para el tipo EAP se configura que.

Configuración de controlador del LWAPP de Cisco

Cree la configuración necesaria para WPAv2/WPA

Complete estos pasos:

Nota: La suposición es que el regulador tiene conectividad básica a la red y el alcance IP a la interfaz de administración es acertado.

1. Hojee a **https://172.16.101.252** para iniciar sesión al regulador.
2. Haga clic el **login**

3. Inicie sesión con el usuario predeterminado **admin** y la contraseña predeterminada **admin**.
4. Cree una nueva interfaz para la asignación del VLA N bajo menú del **regulador**.
5. Haga clic las **interfaces**.
6. Haga clic en **New**.
7. En el **empleado del** tipo de campo de nombre de la interfaz. (Este campo puede ser cualquier valor que usted tenga gusto.)
8. En el tipo de campo **20** VLAN ID. (Este campo puede ser cualquier VLA N que se lleve adentro la red.)
9. Haga clic en Apply (Aplicar).
10. Configure la información como esto interconecta > edita las demostraciones de la ventana.
11. Haga clic en Apply (Aplicar).
12. Haga clic la lengueta **WLAN**.
13. Elija **crean nuevo** y el tecleo **va**.
14. Ingrese un nombre del perfil y en el **empleado del** tipo de campo del theWLAN SSID.
15. Elija un ID para la red inalámbrica (WLAN) y el tecleo **se aplica**.
16. Configure la información para esta red inalámbrica (WLAN) cuando los WLAN > editan las demostraciones de la ventana.**Nota:** WPAv2 es el método de encripción elegido de la capa 2 para este laboratorio. Para permitir que el WPA con los clientes TKIP-MIC se asocie a este SSID, usted puede también marcar al **modo de compatibilidad WPA** y **no prohibir los clientes WPA2 TKIP los** cuadros o a esos clientes que no soportan el método de encripción AES 802.11i.
17. En los WLAN > editan la pantalla, hacen clic la **ficha general**.
18. Asegúrese de que el cuadro del estatus esté marcado para saber si hay **habilitado** y la **interfaz** apropiada (empleado) se elige. También, aseegurese marcar la casilla de verificación habilitada para el broadcast SSID.
19. Haga clic en la ficha Security (Seguridad).
20. Conforme al submenú de la **capa 2** marque **WPA + WPA2** para la Seguridad de la capa 2. Para el control del cifrado WPA2 **AES + TKIP** para permitir a los clientes TKIP.
21. Elija el **802.1x** como el método de autentificación.
22. Salte el submenú de la capa 3 pues no se requiere. Una vez que configuran al servidor de RADIUS el servidor apropiado se puede elegir del menú de la autenticación.
23. **El QoS** y las **fichas Avanzadas** se pueden dejar en el valor por defecto a menos que se requiera cualquier confiugrations especial.
24. Haga clic el **menú de seguridad** para agregar al servidor de RADIUS.
25. Bajo **autenticación del** tecleo del submenú **RADIUS**. Entonces, haga clic **nuevo**.
26. Agregue la dirección IP del servidor de RADIUS (172.16.100.25) que es el servidor ACS configurado anterior.
27. Asegúrese de que la clave compartida haga juego al cliente AAA configurado en el servidor ACS. Asegúrese de que el cuadro del usuario de la red esté marcado y tecleo **se aplican**.
28. La configuración básica es completa ahora y usted puede comenzar a probar el PEAP.

Autenticación PEAP

El PEAP con la versión MS-CHAP 2 requiere los Certificados en los servidores ACS pero no en los clientes de red inalámbrica. La inscripción auto de los Certificados del ordenador para los servidores ACS se puede utilizar para simplificar un despliegue.

Para configurar DC_CA para proporcionar el autoenrollment para el ordenador y los Certificados

de usuario, complete los procedimientos en esta sección.

Nota: Microsoft ha cambiado la plantilla del servidor Web con la versión de la empresa CA de Windows 2003 de modo que las claves sean no más exportables y la opción sea greyed hacia fuera. No hay otros Certificate Template plantilla de certificado suministrados los servicios de certificados que están para la autenticación de servidor y dan la capacidad de marcar las claves pues exportable que están disponibles en el descenso-abajo así que usted tiene que crear una nueva plantilla que lo haga tan.

Nota: El Windows 2000 permite las claves exportables y estos procedimientos no necesitan ser seguidos si usted utiliza el Windows 2000.

