Instale el certificado en el dispositivo del Cisco Secure ACS para los clientes PEAP

Contenido

Introducción

Esta guía describe los Certificados creados con Microsoft CA y también contiene los pasos para cuando usted utiliza un certificado del auto firms, que se soporta a partir del Cisco Secure Access Control Server (ACS) 3.3. El uso de un certificado autofirmado optimiza considerablemente la instalación inicial de PEAP (Protected Extensible Authentication Protocol) puesto que no se requiere ninguna CA externa. Sin embargo, ahora, el período de expiración predeterminado del certificado autofirmado es solamente de un año y no se puede cambiar. Esto es estándar cuando se trata de certificados de servidor. Sin embargo, porque el certificado autofirmado también actúa como certificado raíz CA, esto puede significar la instalación del nuevo certificado en cada cliente cada año en que usted utiliza al solicitante de Microsoft a menos que usted no marque la opción del **certificado de servidor del validar**. Cisco recomienda utilizar certificados autofirmados solamente como medida temporal hasta que pueda utilizar la CA tradicional. Si desea utilizar un certificado autofirmado, pase a la sección de los certificados autofirmados.

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.

- Punto de acceso 12.02T1 de Cisco IOS®
- Cisco Secure ACS para Windows 3.1 y posterior
- Motor de solución del Cisco Secure ACS (SE).
- Microsoft Windows 2000 (SP3 y SP4) o XP con el ACU versión 6 (si usted utiliza el Cisco Secure ACS 3.2 que el ACU no se requiere)

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.

Instalación de Microsoft Certificate Service

Complete estos pasos:

1. Elija el **Start (Inicio)> Settings (Configuración) > Control panel (Panel de control)**.
2. Dentro del panel de control, abierto **agregue/quite los programas.**
3. En agregue/quite los programas, eligen **agregan/quitan a los componentes de Windows**.
4. Marque los **servicios de certificados** y haga clic **después**. Haga clic **sí al** mensaje IIS.
5. Elija un independiente (o la empresa) raíz CA y haga clic **después**.
6. Dé a CA un nombre y haga clic **después**. El resto de cuadros son opcionales.**Nota:** No dé a CA el mismo nombre que un servidor del Cisco Secure ACS. Esto puede hacer a los clientes PEAP fallar la autenticación porque consiguen confusos cuando a certificado raíz CA se encuentra con el mismo nombre que el certificado de servidor. Este problema no es único a los clientes de Cisco.
7. Haga clic en Next (Siguiente).
8. Haga clic en Finish (Finalizar).**Nota:** Usted debe instalar el IIS antes de que usted instale CA.

Cisco Secure ACS para la configuración del certificado de la ventana

Paso 1: Cree un certificado de servidor

Complete estos pasos para crear un certificado de servidor.

1. De su servidor del Cisco Secure ACS, hojee a CA **http://IP_of_CA_server/certsrv/**.
2. Elija la **petición una** opción del **certificado** y haga clic **después**.
3. Elija el **pedido avanzado** y haga clic **después**.
4. Elija **presentan un pedido de certificado a este CA usando una forma** y hacen clic **después**.
5. Teclee algo en el cuadro del nombre (CN).
6. Elija el **Certificado de autenticación de servidor** para el propósito previsto.**Nota:** Elija al **servidor Web** en la primera casilla desplegable si usted utiliza la empresa CA.**CSP** — V1.0 del Proveedor criptográfico de la base de Microsoft**Tamaño de clave** — 1024****Nota:** La empresa CA de Windows 2003 permite los tamaños de clave mayores de 1024. Sin embargo, el uso de un dominante más en gran parte de 1024 no trabaja con el PEAP. La autenticación pudo aparecer pasar en el ACS, pero el cliente apenas cuelga mientras que intenta la autenticación.**Almacenamiento de máquina local del uso del** control (software ACS solamente).Deje todo lo demás como valor por defecto y el tecleo **somete**.Un mensaje aparece `se ha recibido` que estado `su pedido de certificado….`**Nota:** Los Certificados creados con un tamaño de clave mayor de 1024 no trabajan.

Nota 2

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. Por lo tanto, usted necesita crear

una nueva plantilla que lo haga tan.

