Autenticación EAP local en el regulador del Wireless LAN con el ejemplo de configuración del EAP-FAST y del servidor LDAP

Contenido

Introducción

Este documento explica cómo configurar el Protocolo de Autenticación Extensible (EAP) - autenticación flexible vía la autenticación EAP local (RÁPIDA) segura del Tunelización en un regulador del Wireless LAN (WLC). Este documento también explica cómo configurar el servidor LDAP (Lightweight Directory Access Protocol) como la base de datos backend para que la EAP local obtenga los credenciales de usuario y autentique al usuario.

prerrequisitos

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.

- WLC de las Cisco 4400 Series que funciona con el firmware 4.2
- Lightweight Access Point de la serie del Cisco Aironet 1232AG (REVESTIMIENTO)
- Servidor de Microsoft Windows 2003 configurado como el controlador de dominio, servidor del servidor LDAP así como del Certificate Authority.
- Adaptador del cliente del a/b/g del 802.11 del Cisco Aironet que funciona con la versión de firmware 4.2
- Utilidad de escritorio del Cisco Aironet (ADU) esa versión de firmware 4.2 de los funcionamientos

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.

Antecedentes

La autenticación EAP local en los reguladores del Wireless LAN fue introducida con la versión 4.1.171.0 del regulador del Wireless LAN.

El EAP local es un método de autentificación que permite los usuarios y a los clientes de red inalámbrica que se autenticarán localmente en el regulador. Se diseña para el uso en las oficinas remotas que quieren mantener la Conectividad a los clientes de red inalámbrica cuando el sistema backend se interrumpe o va el servidor de autenticación externa abajo. Cuando usted habilita el EAP local, el regulador sirve como el servidor de autenticación y la base de datos de usuarios locales, así que quita la dependencia de un servidor de autenticación externa. El EAP local extrae los credenciales de usuario de la base de datos de usuarios locales o de la base de datos de la parte LDAP para autenticar a los usuarios. Los soportes locales EAP autenticación SALTAN, del EAP-FAST, del EAP-TLS, P EAPv0/MSCHAPv2, y PEAPv1/GTC entre el regulador y los clientes de red inalámbrica.

El EAP local puede utilizar a un servidor LDAP como su base de datos backend para extraer los credenciales de usuario.

Una base de datos de la parte LDAP permite que el regulador pregunte a un servidor LDAP para las credenciales (nombre de usuario y contraseña) de un usuario determinado. Estas credenciales entonces se utilizan para autenticar al usuario.

Los soportes de base de datos de la parte LDAP estos métodos EAP locales:

- EAP-FAST/GTC
- EAP-TLS
- PEAPv1/GTC.

El SALTO, EAP-FAST/MSCHAPv2, y PEAPv0/MSCHAPv2 también se soportan, **pero solamente si configuran al servidor LDAP para volver una contraseña de texto sin cifrar**. Por ejemplo, el Microsoft Active Directory no se soporta porque no vuelve una contraseña de texto sin cifrar. Si el servidor LDAP no puede ser configurado para volver una contraseña de texto sin cifrar, el SALTO, EAP-FAST/MSCHAPv2, y PEAPv0/MSCHAPv2 no se soportan.

Nota: Si configuran a algunos servidores de RADIUS en el regulador, el regulador intenta autenticar a los clientes de red inalámbrica que usan a los servidores de RADIUS primero. El EAP local se intenta solamente si no se encuentra a ningunos servidores de RADIUS, tampoco porque los servidores de RADIUS medidos el tiempo hacia fuera o no se configuró a ningunos servidores de RADIUS. Si configuran a cuatro servidores de RADIUS, el regulador intenta autenticar al cliente con el primer servidor de RADIUS, entonces el segundo servidor de RADIUS, y entonces EAP local. Si las tentativas del cliente entonces de reauthenticate manualmente, el regulador intentan el tercer servidor de RADIUS, entonces el cuarto servidor de RADIUS, y entonces el EAP local.

Este ejemplo utiliza el EAP-FAST como el método EAP local en el WLC, que a su vez se configura para preguntar la base de datos de la parte LDAP para los credenciales de usuario de un cliente de red inalámbrica.

Configurar

Este documento utiliza el EAP-FAST con los Certificados en el cliente y el lado del servidor. Para esto, la configuración utiliza el servidor de **Microsoft Certificate Authority (CA)** para generar los Certificados de cliente y servidor.

Los credenciales de usuario se salvan en el servidor LDAP de modo que en la validación de certificado acertada, el regulador pregunte al servidor LDAP para extraer los credenciales de usuario y autentique al cliente de red inalámbrica.

Este documento asume que estas configuraciones son ya en el lugar:

- UN REVESTIMIENTO se registra al WLC. Refiera al registro ligero AP (REVESTIMIENTO) a un regulador del Wireless LAN (WLC) para más información sobre el proceso de inscripción.
- Configuran a un servidor DHCP para asignar una dirección IP a los clientes de red inalámbrica.
- El servidor de Microsoft Windows 2003 se configura como el controlador de dominio así como servidor de CA. Este ejemplo utiliza **wireless.com** como el dominio.Refiera a configurar Windows 2003 como controlador de dominio para más información sobre configurar un servidor de Windows 2003 como controlador de dominio.Refiérase instalan y configuran el servidor de Microsoft Windows 2003 como servidor del Certificate Authority (CA) para configurar el servidor de Windows 2003 como servidor de CA de la empresa.

Diagrama de la red

En este documento, se utiliza esta configuración de red:

Configuraciones

Complete estos pasos para implementar esta configuración:

- Configure el EAP-FAST como método de autenticación EAP local en el WLC
- Configure al servidor LDAP
- Configure al cliente de red inalámbrica

Configure el EAP-FAST como método de autenticación EAP local en el WLC

Según lo mencionado anterior, este documento utiliza el EAP-FAST con los Certificados en el cliente y el lado del servidor como el método de autenticación EAP local. El primer paso es descargar y instalar los Certificados siguientes al servidor (WLC, en este caso) y al cliente.

El WLC y el cliente cada necesidad estos Certificados de ser descargado del servidor de CA:

- Certificado del dispositivo (uno para el WLC y uno para el cliente)
- Certificado raíz del Public Key Infrastructure (PKI) para el WLC, y certificado de CA para el cliente

Genere un certificado del dispositivo para el WLC

Realice estos pasos para generar un certificado del dispositivo para el WLC del servidor de CA. Este certificado del dispositivo es utilizado por el WLC para autenticar al cliente.

