

answers²

Manual del usuario

Wireless LAN

Español



FUJITSU COMPUTERS
SIEMENS

Dieses Handbuch wurde auf Recycling-Papier gedruckt.
This manual has been printed on recycled paper.
Ce manuel est imprimé sur du papier recyclé.
Este manual ha sido impreso en papel reciclado.
Questo manuale è stato stampato su carta da riciclaggio.
Denna handbok är tryckt på recyclingpapper.
Dit handboek werd op recycling-papier gedrukt.

Publicado por/Published by
Fujitsu Siemens Computers GmbH

Nº de pedido/Order No.: **A26391-K133-Z131-1-7819**

Edición **3**

Printed in the Federal Republic of Germany

AG 0704 07/04

Wireless LAN

Manual del usuario

Generalidades Wireless
LAN

Instalación de Odyssey

Empleo de Odyssey
Client

Índice de materias

Microsoft, MS, MS-DOS, Windows y Windows NT son marcas registradas de Microsoft Corporation.

Odyssey es una marca comercial registrada de software de radiotransmisión

Todas las demás marcas mencionadas son marcas o marcas registradas de los respectivos propietarios y son consideradas como protegidas.

Copyright © Fujitsu Siemens Computers GmbH 2004

La divulgación y reproducción de este documento, así como el aprovechamiento de su contenido no están autorizados, a no ser que se obtenga el consentimiento expreso para ello.

Los infractores quedan obligados a la compensación por daños y perjuicios.

Reservados todos los derechos, en particular para el caso de concesión de patente o de modelo de utilidad.

Reservada la posibilidad de suministro y de modificaciones técnicas.

Este manual ha sido elaborado por
cognitas. Gesellschaft für Technik-Dokumentation mbH
www.cognitas.de

Contenido

Generalidades Wireless LAN	1
Red inalámbrica según la norma IEEE 802.11	1
Modo adhoc	2
Modo de infraestructura	2
Sistemas operativos que reúnen los requisitos indispensables	2
Nombres para redes inalámbricas (SSID)	3
Seguridad de red 802.11	3
Wired-Equivalent Privacy (WEP) con claves preconfiguradas	4
Wi-Fi Protected Access (WPA) y codificación TKIP	4
Estándar 802.1X	5
Extensible Authentication Protocol (EAP)	5
Indicaciones importantes	6
Indicaciones de seguridad	6
Marcado CE	6
Frecuencias de transmisión y normas de seguridad	7
Instalación de Odyssey	9
Instalar Odyssey Client	9
Configure and Enable Wizard	10
Empleo de Odyssey Client	11
Vista general del Odyssey Client Manager	11
Pantalla Odyssey Client Manager	12
Controlar las conexiones de red – Ventana "Connection"	12
Seleccionar tarjeta de red	13
Conectar con una red	13
Buscar redes inalámbricas	13
Conectar de nuevo con una red	15
Reautenticar en la red	15
Desconectar la conexión de red	15
Visualizar datos de conexión	15
Definir perfiles – Ventana "Profiles"	16
Añadir o modificar un perfil – Ventana "Profile Properties"	17
Ficha "Authentication"	20
Configurar las redes inalámbricas – Ventana "Networks"	27
Añadir o modificar redes – Ventana "Network Properties"	28
Especificar servidores fiables - Ventana "Trusted Servers"	34
Procedimiento sencillo para la configuración de servidores Trusted	35
Procedimiento avanzado para la configuración de servidores Trusted	37
Untrusted Server	42
Configurar tarjetas de red – Ventana "Adapters"	43
Añadir tarjeta de red inalámbrica	44
Eliminar tarjeta de red de la lista	45
Odyssey Client Manager - Menú "Settings"	46
Opción de menú "Preferences"	46
Opción de menú "Security settings"	47
Opción de menú "Enable/Disable Odyssey"	49
Opción de menú "Close"	49
Odyssey Client Manager - Menú "Commands"	49
Opción de menú "Forget Password"	50
Opción de menú "Forget Temporary Trust"	50

Contenido

Odyssey Client Manager - Menú "Help" 50

 Opción de menú "Help topics" 50

 Opción de menú "License keys" 51

Menú de contexto "Odyssey" 51

 Opción de menú "Odyssey for Fujitsu Siemens Computers" 51

 Opción de menú "Enable Odyssey/Disable Odyssey" 51

 Opción de menú "Help" 52

 Opción de menú "Exit" 52

Features 53

Overview 53

Technical details 54

Declaration of Conformity 57

Índice de materias..... 59

Generalidades Wireless LAN

En su equipo está integrada una tarjeta de red inalámbrica. En este manual de usuario se describe cómo debe realizar usted los ajustes para su Wireless LAN.

