Latinoamérica

Microsoft TechNet

Seguridad en LAN inalámbricas con PEAP y contraseñas

Capítulo 4: Creación de la entidad emisora de certificados de red

Actualizado: abril 3, aaaa

Ver todos los temas de guía de seguridad

En esta página

Descargue la solución completa en

Seguridad en LAN inalámbricas con PEAP y contraseñas

Descargar la solución completa

Guía de defensa en profundidad antivirus

En esta guía

Información general

Este capítulo sirve de guía para instalar y configurar Servicios de Certificate Server Microsoft® Windows Server™ 2003. Servicios de Certificate Server es un componente opcional de Windows Server 2003 que no se instala de forma predeterminada.

Una instalación de Servicios de Certificate Server se conoce como una Entidad emisora de certificados. Sólo se necesita una entidad emisora de certificados para la solución *Seguridad en LAN inalámbricas con PEAP y contraseñas*. Esta entidad emisora se utilizará para emitir certificados en los servidores IAS (Servicio de autenticación de Internet), tal como se describe en los siguientes capítulos de esta solución.

El objetivo de este capítulo es proporcionar una entidad emisora específica muy sencilla. A diferencia de la mayoría de las entidades emisoras, se utilizará para emitir sólo un tipo de certificado: certificados de servidor para los servidores IAS que se utilizan en esta solución. Por este motivo, se ha diseñado para que se sea especialmente fácil de instalar, configurar y administrar. Es importante tener en cuenta que si la organización tiene previsto utilizar certificados para otros objetivos en el futuro, por ejemplo, IPSec o VPN, Microsoft recomienda una arquitectura de Infraestructura de claves públicas más sólida para el entorno. Consulte los materiales de planeamiento que se describen en el capítulo 2, "Planeamiento de la implementación de seguridad en LAN inalámbricas", para obtener más información.

La información que se incluye en este capítulo se limita a las instrucciones de implementación de la entidad emisora de certificados. En este capítulo no se explica ningún concepto general de infraestructura de claves públicas ni ninguno de los detalles de implementación de Servicios de Certificate Server de Microsoft aparte de los necesarios para completar la instalación. Tampoco se analiza el uso de esta entidad emisora para emitir otro tipo de certificados que no sean los certificados de autenticación de servidores IAS.

Este capítulo se basa en el supuesto de que actualmente no tiene una infraestructura de claves públicas en la organización. Si tiene una, podrá emitir certificados en los servidores IAS desde ella, en lugar de instalar la entidad emisora que se describe en este capítulo. No obstante, no entra en los objetivos de esta solución proporcionar información sobre cómo emitir los certificados desde la infraestructura de claves públicas o sobre cómo instalar esta entidad emisora en una infraestructura de claves públicas existente.

En lugar de instalar su propia entidad emisora, puede obtener certificados de una entidad emisora de certificados comercial como, por ejemplo, VeriSign o Thawte. Si desea ver un análisis sobre las ventajas relativas que ofrece instalar su propia entidad emisora frente a comprar certificados de un proveedor externo, consulte la sección "Obtención de certificados para servidores IAS" en el capítulo 2, "Planeamiento de la implementación de seguridad en LAN inalámbricas". Este capítulo no incluye información sobre la obtención y el uso de certificados de una entidad emisora de certificados comercial. No obstante, al final del capítulo se hace referencia a un documento de Microsoft donde se describe este proceso.

Principio de la página

Requisitos previos del capítulo

Además de los requisitos previos que se describen en el capítulo 3, "Preparación del entorno", debe estar familiarizado con los conceptos de Servicios de Certificate Server y de infraestructura de claves públicas (aunque no se necesita un conocimiento especializado).

Antes de implementar las instrucciones de este capítulo, debe leer e implementar las instrucciones proporcionadas en el capítulo 3, "Preparación del entorno". Asimismo, se recomienda leer también la información sobre el diseño y el planeamiento del capítulo 2, "Planeamiento de la implementación de seguridad en LAN inalámbricas" y tener un buen conocimiento de la arquitectura y el diseño de la solución.

Principio de la página

Preparación de la implementación

Permisos necesarios

Para llevar a cabo los procedimientos de este capítulo, debe iniciar sesión con una cuenta que pertenezca a los siguientes grupos:

- El grupo **Admins. del dominio** para el dominio en el que se va a instalar la entidad emisora.
- El grupo **Administradores de organización** del bosque de servicio de directorios de Microsoft Active Directory®.