1. Vaya a **http:// < a la dirección IP de CA server>/certsrv de** su PC que tenga una conexión de red al servidor de CA. Inicie sesión como el administrador del servidor de CA.
2. Seleccione la **petición un certificado**.
3. En la petición una página del certificado, hace clic el **pedido de certificado avanzado**.
4. En la página avanzada del pedido de certificado, el tecleo **crea y somete una petición a este CA.** Esto le lleva al formulario de solicitud de certificado avanzado.
5. En el formulario de solicitud de certificado avanzado, elija al **servidor Web** como el Certificate Template plantilla de certificado. Entonces, especifique un nombre a este certificado del dispositivo.Este los ejemplos utilizan el nombre del certificado como ciscowlc123. Complete la otra información de identificación según su requisito.
6. Bajo **opciones dominantes** seccione, seleccione las **claves de la marca como opción Exportable**. A veces, esta opción particular será greyed hacia fuera y no puede ser habilitada o ser inhabilitada si usted elige una plantilla del servidor Web. En estos casos, haga clic **detrás del** menú del navegador para volver una página y para volver otra vez a esta página. Esta vez la marca cierra mientras que la opción Exportable debe estar disponible.
7. Configure el resto de campos necesarios y el tecleo **somete**.
8. Haga clic **sí** en la próxima ventana para permitir el proceso del pedido de certificado.
9. La ventana publicada certificado aparece que indica un proceso acertado del pedido de certificado. El siguiente paso es instalar el certificado publicado al almacén de certificados de

este PC. Haga clic en Install this certificate (Instalar este certificado).

10. El nuevo certificado está instalado con éxito al PC de donde la petición se genera al servidor de CA.
11. El siguiente paso es exportar este certificado del almacén de certificados al disco duro como archivo. Este archivo de certificado será utilizado más adelante para descargar el certificado al WLC.Para exportar el certificado del almacén de certificados, abra al buscador Internet Explorer, después haga clic las **herramientas > las opciones de Internet**.
12. Haga clic el **contenido > los Certificados** para ir al almacén de certificados en donde los Certificados están instalados por abandono.
13. Los Certificados del dispositivo están instalados generalmente conforme a la lista del **certificado personal**. Aquí, usted debe ver el certificado nuevamente instalado. Seleccione el certificado y haga clic la **exportación**.
14. Haga clic **después** en las ventanas siguientes. Elija el **sí, exporte la** opción de la **clave privada** en la **ventana del Asistente de la exportación del certificado**. Haga clic en Next (Siguiente).
15. Elija el formato de archivo de la exportación como **.PFX** y elija la **opción de protección fuerte del permiso**. Haga clic en Next (Siguiente).
16. En la ventana de contraseña, ingrese una contraseña. Este ejemplo utiliza **Cisco** como la contraseña.
17. Salve el archivo de certificado (archivo del .PFX) a su disco duro. Haga clic **después** y acabe el proceso de la exportación con éxito.

Descargar el certificado del dispositivo sobre el WLC

Ahora que el certificado del dispositivo del WLC está disponible como archivo del .PFX, el siguiente paso es descargar el archivo al regulador. El WLCs de Cisco valida los Certificados solamente en el formato del .PEM. Por lo tanto, usted necesita primero convertir el archivo con formato del .PFX o del PKCS12 a un archivo PEM usando el programa del openSSL.

Convierta el certificado en PFX al formato PEM usando el programa del openSSL

Usted puede copiar el certificado a cualquier PC donde usted hace el openSSL instalar para convertirlo al formato PEM. Ingrese estos comandos en el archivo Openssl.exe en el bin folder del programa del openSSL:

Nota: Usted puede descargar el openSSL del sitio web del OpenSSL.

```
openssl>pkcs12 -in ciscowlc123.pfx -out ciscowlc123.pem !--- ciscowlc123 is the name used in
this example for the exported file. !--- You can specify any name to your certificate file.
Enter Import Password : cisco !--- This is the same password that is mentioned in step 16 of the
previous section. MAC verified Ok Enter PEM Pass phrase : cisco !--- Specify any passphrase
here. This example uses the PEM passphrase as cisco. Verifying - PEM pass phrase : cisco
```

El archivo de certificado se convierte al formato PEM. El siguiente paso es descargar el certificado del dispositivo de formato PEM al WLC.

Nota: Antes eso, usted necesita un software de servidor TFTP en su PC de donde el archivo PEM va a ser descargado. Este PC debe tener Conectividad al WLC. El servidor TFTP debe hacer su directorio actual y bajo especificar con la ubicación en donde se salva el archivo PEM.

Descargue el certificado convertido del dispositivo de formato PEM al WLC

Este ejemplo explica el proceso de la descarga con el CLI del WLC.

1. Login al regulador CLI.
2. Ingrese el comando del **eapdevcert del datatype de la descarga de la transferencia**.
3. Ingrese el comando de *10.77.244.196 del* **serverip de la descarga de la transferencia**.10.77.244.196 es la dirección IP del servidor TFTP.
4. Ingrese el *comando del* **nombre de fichero** *ciscowlc.pem de la* **descarga de la transferencia**.ciscowlc123.pem es el nombre del archivo usado en este ejemplo.
5. Ingrese el comando del **certpassword de la descarga de la transferencia** de fijar la contraseña para el certificado.
6. Ingrese el **comando transfer download start** de ver las configuraciones actualizadas.Entonces, respuesta **y** cuando está indicado para confirmar las configuraciones actuales y para comenzar el proceso de la descarga.Este ejemplo muestra el comando download hecho salir:
```
(Cisco Controller) >transfer download start
Mode..................................... TFTP Data
Type..................................... Vendor Dev Cert TFTP Server
IP.................................. 10.77.244.196 TFTP Packet
Timeout.............................. 6 TFTP Max Retries.............................
10 TFTP Path..................................... TFTP
Filename................................. ciscowlc.pem This may take some time. Are you
sure you want to start? (y/N) y TFTP EAP CA cert transfer starting. Certificate installed.
Reboot the switch to use the new certificate. Enter the reset system command to reboot the
controller. The controller is now loaded with the device certificate.
```
7. Ingrese el **comando reset system** de reiniciar el regulador. El regulador ahora se carga con el certificado del dispositivo.