Convenciones

En este manual se han seguido determinadas convenciones tipográficas que se definen a continuación.



Identifica indicaciones que debe tener Ud. en cuenta. Si no las observa, puede poner en peligro su vida, deteriorar el equipo o sufrir una pérdida de datos. La garantía vencerá, si daña Ud. el equipo por no observar estas indicaciones.



destaca información importante para el correcto manejo del equipo.

► señala una operación que debe Ud. realizar.

Los textos en escritura mecanográfica representan visualizaciones en la pantalla.

Con *letra cursiva* se han caracterizado nombres de programas, instrucciones y opciones de menú.

Las "comillas" identifican los títulos de los capítulos, nombres de disquetes y otros nombres de medios y conceptos individuales que deben ser resaltados.

Red inalámbrica según la norma IEEE 802.11

La tarjeta de red integrada trabaja según el estándar IEEE 802.11. Como medio de comunicación se utilizarán las frecuencias de las bandas de frecuencias ISM (ISM, Industrial, Scientific, Medical). La tarjeta de red inalámbrica puede utilizarse sin registrarse y libre de impuestos. El estándar IEEE 802.11 contempla más posibilidades para aprovechar las bandas de frecuencia ISM:

IEEE 802.11a	Banda de 5,0-GHz	54 Mbps
IEEE 802.11b	Banda de 2,4-GHz	11 Mbps
IEEE 802.11g	Banda de 2,4-GHz	54 Mbps

Las redes inalámbricas que funcionan según la norma 802.11 permiten conectarse fácilmente con las redes Ethernet existentes. Las tarjetas de red inalámbrica que funcionan según la norma 802.11, salvo unos cuantos parámetros adicionales, conforman un sistema con una tarjeta Ethernet normal. Es decir, que en una red inalámbrica 802.11 podrá utilizar todos los protocolos como si fuese una Ethernet conectada por cable (IP, IPX, NetBIOS,...). La única diferencia es que no necesita tender ningún cable entre los equipos. Las estaciones LAN inalámbricas que pueden comunicarse directamente forman una célula de radio. El estándar IEEE ofrece dos tipos de funcionamiento, el modo *ad hoc* (Peer-to-Peer) y el modo de infraestructura.

Además de la descripción de la modulación y del Data Framing esta norma contiene un procedimiento de autenticación y codificación con la denominación Wired Equivalent Privacy (WEP). Muchas empresas aplican redes inalámbricas 802.11. Las redes inalámbricas 802.11 ahora también se pueden encontrar en hoteles, en aeropuertos y en otros "hotspots" con acceso a Internet.

Modo adhoc

Una red local inalámbrica en modo adhoc, también llamado modo Peer-to-Peer, se compone de una única célula de radio aislada. Se crean redes inalámbricas Adhoc, cuando concurre un grupo de trabajo con sus equipos y los quiere conectar entre sí para el intercambio de datos. Los equipos podrán acceder y abandonar tal tipo de red en cualquier momento.

Para que varias redes inalámbricas Adhoc no se interfieran, existe un nombre de red unívoco llamado SSID (Service Set Identifier). El SSID se utiliza para el direccionamiento, de modo que un paquete de datos siempre se pueda asignar a una determinada célula de radio.

Cuando quiera acceder a una red inalámbrica vigente, necesitará el nombre de red (SSID), el cual registrará en los ajustes para la tarjeta de red. La tarjeta de red busca entonces durante el inicio una red de radio con este SSID. Cuando la tarjeta de red encuentra una red inalámbrica, ésta se registra en ésta y Ud. podrá comunicar con los equipos en esta red inalámbrica. Cuando dos células de radio se encuentren muy cerca entre ellas, los canales de radio de esta red deberían separarse entre ellos de 4 a 5 canales. Esto es válido para el protocolo 802.11b y 802.11g.

Modo de infraestructura

En el modo de infraestructura existe, junto a las estaciones móviles, una estación base que se denomina AccessPoint (punto de acceso). En el modo de infraestructura, el punto de acceso (AccessPoint) adopta la función de un "vigilante". Al contrario que en el modo adhoc, cada equipo tendrá que darse de alta en el punto de acceso (AccessPoint), antes de poder intercambiar datos en la célula de radio.

Otra función del punto de acceso (AccessPoint) es la conexión de la célula de radio con una red Ethernet conectada por cable. Puesto que el punto de acceso (AccessPoint), por medio de la obligación de darse de alta, sabe exactamente y en cualquier momento las estaciones que se encuentran en la red, podrá decidir exactamente los datos que deben transferirse y los que no. Este proceso también se denomina como Bridging.