De forma predeterminada, la cuenta de administrador integrada del dominio raíz del bosque (el primer dominio creado en el bosque) pertenece a ambos grupos, aunque puede utilizar cualquier otra cuenta que pertenezca a esos grupos.

Nota: si no instala la entidad emisora de certificados en el dominio raíz del bosque y el bosque es Windows 2000 Active Directory (o se ha actualizado desde Windows 2000 Active Directory), la cuenta utilizada para la instalación también tendrá que ser miembro del dominio raíz del bosque.

Herramientas necesarias

Necesita las siguientes herramientas para llevar a cabo los procedimientos de este capítulo.

Tabla 4.1. Herramientas necesarias para crear e instalar una entidad emisora de certificados

Herramienta	Descripción	Fuente
Herramientas de seguridad en WLAN de MSS	Conjunto de secuencias de comandos y herramientas que se incluyen en esta solución.	Los pasos de instalación se incluyen en el capítulo 3.

Consola de administración de directivas de grupo	Herramienta de administración avanzada para importar y exportar grupos de directiva de grupo.	Los pasos de instalación se incluyen en el capítulo 3. Se puede descargar de Microsoft.com.
CAPICOM	Biblioteca del sistema que permite ejecutar secuencias de comandos de operaciones de certificado y seguridad.	Los pasos de instalación se incluyen en el capítulo 3. Se puede descargar de Microsoft.com.
DSACLs.exe	Herramienta de línea de comandos, que permite establecer permisos en los objetos de Active Directory.	Los pasos de instalación se incluyen en el capítulo 3. Disponible como parte del CD de instalación de Windows Server 2003.
Usuarios y equipos de Active Directory	Herramienta de Microsoft Management Console (MMC) utilizada para administrar usuarios, grupos, equipos y otros objetos de Active Directory.	Instalado como parte de Windows Server 2003.
Herramienta administrativa de entidad emisora de certificados.	Una herramienta de MMC que se utiliza para administrar la entidad emisora.	Se instala como parte de la instalación de Servicios de Certificate Server en Windows Server 2003.

Parámetros de la entidad emisora de certificados

En la siguiente tabla se muestran los parámetros utilizados en la instalación y configuración de la entidad emisora en esta solución. Todos estos parámetros se definen en el archivo de secuencia de comandos PKIparams.vbs y se pueden modificar en él cuando sea necesario.

Tabla 4.2. Configuración de la entidad emisora de certificados utilizada en la solución

Parámetros de configuración de la entidad emisora	Valor de configuración
Unidad y ruta de acceso de los archivos de solicitud de Servicios de Certificate Server	C:\CAConfig
Longitud de clave de la entidad emisora	2048 bits
Período de validez del certificado de la entidad emisora	25 años
Período máximo de validez de los certificados emitidos por la entidad emisora	2 años
Intervalo de publicación de lista de revocación de certificados para la entidad emisora de certificados	7 días
Período de coincidencia de la lista de revocación de certificados (es decir, el tiempo transcurrido entre la publicación de una nueva lista de revocación de certificados y la fecha de caducidad de una lista de revocación de certificados antigua)	4 días
Publicación de diferencias entre listas de revocación de certificados desactivada	0
Plantillas de certificado disponibles en la entidad emisora	Equipo (máquina)

Nota: el período de validez de la entidad emisora de certificados se define con un valor grande para evitar la carga administrativa adicional que supone tener que renovar el certificado de la entidad emisora periódicamente. A diferencia de los certificados emitidos en equipos y usuarios, los certificados de la entidad emisora no se pueden renovar automáticamente y si no se renuevan antes de caducar, todos los certificados emitidos por la entidad emisora fallarán.

Importante: la configuración incluida en la tabla anterior se utilizó en las pruebas internas de esta solución y su funcionamiento está garantizado tal y como se describe. Muchos de estos valores se pueden modificar, pero sólo debería hacerlo si comprende perfectamente la finalidad de un valor de configuración concreto y lo que implicaría su modificación.

Principio de la página

Comprobación de la preparación para la instalación

Antes de instalar los Servicios de Certificate Server en el servidor, asegúrese de que se pueda conectar con el dominio y que se hayan instalado las herramientas necesarias.