Instale el certificado raíz de PKI en el WLC

Ahora que el certificado del dispositivo está instalado en el WLC, el siguiente paso es instalar el certificado raíz del PKI al WLC del servidor de CA. Siga estos pasos:

1. Vaya a **http:// < a la dirección IP de CA server>/certsrv de** su PC que tenga una conexión de red al servidor de CA. Inicie sesión como el administrador del servidor de CA.
2. Haga clic la **descarga un certificado de CA, una Cadena de certificados, o un CRL**.
3. En la página resultante, usted puede ver los Certificados de CA actuales disponibles en el servidor de CA bajo el cuadro del **certificado de CA**. Elija el **DER** como el método de codificación y haga clic el **certificado de CA de la descarga**.
4. Salve el certificado como archivo de **.cer**. Este ejemplo utiliza **certnew.cer** como el nombre del archivo.
5. El siguiente paso es convertir el archivo de .cer al formato PEM y descargarlo al regulador. Para realizar estos pasos, relance el mismo procedimiento explicado en la transferencia el certificado del dispositivo a la sección del WLC con estos cambios:El openSSL “- en” y “- hacia fuera” archivos es **certnew.cer** y **certnew.pem.**También, no se requiere ninguna palabra clave PEM o contraseñas de la importación en este proceso.También, el comando del openSSL de convertir el archivo de **.cer al** archivo del **.pem** es:**x509 - en** *certnew.cer* **- informan al DER - hacia fuera** *certnew.pem - el outform* **PEM**En el paso 2 de la descarga el certificado convertido del dispositivo de formato PEM a la sección del WLC, el comando de descargar el certificado al WLC es:(**Eapcacert del datatype de la descarga del** >transfer del regulador de Cisco)El archivo que se descargará al WLC es **certnew.pem.**

Usted puede verificar si los Certificados estén instalados en el WLC del regulador GUI como

sigue:

- Del WLC GUI, **Seguridad del** tecleo. En la página Seguridad, el tecleo **avanzó > IPSec Certs de las** tareas que aparecen a la izquierda. **Certificado de CA del** tecleo para ver el certificado de CA instalado. Aquí está el ejemplo:
- Para verificar si el certificado del dispositivo esté instalado en el WLC, del WLC GUI, **Seguridad del** tecleo. En la página Seguridad, el tecleo **avanzó > IPSec Certs de las** tareas que aparecen a la izquierda. **Certificado del** tecleo **ID** para ver el certificado del dispositivo instalado. Aquí está el ejemplo:

Genere un certificado del dispositivo para el cliente

Ahora que el certificado del dispositivo y el certificado de CA están instalados en el WLC, el siguiente paso es generar estos Certificados para el cliente.

Realice estos pasos para generar el certificado del dispositivo para el cliente. Este certificado será utilizado por el cliente para autenticar al WLC. Este documento explica los pasos implicados en la generación de los Certificados para el cliente profesional de Windows XP.

1. Vaya a **http:// < a la dirección IP de CA server>/certsrv del** cliente que requiere el certificado para ser instalado. Inicie sesión como el Domain Name \ nombre de usuario al servidor de CA. El nombre de usuario debe ser el nombre del usuario que está utilizando esta máquina de XP, y el usuario debe ser configurado ya como parte del mismo dominio que el servidor de CA.
2. Seleccione la **petición un certificado**.
3. En la petición una página del certificado, hace clic el **pedido de certificado avanzado**.
4. En la página avanzada del pedido de certificado, el tecleo **crea y somete una petición a este CA.** Esto le lleva al formulario de solicitud de certificado avanzado.
5. En el formulario de solicitud de certificado avanzado, elija al **usuario del** menú desplegable del Certificate Template plantilla de certificado.Bajo opciones dominantes seccione, elija estos parámetros:Ingrese el Sizein dominante el campo del tamaño de clave. Este ejemplo utiliza **1024**.Marque las **claves de la marca como opción Exportable**.
6. Configure el resto de campos necesarios y el tecleo **somete**.
7. El certificado del dispositivo del cliente ahora se genera según la petición. El tecleo **instala el certificado** para instalar el certificado al almacén de certificados.
8. Usted debe poder encontrar el certificado del dispositivo del cliente instalado conforme a la lista del certificado personal conforme a las **herramientas > a las opciones de Internet > al contenido > a los Certificados** en el navegador IE del cliente.El certificado del dispositivo para el cliente está instalado en el cliente.

Genere certificado raíz CA para el cliente

El siguiente paso es generar el certificado de CA para el cliente. Complete estos pasos del PC del cliente:

1. Vaya a **http:// < a la dirección IP de CA server>/certsrv del** cliente que requiere el certificado para ser instalado. Inicie sesión como el Domain Name \ nombre de usuario al servidor de CA. El nombre de usuario debe ser el nombre del usuario que está utilizando esta máquina

de XP, y el usuario debe ser configurado ya como parte del mismo dominio que el servidor de CA.
2. En la página resultante, usted puede ver los Certificados de CA actuales disponibles en el servidor de CA bajo el cuadro del **certificado de CA**. Elija el **base 64** como el método de codificación. Entonces, el **certificado de CA de la descarga del** tecleo y salva el archivo al PC del cliente como archivo de **.cer**. Este ejemplo utiliza **rootca.cer** como el nombre del archivo.
3. Después, instale el certificado de CA guardado en el formato de .cer al almacén de certificados del cliente. Haga doble clic en el archivo de rootca.cer y el tecleo **instala el certificado**.
4. Haga clic **después** para importar el certificado del disco duro del cliente al almacén de certificados.
5. Elija **automáticamente selecto el almacén de certificados basado en el tipo de certificado** y haga clic **después**.
6. Clic en Finalizar para acabar el proceso de la importación.
7. Por abandono, los Certificados de CA están instalados conforme a la lista de Trusted Root Certification Authority en el navegador IE del cliente conforme a las **herramientas > a las opciones de Internet > al contenido > a los Certificados**. Aquí está el ejemplo:

Todos los Certificados requeridos están instalados en el WLC así como el cliente para la autenticación EAP del Local del EAP-FAST. El siguiente paso es configurar el WLC para la autenticación EAP local.

Configuración EAP local en el WLC

Complete estos pasos del **modo GUI del WLC** para configurar la autenticación EAP local en el WLC:

1. Haga clic la **Seguridad > EAP local**.
2. Bajo el EAP local, haga clic los **perfiles** para configurar el perfil local EAP.
3. Haga clic **nuevo** para crear un nuevo perfil del Local EAP.
4. Configure un nombre para este perfil y el tecleo **se aplica**. En este ejemplo, el nombre del perfil es **ldap**. Esto le lleva a los perfiles locales EAP creados en el WLC.
5. Haga clic el perfil del **ldap** que acaba de ser creado, que aparece bajo campo de nombre del perfil de la página local de los perfiles EAP. Esto le lleva a los **perfiles locales EAP > edita la** página.
6. Configure los parámetros específicos a este perfil en los **perfiles locales EAP > editan la** página.Elija el **EAP-FAST** como el método de autenticación EAP local.Habilite las casillas de verificación al lado del **certificado local requerido** y del **certificado del cliente requerido**.Elija al **vendedor** como el emisor del certificado porque este documento utiliza un servidor de CA del otro vendedor.Permita a la casilla de verificación al lado del **control contra los Certificados de CA** para permitir que el certificado entrante del cliente sea validado contra los Certificados de CA en el regulador.Si usted quisiera que el Common Name (CN) en el certificado entrante fuera validado contra el CN de los Certificados de CA en el regulador, marque la casilla de verificación de la **identidad del certificado CN del verificar**. La configuración predeterminada está desactivada. Para permitir que el regulador verifique que el certificado entrante del dispositivo sea todavía válido y no haya expirado, marque el cuadro de **comprobación de validez de la fecha del certificado del control**.**Nota:** La validez de la fecha del certificado se marca contra el tiempo actual UTC (GMT) que se configura en el regulador. Se ignora el desplazamiento del huso horario.Haga clic en Apply (Aplicar).