Para ampliar el alcance de una red de radio, podrán utilizarse varios puntos de acceso (AccessPoints) con el mismo SSID.

Si entra un equipo en la red inalámbrica, examinará entre los puntos de acceso (AccessPoints) accesibles los que cuenten con la señal más fuerte y se registrará en ese punto. De esta forma, dos equipos que se encuentran fuera de alcance de radio el uno del otro y que se han dado de alta en diferentes puntos de acceso (AccessPoints), pueden comunicarse a través de éstos. Después de darse alta en un punto de acceso (AccessPoint), el equipo vigila las señales de los otros puntos de acceso, pudiendo registrarse en otro punto de acceso con una señal más fuerte de modo transparente para el usuario. Este proceso se denomina itinerancia.

Sistemas operativos que reúnen los requisitos indispensables

Sistema operativo Windows 2000 y Windows XP

Nombres para redes inalámbricas (SSID)

Cada red inalámbrica dispone de su propio nombre. Usted puede seleccionar la red a la que usted desea conectarse por su propio nombre. Los nombres de red posibilitan el servicio simultáneo de varias redes inalámbricas en coexistencia en el mismo entorno sin que estas se interfieran mutuamente. Cuando por ejemplo la empresa al lado suyo utiliza igualmente redes inalámbricas, usted quiere asegurarse que su ordenador está conectado con la red de su empresa y no con la otra, incluso cuando su ordenador esté situado en la zona del punto de acceso (AccessPoint) colindante. (Cómo impedir que personas ajenas accedan a su red corporativa, es objeto de la siguiente discusión de seguridad.) Un nombre de red es sencillamente una secuencia de un máximo de 32 caracteres, como p. ej. "Bayonne Office" o "Acme-Marketronics" o "BE45789". Para nombres de redes tiene vigor la escritura en mayúscula o en minúscula, por ello usted deberá ser cuidadoso al introducir el nombre. Sin embargo usted tiene la libertad de seleccionar nombres de redes ya disponibles. Si usted selecciona la red de una lista se evitan fallos al introducir el nombre de red. La norma 802.11 determina nombres de red como por ejemplo el "Service Set Identifier" (SSID).

Seguridad de red 802.11

Desde la aparición de las redes inalámbricas la seguridad juega un papel crítico mucho mayor que antes, por la simple razón de que para los intrusos es más sencillo interceptar estas conexiones. En las redes conectadas por cables, la mayoría de las empresas pueden asegurar la protección de su red por medio de dispositivos técnicos. Un agresor debería llegar hasta los locales de la empresa para poder conectarse en la LAN para espiar el tráfico de la red.

Todo lo que se necesita para poder acceder a datos en una red inalámbrica, es un ordenador con una tarjeta de red inalámbrica y un lugar apropiado en el exterior en el aparcamiento o en la oficina. A continuación se describen algunas condiciones para una interconexión en red segura.

- Un usuario deberá ser autenticado por la red, antes de concederle el acceso a la misma; con ello la red quede a salvo de intrusos.
- La red deberá ser autenticada por el usuario, antes de que su ordenador establezca la conexión con la red. De este modo se evita que un dispositivo de radiocomunicación se identifique como una red legítima y reciba acceso al ordenador del usuario.
- La autenticación recíproca entre el usuario y la red debe ser protegida criptográficamente. Con ello se asegura que usted se conecte con la red deseada y no con una errónea.
- La conexión de red entre un ordenador y el punto de acceso (AccessPoint) debe estar codificada de tal forma que los intrusos no reciban acceso a los datos confidenciales.

Para este tipo de codificaciones seguras a través de una red inalámbrica hay dos mecanismos fundamentales:

- Indicaciones preconfiguradas secretas denominadas como clave WEP. Las claves WEP mantienen alejados de la red inalámbrica a usuarios no autorizados y codifican los datos del usuario legítimo.
- Autenticación con ayuda de un protocolo 802.1X. Aquí se utilizan múltiples protocolos de autenticación tomados como base para el control de acceso a la red. Los protocolos más fuertes de ellos pueden asegurar una autenticación recíproca de usuario y red y pueden generar claves de forma dinámica para la codificación de los datos de radio.

Wired-Equivalent Privacy (WEP) con claves preconfiguradas

Con claves WEP preconfiguradas (Wired-Equivalent Privacy) se asigna al ordenador cliente, así como al punto de acceso (AccessPoint) la misma clave secreta. Esta clave se utiliza para codificar todos los datos intercambiados entre el ordenador y el punto de acceso (AccessPoint).