Para comprobar el servidor antes de instalar la entidad emisora de certificados

1. Inicie una sesión en el servidor donde desee instalar la entidad emisora de certificados y la primera instancia del servidor IAS (utilizando una cuenta con los permisos administrativos adecuados).
2. Haga clic en el acceso directo **MSS WLAN Tools** para abrir el shell de comandos y, en el símbolo del sistema, escriba:

   MSSsetup CheckCAenvironment

   El nombre del dominio en el que se instala la entidad emisora de certificados aparece en formato de nombre distintivo (DN) (por ejemplo, dc=Treyresearch, dc=net), que es equivalente a un formato de sistema de nombres de dominio (DNS) (Treyresearch.net).
3. Si el nombre del dominio es correcto, haga clic en **Aceptar**. Si es incorrecto, haga clic en **Cancelar**, inicie una sesión en el dominio correcto y repita los pasos 1 y 2.

La secuencia de comandos comprueba que:

- Se puede conectar con el controlador de dominio de Active Directory.
- CAPICOM está instalado.
- GPMC está instalado.
- DSACLs.exe está instalado y se puede tener acceso a él.

Si se detecta algún problema, se le notifica con un error registrado en la ventana de la consola de la secuencia de comandos. Debe investigar y corregir este error antes de continuar.

Principio de la página

Instalación de Servicios de Certificate Server

En esta sección se describe la instalación de Servicios de Certificate Server para crear una entidad emisora de certificados. La entidad emisora de certificados se instala como una entidad emisora raíz de empresa.

Instalación de componentes de software de Servicios de Certificate Server

Debe instalar los componentes de software de la entidad emisora de certificados mediante la secuencia de comandos proporcionada. Esta secuencia de comandos utiliza el administrador de instalación de componentes opcionales de Windows para instalar la entidad emisora de certificados y crea todos los archivos de

configuración necesarios a medida que se ejecuta. Para realizar la instalación, utilice el CD de instalación de Windows Server 2003 (o la ruta de red del origen de instalación de Windows).

Precaución: si se ha instalado una entidad emisora de certificados anteriormente, o si intenta reinstalar la entidad emisora, debe eliminar primero la instalación existente. Antes de eliminar la entidad emisora, asegúrese de que no la esté utilizando ninguna otra aplicación.

Utilice **Agregar o quitar componentes de Windows** del subprograma **Agregar o quitar programas** en el **Panel de control** para eliminar los Servicios de Certificate Server.

Para instalar Servicios de Certificate Server

1. Utilice el acceso directo **MSS WLANTools** para abrir un shell de comandos.
2. En el símbolo del sistema, escriba lo siguiente para instalar los componentes de software de Servicios de Certificate Server:

   MSSsetup InstallCA y, a continuación, presione **ENTRAR**.
3. Cuando se le indique, escriba un nombre para la entidad emisora de certificados.

   El nombre debe ser descriptivo y exclusivo en la organización (por ejemplo, entidad emisora de certificados de red de investigación de Trey).
4. Para confirmar el nombre, haga clic en **Aceptar**.

   Para editar el nombre, haga clic en **No**.

   Para detener la instalación, haga clic en **Cancelar**.

   La secuencia de comandos creará los archivos de parámetros de instalación. Cuando finalice esta operación, se le solicitará que continúe con la instalación.
5. Haga clic en **Aceptar** para continuar o haga clic en **Cancelar** para detener la instalación.

   Nota: si cancela aquí la instalación, el archivo de configuración — CAPolicy.inf — y el archivo de parámetros de componentes opcionales — OC_CertSrv.txt — se dejarán en la carpeta Windows y en la carpeta de trabajo actual, respectivamente. Puede modificar estos archivos y utilizarlos en la instalación personalizada si no desea aceptar los valores predeterminados de la solución.
6. Cuando aparezca el mensaje de confirmación indicándole que la instalación ha finalizado, haga clic en **Aceptar**.

Comprobación de la instalación de la entidad emisora de certificados

Puede comprobar que la instalación de los Servicios de Certificate Server ha sido correcta mediante el siguiente procedimiento.

Para comprobar que la instalación de la entidad emisora de certificados es correcta

1. Utilice el acceso directo **MSS WLAN Tools** para abrir el shell de comandos.
2. En el símbolo del sistema, escriba:

   MSSsetup VerifyCAInstall y, a continuación, presione **ENTRAR**.