7. El perfil local EAP con la autenticación del EAP-FAST ahora se crea en el WLC.
8. El siguiente paso es configurar los parámetros específicos del EAP-FAST en el WLC. En la página Seguridad del WLC, haga clic **local los parámetros EAP > del EAP-FAST** para moverse a la página de los parámetros de método del EAP-FAST.Desmarque la casilla de verificación **anónima de la disposición** porque este ejemplo explica el EAP-FAST usando los Certificados. Deje el resto de los parámetros en sus valores por defecto. Haga clic en Apply (Aplicar).

WLC de la configuración con los detalles del servidor LDAP

Ahora que el WLC se configura con el perfil local y la información relacionada EAP, el siguiente paso es configurar el WLC con los detalles del servidor LDAP. Complete estos pasos en el WLC:

1. En la **página Seguridad del** WLC, seleccione **AAA > LDAP del** panel de tareas del lado izquierdo para moverse a la página de configuración del servidor LDAP. Para agregar a un servidor LDAP, haga clic **nuevo**. **Los servidores LDAP > nueva** página aparecen.
2. En los servidores LDAP edite la página, especifican a los detalles del servidor LDAP tales como dirección IP del servidor LDAP, número del puerto, estado del servidor del permiso y así sucesivamente.Elija un número de la casilla desplegable del **índice del servidor (prioridad)** para especificar la orden de la prioridad de este servidor en relación con cualquier otro servidor LDAP configurado. Usted puede configurar hasta diecisiete servidores. Si el regulador no puede alcanzar el primer servidor, intenta segundo en la lista y así sucesivamente.Ingrese el IP Address del servidor LDAP en el campo de **dirección IP del servidor**.Ingrese el número del puerto TCP del servidor LDAP en el campo de **número del puerto**. El intervalo válido es 1 a 65535, y el valor predeterminado es **389**.En el campo de la **Base del usuario DN**, ingrese el Nombre distintivo (DN) de la sub-estructura en el servidor LDAP que contiene una lista de todos los usuarios. Por ejemplo, unidad del ou=organizational, unidad organizativa .ou=next, y o=corporation.com. Si el árbol que contiene a los usuarios es la base DN, ingrese o=corporation.com o el dc=corporation, dc=com.En este ejemplo, el usuario está situado bajo **ldapuser de la** unidad organizativa (OU) que a su vez se crea como parte del dominio de **Wireless.com**.La Base del usuario DN debe señalar la ruta completa en donde se encuentra la información del usuario (credencial de usuario según el método de autentificación del EAP-FAST). En este ejemplo, el usuario está situado bajo base DN OU=ldapuser, DC=Wireless, dc=com.Más detalles en el OU, así como la configuración de usuario, se explican en los usuarios que crean en la sección del controlador de dominio de este documento.En el campo del **atributo de usuario**, ingrese el nombre del atributo en el registro del usuario que contiene el nombre de usuario.En el campo del **tipo de objeto de usuario**, ingrese el valor del atributo del objectType del LDAP que identifica el expediente como usuario. A menudo, los registros del usuario tienen varios valores para el atributo del objectType, algunos de los cuales son únicos al usuario y comparten algunos de los cuales con otros tipos de objeto.**Nota:** Usted puede obtener el valor de estos dos campos de su Servidor del directorio con la utilidad del navegador LDAP, que viene como parte de Windows 2003 instrumentos de apoyo. **Esta herramienta del navegador de Microsoft LDAP se llama LDP.** Con la ayuda de esta herramienta, usted puede conocer la Base del usuario DN, el atributo de usuario, y los campos del tipo de objeto de usuario de este usuario determinado. La información detallada sobre usar el LDP para conocer estos atributos específicos del usuario se discute en el LDP que usa para identificar la sección de los atributos de usuario de este documento.Elija **seguro de la** casilla

desplegable del modo de servidor si usted quisiera que todas las transacciones LDAP utilizaran un túnel seguro de TLS. Si no, no elija **ninguno**, que es la configuración predeterminada.En el campo del **tiempo de espera del servidor**, ingrese el número de segundos entre las retransmisiones. El intervalo válido es 2 a 30 segundos, y el valor predeterminado es 2 segundos.Marque la casilla de verificación del **estado del servidor del permiso** para habilitar a este servidor LDAP, o desmarquela para inhabilitar. Se inhabilita el valor predeterminado.El tecleo **se aplica** para confiar sus cambios.Aquí está un ejemplo configurado ya con esta información:Ahora que los detalles sobre el servidor LDAP se configuran en el WLC, el siguiente paso es configurar el LDAP como la base de datos de la parte de la prioridad de modo que el WLC primero mire a la base de datos de LDAP para los credenciales de usuario bastante que cualquier otra base de datos.

Configuración LDAP como la base de datos de la parte de la prioridad

Complete estos pasos en el WLC para configurar el LDAP como la base de datos de la parte de la prioridad:

1. En la página Seguridad, haga clic **local EAP > prioridad de la autenticación**. En la página de la orden **>** del Local-auth de la prioridad, usted puede encontrar dos bases de datos (Local y LDAP) que puedan salvar los credenciales de usuario.Para hacer el LDAP como la base de datos de la prioridad, elegir el **LDAP de los** credenciales de usuario del lado izquierdo encajona y hace clic **>** botón para mover el LDAP al cuadro de la orden de la prioridad en el lado derecho.
2. Este ejemplo ilustra claramente que el LDAP está elegido en el cuadro del lado izquierdo y **>** **el** botón está seleccionado. Como el resultado, el LDAP se mueve al cuadro en el lado derecho que decide la prioridad. La base de datos de LDAP se elige como la base de datos de la Autenticación-prioridad.Haga clic en Apply (Aplicar).**Nota:** Si el LDAP y el LOCAL aparecen en el cuadro de las credenciales del usuario correcto con el LDAP en el top y el LOCAL en la parte inferior, el EAP local intenta autenticar a los clientes que usan la base de datos de la parte LDAP y falla encima a la base de datos de usuarios locales si los servidores LDAP no son accesibles. Si no encuentran al usuario, se rechaza el intento de autenticación. Si el LOCAL está en el top, el EAP local intenta autenticar usando solamente la base de datos de usuarios locales. No falla encima a la base de datos de la parte LDAP.