Complete estos pasos:

1. Elija el **Start (Inicio) > Run (Ejecutar) > certtmpl.msc.**
2. Haga clic con el botón derecho del ratón la plantilla del **servidor Web** y elija la **plantilla duplicado**.
3. Nombre la plantilla con un nombre que sea fácil de identificar.
4. Vaya a la lengueta de la dirección de petición y el control **permite que la clave privada sea exportada**.
5. Haga clic en los **CSP** abotonan y marcan el **v1.0 del Proveedor criptográfico de la base de Microsoft**. Haga clic en OK.
6. Todas las otras opciones se pueden dejar en el valor por defecto.
7. El tecleo **se aplica** y **APRUEBA**.
8. Abra CA MMC broche-en.
9. Haga clic con el botón derecho del ratón los **Certificate Template plantilla de certificado** y elija **nuevo > Certificate Template plantilla de certificado a publicar**.
10. Elija la nueva plantilla que usted creó y haga clic la **AUTORIZACIÓN**.
11. Recomience CA.

Los servicios de certificados pueden también dar `no podido para crear el` error del `objeto del “CertificateAuthority.Request”` cuando una tentativa se hace para crear un nuevo certificado. Complete estos pasos para corregir este problema:

1. Elija el **Start (Inicio) > Administrative Tools (Herramientas administrativas) > el IIS**.
2. Amplíe los **sitios web > el Sitio Web predeterminado**.
3. Haga clic con el botón derecho del ratón **CertSrv** y elija las **propiedades**.
4. Haga clic el botón de la **configuración** en la sección de las configuraciones de aplicaciones de la lengueta del directorio virtual.
5. Vaya a las opciones lengueta y al **estado de la sesión del permiso del** control.
6. Todo lo demás se puede dejar solo.
7. Haga clic en OK dos veces.
8. Reinicio IIS.Si su navegador bloquea con un `ActiveX que descarga de mensaje de control`, ejecute el arreglo discutido en las paradas del Internet Explorer del documento de Microsoft que responden en “el mensaje del control ActiveX de la transferencia” cuando usted intenta utilizar a un servidor de certificados . Si el campo CSP estado solamente el `cargamento…`, aseegurese le no ejecutan un Firewall de software en la máquina que somete la petición.

Paso 2: Apruebe el certificado de CA

Complete estos pasos:

1. Abra CA y el **> Programs (Programas) del** chooseStart **> Administrative Tools > Certificate Authority**.
2. A la izquierda, amplíe el certificado, después haga clic **hasta que finalicen las peticiones**.
3. Haga clic con el botón derecho del ratón en el certificado, elija **todas las tareas**, y elija el **problema**.

Paso 3: Descargue el certificado de servidor al servidor del Cisco Secure ACS

Complete estos pasos:

1. De su servidor del Cisco Secure ACS, hojee al directorio de **CA - de http://IP_of_CA_server/certsrv/**.
2. Elija el **control en un certificado pendiente** y haga clic **después**.
3. Seleccione el certificado y haga clic **después**.
4. El tecleo **instala**.

Paso 4: Instale el certificado de CA en el servidor del Cisco Secure ACS

Complete estos pasos:

Nota: Este paso no se requiere si el Cisco Secure ACS y CA están instalados en el mismo servidor.

1. De su servidor del Cisco Secure ACS, hojee al directorio de **CA - de http://IP_of_CA_server/certsrv/**.
2. Elija **extraen el certificado de CA o el Lista de revocación de certificados (CRL)** y hacen clic **después**.
3. Elija el **certificado de CA de la descarga del** tecleo del **encodedand del base 64**.
4. Haga clic **abierto** y elija **instalan el certificado**.
5. Haga clic en Next (Siguiente).
6. Elija el **lugar todos los Certificados en el almacén siguiente** y el tecleo **hojea**.
7. Marque el cuadro de los **almacenes del show physical**.
8. Amplíe los **Trusted Root Certification Authority**, elija la **computadora local**, y haga clic la **AUTORIZACIÓN**.
9. Haga clic **después**, **acabe**, y la **AUTORIZACIÓN del** tecleo para la **importación era** cuadro **acertado**.

Paso 5: Cisco Secure ACS de la configuración para utilizar el certificado de servidor

Complete estos pasos:

1. En el servidor del Cisco Secure ACS, haga clic la **configuración del sistema**.
2. Elija la **configuración del certificado ACS** y **instale el certificado ACS**.
3. Elija el **certificado del uso del almacenamiento**.
4. Teclee adentro el nombre CN y el tecleo **somete**.
5. En el servidor del Cisco Secure ACS, **configuración del sistema del** tecleo.
6. Elija el **certificado ACS puesto** y **editelo Certificate Trust List (Lista de confianza del certificado)**.
7. Marque el cuadro para CA y el tecleo **somete**.