Instale los Certificate Template plantilla de certificado Broche-en

Complete estos pasos:

1. Elija el **Start (Inicio) > Run (Ejecutar)**, teclee el **mmc**, y haga clic la **AUTORIZACIÓN**.
2. En el menú de archivos, el tecleo **agrega/quita Broche-en** y entonces haga click en Add
3. Bajo Broche-en, los **Certificate Template plantilla de certificado del** clic doble, **cierre del** tecleo, y entonces hacen clic la **AUTORIZACIÓN**.
4. En el árbol de la consola, **Certificate Template plantilla de certificado del** tecleo. Todos los Certificate Template plantilla de certificado aparecen en el panel de detalles.
5. Para desviar los pasos 2 a 4, tipo **certtmpl.msc broche-**en **quien** abre los Certificate Template plantilla de certificado.

Cree el Certificate Template plantilla de certificado para el servidor Web ACS

Complete estos pasos:

1. En el panel de detalles de los Certificate Template plantilla de certificado broche-en, haga clic la plantilla del **servidor Web**.
2. En el Menú Action (Acción), haga clic la **plantilla duplicado**.
3. En el campo de nombre de la visualización de la plantilla, teclee el **ACS**.
4. Vaya a la lengueta de la dirección de petición y el control **permite que la clave privada sea exportada**. También asegúrese de que la **firma y el cifrado** esté seleccionada del menú desplegable del propósito.
5. Elija las **peticiones debe utilizar uno de los CSP siguientes** y marcar el **v1.0 del Proveedor criptográfico de la base de Microsoft**. Desmarque cualquier otro CSP se marque que y después haga clic la **AUTORIZACIÓN**.
6. Vaya a la lengueta del asunto, elija la **fuente en la petición** y haga clic la **AUTORIZACIÓN**.
7. Vaya a la ficha de seguridad, resalte el **grupo de Admins del dominio** y asegúrese de que la opción del **alistar** está marcada bajo permitido.**Importante:** Si usted elige construir de este control de la información del Active Directory solamente el **nombre principal de usuario (UPN)** y desmarcar el **nombre del email del incluido** en el asunto y el email nombre porque un nombre del email no fue ingresado para la cuenta de usuario de red inalámbrica en los usuarios de directorio activo y computadora broche-en. Si usted no inhabilita estas dos opciones, el autoenrollment intenta utilizar el email, que da lugar a un error del autoenrollment.
8. Hay medidas de seguridad complementaria si es necesario para evitar que los Certificados

sean eliminados automáticamente. Éstos se pueden encontrar bajo lengueta de los requisitos de la emisión. Esto no se discute más lejos en este documento.
9. Haga Click en OK para salvar la plantilla y a moverse sobre la publicación de esta plantilla desde el Certificate Authority broche-en.

Habilite el nuevo Certificate Template plantilla de certificado del servidor Web ACS

Complete estos pasos:

1. Abra las autoridades de certificación broche-en. Siga los pasos 1-3 en el crear el Certificate Template plantilla de certificado para la sección del servidor Web ACS, elija la opción del **Certificate Authority**, elija la **computadora local** y el clic en Finalizar.
2. En el árbol de la consola, amplíe el **wirelessdemoca**, y después haga clic con el botón derecho del ratón los **Certificate Template plantilla de certificado**.
3. Elija **nuevo > Certificate Template plantilla de certificado a publicar**.
4. Haga clic el Certificate Template plantilla de certificado **ACS**.
5. El Haga Click en OK y abre a los **usuarios de directorio activo y computadora broche-en**.
6. En el árbol de la consola, los **usuarios de directorio activo y computadora del** clic doble, el click derecho **wirelessdemo.local, y** entonces hacen clic las propiedades**.**
7. En la lengueta de la directiva del grupo, la **directiva del Default Domain del** tecleo, y entonces hace clic **edita**. Esto abre el editor del objeto de la directiva del grupo broche-en.
8. En el árbol de la consola, amplíe el **Computer Configuration (Configuración de la computadora) > Windows Settings (Configuración de Windows) > Security Settings (Configuración de seguridad) > las directivas de la clave pública**, y después seleccione las **configuraciones automáticas del pedido de certificado**.
9. Haga clic con el botón derecho del ratón las **configuraciones automáticas del pedido de certificado** y elija el **nuevo > automático pedido de certificado**.
10. En la recepción a la página automática del asistente para la configuración del pedido de certificado, haga clic **después**.
11. En la página del Certificate Template plantilla de certificado, haga clic la **Computadora** y haga clic **después**.
12. Cuando usted completa la página automática del asistente para la configuración del pedido de certificado, clic en Finalizar.El tipo de certificado de la Computadora ahora aparece en el panel de detalles del editor del objeto de la directiva del grupo broche-en.
13. En el árbol de la consola, amplíe la **configuración de usuario > las configuraciones del > Security (Seguridad) de las configuraciones de Windows > las directivas de la clave pública**.
14. En el panel de detalles, haga doble clic las **configuraciones de Autoenrollment**.
15. Elija **alistan los Certificados automáticamente** y el control **renueva los certificados vencidos, se pone al día hasta que finalicen los Certificados y quita los Certificados revocados** y los **Certificados de la actualización que utilizan los Certificate Template plantilla de certificado**.
16. Haga clic en OK.

