Guía de configuración de la versión 1.01 del EAP-TLS

ID del Documento: 64064

Actualizado: De oct el 14 de 2009

 Descarga PDF

 Imprimir

_ Comentarios

Productos Relacionados

- Punto de acceso del Cisco Aironet 1200
- Puntos de acceso del Cisco Aironet 350
- Cisco Secure Access Control Server para Unix
- Cisco Secure Access Control Server para Windows

Contenido

Introducción

Este documento proporciona una configuración de muestra para la versión 1.01 de la Seguridad de la capa del Protocolo-transporte de la autenticación ampliable (EAP-TLS).

Nota: Este documento asume que usted utiliza Microsoft Certificate Authority (CA). Mientras que usted puede utilizar un certificado autofirmado, el cisco altamente desalienta esta práctica, y este documento no cubre los certificados autofirmados. El período predeterminado de la expiración de los certificados autofirmados es solamente un año, y usted no puede cambiar esta configuración. Esto es bastante estándar para los certificados de servidor. Sin embargo, el certificado autofirmado también actúa como certificado raíz CA. Por lo tanto, usted necesita instalar el nuevo certificado en cada cliente cada año a menos que usted no marque “valide la opción del certificado de servidor”. CA real debe estar disponible obtener los certificados del cliente de todos modos, y por eso, no hay realmente razón para emplear los certificados autofirmados con el EAP-TLS.

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
- Access Control Server (ACS) 3.1, 3.2, y 3.3
- Windows 2000 y XP
- Certificate Authority (CA) de la raíz de la empresa

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.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Utilice la herramienta Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos utilizados en esta sección.

Instale el servidor del certificado de Microsoft (CA)

Complete estos pasos:

1. Elija el **Start (Inicio)> Settings (Configuración) > Control panel (Panel de control)**.
2. El tecleo **agrega/quita los programas** en el panel de control.
3. Selecto **agregue/quite a los componentes de Windows**.
4. Seleccione los servicios de certificados.
5. Haga clic en Next (Siguiente).
6. Haga clic **sí al** mensaje IIS.
7. Seleccione un independiente (o la empresa) raíz CA.
8. Haga clic en Next (Siguiente).
9. Nombre CA.**Nota:** El resto de cuadros son opcionales.**Nota:** No utilice el mismo nombre para CA que el servidor ACS, porque esto puede hacer a los clientes PEAP fallar la autenticación. A certificado raíz CA con el mismo nombre que el certificado de servidor confunde a los clientes PEAP. Este problema no es único a los clientes de Cisco. Por supuesto, si usted no planea utilizar el PEAP, esto no se aplica.
10. Haga clic en Next (Siguiente).El valor por defecto de la base de datos está correcto.
11. Haga clic en Next (Siguiente).El IIS debe ser instalado antes de que usted instale CA.

Cree un certificado de servidor

Complete estos pasos:

1. Hojee a CA (**http://IP_of_CA_server/certsrv/) de** su servidor ACS.
2. Marque la **petición un** cuadro del **certificado**.

3. Haga clic en Next (Siguiente).
4. Seleccione el **pedido avanzado**.
5. Haga clic en Next (Siguiente).
6. Selecto **presente un pedido de certificado a este CA usando una forma**.
7. Haga clic en Next (Siguiente).
8. Teclee un nombre en el cuadro del nombre (CN).
9. Marque el cuadro del **Certificado de autenticación de servidor** para el propósito previsto.**Nota:** Si usted utiliza la empresa CA, seleccione al **servidor Web** en la primera lista.
10. Seleccione estas opciones bajo opción dominante para crear una nueva plantilla:**CSP — V1.0 del Proveedor criptográfico de la base de MicrosoftTamaño de clave — 1024Nota:** Los Certificados creados con un tamaño de clave mayor de 1024 pueden trabajar para el HTTPS pero no para el PEAP.**Nota:** La empresa CA de Windows 2003 permite los tamaños de clave mayores de 1024, pero un dominante más en gran parte de 1024 no trabaja con el PEAP. La autenticación puede aparecer pasar en el ACS, pero el cliente apenas cuelga en el intento de autenticación.Marque las **claves de la marca como opción ExportableNota:** Microsoft ha cambiado la plantilla del servidor Web con la versión de la empresa CA de Windows 2003. Con este cambio de la plantilla, usted puede exportar no más las claves, y la opción es greyed hacia fuera. No hay otros Certificate Template plantilla de certificado suministrados los servicios de certificados que están para la autenticación de servidor, o que dan la capacidad de marcar las claves como exportables. Para crear una nueva plantilla que lo hace así pues, ver el crear una nueva sección del Certificate Template plantilla de certificado.Marque la opción del **almacenamiento de máquina local del usoNota:** Conserve las selecciones predeterminadas para todas las otras opciones.
11. Haga clic en Submit (Enviar).Usted debe recibir este mensaje: **Se ha recibido su pedido de certificado**.