Configuración del certificado del dispositivo del Cisco Secure ACS

Paso 1: Cree un pedido de firma de certificado

Complete estos pasos:

1. Elija la **configuración del sistema > el certificado ACS puestos > generan el pedido de firma de certificado**.
2. Ingrese un nombre en el campo Subject del certificado con el formato del `cn=name`.
3. Ingrese un nombre para el archivo de clave privado.**Nota:** La trayectoria a la clave privada se oculta en este campo. Si usted presiona **someta un** por segunda vez después de que se cree el CSR, la clave privada está sobregrabado y no hace juego el CSR original. Este resultado en una `clave privada no hace juego el` mensaje de error cuando usted intenta instalar el certificado de servidor.
4. Ingrese la contraseña de la clave privada y confírmela.
5. Elija una longitud de clave de 1024.**Nota:** Mientras que el Cisco Secure ACS puede generar los tamaños de clave mayores de 1024, el uso de un dominante más en gran parte de 1024 no trabaja con el PEAP. La autenticación pudo aparecer pasar en el Cisco Secure ACS, pero el cliente cuelga mientras que se intenta la autenticación.
6. El tecleo **somete**
7. Copie el CSR hecho salir en el Lado derecho para el submittal a CA.

Paso 2: Cree un certificado de servidor con su CSR

Complete estos pasos.

1. De su servidor FTP, hojee al directorio de **CA - de http://IP_of_CA_server/certsrv/**.
2. Elija la **petición una** opción del **certificado** y haga clic **después**.
3. Elija el **pedido avanzado** y haga clic **después**.
4. Elija **presentan un pedido de certificado usando PKCS-10 un archivo codificado base64 o un pedido de renovación usando PKCS-7 un archivo codificado base64**.
5. Pegue la salida del pedido de firma de certificado en el campo codificado base64 del pedido de certificado y el tecleo **somete**.
6. **Certificado de CA de la descarga del** tecleo.
7. Haga clic la **salvaguardia**, nombre el certificado, y sálvelo a su directorio FTP.

Paso 3: Certificado de CA de la descarga a su servidor FTP

Complete estos pasos:

Nota: Si usted salta estos pasos, da lugar a cualquiera que no puede habilitar el PEAP. Usted también recibe un error que el certificado de servidor no está instalado aunque es o usted recibe un error `no configurado del tipo EAP` en los intentos fallidos aunque configuran al tipo EAP.

Nota: También observe que si su certificado de servidor se crea usando CA intermedio, usted necesita relanzar estos pasos para cada CA en el encadenamiento entre raíz CA y el certificado de servidor, que incluye certificado raíz CA.

1. De su servidor FTP, hojee al directorio de **CA - de http://IP_of_CA_server/certsrv/**.
2. Elija **extraen el certificado de CA o el Lista de revocación de certificados (CRL)** y hacen clic **después**.
3. Elija el **base 64 codificado** y haga clic el **certificado de CA de la descarga**.
4. Haga clic la **salvaguardia** y nombre el certificado. Sálvelo a su directorio FTP.

Paso 4: Instale el certificado de CA en su dispositivo

Complete estos pasos:

Nota: Si usted salta estos pasos, da lugar a cualquiera que no puede habilitar el PEAP. Usted también recibe un error que el certificado de servidor no está instalado aunque es o usted recibe un error `no configurado del tipo EAP` en los intentos fallidos aunque configuran al tipo EAP.

Nota: También observe que si su certificado de servidor se crea usando CA intermedio, usted necesita relanzar estos pasos para cada CA en el encadenamiento entre raíz CA y el certificado de servidor, que incluye certificado raíz CA.

1. Elija la **configuración del sistema > el certificado ACS puestos > configuración de las autoridades de certificación ACS**.
2. Haga clic el **archivo del certificado de CA de la descarga**.
3. Teclee la dirección IP o el nombre de host del servidor FTP en el campo del servidor FTP.
4. Teclee un nombre de usuario válido que el Cisco Secure ACS pueda utilizar para acceder al servidor FTP en el campo del login.
5. Teclee la contraseña del usuario en el campo de contraseña.
6. Teclee la ruta relativo del directorio raíz del servidor FTP al directorio que contiene el archivo del certificado de CA en el campo remoto del directorio FTP.
7. Teclee el nombre del archivo del certificado de CA en el campo de nombre del archivo del telecontrol FTP.
8. Haga clic en Submit (Enviar).
9. Verifique el nombre de fichero en el campo y el tecleo **somete**.
10. Recomience los servicios ACS en la **configuración del sistema > el control de servicio**.