Configuración del certificado ACS 4.0

Certificado exportable de la configuración para el ACS

Importante: El servidor ACS debe obtener un certificado de servidor del servidor de la empresa raíz CA para autenticar a un cliente PEAP de la red inalámbrica (WLAN).

Importante: Asegúrese de que el Administrador IIS no esté abierto durante el proceso de configuración del certificado como problemas de las causas con la información guardada en memoria caché.

1. El registro en el servidor ACS con una cuenta que tenga empresa Admin endereza.
2. En la máquina local ACS, señale al navegador en el servidor de las autoridades de certificación de Microsoft en **http://IP-address-of-Root-CA/certsrv**. En este caso, la dirección IP es **172.16.100.26**.
3. Login como el **administrador**.
4. Elija la **petición un certificado** y haga clic **después**.
5. Elija el **pedido avanzado** y haga clic **después**.
6. Elija **crean y someten una petición a este CA** y hacen clic **después**.**Importante:** La razón de este paso es debido al hecho que Windows 2003 no permite para las claves exportables y usted necesita generar un pedido de certificado basado en el certificado ACS que usted creó eso lo hace anterior.
7. De los Certificate Template plantilla de certificado seleccione el **ACS** anterior nombrado creado Certificate Template plantilla de certificado. Las opciones cambian después de que usted seleccione la plantilla.
8. Configure el **nombre** para ser el Nombre de dominio totalmente calificado (FQDN) del servidor ACS. En este caso el nombre de servidor ACS es cisco_w2003.wirelessdemo.local. Asegúrese de que el **certificado del almacén en el almacén de certificados de computadora local** esté marcado y tecleo **someten**.
9. Un hacer estallar encima de la ventana aparece de cuidado sobre una infracción potencial del scripting. Elija **sí**.
10. Haga clic en Install this certificate (Instalar este certificado).
11. Un hacer estallar encima de la ventana aparece otra vez y advierte sobre una infracción potencial del scripting. Elija sí.
12. Después de que usted haga clic **sí**, el certificado está instalado.
13. En este momento, el certificado está instalado en los Certificados MMC bajo **personal > los Certificados**.
14. Ahora que el certificado está instalado a la computadora local (ACS o cisco_w2003 en este ejemplo), usted necesita generar un archivo de certificado (.cer) para la configuración del archivo de certificado ACS 4.0.
15. En el servidor ACS (cisco_w2003 en este ejemplo), señale al navegador en el servidor de las autoridades de certificación de Microsoft a **http://172.16.100.26 /certsrv**.

Instale el certificado en el software ACS 4.0

Complete estos pasos:

1. En el servidor ACS (cisco_w2003 en este ejemplo), señale al navegador en el Microsoft CA server a **http://172.16.100.26 /certsrv**.
2. Del selecto una opción de la tarea elige la **descarga un certificado de CA, una Cadena de certificados o un CRL**.
3. Elija el método de codificación de la radio del **base 64** y haga clic el **certificado de CA de la**

descarga.
4. Una ventana de la advertencia de seguridad de la descarga del archivo aparece. Haga clic en Save (Guardar).
5. Salve el archivo con un nombre tal como ACS.cer o cualquier nombre que usted desee. Recuerde este nombre puesto que usted lo utiliza durante el Certificate Authority ACS puesto en ACS 4.0.
6. Abra **ACS Admin del** acceso directo en el escritorio creado durante la instalación.
7. Haga clic la **configuración del sistema**.
8. Haga clic la **configuración del certificado ACS**.
9. Haga clic en Install ACS Certificate (Instalar certificado ACS).
10. Elija el **certificado del uso del almacenamiento** y teclee adentro el Nombre de dominio totalmente calificado (FQDN) de **cisco_w2003.wirelessdemo.local** (o de ACS.wirelessdemo.local si usted utilizó el ACS como el nombre).
11. Haga clic en Submit (Enviar).
12. **Configuración del sistema del** tecleo.
13. **El control de servicio del** tecleo y entonces hace clic el **reinicio**.
14. **Configuración del sistema del** tecleo.
15. **Configuración de la autenticación global del** tecleo.
16. Marque **permiten el EAP MSCHAPV2** y **permiten el EAP-GTC**.
17. Tecleo **Submit + Restart**.
18. **Configuración del sistema del** tecleo.
19. **Configuración de las autoridades de certificación del** tecleo **ACS**.
20. Bajo la ventana de la configuración de las autoridades de certificación ACS, teclee el nombre y la ubicación del archivo *.cer creado anterior. En este ejemplo, el archivo *.cer creado es **ACS.cer** en el directorio raíz c:\.
21. El tipo **c:\acs.cer** en el campo del archivo del certificado de CA y el tecleo **someten**.
22. Recomience el servicio ACS.