Cree un nuevo Certificate Template plantilla de certificado

Complete estos pasos:

1. Elija **Start > Run**.
2. Teclee **certtmpl.msc en el** cuadro de diálogo del funcionamiento, y el Presione ENTER.
3. Haga clic con el botón derecho del ratón la **plantilla del servidor Web**, y seleccione la **plantilla duplicado**.
4. Nombre la plantilla, por ejemplo, ACS.
5. Seleccione la lengueta de la **dirección de petición**.
6. Marque la **clave privada de la permit para ser** opción **exportada**.
7. Seleccione el botón **CSP**.
8. Marque la opción del **v1.0 del Proveedor criptográfico de la base de Microsoft**.
9. Haga clic en OK.**Nota:** Conserve las selecciones predeterminadas para todas las otras opciones.
10. Haga clic en Apply (Aplicar).
11. Haga clic en OK.
12. Abra CA MMC broche-en.
13. Haga clic con el botón derecho del ratón los **Certificate Template plantilla de certificado**, y elija **nuevo > Certificate Template plantilla de certificado a publicar**.
14. Elija la nueva plantilla que usted creó.

15. Haga clic en OK.
16. Recomience CA.La nueva plantilla se incluye en la lista del Certificate Template plantilla de certificado.

A veces, "`no podido para crear "el` error del`" objeto`" del `CertificateAuthority.Request` ocurre cuando usted intenta crear un nuevo certificado.

Complete estos pasos para corregir este error:

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. Seleccione la lengueta de las **opciones**.
6. Marque la opción del **estado de la sesión del permiso**.**Nota:** Conserve las selecciones predeterminadas para todas las otras opciones.
7. Haga clic en OK dos veces.
8. Reinicio IIS.**Nota:** 2003 CA en un dominio 2000 cuyo esquema no se ha preparado para la compatibilidad 2003 con adprep/forestprep/domainprep no trabajan con el EAP. Si su navegador bloquea con "un mensaje del `control ActiveX de la transferencia`", usted necesita ejecutar el arreglo en este URL: http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B330389 .**Nota:** Si el campo CSP apenas visualiza el "`cargamento….`" asegúrese de que usted no tenga un Firewall de software en la máquina que somete la petición. ZoneAlarm de ZoneLabs causa este error más o menos cada vez. Cierto otro software puede también causar este error.

Apruebe el certificado de CA

Complete estos pasos:

1. Elija el **Start (Inicio) > Programs (Programas) > Administrative Tools (Herramientas administrativas) > el Certificate Authority**.
2. Amplíe el certificado en el panel izquierdo.
3. Seleccione **hasta que finalicen las peticiones**.
4. Haga clic con el botón derecho del ratón en el certificado.
5. Seleccione todas las tareas.
6. Seleccione el **problema**.

Instale el certificado en un Servidor Windows

Descargue el certificado de servidor al servidor ACS

Complete estos pasos:

1. Hojee a CA (**http://IP_of_CA_server/certsrv/) de** su servidor ACS.
2. Seleccione el **control en un certificado pendiente**.
3. Haga clic en Next (Siguiente).

4. Seleccione el certificado.
5. Haga clic en Next (Siguiente).
6. El tecleo **instala**.

Instale el certificado de CA en el servidor ACS

Nota: Estos pasos no son necesarios si el ACS y CA están instalados en el mismo servidor.