Paso 5: Instale el certificado de servidor en su dispositivo

Complete estos pasos:

1. Elija la **configuración de la configuración del sistema > del certificado ACS**.
2. Haga clic en Install ACS Certificate (Instalar certificado ACS).
3. Elija el **certificado leído de la** opción de archivos y después haga clic el link de **archivo de certificado de la descarga**.
4. Teclee la dirección IP o el nombre de host del servidor FTP en el campo del servidor FTP.
5. Teclee un nombre de usuario válido que el Cisco Secure ACS pueda utilizar para acceder al servidor FTP en el campo del login.
6. Teclee la contraseña del usuario en el campo de contraseña.
7. Teclee la ruta relativo del directorio raíz del servidor FTP al directorio que contiene el archivo de certificado de servidor en el campo remoto del directorio FTP.
8. Teclee el nombre del archivo de certificado de servidor en el campo de nombre del archivo del telecontrol FTP.
9. Haga clic en Submit (Enviar).
10. Ingrese la trayectoria a la clave privada.
11. Ingrese la contraseña para la clave privada.
12. Haga clic en Submit (Enviar).

Certificado autofirmado puesto (solamente si usted no utiliza CA externo)

Nota: Cuando usted prueba en el laboratorio con los certificados autofirmados, da lugar a un rato más largo de la autenticación la primera vez que un cliente autentica con el solicitante de Microsoft. Todas las autenticaciones subsiguientes están muy bien.

Complete estos pasos:

1. En el servidor del Cisco Secure ACS, haga clic la **configuración del sistema**.
2. Haga clic la **configuración del certificado ACS**.
3. El tecleo **genera el certificado autofirmado**.
4. Teclee algo en el campo Subject del certificado precedido por el **cn=**, por ejemplo, cn=ACS33.
5. Teclee la ruta completa y el nombre del certificado que usted quiere para crear, por ejemplo, c:\acscert \acs33.cer.
6. Teclee la ruta completa y el nombre del archivo de clave privado que usted quiere para crear, por ejemplo, c:\acscert \acs33.pvk.
7. Ingrese y confirme la contraseña de la clave privada.
8. Elija **1024 del** menú desplegable de la longitud de clave.**Nota:** Mientras que el Cisco Secure ACS puede generar los tamaños de clave mayores de 1024, el uso de un dominante más en gran parte de 1024 no trabaja con el PEAP. La autenticación pudo aparecer pasar en el ACS, pero el cliente cuelga mientras que se intenta la autenticación.
9. **Certificado generado Install del** control.
10. Haga clic en Submit (Enviar).

Configuraciones de la autenticación global de la configuración

Complete estos pasos.

1. En el servidor del Cisco Secure ACS, haga clic la **configuración del sistema**.
2. Haga clic la **configuración de la autenticación global**.**Para la versión 3.2 y posterior del Cisco Secure ACS**El control **permite el EAP MSCHAPv2** si usted utiliza Microsoft PEAP.El control **permite el EAP-GTC** si usted utiliza Cisco PEAP.El control **no prohibe a versión MS-CHAP 1 autenticación**.El control **permite la autenticación de la versión MS-CHAP 2**.Tecleo **Submit And Restart Button**.**Para la versión 3.1 del Cisco Secure ACS**El control **permite el PEAP**.El control **no prohibe a versión MS-CHAP 1 autenticación**.El control **permite la autenticación de la versión MS-CHAP 2**.Tecleo **Submit And Restart Button**.

Configure el AP en el Cisco Secure ACS

Complete estos pasos:

1. En el servidor del Cisco Secure ACS, haga clic la **configuración de red**.
2. El tecleo **agrega la entrada** para agregar a un cliente AAA.
3. Complete estos cuadros:**Dirección IP del cliente AAA** — IP_of_your_AP**Clave** — Componga una clave, y aseegurese esto las coincidencias en el secreto compartido AP.**Autentique**

usando — RADIUS (Cisco Aironet)
4. Tecleo **Submit And Restart Button**.**Nota:** No se cambió ningunos de los valores por defecto en la configuración del cliente AAA.

Configure el AP

Con VxWorks

Complete estos pasos:

1. Abra el AP y elija al **servidor de autenticación del Setup (Configuración) > Security (Seguridad) >**.Ingrese el IP Address del Cisco Secure ACS.Ingrese el secreto compartido, que debe corresponder con la CLAVE en el Cisco Secure ACS.Marque la **autenticación EAP**.Haga clic en OK.
2. Elija el **Setup (Configuración) > Security (Seguridad) > Radio Data Encryption (encripción de datos de radio)**.Marque **abierto** y el **Network EAP** para valida el tipo de autenticación.El control **abierto** para requiere el EAP.Fije la **clave WEP 1** y elija el **128 mordido** si usted no utiliza la rotación dominante del broadcast.Cambie Use of Data Encryption por las estaciones a la **encripción completa**. Si usted no puede cambiar Use of Data Encryption, el tecleo **se aplica** primero.Haga clic en OK.