red inalámbrica (WLAN) de la configuración en el WLC con la autenticación EAP local

El paso más reciente del WLC es configurar una red inalámbrica (WLAN) que utilice el EAP local como su método de autentificación con el LDAP como su base de datos backend. Siga estos pasos:

1. Del menú principal del regulador, haga clic los **WLAN** para moverse a la página de configuración WLAN. En los WLAN pagine, haga clic **nuevo** para crear una nueva red inalámbrica (WLAN). Este ejemplo crea un nuevo **ldap de la** red inalámbrica (WLAN).El tecleo **aplica el** siguiente paso es configurar los parámetros de WLAN en los WLAN **>** edita la página.
2. En la red inalámbrica (WLAN) edite la página, habilitan el estatus de esta red inalámbrica (WLAN). Configure el resto de parámetros necesarios.
3. Haga clic la **Seguridad** para configurar los parámetros relacionados con la seguridad para

esta red inalámbrica (WLAN). Este ejemplo utiliza la Seguridad de la capa 2 como 802.1x con 104 bits WEP dinámico.**Nota:** Este documento utiliza el 802.1x con el WEP dinámico como un ejemplo. Se recomienda para utilizar métodos de autentificación más seguros, tales como WPA/WPA2.

4. En la página de configuración de la Seguridad de WLAN, lengueta de los **servidores del** theAAA del tecleo. En los servidores de AAA pagine, habilite el método de autenticación EAP local y elija el **ldap de la** casilla desplegable que corresponde al parámetro del nombre del perfil EAP. Éste es el perfil local EAP creado en este ejemplo.
5. Elija al servidor LDAP (que fue configurado previamente en el WLC) de la casilla desplegable. Aseegurese que el servidor LDAP es accesible del WLC.Haga clic en Apply (Aplicar).
6. Los nuevos **ldaphas de la** red inalámbrica (WLAN) configurado en el WLC. Esta red inalámbrica (WLAN) autentica a los clientes con la autenticación EAP local (EAP-FAST en este caso) y pregunta una base de datos de la parte LDAP para la validación de los credenciales del cliente.

Servidor LDAP de la configuración

Ahora que el EAP local se configura en el WLC, el siguiente paso es configurar al servidor LDAP que sirve como base de datos backend autenticar a los clientes de red inalámbrica sobre la validación de certificado acertada.

El primer paso en configurar al servidor LDAP es crear una base de datos de usuarios en el servidor LDAP de modo que el WLC pueda preguntar esta base de datos para autenticar al usuario.

Crear a los usuarios en el controlador de dominio

En este ejemplo, se crea un nuevo **ldapuser** OU y crean al usuario **user2** bajo este OU. Configurando a este usuario para el acceso LDAP, el WLC puede preguntar esta base de datos de LDAP para la autenticación de usuario.

El dominio usado en este ejemplo es **wireless.com**.

Cree una base de datos de usuarios bajo un OU

Esta sección explica cómo crear un nuevo OU en su dominio y crear a un usuario nuevo en este OU.

1. En el controlador de dominio, **Start (Inicio) > Programs (Programas) > Administrative Tools (Herramientas administrativas) > Active Directory Users and Computers (Computadoras y usuarios de Active Directory) del** tecleo para iniciar la consola de administración de los **usuarios de directorio activo y computadora**.
2. Haga clic con el botón derecho del ratón en su Domain Name (wireless.com, en este ejemplo), después seleccione el New (Nuevo) > Organizational Unit (Unidad Organizacional) del menú contextual para crear un nuevo OU.
3. Asigne un nombre a este OU y haga clic la **AUTORIZACIÓN**.

Ahora que el nuevo **ldapuser** OU se crea en el servidor LDAP, el siguiente paso es crear al

usuario **user2** bajo este OU. Para alcanzar esto, complete estos pasos:

1. Haga clic con el botón derecho del ratón en el nuevo OU creado. Seleccione el **New (Nuevo) > User (Usuario) de los** menús contextuales resultantes para crear a un usuario nuevo.
2. En la página de la configuración de usuario, complete los campos obligatorios tal y como se muestra en de este ejemplo. Este ejemplo tiene **user2** como el nombre de inicio del usuario.Éste es el nombre de usuario que será verificado en la base de datos de LDAP para autenticar al cliente. Este ejemplo utiliza el **abcd** como el primer nombre y el último nombre. Haga clic en Next (Siguiente).
3. Ingrese una contraseña y confirme la contraseña. Elija la **contraseña nunca expira** opción y hace clic **después**.
4. Haga clic en Finish (Finalizar).Crean a un usuario nuevo **user2** bajo **ldapuser** OU. Los credenciales de usuario son:nombre de usuario: **user2**contraseña: **Laptop123**

Ahora que crean al usuario bajo un OU, el siguiente paso es configurar a este usuario para el acceso LDAP.

Configure al usuario para el acceso LDAP

Realice los pasos en esta sección para configurar a un usuario para el acceso LDAP.

Habilite la característica anónima del lazo en el servidor de Windows 2003

Para que cualquier aplicación de terceros acceda Windows 2003 AD en el LDAP, la característica anónima del lazo se debe habilitar en Windows 2003. Por abandono, las operaciones LDAP anónimas no se permiten en Windows 2003 controladores de dominio.