1. Complete estos pasos:

2. De su servidor ACS, hojee a CA (**http://IP_of_CA_server/certsrv/**).
3. Selecto **extraiga el certificado de CA o el Lista de revocación de certificados (CRL)**.
4. Haga clic en Next (Siguiente).
5. Seleccione el **base 64 codificado**.
6. Haga clic el **certificado de CA de la descarga**.
7. Haga clic **abierto**.
8. El tecleo **instala el certificado**.
9. Haga clic en Next (Siguiente).
10. **Lugar** selecto **todos los Certificados en el almacén siguiente**.
11. El tecleo **hojea**.
12. Marque el cuadro de los **almacenes del show physical**.
13. Amplíe la lista de **Trusted Root Certification Authority**.
14. Seleccione la computadora local.
15. Haga clic en OK.
16. Haga clic en Next (Siguiente).
17. Haga clic en Finish (Finalizar).Una casilla de mensaje aparece.
18. Haga clic en OK.**Nota:** Si sus certificados del cliente fueron creados con CA diferente de su certificado de servidor, usted debe relanzar estos pasos para raíz CA y cualquier CA intermedio implicado en la creación del certificado del cliente.

Configuración ACS para utilizar el certificado de servidor

Complete estos pasos:

1. Haga clic la **configuración del sistema** en el servidor ACS.
2. Seleccione el **certificado ACS para poner**.
3. Selecto **instale el certificado ACS**.
4. Seleccione Use Certificate from storage (Usar certificado desde almacenamiento).
5. Teclee adentro el nombre CN (el mismo nombre que usted tecleó en el paso 8 del crear una sección del certificado de servidor).
6. Haga clic en Submit (Enviar).
7. **Configuración del sistema del** tecleo en el servidor ACS.
8. Seleccione el **certificado ACS para poner**.
9. Selecto **edite Certificate Trust List (Lista de confianza del certificado)**.
10. Marque el cuadro de **CA**.
11. Haga clic en Submit (Enviar).

Cree un pedido de firma de certificado

Complete estos pasos:

1. Vaya a la **configuración del sistema > al certificado ACS puestos > generan el pedido de firma de certificado**.
2. Teclee un nombre en el campo Subject del certificado en el formato del `cn=name`.
3. Teclee un nombre para el archivo de clave privado.**Nota:** Este campo oculta la trayectoria a la clave privada. Por lo tanto, si usted tecleo **somete un** por segunda vez después de que se cree el CSR, la clave privada está sobregrabada, y no hará juego el CSR original. Esto puede dar lugar a la "`clave privada no hace juego`" el error cuando usted intenta instalar el certificado de servidor.
4. Teclee la contraseña de la clave privada.
5. Confirme la contraseña.
6. Elija una longitud de clave de 1024.**Nota:** El ACS puede generar los tamaños de clave mayores de 1024. Sin embargo, un dominante más en gran parte de 1024 no trabaja con el EAP. La autenticación puede aparecer pasar en el ACS, pero el cliente apenas cuelga en el intento de autenticación.
7. Haga clic en Submit (Enviar).
8. Copie la salida CSR en el Lado derecho para someter a CA.

Utilice su CSR para crear un certificado de servidor

Complete estos pasos:

1. Hojee a CA (**http://IP_of_CA_server/certsrv/) de** su servidor FTP.
2. Seleccione la **petición una** opción del **certificado**.
3. Haga clic en Next (Siguiente).
4. Seleccione el **pedido avanzado**.
5. Haga clic en Next (Siguiente).
6. Selecto **presente un pedido de certificado usando PKCS-10 un archivo codificado base64 o un pedido de renovación usando PKCS-7 un archivo codificado base64**.
7. Pegue la salida del paso 8 del crear una sección del pedido de firma de certificado en el campo codificado base64 del pedido de certificado.
8. Haga clic en Submit (Enviar).
9. **Certificado de CA de la descarga del** tecleo.
10. Haga clic la **salvaguardia**, teclee un nombre para el certificado, y sálvelo a su directorio FTP.

Instale el certificado en un dispositivo de Windows

Descargue el certificado de CA a su servidor FTP

Complete estos pasos:

1. Hojee a CA (**http://IP_of_CA_server/certsrv/) de** su servidor FTP.
2. Selecto **extraiga el certificado de CA o el Lista de revocación de certificados (CRL)**.
3. Haga clic en Next (Siguiente).
4. Seleccione el **base 64 codificado**.

5. Haga clic el **certificado de CA de la descarga**.
6. Haga clic la **salvaguardia**, teclee un nombre para el certificado, y sálvelo a su directorio FTP.