Con la interfaz Web del Cisco IOS AP

Complete estos pasos:

1. Abra el AP y elija la **Seguridad > al administrador de servidor**.Elija el **RADIUS del** descenso-abajo de la lista del servidor actual.Ingrese el IP Address del Cisco Secure ACS.Ingrese el secreto compartido, que debe corresponder con la “CLAVE” en el Cisco Secure ACS.Marque la **autenticación EAP**.El Haga Click en OK en el diálogo amonestador y entonces hace clic **se aplica**.
2. Elija la **Seguridad > al administrador SSID**.**Nota:** La configuración diferencia si usted utiliza el WPA. Vea el suplemento de la administración de claves WPA en el extremo de este documento para los detalles.Elija el SSID de la lista actual SSID o ingrese un nuevo SSID en el campo SSID.Marque la **autenticación abierta** y elija **con el EAP del** menú desplegable.Marque la **red EAP**.Deje el resto de los valores en sus valores por defecto y el tecleo **se aplica**.
3. Elija **Security > Encryption Manager**.**Nota:** La configuración diferencia si usted utiliza el WPA. Vea el suplemento de la administración de claves WPA en el extremo de este documento para los detalles.Haga clic el botón de radio de la **encripción WEP** y elija **obligatorio del** descenso-abajo.Haga clic el botón de radio de la **clave de encripción 1** y ingrese la clave en el campo.Elija el **128 mordido del** descenso-abajo del tamaño de clave.Haga clic en Apply (Aplicar).

Nota: Se requiere la red EAP si usted instala el ACU.

Nota: Si usted utiliza la rotación dominante del broadcast, usted no necesita fijar una clave puesto que la clave debe ser fijada ya. Si la clave no se fija, elija el **avance del >Radio de la configuración** y fije un valor para la rotación de la clave del broadcast. No hay necesidad de fijar esto ningunos entonces cinco minutos más bajos (300 segundos). Una vez que se fija el valor, haga clic la

AUTORIZACIÓN y vaya nuevamente dentro de la página del Radio Data Encryption.

Instale el ACU versión 6 (solamente si usted utiliza el Cisco Secure ACS 3.1 o si usted requiere el EAP-GTC)

Usted necesita seleccionar la ADUANA instala porque el solicitante PEAP de Cisco no es instalado por la configuración expresa. Usted puede decir si el supplicant de Cisco está instalado cuando usted mira el EAP teclea adentro la lengueta de la autenticación de sus propiedades de conexión de red. Si aparece como PEAP, éste es el solicitante de Microsoft PEAP. Si aparece como apenas PEAP, después usted uso el solicitante PEAP de Cisco.

Instale certificado raíz CA para el cliente (solamente para EAP-MSCHAP-V2)

Si usted utiliza el certificado de Microsoft CA

Complete estos pasos:

1. Del PC del cliente, hojee a CA **- http://IP_of_CA_server/certsrv/**.
2. Elija **extraen un certificado de CA** y hacen clic **después**.
3. Elija el **base64 que codifica** y **descargue el certificado de CA**.
4. Haga clic **abierto** y selecto **instale el certificado**.
5. Haga clic en Next (Siguiente).
6. Elija el **lugar todos los Certificados en el almacén siguiente** y después haga clic **hojean**.
7. Marque el cuadro de los **almacenes del show physical**.
8. Amplíe los **Trusted Root Certification Authority**, elija la computadora local, y haga clic la **AUTORIZACIÓN**.
9. Haga clic **después**, clic en Finalizar, y la **AUTORIZACIÓN del** tecleo para la **importación era** cuadro **acertado**.

Si usted utiliza un certificado autofirmado del Cisco Secure ACS

Complete estos pasos:

1. Copie el certificado de su ubicación al cliente.
2. Haga clic con el botón derecho del ratón el archivo de **.cer** y el tecleo **instala el certificado**.
3. Haga clic en Next (Siguiente).
4. Elija el **lugar todos los Certificados en el almacén siguiente** y el tecleo **hojea**.
5. **Almacenes del show physical del** control.
6. Amplíe los **Trusted Root Certification Authority**, la **computadora local** selecta, y la **AUTORIZACIÓN del** tecleo.
7. Haga clic **después**, clic en Finalizar, y **AUTORIZACIÓN del** tecleo.**Nota:** Configure el AP para el Cisco Secure ACS se requiere para cada cliente si usted utiliza EAP-MSCHAP-V y tiene las propiedades PEAP del **validar de** Windows adentro marcado cuadro del **certificado de servidor**.