Realice estos pasos para habilitar la característica anónima del lazo:

1. Inicie el **ADSI editan la** herramienta del Start (Inicio) > Run (Ejecutar) > del tipo de la ubicación: **ADSI Edit.msc. Esta** herramienta es parte de Windows 2003 instrumentos de apoyo.
2. En el ADSI edite la ventana, amplían el dominio de la raíz ([tsweb-lapt.Wireless.com] de la configuración).Amplíe **CN=Services > el Windows NT CN= > el servicio de CN=Directory**. Haga clic con el botón derecho del ratón el envase del **servicio de CN=Directory** y seleccione las **propiedades del** menú contextual.
3. En el **CN=Directory mantenga la ventana de pPropiedades**, haga clic el atributo del **dsHeuristics** bajo campo del atributo y elija **editan**. En la **ventana del Editor del atributo de la cadena de** este atributo, ingrese el valor **0000002** y el tecleo **se aplica** y **APRUEBA**. La característica anónima del lazo se habilita en el servidor de Windows 2003.**Nota:** (El séptimo) carácter más reciente es el que controla la manera que usted puede atar al servicio LDAP. "0" o ningunos séptimos caracteres significan que las operaciones LDAP anónimas están inhabilitadas. **La determinación del séptimo carácter hasta el "2" habilita la característica anónima del lazo.Nota:** Si este atributo contiene ya un valor, aseegurese le están cambiando solamente el séptimo carácter de la izquierda. Éste es el único carácter que necesita ser cambiado para habilitar los lazos anónimos. Por ejemplo, si el valor actual es el "0010000", usted necesitará cambiarlo hasta el "0010002". Si el valor actual es menos de siete caracteres, usted necesitará introducir los ceros los lugares no usados: el "001" se convertirán en el "0010002".

Concediendo a acceso ANÓNIMO del INICIO al usuario el "user2"

El siguiente paso es conceder el acceso **ANÓNIMO del INICIO al** usuario **user2**. Complete estos pasos para alcanzar esto:

1. Abra a los **usuarios de directorio activo y computadora**.
2. Aseegurese las **funciones avanzadas de la visión** se marca.
3. Navegue al usuario **user2** y hagala clic con el botón derecho del ratón. Propiedades Select del menú contextual. Identifican a este usuario con el primer nombre “abcd”.
4. Vaya a la **Seguridad** en la ventana de pPropiedades del abcd.
5. El tecleo **agrega** en la ventana resultante.
6. Ingrese la **CONEXIÓN A LA COMUNICACIÓN ANÓNIMA** bajo **ingresar los nombres del objeto para seleccionar el** rectángulo y para reconocer el diálogo.
7. En el ACL, usted notará que el **INICIO ANÓNIMO** tiene acceso a algunos conjuntos de la propiedad del usuario. Haga clic en OK. El acceso ANÓNIMO del INICIO se concede en este usuario.

La concesión de la lista contenta el permiso en el OU

El siguiente paso es conceder por lo menos el permiso del **contenido de la lista al INICIO ANÓNIMO** en el OU que localizan al usuario. En este ejemplo, el "user2" está situado en el OU “ldapuser”. Complete estos pasos para alcanzar esto:

1. En los usuarios de directorio activo y computadora, haga clic con el botón derecho del ratón el **ldapuser** OU y elija las **propiedades**.
2. Haga clic la **Seguridad** y después **avanzó**.
3. Haga clic en Add (Agregar). En el diálogo que se abre, ingrese la **CONEXIÓN A LA COMUNICACIÓN ANÓNIMA**.
4. Reconozca el diálogo. Esto abre una nueva ventana de diálogo.
5. En la **aplicación sobre la** casilla desplegable, elija **este objeto solamente** y habilite el **contenido de la lista** permiten la casilla de verificación.

Usando el LDP para identificar los atributos de usuario

Esta herramienta GUI es un cliente LDAP que permite que los usuarios realicen las operaciones (por ejemplo conecte, ate, busque, modifiqúese, agregue, cancelación) contra cualquier directorio LDAP-compatible, tal como Active Directory. El LDP se utiliza a los objetos de visión salvados en el Active Directory junto con sus meta datos, tales como descriptores de seguridad y meta datos de la replicación.

La herramienta LDP GUI es incluida cuando usted instala los instrumentos de apoyo del Servidor Windows 2003 del CD del producto. Esta sección explica usando la utilidad LDP para identificar los atributos específicos asociados al usuario **user2**. Algunos de estos atributos se utilizan para completar los parámetros de la configuración del servidor LDAP en el WLC, tal como tipo del atributo de usuario y tipo de objeto de usuario.

1. En el servidor de Windows 2003 (incluso en el mismo servidor LDAP), el **Start (Inicio) > Run (Ejecutar) del** tecleo y ingresa el **LDP** para acceder el hojeador LDP.
2. En la ventana principal LDP, la **conexión del** tecleo **> conecta** y conecta con el servidor

LDAP ingresando el IP Address del servidor LDAP.

3. Conectado una vez con el servidor LDAP, seleccione la **visión del** menú principal y haga clic el **árbol**.
4. En la ventana resultante de la vista de árbol, ingrese el BaseDN del usuario. En este ejemplo, **user2 está situado bajo el OU "ldapuser" bajo dominio Wireless.com**. Por lo tanto, el BaseDN para el usuario **user2** es **OU=ldapuser, dc=wireless, dc=com**. Haga clic en OK.
5. El lado izquierdo del navegador LDP visualiza el árbol entero que aparece bajo el BaseDN especificado (**OU=ldapuser, dc=wireless, dc=com**). Amplíe el árbol para localizar al usuario **user2**. Este usuario puede ser identificado con el valor CN que representa el primer nombre del usuario. En este ejemplo, es **CN=abcd**. Clic doble **CN=abcd**. En el cristal del lado derecho del navegador LDP, el **LDP visualizará todos los atributos asociados a user2**. Este ejemplo explica este paso:En este ejemplo, observe los campos cercados a la derecha.
6. Como se menciona en el WLC de la configuración con los detalles de la sección del servidor LDAP de este documento, en el campo del **atributo de usuario**, ingrese el nombre del atributo en el registro del usuario que contiene el nombre de usuario.De esta salida LDP, usted puede ver que el **sAMAccountName** es un atributo que contiene el nombre de usuario el "user2". Por lo tanto, ingrese el atributo del **sAMAccountName** que corresponde al campo del **atributo de usuario** en el WLC.
7. En el campo del **tipo de objeto de usuario**, ingrese el valor del atributo del objectType del LDAP que identifica el expediente como usuario. A menudo, los registros del usuario tienen varios valores para el atributo del objectType, algunos de los cuales son únicos al usuario y comparten algunos de los cuales con otros tipos de objeto.En la salida LDP, **CN=Person** es un valor que identifica el expediente como usuario. Por lo tanto, especifique a la **persona** como el **atributo type del objeto de usuario** en el WLC.