Instale el certificado de CA en su dispositivo

Complete estos pasos.

1. Va a la **configuración del sistema > al certificado ACS puestos > la configuración de las autoridades de certificación ACS**.
2. **Archivo del certificado de CA de la descarga del** tecleo.
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 correcta para el nombre de 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.
10. Haga clic en Submit (Enviar).
11. Recomience los servicios ACS en la **configuración del sistema > el control de servicio**.**Nota:** Si usted salta los pasos en el certificado de CA de la descarga a su servidor FTP y los instala el certificado de CA en sus secciones una del dispositivo de estas dos situaciones puede presentarse:Usted no puede habilitar el EAP-TLS, y un mensaje de error aparece estado que el certificado de servidor no está instalado aunque el certificado está instalado.Alternativamente, el error `no configurado del tipo EAP` ocurre en los intentos fallidos aunque configuran al tipo EAP.**Nota:** También observe que, si usted utilizó un intermedio CA para crear su certificado de servidor, usted necesita relanzar estos pasos para cada CA en el encadenamiento entre raíz CA y el certificado de servidor (incluyendo certificado raíz CA). Además, si usted creó sus certificados del cliente con CA diferente de su certificado de servidor, usted debe relanzar estos pasos para raíz CA y cualquier CA intermedio implicado en la creación del certificado del cliente.

Instale el certificado de servidor en su dispositivo

Complete estos pasos:

1. Vaya a la **configuración de la configuración del sistema > del certificado ACS**.
2. Haga clic en Install ACS Certificate (Instalar certificado ACS).
3. Seleccione el certificado leído de la opción de archivos.
4. Haga clic el link de **archivo de certificado de la descarga**.
5. Teclee la dirección IP o el nombre de host del servidor FTP en el campo del servidor FTP.
6. Teclee un nombre de usuario válido que el Cisco Secure ACS pueda utilizar para acceder al servidor FTP en el campo del login.
7. Teclee la contraseña correcta en el campo de contraseña.
8. 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.

9. Teclee el nombre del archivo de certificado de servidor en el campo de nombre del archivo del telecontrol FTP.
10. Haga clic en Submit (Enviar).
11. Teclee la trayectoria y la contraseña para la clave privada. Refiera a los pasos 3 y 4 del crear una sección del pedido de firma de certificado.
12. Haga clic en Submit (Enviar).

Otro tareas

Configuraciones de la autenticación global de la configuración

Complete estos pasos:

1. Haga clic la **configuración del sistema** en el servidor ACS.
2. Haga clic la **configuración de la autenticación global**.
3. El control **permite el EAP-TLS**.
4. Seleccione una o más opciones de la verificación del certificado. Si usted selecciona todos los métodos, el ACS intenta cada método en orden hasta que ocurra una verificación exitosa o hasta el método más reciente falla.
5. Haga clic en Submit (Enviar).
6. Recomience el PC.

Configure el AP en el ACS

Complete estos pasos para configurar el AP en el ACS:

1. Haga clic la **configuración de red** en el servidor ACS.
2. El tecleo **agrega la entrada** para agregar a un cliente AAA.
3. Especifique estos valores en los cuadros:Dirección IP del cliente AAA — IP_of_your_APClave — Componga un dominante (aseegurese la clave hace juego la clave secreta compartida AP)Autentique usando — RADIUS (Cisco Aironet)
4. Haga clic en Submit (Enviar).
5. Recomience el PC.**Nota:** No cambie los valores por defecto uces de los en la configuración del cliente AAA.

Configure el AP

Nota: El red-EAP es necesario si usted quiere instalar el ACU.

Si usted utiliza la rotación dominante del broadcast, usted no necesita fijar una clave mientras que la clave debe ser fijada ya. Si la clave no se fija, vaya **a poner el avance del >Radio** y a fijar un valor para la rotación de la clave del broadcast. Usted no necesita probablemente fijar esto ninguna entonces 5 minutos más baja (300 secs). Después de que usted fije el valor, haga clic la **AUTORIZACIÓN**, y vuelva a la página del Radio Data Encryption.