Configure al cliente para el PEAP

Configure Windows XP SP1 o el SP para el PEAP

Complete estos pasos:

Nota: Esta configuración diferencia si usted utiliza el WPA. Vea la sección de administración de claves WPA de este documento para los detalles.

Nota: Windows XP SP2 tiene actualmente problemas con la autenticación PEAP a los servidores de RADIUS con excepción de IAS. Esto se documenta adentro KB885453 y Microsoft tiene una corrección disponible a petición.

1. Las conexiones de red abierta en el panel de control y eligen el **comienzo > al panel de control**).
2. Haga clic con el botón derecho del ratón la red inalámbrica y elija las **propiedades**.
3. En la lengueta de la red inalámbrica, aseegurese las **ventanas del uso para configurar…** se marca.
4. Si usted ve el SSID en la lista, haga clic la **configuración**. Si no, haga click en Add
5. Ponga en el SSID y marque el **WEP** y la **clave se proporciona para mí automáticamente**.
6. Elija la lengueta de la autenticación y aseegurese el **Control de acceso a la red del permiso usando…** se marca.
7. Elija el **EAP protegido** y las **propiedades del** tecleo para el tipo EAP.
8. Marque el cuadro para **CA** conforme al certificado de la Raíz confiable.
9. Haga Click en OK tres veces.

Configuración Windows XP para el certificado (sin el SP1)

Complete estos pasos:

1. Las conexiones de red abierta en el panel de control y eligen el **comienzo > al panel de control**).
2. Haga clic con el botón derecho del ratón la red inalámbrica y elija las **propiedades**.
3. En la lengueta de la red inalámbrica, aseegurese las **ventanas del uso para configurar…** se marca.
4. Elija la lengueta de la autenticación y aseegurese el **Control de acceso a la red del permiso usando…** se marca.
5. Elija el **PEAP** y las **propiedades del** tecleo para el tipo EAP.
6. Marque el cuadro para **CA** conforme al certificado de la Raíz confiable.
7. Haga Click en OK tres veces.

Windows 2000 de la configuración para el PEAP

Complete estos pasos:

1. Si usted ejecuta el SP3, descargue y instale el hotfix del 802.1x de Microsoft. Esto no se requiere para el SP4.
2. Elija el **comienzo > el panel de control > la red y las conexiones por línea telefónica**.
3. Haga clic con el botón derecho del ratón su conexión de red inalámbrica y elija las **propiedades**.
4. Haga clic en la lengueta de la autenticación.**Nota:** Si no hay lengueta de la autenticación el servicio del 802.1x está instalado en un estado inhabilitado. Para solucionar esto, usted

debe habilitar el **servicio de configuración de red inalámbrica** en la lista de servicios:**El mi PC** y el tecleo del click derecho **manejan**.Elija los **servicios > las aplicaciones** y haga clic los **servicios**.Fije el valor de lanzamiento para el servicio a **automático**, y después comience el servicio.**Nota:** Si la lengueta de la autenticación es presente pero es inasequible, ésta indica que el driver del adaptador de red no soporta el 802.1x correctamente. Marque la lista en la parte inferior de la página del hotfix del 802.1x o del sitio Web del fabricante para los drivers soportados.
5. Marque el **Control de acceso a la red del permiso usando el IEEE 802.1X**.
6. Elija el **PEAP del** menú desplegable del tipo EAP y haga clic la **AUTORIZACIÓN**.

Si usted utiliza el ACU

Complete estos pasos:

1. Abra el ACU.
2. Elija **manejan el perfil** y crean un perfil o editan uno.
3. Ponga en el Nombre del cliente y el SSID del AP.
4. Elija la ficha de seguridad de la red.
5. Elija el **EAP basado en el host** para el tipo de la seguridad de la red.
6. Elija las **claves WEP dinámicas del uso** para el WEP.
7. Haga clic en OK dos veces.
8. Elija el perfil que usted creó.**Nota:** Si usted utiliza el supplicant de Cisco, en la lengueta de la autenticación usted tiene solamente PEAP. Si usted utiliza al solicitante de Microsoft, estado `EAP protegido (PEAP)`.**Nota:** Hay mismo un retardo prolongado antes de que el cliente intente asociarse al AP (alrededor de un minuto), que se puede paliar parcialmente con el paquete inalámbrico del rollup de la actualización para Windows XP es corrección disponible de Microsoft. Esta corrección puede potencialmente reinstalar el supplicant del EAP MSCHAPv2 que evita que funcionen los tipos de la base de datos compatible EAP-GTC.**Nota:** Si usted no consigue asociado, intente inhabilitar y después volver a permitir el indicador luminoso LED amarillo de la placa muestra gravedad menor.