Configure al cliente de red inalámbrica

El paso más reciente es configurar al cliente de red inalámbrica para la autenticación del EAP-FAST con los Certificados de cliente y servidor. Complete estos pasos para alcanzar esto:

1. Ponga en marcha la **utilidad de escritorio del Cisco Aironet** (ADU). En la ventana principal ADU, haga clic la **Administración del perfil > nuevo** para crear un nuevo perfil del cliente de red inalámbrica.
2. Especifique un nombre del perfil y asigne un nombre SSID a este perfil. Este nombre SSID debe ser lo mismo configurado en el WLC. En este ejemplo, el nombre SSID es **ldap**.
3. Haga clic la **ficha de seguridad** y elija **802.1x/EAP** como la Seguridad de la capa 2. Elija el **EAP-FAST** como el método EAP y haga clic la **configuración**.
4. En la página de configuración del EAP-FAST, elija el **certificado del cliente de TLS de la** casilla desplegable del método de autentificación del EAP-FAST y haga clic la **configuración**.
5. En la ventana de configuración del certificado del cliente de TLS:Habilite la casilla de verificación de la **identidad del servidor del validar** y seleccione el certificado de CA instalado en el cliente (explicado en la generación certificado raíz CA para la sección del cliente de este documento) como el Trusted Root Certification Authority.Seleccione el certificado del dispositivo instalado en el cliente (explicado en la generación un certificado del dispositivo para la sección del cliente de este documento) como el certificado del cliente.Haga clic en OK.Este ejemplo explica este paso:

Se crea el perfil del cliente de red inalámbrica.

Verificación

Realice estos pasos para verificar si su configuración trabaja correctamente.

1. Active el **ldap** SSID en el ADU.
2. Tecleo **sí** u **OK** como sea necesario en las próximas ventanas. Usted debe poder ver todos los pasos de la autenticación de cliente así como de la asociación para ser acertados en el ADU.

Use esta sección para confirmar que su configuración funciona correctamente. Utilice al modo CLI del WLC.

- Para verificar si el WLC pueda comunicar con el servidor LDAP y localizar al usuario, especifique el **comando enable del ldap aaa del debug del** WLC CLI. Este ejemplo explica un proceso de la comunicación satisfactoria LDAP:**Nota:** Algo de la salida en esta sección ha sido segundas líneas movidas debido a la consideración del espacio.(**Permiso del ldap aaa del >**debug del regulador de Cisco)
```
Sun Jan 27 09:23:46 2008: AuthenticationRequest: 0xba96514
Sun Jan 27 09:23:46 2008:       Callback.....................................0x8
344900
Sun Jan 27 09:23:46 2008:       protocolType.................................0x0
0100002
Sun Jan 27 09:23:46 2008:       proxyState...................................00:
40:96:AC:E6:57-00:00
Sun Jan 27 09:23:46 2008:       Packet contains 2 AVPs (not shown)
Sun Jan 27 09:23:46 2008: ldapTask [1] received msg 'REQUEST' (2) in state 'IDLE' (1)
Sun Jan 27 09:23:46 2008: LDAP server 1 changed state to INIT
Sun Jan 27 09:23:46 2008: ldapInitAndBind [1] called lcapi_init (rc = 0 - Success)
Sun Jan 27 09:23:46 2008: ldapInitAndBind [1] called lcapi_bind (rc = 0 - Success)
Sun Jan 27 09:23:46 2008: LDAP server 1 changed state to CONNECTED
Sun Jan 27 09:23:46 2008: LDAP server 1 now active
Sun Jan 27 09:23:46 2008: LDAP_CLIENT: UID Search (base=OU=ldapuser,DC=wireless, DC=com,
pattern=(&(objectclass=Person)(sAMAccountName=user2))) Sun Jan 27 09:23:46 2008:
LDAP_CLIENT: Returned msg type 0x64 Sun Jan 27 09:23:46 2008: ldapAuthRequest [1] called
lcapi_query base="OU=ldapus er,DC=wireless,DC=com" type="Person" attr="sAMAccountName"
user="user2" (rc = 0 - Success) Sun Jan 27 09:23:46 2008: LDAP ATTR> dn =
CN=abcd,OU=ldapuser,DC=Wireless,DC=com (size 38) Sun Jan 27 09:23:46 2008: Handling LDAP
response Success
```
De la información resaltada en esta salida de los debugs, está claro que el WLC con los atributos de usuario pregunta al servidor LDAP especificados en el WLC y el proceso LDAP es acertado.
- Para verificar si la autenticación EAP local sea acertada, especifique el **comando enable de los eventos del método del eap del local-auth aaa del debug del** WLC CLI. Aquí tiene un ejemplo:(**Permiso de los eventos del método del eap del local-auth aaa del >**debug del regulador de Cisco)
```
Sun Jan 27 09:38:28 2008: eap_fast.c-EVENT: New context
(EAP handle = 0x1B000009)

Sun Jan 27 09:38:28 2008: eap_fast.c-EVENT: Allocated new EAP-FAST context
(handle = 0x22000009)

Sun Jan 27 09:38:28 2008: eap_fast_auth.c-AUTH-EVENT: Process Response
(EAP handle = 0x1B000009)

Sun Jan 27 09:38:28 2008: eap_fast_auth.c-AUTH-EVENT: Received Identity Sun Jan 27 09:38:28
2008: eap_fast_tlv.c-AUTH-EVENT: Adding PAC A-ID TLV (436973636f0000000000000000000000) Sun
Jan 27 09:38:28 2008: eap_fast_auth.c-AUTH-EVENT: Sending Start Sun Jan 27 09:38:29 2008:
eap_fast.c-AUTH-EVENT: Process Response, type: 0x2b Sun Jan 27 09:38:29 2008:
eap_fast_auth.c-AUTH-EVENT: Process Response (EAP handle = 0x1B000009) Sun Jan 27 09:38:29
2008: eap_fast_auth.c-AUTH-EVENT: Received TLS record type: Handshake in state: Start Sun
```

Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Local certificate found Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Reading Client Hello handshake Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: TLS_DHE_RSA_AES_128_CBC_SHA proposed... Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: Proposed ciphersuite(s): Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: TLS_DHE_RSA_WITH_AES_128_CBC_SHA Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: TLS_RSA_WITH_AES_128_CBC_SHA Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: TLS_RSA_WITH_RC4_128_SHA Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: Selected ciphersuite: Sun Jan 27 09:38:29 2008: eap_fast.c-EVENT: TLS_DHE_RSA_WITH_AES_128_CBC_SHA Sun Jan 27 09:38:29 2008: eap_fast_auth.c-AUTH-EVENT: Building Provisioning Server Hello **Sun Jan 27 09:38:29 2008: eap_fast_crypto.c-EVENT: Starting Diffie Hellman phase 1 ... Sun Jan 27 09:38:30 2008: eap_fast_crypto.c-EVENT: Diffie Hellman phase 1 complete** Sun Jan 27 09:38:30 2008: eap_fast_auth.c-AUTH-EVENT: DH signature length = 128 Sun Jan 27 09:38:30 2008: eap_fast_auth.c-AUTH-EVENT: Sending Provisioning Serving Hello Sun Jan 27 09:38:30 2008: eap_fast.c-EVENT: Tx packet fragmentation required Sun Jan 27 09:38:30 2008: eap_fast.c-AUTH-EVENT: eap_fast_rx_packet(): EAP Fast NoData (0x2b) Sun Jan 27 09:38:30 2008: eap_fast.c-AUTH-EVENT: eap_fast_rx_packet(): EAP Fast NoData (0x2b) Sun Jan 27 09:38:30 2008: eap_fast.c-AUTH-EVENT: eap_fast_rx_packet(): EAP Fast NoData (0x2b) Sun Jan 27 09:38:32 2008: eap_fast.c-AUTH-EVENT: Process Response, type: 0x2b Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Reassembling TLS record **Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Sending EAP-FAST Ack**

.....