Configuración del cliente para el PEAP usando Windows cero tacto

En nuestro ejemplo, el CLIENTE es un ordenador que funciona con al profesional de Windows XP con el SP que actúa como cliente de red inalámbrica y obtiene el acceso a los recursos del Intranet a través de la Tecnología inalámbrica AP. Complete los procedimientos en esta sección para configurar al CLIENTE como cliente de red inalámbrica.

Realice una instalación básica y una configuración

Complete estos pasos:

1. Conecte al CLIENTE con el segmento de red del Intranet usando un cable Ethernet conectado con el concentrador.
2. En el CLIENTE, instale al profesional de Windows XP con el SP2 como ordenador del miembro nombrado CLIENT del dominio wirelessdemo.local.
3. Instale al profesional de Windows XP con el SP2. Esto se debe instalar para tener soporte PEAP.**Nota:** Firewall de Windows se gira automáticamente en el profesional de Windows XP con el SP2. No apague el Firewall.

Instale el adaptador de red inalámbrica

Complete estos pasos:

1. Apague la computadora cliente.
2. Desconecte la computadora cliente del segmento de red del Intranet.
3. Recomience la computadora cliente, y después abra una sesión usando la cuenta del administrador local.
4. Instale el adaptador de red inalámbrica.**Importante:** No instale el software de configuración del fabricante para el adaptador de red inalámbrica. Instale los drivers del adaptador de red inalámbrica que usan al asistente de hardware del agregar. También, cuando está indicado, proporcione el CD proporcionado por el fabricante o un disco de los drivers actualizados para el uso del profesional de Windows XP el SP2.

Configure la conexión de red inalámbrica

Complete estos pasos:

1. Termine una sesión y después abra una sesión usando la cuenta de WirelessUser en el dominio wirelessdemo.local.
2. Elija el **comienzo > al panel de control**, haga doble clic las **conexiones de red**, y después haga clic con el botón derecho del ratón la **conexión de red inalámbrica**.
3. Haga clic las **propiedades**, vaya a la lengueta de las redes inalámbricas, y asegúrese de que el **uso Windows de configurar mis configuraciones de la red inalámbrica** está marcado.
4. Haga clic en Add (Agregar).
5. Bajo lengueta de la asociación, **empleado del** tipo en el campo del nombre de red (SSID).
6. Seleccione el **WPA** para la autenticación de red y asegúrese de que la encripción de datos está fijada al **TKIP**.
7. Vaya a la lengueta de la autenticación.
8. Valide que configuran al tipo EAP para utilizar **EAP protegido (PEAP)**. Si no es, selecciónelo del menú desplegable.
9. Si usted quiere la máquina que se autenticará antes del control del login (que permite los scripts del login o directiva del grupo avanza para ser aplicado) **autentica como ordenador cuando información acerca de la computadora está disponible**.
10. Haga clic en Properties (Propiedades).
11. Como el PEAP implica la autenticación del servidor del cliente asegúrese que valida se marca el certificado de servidor. También, aseegurese CA que publicó el certificado ACS se marca bajo menú de los *Trusted Root Certification Authority*.
12. Elija la **contraseña asegurada (v2 EAP-MSCHAP)** bajo método de autentificación como se utiliza para la autenticación interna.
13. Aseegurese el permiso rápido volver a conectar la casilla de verificación se marca. Entonces, **AUTORIZACIÓN del** tecleo tres veces.
14. Haga clic con el botón derecho del ratón el icono de la conexión de red inalámbrica en systray y después haga clic las **redes inalámbricas disponibles de la visión**.
15. Haga clic la red inalámbrica del **empleado** y el tecleo **conecta**.Estas capturas de pantalla indican si la conexión completa con éxito.
16. Después de que la autenticación sea acertada, marque la configuración TCP/IP para el adaptador de red inalámbrica usando las conexiones de red. Debe tener un intervalo de

direcciones de 172.16.100.100-172.16.100.254 del alcance de DHCP o del alcance creado para los clientes de red inalámbrica.