   El visor de certificados muestra el certificado de la entidad emisora.
3. Haga clic en la ficha **General** del certificado y compruebe que los valores coinciden con los de la siguiente tabla.

   Tabla 4.3. Propiedades de certificados de la entidad emisora

Atributo del certificado	Valor de configuración requerido
Emitido para	El nombre de la entidad emisora que se ha introducido durante la instalación.
Emitido por	El nombre de la entidad emisora que se ha introducido durante la instalación.
Válido de...a...	El intervalo que se especifica aquí debe ser de 25 años.

4. Haga clic en la ficha **Ruta de certificación** y compruebe que sólo aparece un certificado en el campo de ruta de certificación. El estado del certificado debe mostrar **El certificado es correcto**.

5. Haga clic en **Aceptar** para cerrar el visor de certificados.

Si alguno de los valores anteriores no es el que esperaba, debe volver a iniciar la instalación de los Servicios de Certificate Server.

Nota: si tiene que volver a ejecutar la instalación de la entidad emisora de certificados, debe eliminar primero los Servicios de Certificate Server instalados tal como se ha descrito anteriormente.

Principio de la página

Configuración de la entidad emisora

Una vez instalada la entidad emisora de certificados, debe ejecutar algunas secuencias de comandos adicionales para configurar los parámetros de la entidad emisora que quedan.

Configuración de las propiedades de la entidad emisora

Este procedimiento establece un número de parámetros en la entidad emisora de certificados que controlan su comportamiento. Algunos de estos parámetros se establecen durante la instalación de la entidad emisora, mientras que otros se deben establecer después de la instalación. Los valores de dichos parámetros se especifican en la sección "Parámetros de la entidad emisora de certificados" que aparece anteriormente en este capítulo. La secuencia de comandos utilizada en este procedimiento configura las propiedades de la entidad emisora, como se describe en la siguiente tabla.

Tabla 4.4. Propiedades de configuración de la entidad emisora de certificados

Propiedad de la entidad emisora	Descripción del valor de configuración
Direcciones URL de punto de distribución de la lista de revocación de certificados (CDP)	Especifica las ubicaciones desde las que se puede obtener una lista de revocación de certificados actual. En esta solución sólo se utiliza una dirección URL de Protocolo ligero de acceso a directorios (LDAP). Contiene la ruta de acceso LDAP de la lista de revocación de certificados publicada en Active Directory.
Direcciones URL de Acceso a la información de entidad emisora (AIA)	Indica la ubicación desde la que se puede obtener un certificado de la entidad emisora. Como ocurre con el CDP, sólo se utiliza la dirección URL de LDAP que apunta a Active Directory.
Período de validez	Indica el período de validez máximo de los certificados emitidos (no es el mismo que el período de validez del certificado de entidad emisora, que se establece durante la instalación).
Período de la lista de revocación de certificados	Indica la frecuencia de publicación de la lista de revocación de certificados.
Período de coincidencia de la lista de revocación de	Indica el período de coincidencia entre la emisión de una nueva lista de revocación de certificados y la caducidad de la lista de revocación de

certificados	certificados anterior.
Período de diferencia entre listas de revocación de certificados	Indica la frecuencia de publicación de diferencias entre listas de revocación de certificados. (En esta entidad emisora de certificados, la diferencia entre listas de revocación de certificados está deshabilitada.)
Auditoría de la entidad emisora	Indica la configuración de auditoría de la entidad emisora de certificados. (Toda la auditoría está habilitada de manera predeterminada.)

Nota: muchos de estos parámetros afectan a la configuración de la lista de revocación de certificados de la entidad emisora de certificados. Una lista de revocación de certificados es una lista de certificados que ha emitido la entidad emisora pero que el administrador ha cancelado (o revocado) posteriormente. Aunque probablemente no necesitará revocar ningún certificado durante la administración de esta solución, muchas aplicaciones se basan en la capacidad de leer una lista de revocación de certificados actual para comprobar el estado de revocación de un certificado (aunque la lista de revocación de certificados esté vacía). Si la aplicación no puede encontrar una lista de revocación de certificados, puede rechazar el certificado.

Para configurar las propiedades de la entidad emisora de certificados

1. Utilice el acceso directo **MSS WLAN Tools** para abrir el shell de comandos.
2. En el símbolo del sistema, escriba lo siguiente para configurar los componentes de la entidad emisora:

   MSSsetup ConfigureCA y, a continuación, presione **ENTRAR**.