VxWorks

Complete estos pasos:

1. Abra el AP.
2. Elija al **servidor de autenticación del Setup (Configuración) > Security (Seguridad) >**.
3. Ingrese el IP Address ACS.
4. Ingrese el secreto compartido. Este valor debe hacer juego la clave ACS.
5. Marque el cuadro de la **autenticación EAP**.
6. Haga clic en OK.
7. Elija el **Setup (Configuración) > Security (Seguridad) > Radio Data Encryption (encripción de datos de radio)**.
8. Marque el cuadro **abierto**.
9. Si usted no utiliza la rotación dominante del broadcast, seleccione la **clave WEP 1** y **128**.
10. Cambie Use of Data Encryption por las estaciones a la **encripción completa** (si usted no puede cambiar esto, el tecleo **se aplica** primero).
11. Haga clic en OK.

Interfaz Web IOS AP

Complete estos pasos:

1. Elija la **Seguridad > al administrador de servidor**.
2. Elija el RADIUS de la lista del servidor actual.
3. Teclee la dirección IP ACS.
4. Teclee el secreto compartido. Este valor debe hacer juego la clave en el ACS.
5. Marque el cuadro de la **autenticación EAP**.
6. De la lista de la autenticación EAP, elija la dirección IP del servidor de RADIUS.
7. Haga Click en OK en el cuadro de diálogo amonestador.
8. Haga clic en Apply (Aplicar).

Administrador SSID (encripción WEP solamente)

Complete estos pasos para la encripción WEP solamente:

1. Elija el SSID de la lista actual SSID, o especifique un nuevo SSID en el campo SSID.
2. Marque el cuadro de la **autenticación abierta**.
3. Elija **con el EAP de la** lista.
4. Marque el cuadro de la **red EAP**.
5. Haga clic en Apply (Aplicar).

Administrador del cifrado (encripción WEP solamente)

Complete estos pasos para la encripción WEP solamente:

1. Elija **Security > Encryption Manager**.
2. Haga clic el botón de radio de la **encripción WEP**.
3. Elija obligatorio de la lista.
4. Haga clic el botón de radio de la **clave de encripción 1**.
5. Especifique la clave.
6. Elija el **128 de la** lista del tamaño de clave.
7. Haga clic en Apply (Aplicar).**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.

Descargue y instale certificado raíz CA para el cliente

Este paso *se requiere* para *cada* cliente para que el EAP-TLS trabaje en ese cliente. Complete estos pasos:

1. Hojee a CA (**http://IP_of_CA_server/certsrv/) del** PC del cliente.
2. Selecto **extraiga un certificado de CA**.
3. Haga clic en Next (Siguiente).
4. Seleccione el **base 64 codificado**.
5. Haga clic el **certificado de CA de la descarga**.
6. Haga clic **abierto**.
7. El tecleo **instala el certificado**.
8. Haga clic en Next (Siguiente).
9. **Lugar** selecto **todos los Certificados en el almacén siguiente**.
10. El tecleo **hojea**.
11. Marque el cuadro de los **almacenes del show physical**.
12. Amplíe los **Trusted Root Certification Authority**, y seleccione la **computadora local**.
13. Haga clic en OK.
14. Haga clic en Next (Siguiente).
15. Haga clic en Finish (Finalizar).
16. El Haga Click en OK en la casilla de mensaje con la `importación era` mensaje `acertado`.

Cree el certificado del cliente

Empresa CA

Complete estos pasos:

1. Hojee a CA (**http://IP_of_CA_server/certsrv/) de la** cuenta de usuario del cliente.
2. Seleccione la **petición una** opción del **certificado**.
3. Haga clic en Next (Siguiente).
4. Seleccione el **pedido avanzado**.
5. Haga clic en Next (Siguiente).
6. Selecto **presente un pedido de certificado a este CA usando una forma**.
7. Haga clic en Next (Siguiente).
8. Elija al **usuario** en la lista del Certificate Template plantilla de certificado.
9. Fije estos valores bajo opciones dominantes:CSP — V1.0 del Proveedor criptográfico de la base de MicrosoftTamaño de clave — 1024Todas las otras opciones — Conserve los valores predeterminados
10. Haga clic en Submit (Enviar).Una casilla de mensaje aparece con su `pedido de certificado ha sido…` mensaje `recibido`.