.....

..... **Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT: Received TLS record type: Handshake in state: Sent provisioning Server Hello Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT: Reading Client Certificate handshake Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Added certificate 1 to chain Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Added certificate 2 to chain Sun Jan 27 09:38:32 2008: eap_fast.c-EVENT: Successfully validated received certificate** Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT: Rx'd I-ID: "EAP-FAST I-ID" from Peer Cert Sun Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT: Reading Client Key Exchange handshake **Sun Jan 27 09:38:32 2008: eap_fast_crypto.c-EVENT: Starting Diffie Hellman phase 2 ... Sun Jan 27 09:38:32 2008: eap_fast_crypto.c-EVENT: Diffie Hellman phase 2 complete.** Sun **Jan 27 09:38:32 2008: eap_fast_auth.c-AUTH-EVENT: Reading Client Certificate Verify handshake Sun Jan 27 09:38:32 2008: eap_fast_crypto.c-EVENT: Sign certificate verify succeeded (compare)**

.....

.....

.....

.....

.

- El comando enable DB del local-auth aaa del debug es también muy útil. Aquí tiene un ejemplo:(Permiso DB del local-auth aaa del >debug del regulador de Cisco)Sun Jan 27 09:35:32 2008: LOCAL_AUTH: EAP: Received an auth request

Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Creating new context
Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Local auth profile name for context 'ldapuser' Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Created new context eap session handle fb000007 Sun Jan 27 09:35:32 2008: LOCAL_AUTH: (EAP:8) Sending the Rxd EAP packet (id 2) to EAP subsys Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Found matching context for id - 8 **Sun Jan 27 09:35:32 2008: LOCAL_AUTH: (EAP) Sending user credential request username 'user2' to LDAP** Sun Jan 27 09:35:32 2008: LOCAL_AUTH: Found context matching MAC address - 8

.....

.....

.....

..... Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) Sending the Rxd EAP packet (id 12) to EAP subsys Sun Jan 27 09:35:36 2008: LOCAL_AUTH: Found matching context for id - 8 Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) ---> [KEY AVAIL] send_len 64, recv_len 0 Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) received keys waiting for success Sun Jan 27 09:35:36 2008: LOCAL_AUTH: Found matching context for id - 8 **Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) Received success event Sun Jan 27 09:35:36 2008: LOCAL_AUTH: (EAP:8) Processing keys success**

- Para ver los Certificados instalados en el WLC que se utilizará para la autenticación local, publique los Certificados del local-auth de la demostración ordenan del WLC CLI. Aquí tiene

un ejemplo:(**Certificados del local-auth del >**show del regulador de Cisco)
```
Certificates available for Local EAP authentication:


Certificate issuer ..... vendor

  CA certificate:

    Subject: DC=com, DC=Wireless, CN=wireless

     Issuer: DC=com, DC=Wireless, CN=wireless

      Valid: 2008 Jan 23rd, 15:50:27 GMT to 2013 Jan 23rd, 15:50:27 GMT

  Device certificate:

    Subject: O=cisco, CN=ciscowlc123

     Issuer: DC=com, DC=Wireless, CN=wireless

      Valid: 2008 Jan 24th, 12:18:31 GMT to 2010 Jan 23rd, 12:18:31 GMT


Certificate issuer ..... cisco

  CA certificate:

    Subject: O=Cisco Systems, CN=Cisco Manufacturing CA

     Issuer: O=Cisco Systems, CN=Cisco Root CA 2048

      Valid: 2005 Jun 10th, 22:16:01 GMT to 2029 May 14th, 20:25:42 GMT

   Device certificate:

            Not installed.
```

- Para ver la configuración de la autenticación local en el WLC del modo CLI, publique el **comando config del local-auth de la demostración**. Aquí tiene un ejemplo:(**Config del local-auth del >**show del regulador de Cisco)
```
User credentials database search order:

    Primary ..... LDAP


Timer:

    Active timeout ..... 300


Configured EAP profiles:

    Name ..... ldapuser

      Certificate issuer ..... vendor

      Peer verification options:

        Check against CA certificates ..... Enabled
```

```
        Verify certificate CN identity ..... Disabled

        Check certificate date validity ..... Disabled

      EAP-FAST configuration:

        Local certificate required ..... Yes

        Client certificate required ..... Yes

      Enabled methods ..... fast

      Configured on WLANs ..... 2


EAP Method configuration:

    EAP-FAST:

--More-- or (q)uit

      Server key ..... <hidden>

      TTL for the PAC ..... 10

      Anonymous provision allowed ..... No

      ........................................

      ........................................

      Authority Information ..... Cisco A-ID
```

Troubleshooting

Usted puede utilizar estos comandos de resolver problemas su configuración:

- **permiso de los eventos del método del eap del local-auth aaa del debug**
- **debug aaa all enable**
- **permiso del paquete del dot1x del debug**

Información Relacionada

- Autenticación del EAP-FAST con el ejemplo de configuración de los reguladores y del servidor RADIUS externo del Wireless LAN
- PEAP bajo Redes Inalámbricas Unificadas con Microsoft Internet Authentication Service (IAS)
- Asignación del VLAN dinámico con el WLCs basado en el ACS al ejemplo de configuración de la asignación del grupo del Active Directory
- Guía de configuración del controlador LAN de la tecnología inalámbrica de Cisco - Soluciones de Configurar directivo de seguridad
- Guía de configuración del controlador LAN de la tecnología inalámbrica de Cisco - Manejo del software y de las configuraciones del regulador
- Ejemplo de Configuración de Autenticación de EAP con Controladores de WLAN (WLC)
- Diseño y características FAQ del regulador del Wireless LAN (WLC)

- Cisco Secure Services Client con la autenticación del EAP-FAST
- Regulador del Wireless LAN (WLC) FAQ
- Mensajes de error y de sistema FAQ del regulador del Wireless LAN de los reguladores (WLC)
- Soporte Técnico y Documentación - Cisco Systems