Configure el móvil de Windows 2003 para el PEAP

Complete estos pasos:

1. Instale la última versión del Cisco ACU para Windows CE y esté seguro de instalar al solicitante PEAP durante el instalar.
2. Abra el ACU y elija el **<External Settings> del** menú desplegable activo del perfil.
3. Inserte su indicador luminoso LED amarillo de la placa muestra gravedad menor de red de Cisco, haga clic en el icono de red en el taskbar, y elija las **configuraciones > avanzó > placa de red**.
4. Haga clic en su SSID (si está disponible) o **agregue las nuevas configuraciones**.
5. Verifique el SSID en el campo de nombre de red y la red para conectar con.
6. Haga clic en la lengueta de la autenticación.
7. Marque la **encripción de datos (WEP)** y la **clave se proporciona para mí….**"
8. **La red access...802.1x del permiso del** incorporar y elige **Cisco PEAP**.
9. **Las propiedades** y el control del tecleo **validan el certificado de servidor** (opcional).**Nota:** Cuando usted marca esta opción, requiere que usted instale certificado raíz

CA encendido el PocketPC. Windows Mobile no incluye un buen método que usted puede utilizar para importar/que maneja los Certificados. Hay varias utilidades disponibles . Estas utilidades no son soportadas por Cisco. La importación de a certificado raíz CA no se requiere manualmente cuando usted utiliza el ACU, puesto que el solicitante PEAP de Cisco lo importa para usted. Ninguna versión de los certificados autofirmados de los soportes de sistema operativo del PocketPC ahora usted no puede importar tan los certificados autofirmados en el PocketPC para la validación. Usted puede todavía utilizar un certificado autofirmado si usted desmarca la opción del **certificado de servidor del validar**.

10. Haga Click en OK hasta que usted esté detrás en la pantalla de las redes inalámbricas de la configuración.
11. Haga clic en Connect (Conectar)

Suplemento de la autenticación de la máquina

El propósito de la autenticación de la máquina es permitir la autenticación EAP y la conectividad de red que se establecerán antes de la autenticación de usuario de modo que las secuencias de comandos de inicio puedan ejecutarse y un usuario pueda registrar sobre un dominio. El La pertenencia al dominio se requiere para que las credenciales de la máquina sean establecidas y autenticación para ocurrir.

Configuración ACS para permitir la autenticación de la máquina

Complete estos pasos:

1. Elija las **Bases de datos de usuarios externas > la configuración de la base de datos**.
2. Haga clic la **base de datos de Windows** y elija la **configuración**.
3. Marque la **autenticación de la máquina PEAP del permiso**.
4. Haga clic en Submit (Enviar).

Configure la autenticación del cliente para máquina

Únase al dominio (si no ya miembro del dominio)

Complete estos pasos:

1. Registro en Windows con una cuenta que tiene privilegios de administrador.
2. Haga clic con el botón derecho del ratón en el **mi PC** y elija las **propiedades**.
3. Elija la lengueta del nombre de computadora y haga clic el **cambio**.
4. Ingrese el hostname en el campo de nombre de la computadora.
5. Elija el **dominio**, ingrese el nombre del dominio, y haga clic la **AUTORIZACIÓN**.
6. Para unirse al dominio, visualizaciones de un diálogo del login. Inicie sesión con una cuenta que tenga permiso para unirse al dominio.
7. Una vez que el ordenador se une a con éxito el dominio, recomience el ordenador. La máquina es un miembro del dominio, y tiene credenciales de autenticación negociados con el dominio que sean sabidos solamente por el OS. En el Cisco Secure ACS, el nombre de usuario aparece como el host/nombre de host.

Solicitante PEAP de la configuración para la autenticación de la máquina

Complete estos pasos:

1. Elija las conexiones de red abierta del **comienzo > del panel de control** para en el panel de control.
2. Haga clic con el botón derecho del ratón la conexión de red y elija las **propiedades**.
3. Elija la lengueta de la autenticación y el control **autentica como ordenador**.

Suplemento de la administración de claves WPA

Escrito para el Cisco IOS AP 12.02(13)JA1, el Cisco Secure ACS 3.2, y Windows XP SP1 con la revisión de WPA.