CA independiente

Complete estos pasos:

1. Hojee a CA (**http://IP_of_CA_server/certsrv/) de la** cuenta de usuario del cliente.
2. Seleccione la **petición una** opción del **certificado**.
3. Haga clic en Next (Siguiente).
4. Seleccione el **pedido avanzado**.
5. Haga clic en Next (Siguiente).
6. Selecto **presente un pedido de certificado a este CA usando una forma**.
7. Haga clic en Next (Siguiente).
8. Teclee el nombre de usuario en el campo CN. Este valor debe hacer juego el nombre de usuario en la base de datos de autenticación.
9. Seleccione el Certificado de autenticación del cliente para el propósito previsto.
10. Fije estos valores bajo opciones dominantes:CSP — V1.0 del Proveedor criptográfico de la base de MicrosoftTamaño de clave — 1024Todas las otras opciones — Conserve los valores predeterminados
11. Haga clic en Submit (Enviar).Una casilla de mensaje aparece con su `pedido de certificado ha sido…` mensaje `recibido`.

Apruebe el certificado del cliente de CA

Complete estos pasos:

1. Elija el **Start (Inicio) > Programs (Programas) > Administrative Tools (Herramientas administrativas) > el Certificate Authority** para abrir CA.
2. Amplíe el certificado a la izquierda.
3. Haga clic **hasta que finalicen las peticiones**.
4. Haga clic con el botón derecho del ratón en el certificado y seleccione todas las tareas.
5. Seleccione el **problema**.

Instale el certificado del cliente en PC del cliente

Complete estos pasos:

1. Hojee a CA (**http://IP_of_CA_server/certsrv/) de la** cuenta de usuario del cliente.
2. Seleccione el **control en un certificado pendiente**.
3. Haga clic en Next (Siguiente).
4. Seleccione el certificado.
5. Haga clic en Next (Siguiente).
6. El tecleo **instala**.**Nota:** Para verificar la instalación del certificado, ir a Microsoft Internet Explorer, y a las **herramientas** selectas **> a las opciones de Internet > al contenido > a los Certificados**. Un certificado con el nombre de la identificación del usuario o del nombre de usuario abierta una sesión debe estar presente.

Confíe en el certificado del cliente en el ACS

Usted necesita realizar estos pasos solamente si los certificados del cliente y el certificado de servidor fueron creados con diversos CA.

1. Asegúrese de que certificado raíz CA y los Certificados de CA intermedios fueran instalados según los pasos en el instalar el certificado de CA en el servidor ACS y instale el certificado

de CA en sus secciones del dispositivo.
2. Vaya a la **configuración del sistema > al certificado ACS puestos** en el ACS.
3. Haga clic en Edit Certificate Trust List (Editar lista de confianza del certificado).
4. Marque el cuadro al lado del raíz CA que creó el certificado del cliente.
5. Haga clic en Submit (Enviar).

Ponga al cliente para el EAP-TLS

Complete estos pasos:

1. Elija el **Start (Inicio) > Control Panel (Panel de control) > Network Connections (Conexiones de red)**.
2. Haga clic con el botón derecho del ratón la red inalámbrica, y seleccione las **propiedades**.
3. Haga clic la lengueta de la **red inalámbrica**.
4. Asegúrese de que las **ventanas del uso a configurar…** estén marcadas.
5. Haga clic la **configuración** si usted ve el SSID en la lista. Si no, haga click en Add
6. Ponga en el SSID.
7. Marque el **WEP** y la **clave se proporciona para mí automáticamente las** casillas de verificación.
8. Seleccione la lengueta de la **autenticación**.**Nota:** Si usted no ve la lengueta de la autenticación, el servicio del 802.1x está instalado en un estado inhabilitado. Para solucionar este problema, usted debe habilitar el servicio de configuración de red inalámbrica en la lista de servicios. Complete estos pasos:Haga clic con el botón derecho del ratón el **mi PC**, y selecto **maneje**.Haga clic los **servicios y las aplicaciones**.Haga clic en **Services**.Fije el valor de lanzamiento para el servicio a **automático**.Inicie 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. Refiérase con la autenticación del 802.1x en las computadoras cliente que están funcionando con el Windows 2000 .
9. Asegúrese de que el **Control de acceso a la red del permiso usando…** esté marcado.
10. Seleccione la **placa inteligente o el otro certificado** para el tipo EAP, y haga clic las **propiedades**.
11. Seleccione el **certificado del uso en esta opción computadora**.
12. Marque la casilla de verificación del **simple certificate selection (Usar selección de certificado simple) del uso**.
13. Marque el cuadro para CA conforme al certificado de la Raíz confiable.
14. Haga Click en OK tres veces.