17. Para probar las funciones, abra a un navegador y hojee a **http://wirelessdemoca** (o a la dirección IP del servidor de CA de la empresa).

Problema: El cliente Odyssey indica tres veces para la plataforma simbólica de la autenticación

Este problema ocurre en todas las versiones de Windows y solución 2.x.

Típicamente, los Servicios inalámbricos que fijan en XP hacen esto suceder.

Complete estos pasos para corregir este problema:

1. Elija el **Start (Inicio) > Settings (Configuración) > Control Panel (Panel de control) > Administrative Tools (Herramientas administrativas) > Services (Servicios)**.
2. Vaya a la parte inferior de la lista y busque la **configuración cero de la Tecnología inalámbrica**.
3. Haga doble clic esta configuración.
4. Seleccione la opción para parar este servicio.
5. Bajo configuración para la **neutralización** selecta del tipo de lanzamiento.**Nota:** Si toda lo que usted lo hace es parada el servicio, comienza otra vez en la reinicialización, así que usted debe inhabilitarla para que este problema no ocurra otra vez.
6. Salve las configuraciones y ciérrese.

La autenticación PEAP falla con el servidor ACS

Cuando su cliente falla la autenticación PEAP con un servidor ACS, marque si usted encuentra el mensaje de error *"del intento de autenticación duplicado NAS"* en la opción de los **intentos fallidos** bajo menú del **informe y de la actividad del** ACS.

Usted puede ser que reciba este mensaje de error cuando el Microsoft Windows XP SP2 está instalado en la máquina del cliente y Windows XP SP2 autentica contra un servidor del otro vendedor con excepción de un servidor del Microsoft IAS. Particularmente, el servidor del RADIUS de Cisco (ACS) utiliza un método distinto para calcular el tipo de protocolo extensible authentication: Longitud: Formato del valor (EAP-TLV) ID que las aplicaciones de Windows XP del método. Microsoft ha identificado esto como defecto en el supplicant de XP SP2.

Para un hotfix, entre en contacto Microsoft y refiera al artículo KB885453. El problema subyacente es ése en el lado del cliente, con la *utilidad de Windows*, el **rápido vuelve a conectar la** opción se inhabilita para el PEAP por abandono. Sin embargo, esta opción se habilita por abandono en el lado del servidor (ACS). Para resolver este problema, desmarque el **rápido vuelven a conectar la** opción en el servidor ACS y la prensa **submit+restart**. Alternativamente, usted puede habilitar el rápido vuelve a conectar la opción en el lado del cliente para resolver el problema.

Complete estos pasos para habilitar rápidamente vuelven a conectar en el cliente que ejecuta Windows XP usando la utilidad de Windows:

1. Haga clic el **Start (Inicio)> Settings (Configuración) > Control panel (Panel de control)**.
2. Doble el tecleo el icono de las **conexiones de red**.

3. Haga clic con el botón derecho del ratón el icono de la **conexión de red inalámbrica** y haga clic las **propiedades**.
4. Haga clic la lengueta de las **redes inalámbricas**.
5. Marque el *uso Windows de configurar mi opción Settings de la red inalámbrica* de permitir a las ventanas para configurar el adaptador del cliente.
6. Si usted ha configurado ya un SSID, elija el SSID y haga clic las **propiedades**. Si no, haga clic *nuevo* para agregar una nueva red inalámbrica (WLAN).
7. Ingrese el SSID bajo **asociación** cuadro se aseeguran que la *autenticación de red* está **abierta** y la *encripción de datos* está fijada al **WEP**.
8. Haga clic la **autenticación**.
9. Marque la *autenticación del IEEE 802.1X del permiso para esta opción de red*.
10. Elija el *tipo EAP* como **PEAP** y haga clic las **propiedades**.
11. Marque el **permiso rápidamente vuelven a conectar la** opción en la parte inferior de la página.

Información Relacionada

- Ejemplo de Configuración de Autenticación de EAP con Controladores de WLAN (WLC)
- Guía de configuración de controlador del Wireless LAN
- Ejemplo de la configuración básica del controlador y del Lightweight Access Point del Wireless LAN
- Ejemplo de Configuración de VLANs en Controladores de LAN Inalámbrica
- VLA N del grupo AP con el ejemplo de configuración de los reguladores del Wireless LAN
- Soporte Técnico y Documentación - Cisco Systems