   Durante la configuración, la secuencia de comandos se detiene durante 20 segundos para esperar a que termine una tarea en la entidad emisora de certificados. No es necesario responder los mensajes emergentes que anuncian este retraso.
3. Haga clic en **Aceptar** para descartar este mensaje.

Si la secuencia de comandos informa de un error, investigue el motivo mediante un seguimiento del archivo de registro (%systemroot%\debug\MSSWLAN-Setup.log) y vuelva a ejecutar la secuencia de comandos después de corregir el problema.

Nota: puede volver a ejecutar esta secuencia de comandos de configuración las veces que sea necesario.

Importación del objeto de directiva de grupo de la solicitud de certificados automática

Este procedimiento importa el objeto de directiva de grupo de la directiva de inscripción automática de certificados IAS preconfigurado para permitir la emisión automática de certificados en los servidores IAS del dominio. Utiliza el servicio de solicitud de certificados automática (ACRS).

El ACRS no se debe confundir con las posibilidades de inscripción automática de Windows Server 2003, Enterprise Edition, aunque ambos realizan funciones parecidas. Es un servicio más limitado que la inscripción automática y ya se utilizó antes en Windows 2000. Sólo permite inscribir certificados de *equipo* (no de usuario) y sólo funciona con las plantillas de certificado de la versión 1. No obstante, el ACRS es adecuado para el uso limitado de certificados de esta solución y permite instalar la entidad emisora en la Standard Edition de Windows Server 2003 (más económica).

Importante: si hay varios dominios en el bosque de Active Directory, deberá repetir este procedimiento para cada dominio en el que instale un servidor IAS.

La secuencia de comandos que se utiliza en el siguiente procedimiento importa un objeto de directiva de grupo preconfigurado con una directiva para inscribir automáticamente los certificados. El objeto de directiva de grupo especifica el tipo de certificado "Equipo" predefinido como el tipo de la inscripción. A continuación, la secuencia de comandos aplica permisos de seguridad al objeto de directiva de grupo para que sólo afecte a los miembros del grupo de servidores IAS y RAS (el valor de configuración predeterminado es aplicar el objeto de directiva de

grupo a todos los usuarios y equipos autenticados).

Nota: en algunos contextos, la plantilla de certificado Equipo se denomina plantilla Máquina. "Máquina" es el nombre interno de la plantilla, mientras que "Equipo" es el nombre de visualización.

Para instalar en su dominio el objeto de directiva de grupo de la solicitud de certificados automática

1. Utilice el acceso directo **MSS WLAN Tools** para abrir el shell de comandos.
2. En el símbolo del sistema, escriba lo siguiente para importar en el dominio el objeto de directiva de grupo de la directiva de inscripción automática de certificados IAS:

   MSSsetup ImportAutoenrollGPO y, a continuación, presione **ENTRAR**.

A continuación, vincule este objeto de directiva de grupo con el dominio para que se aplique la configuración del objeto de directiva de grupo a los servidores IAS. Éste es el procedimiento manual que permite controlar el proceso de vinculación del objeto de directiva de grupo. La automatización de este paso supone el riesgo de sobrescribir la configuración de vínculos del objeto de directiva de grupo existente del dominio.

Para aplicar el objeto de directiva de grupo de la solicitud de certificados automática

1. Haga clic en **Inicio**, **Todos los programas**, **Herramientas administrativas** y, a continuación, en **Administración de directiva de grupo** para iniciar la **GPMC**.
2. En el panel izquierdo de la **GPMC**, desplácese hasta el objeto de dominio correspondiente a su dominio.

   El objeto de dominio se encuentra en el contenedor de **Dominios** de nivel superior y tiene el mismo nombre que el nombre DNS del dominio.
3. Haga clic con el botón secundario en el objeto de domino y, a continuación, seleccione **Vincular objeto de directiva de grupo existente**.
4. En la lista de objetos de directiva de grupo, seleccione **Directiva de inscripción automática de certificados IAS**.
5. Haga clic en **Aceptar** para volver a ejecutar la ventana principal de la **GPMC**.
6. En el panel derecho, haga clic en la ficha **Objetos de directiva de grupo vinculados** y, a continuación, seleccione **Directiva de inscripción automática de certificados IAS**.
7. Cierre la **GPMC**.