Suplemento de la autenticación de la máquina

La autenticación de la máquina del EAP-TLS *requiere el* Active Directory y una raíz CA de la empresa para adquirir un certificado para la autenticación de la máquina del EAP-TLS, el ordenador debe tener Conectividad a la empresa CA a través de una conexión alámbrica o a través de la conexión de red inalámbrica con la Seguridad del 802.1x inhabilitada. Ésta es la *única forma* de obtener un certificado de la máquina válido (con “máquina” en el campo del “Certificate Template plantilla de certificado”). Cuando está completado, el certificado de la máquina está instalado en los **Certificados (computadora local) > personal >** carpeta de los **Certificados** cuando está visto en los Certificados (computadora local) MMC broche-en. El certificado contiene el nombre de la máquina calificado completamente AD en el tema y los campos SAN. Un certificado

que lleva el nombre del ordenador pero no fue creado según lo descrito en esta sección no es un certificado de la máquina verdadero (con la “máquina” en el campo del Certificate Template plantilla de certificado). Tal certificado no se utiliza para la autenticación de la máquina pero el OS ve bastante un certificado tal como un certificado del usuario normal.

Configuración ACS para permitir la autenticación de la máquina

Complete estos pasos:

1. Vaya a las **Bases de datos de usuarios externas > a la configuración de la base de datos**.
2. Haga clic en base de datos de Windows.
3. Haga clic en Configure (Configurar).
4. Marque la casilla de verificación de la **autenticación de la máquina del EAP-TLS del permiso**.
5. Haga clic en Submit (Enviar).

Configure el dominio para el Autoregistro del certificado

Complete estos pasos:

1. Abra los usuarios y las Computadoras MMC broche-en encendido un controlador de dominio.
2. Haga clic con el botón derecho del ratón la entrada de dominio y seleccione las **propiedades**.
3. Vaya a la lengueta de la **directiva del grupo**.
4. seleccione la **directiva del Default Domain**.
5. Haga clic en **Editar**.
6. Vaya al **Computer Configuration (Configuración de la computadora) > Windows Settings (Configuración de Windows) > Security Settings (Configuración de seguridad) > a las directivas de la clave pública**.
7. Haga clic con el botón derecho del ratón las **configuraciones automáticas del pedido de certificado**.
8. Elija el **nuevo > automático pedido de certificado**.
9. Haga clic en Next (Siguiente).
10. Resalte la **Computadora**.
11. Haga clic en Next (Siguiente).
12. Marque la empresa CA.
13. Haga clic en Next (Siguiente).
14. Haga clic en Finish (Finalizar).

Ponga la autenticación del cliente para máquina

Unirse al dominio

Si el cliente se unió al dominio antes de que usted configurara el Autoregistro, el certificado se debe publicar a la máquina la próxima vez que usted reinicia el ordenador después de que el Autoregistro se configure sin la necesidad re-de unirse al ordenador al dominio.

Complete estos pasos para unirse al dominio:

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. Seleccione la lengueta del **nombre de computadora**.
4. Haga clic el **cambio**.
5. Teclee el hostname en el campo de nombre de la computadora.
6. Seleccione el **dominio**.
7. Teclee el nombre del dominio.
8. Haga clic en OK.Un cuadro de diálogo del login aparece.
9. Inicie sesión con las credenciales de una cuenta que tenga permiso para unirse al dominio.El ordenador se une al dominio.
10. Reinicie el equipo.El ordenador ahora es un miembro del dominio, y tiene un certificado para CA y un certificado de la máquina instalados.

Supplicant del EAP-TLS de la configuración para la autenticación de la máquina

Complete estos pasos:

1. Elija el **Start (Inicio) > Control Panel (Panel de control) > Network Connections (Conexiones de red)**.
2. Haga clic con el botón derecho del ratón la conexión de red y seleccione las **propiedades**.
3. Seleccione la lengueta de la **autenticación**.
4. El control **autentica como ordenador**.