Nota: Los clientes del Windows 2000 no soportan nativo la administración de claves WPA . Usted debe utilizar el software de cliente del vendedor para conseguir este soporte:

Nota: El Cisco ACU no soporta la administración de claves WPA para el EAP basado en el host (EAP-TLS y PEAP) ahora. Usted debe instalar a un cliente del otro vendedor tal como el cliente Odyssey del miedo o el AEGIS Client de Meetinghouse. Refiera al soporte WPA para más información sobre el soporte WPA para los Productos Cisco.

Nota: También observe que los drivers instalados para los indicadores luminosos LED amarillo de la placa muestra gravedad menor de Cisco por la versión del Pocket PC del ACU no soportan el WPA ahora. El WPA no trabaja para los clientes de Cisco en un PocketPC incluso con un supplicant del otro vendedor.

Configure el AP

Complete estos pasos:

1. Elija **Security > Encryption Manager**.**La cifra de** ChooseWEP y elige el **TKIP del** descenso-abajo.Haga clic en Apply (Aplicar).
2. Elija la **Seguridad > al administrador SSID**.Elija el SSID de la lista actual SSID o ingrese un nuevo SSID en el campo SSID.Marque la **autenticación abierta** y elija **con el EAP del** menú desplegable.Marque la **red EAP**.Bajo administración de claves autenticada, elija **obligatorio del** menú desplegable y haga clic el **WPA**.Haga clic en Apply (Aplicar).

Configure Windows XP SP1 (con KB826942 instalado) o al cliente SP2 para el PEAP y el WPA

Complete estos pasos:

1. Elija las conexiones de red abierta del **comienzo > del panel de control** para en el panel de control.
2. Haga clic con el botón derecho del ratón la red inalámbrica y elija las **propiedades**.
3. En la lengueta de la red inalámbrica, aseegurese las **ventanas del uso para configurar…** se marca.
4. Si usted ve el SSID en la lista, haga clic la **configuración**. Si no, haga click en Add

5. Ponga en el SSID y elija el **WPA** para la autenticación de red y el **TKIP** para la encripción de datos.
6. Elija la lengueta de la autenticación y aseegurese que el **Control de acceso a la red del permiso usando…** está marcado.
7. Elija el **EAP protegido** y las **propiedades del** tecleo para el tipo EAP.
8. Marque el cuadro para **CA** conforme al certificado de la Raíz confiable.
9. Haga Click en OK tres veces.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

Problema 1

Este error ocurre durante la instalación del certificado/la autenticación con el ACS.

```
Unsupported private key file format
Failed to initialize PEAP or EAP-TLS authentication protocol because ACS certificate is
not installed
```

Solución

El error ocurre porque el certificado del peap no está instalado properally. Quite el certificado y instale el nuevo certificado autofirmado para resolver el problema.

Problema 2

Este error ocurre durante la instalación del certificado/la autenticación con el ACS.

```
Failed to initialize PEAP or EAP-TLS authentication protocol because CA certificate is
 not installed.
```

Solución

Para resolver el error, instale el certificado de CA usando la configuración de las autoridades de certificación ACS. Este error ocurre debido al certificado de CA incorrecto si el certificado autofirmado no se utiliza.

Problema 3

Este error ocurre cuando se hace la actualización ACS.

```
A required certificate is not within its validity period when verifying
against the current system clock or the timestamp in the signed file.
(800B0101)
```

Solución

Este error ocurre cuando se hace la actualización de software ACS si usted no actualiza el

software de administración. Realice la actualización de software de administración y entonces la actualización de software ACS para resolver el problema. Refiera a actualizar la sección del dispositivo de administrar el dispositivo del Cisco Secure ACS para más información sobre cómo actualizar el ACS.

Problema 4

Este error ocurre durante la instalación del certificado con el ACS.

```
Private key you've selected doesn't fit to this certificate
```

Solución

La mayoría de la causa común de esto está sobregrabando accidentalmente la clave privada por genera un nuevo CSR.

Verifique esta información:

1. Usted carga el certificado correcto como el certificado ACS.
2. La longitud de clave del pub RSA es 1024 bits durante la creación de la petición.
3. Usted utiliza el CN=string completo cuando usted genera el CSR.

Información Relacionada

- Página de soporte de Cisco Secure ACS para Windows
- Field Notice de los productos de seguridad (CiscoSecure UNIX incluyendo)
- Documentación para el Cisco Secure Access Control Server para Unix
- Página de soporte de Cisco Secure ACS para Windows
- Documentación de Cisco Secure ACS para Windows
- Soporte Técnico y Documentación - Cisco Systems