   La configuración de la solicitud de certificados automática se aplicará a los servidores sólo si han sido agregado como miembros del grupo de servidores IAS y RAS. Este asunto se tratará en un procedimiento del siguiente capítulo.

   Importante: si el dominio está en modo mixto y está instalando IAS en los servidores miembros (en lugar de en los controladores de dominio), el grupo local de servidores IAS y RAS no estará visible en los servidores miembros. Esto impide que el objeto de directiva de grupo de ACRS se aplique a estos servidores y detenga la inscripción de certificados de estos servidores. Para evitarlo, cree un grupo global de dominio, agregue a este grupo las cuentas de servidores miembros IAS y agregue el grupo a la lista de control de acceso (ACL) del objeto de directiva de grupo, otorgándole los permisos de **Aplicación** y **Lectura**.

Comprobación de la configuración de la entidad emisora

El siguiente procedimiento confirma que ha configurado correctamente la entidad emisora de certificados. La secuencia de comandos comprueba que:

- La entidad emisora de certificados tiene el período de validez correcto (para los certificados emitidos).
- El período de publicación de la lista de revocación de certificados es el correcto.

- La entidad emisora de certificados tiene la plantilla de certificado Equipo asignada.
- El objeto de directiva de grupo de la solicitud de certificados automática (inscripción automática) se ha importado correctamente al dominio.

Estos valores se comparan con la configuración almacenada en el archivo PKIParams.vbs. La secuencia de comandos no comprueba valores absolutos; sólo comprueba si la configuración se ha establecido correctamente en la entidad emisora de certificados.

Para comprobar la configuración de la entidad emisora de certificados

1. Utilice el acceso directo **MSS WLAN Tools** para abrir el shell de comandos.
2. En el símbolo del sistema, escriba lo siguiente para configurar los componentes de la entidad emisora:

   MSSsetup VerifyCAConfig y, a continuación, presione **ENTRAR**.

Si la salida de la secuencia de comandos muestra errores, debe revisar los pasos de este capítulo y rectificar los problemas indicados.

Principio de la página

Resumen

Este capítulo sirve de guía en el proceso de instalación de una entidad emisora de propósito específico para emitir certificados de servidor en servidores IAS. La configuración de la entidad emisora utilizada está diseñada para necesitar muy poco mantenimiento, por lo que necesitará una administración mínima en el futuro. No obstante, la información operativa y de soporte que necesite se incluye en el capítulo 8, "Mantenimiento de soluciones de seguridad en LAN inalámbricas".

Está listo para instalar los servidores IAS. Esto se describe en el capítulo 5, "Creación de la infraestructura de seguridad en LAN inalámbricas".

Principio de la página

Referencias

Esta sección ofrece referencias a otra información complementaria importante u otro material informativo de relevancia para el contenido de este capítulo.

- Si desea una introducción a los conceptos de la infraestructura de claves públicas y las características de Servicios de Certificate Server de Windows 2000, consulte el documento "An Introduction to the Windows 2000 Public-Key Infrastructure" que hay disponible en la siguiente dirección URL:

  http://www.microsoft.com/technet/prodtechnol/windows2000serv/evaluate/featfunc/pkiintro.mspx

- Si desea una introducción a los conceptos de la infraestructura de claves públicas y las características de Servicios de Certificate Server de Windows 2000, consulte el documento "An Introduction to the Windows 2000 Public-Key Infrastructure" que hay disponible en la siguiente dirección URL:

  http://www.microsoft.com/windowsxp/pro/techinfo/planning/pkiwinxp/default.asp

- Para obtener la documentación del producto que describe los conceptos clave y las tareas de administración, consulte la sección "Servicios de Certificate Server" en la documentación del producto Windows Server 2003 que hay disponible en la siguiente dirección URL:

  http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/standard/SE_PKI.mspx

- Para obtener información sobre cómo obtener y utilizar los certificados de una entidad emisora comercial, consulte el artículo "Obtaining and Installing a VeriSign WLAN Server Certificate for PEAP-MS-CHAP v2

Wireless Authentication", que hay disponible en la siguiente dirección URL:

http://download.microsoft.com/download/9/f/d/9fd73f17-2fdf-4409-b2d2-31437c7f29f3/WLANCertEnroll.doc

(Este artículo contiene referencias a guías de otros productos y vínculos a sitios Web que sólo están disponibles en inglés.)

Principio de la página

Administre su perfil