Suplemento de la administración de claves WPA

Esta sección es aplicable al Cisco IOS AP 12.02(13)JA1, ACS 3.2, y XP SP1 con la revisión de WPA. Según la documentación en esta sección, los clientes del Windows 2000 no soportan nativo la administración de claves WPA y usted debe utilizar el software de cliente del vendedor para conseguir este soporte. Refiera a la descripción de la actualización de la seguridad de red inalámbrica WPA en Windows XP .

El Cisco ACU no soporta la administración de claves WPA para el EAP basado en el host (EAP-TLS y PEAP) actualmente. Usted debe instalar un cliente de tercera persona, por ejemplo, el cliente Odyssey del miedo o al AEGIS Client de Meetinghouse. Refiera a los documentos del adaptador de red inalámbrica LAN para Windows para más información sobre el soporte WPA para los Productos Cisco. Esta información es aplicable a Windows Mobile 2003 clientes (del Pocket PC) también.

La administración de claves WPA es básicamente lo mismo, pero diferencia en estos dos procedimientos:

1. Configure el AP.
2. Configure al cliente de XP para el EAP-TLS y el WPA.

Configure el AP

Complete estos pasos:

1. Vaya al **administrador de la Seguridad > del cifrado**.

2. Haga clic la **opción WEP cipher (cifrado WEP)**.
3. Elija el **TKIP**.
4. Haga clic en Apply (Aplicar).
5. Vaya a la **Seguridad > al administrador SSID**.
6. Elija el SSID de la lista actual SSID. Alternativamente, usted puede especificar un nuevo SSID en el campo SSID.
7. **Autenticación abierta del** control.
8. Elija **con el EAP de la** lista.
9. Marque la **red EAP**.
10. Seleccione **obligatorio de la** lista bajo administración de claves autenticada.
11. Haga clic el **WPA**.
12. Haga clic en Apply (Aplicar).

Configure al cliente de XP para el EAP-TLS y el WPA

Complete estos pasos:

1. Elija el **Start (Inicio) > Control Panel (Panel de control) > Network Connections (Conexiones de red)**.
2. Haga clic con el botón derecho del ratón la red inalámbrica, y seleccione las **propiedades**.
3. Seleccione la lengueta de la **red inalámbrica**.
4. Asegúrese de que las **ventanas del uso para configurar la** opción estén marcadas.
5. Haga clic la **configuración** si usted ve el SSID en la lista. Si no, haga click en Add
6. Ponga en el SSID.
7. Elija el **WPA** para la autenticación de red.
8. Elija el **TKIP** para la encripción de datos.
9. Seleccione la lengueta de la **autenticación**.
10. Asegúrese de que el **usar del Control de acceso a la red del permiso** esté marcado.
11. Seleccione la **placa inteligente o el otro certificado** para el tipo EAP.
12. Haga clic en Properties (Propiedades).
13. Seleccione el **certificado del uso en esta opción computadora**.
14. Marque la casilla de verificación del **simple certificate selection (Usar selección de certificado simple) del uso**.
15. Marque el cuadro para CA conforme al certificado de la Raíz confiable.
16. Haga Click en OK tres veces.

Verificación

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

Troubleshooting

Error: Problema con el certificado mientras que conecta con la red inalámbrica (WLAN)

Este error aparece en el cliente de red inalámbrica.

```
El servidor "server> del <Authentication" presentó un certificado válido publicado por el "name>
<CA", pero el "name> <CA" no se configura como ancla válida de la confianza para este perfil.
```

Solución

Para resolver este problema, usted puede exportar el certificado raíz de CA que publicó el certificado al servidor de autenticación a un archivo. Copie el archivo al cliente de red inalámbrica y después funcione con este comando de un comando prompt elevado.

```
certutil - empresa - addstore NTAuth CA_CertFilename.cer
```

Refiera a la alerta de seguridad de Windows aparece al conectar con una red inalámbrica en una máquina del grupo de trabajo para más información.

Información Relacionada

- Página de soporte de Cisco Secure ACS para Windows
- Página de soporte de Cisco Secure ACS para Windows
- Soporte Técnico y Documentación - Cisco Systems

Discusiones relacionadas de la comunidad del soporte de Cisco

La comunidad del soporte de Cisco es un foro para que usted haga y conteste a las preguntas, las sugerencias de la parte, y colabora con sus pares.

Refiera a los convenios de los consejos técnicos de Cisco para la información sobre los convenios usados en este documento.

Actualizado: De oct el 14 de 2009
ID del Documento: 64064