Adicionalmente la clave WEP puede ser utilizada para la autenticación del ordenador cliente en el punto de acceso (AccessPoint). En caso de que el ordenador no pueda demostrar que conoce la clave WEP, se le deniega el acceso a la red.

- Si el punto de acceso (AccessPoint) requiere una clave WEP para la autenticación, deberá realizar la asignación al punto de acceso (AccessPoint) en el modo Shared. El modo de asignación se configura en las propiedades de red.
- Si el punto de acceso (AccessPoint) no requiere clave WEP para la autenticación, esto se denominará modo abierto (open). El modo de asignación se configura en las propiedades de red.
- Si el punto de acceso (AccessPoint) requiere una codificación WEP para WPA en lugar de TKIP para la autenticación, todas las claves WEP necesarias serán generadas a partir de una frase de acceso ASCII que usted configurará tanto para su punto de acceso (AccessPoint) como para Odyssey Client.

Véanse los siguientes temas:

- "Indicar el modo de asignación", con instrucción para la selección de un modo de asignación en Odyssey Client
- "Indicar un procedimiento de codificación adecuado para su modo de asignación", con instrucción para la selección de la codificación WEP en el modo Shared
- "Clave preconfigurada (WEP)", para la utilización de claves WEP estáticas en Odyssey Client
- "Claves Pre-shared (WPA)", para configurar la codificación WEP en el modo WPA

Wi-Fi Protected Access (WPA) y codificación TKIP

Como extensión de la norma 802.11 el Wi-Fi Protected Access (WPA) comprende una serie de suplementos de seguridad más allá del Wired-Equivalent Privacy. Estas extensiones contienen lo siguiente:

- Codificación de datos mejorada a través de TKIP (protocolo temporal de integridad de clave) TKIP ofrece una codificación de más alto rendimiento que WEP, ya que las claves se actualizan de forma dinámica después de cada 10.000 paquetes.
- Autenticación 802.1X con EAP. Cuando el hardware del punto de acceso (AccessPoints) en su red exige que usted realice la autenticación a través del modo WPA extendido, usted puede configurar el Odyssey Client de forma que la autenticación se produzca en el modo WPA. En el caso de que el hardware esté configurado para la codificación TKIP, usted puede configurar también el Odyssey Client para este procedimiento de codificación extendido. Además de la conformidad con la especificación 802.1X para la generación dinámica de claves (disponible con los métodos de autenticación más potentes), WPA permite la generación de claves Pre-shared para la codificación TKIP (o WEP) por medio de una frase de acceso. Si usted configura una frase de acceso para la generación de claves en sus puntos de acceso (AccessPoints), deberá configurar la misma frase de acceso en el Odyssey Client.

Véanse los siguientes temas:

- "Indicar el modo de asignación", para la aplicación del modo WPA en Odyssey Client
- "Indicar un procedimiento de codificación adecuado para su modo de asignación", para la aplicación de la codificación TKIP en el modo WPA
- "Claves Pre-shared (WPA)" para configurar una frase de acceso estática

Estándar 802.1X

El protocolo IEEE 802.1X posibilita el acceso autenticado a una LAN. Esta norma sirve tanto para redes inalámbricas como para redes conectadas por cable. En la red inalámbrica la autenticación 802.1X se realiza después de que la asignación 802.11 esté implementada. Las redes conectadas por cable utilizan la norma 802.1X sin asignación 802.11.

El protocolo WEP, que utiliza claves preconfiguradas, muestra diferentes deficiencias con respecto a una administración sencilla, así como en materia de seguridad. Para solucionar estos problemas, IEEE ha introducido una norma adicional: 802.1X. 802.1X ofrece una mejor seguridad que la clave WEP preconfigurada y es sencilla de manejar, especialmente en el caso de grandes redes.

Al aplicar la clave preconfigurada WEP el ordenador cliente inalámbrico es autenticado frente a la red. En el caso de la 802.1X el usuario es autenticado frente a la red con las certificaciones de autorización (contraseña, certificado o tarjeta Token) La autenticación no es realizada por el punto de acceso (AccessPoint), sino más bien a través de un servidor central. En el caso de que este servidor emplee el protocolo RADIUS, es denominado como servidor RADIUS.

En el caso de la 802.1X un usuario puede registrarse en la red de cada ordenador, y muchos puntos de acceso (AccessPoints) pueden utilizar conjuntamente un único servidor RADIUS para la autenticación. De este modo es mucho más fácil para el administrador de red controlar el acceso a la red.

Puede obtener más detalles en los siguientes temas:

- Protocolo EAP (Extensible Authentication Protocol)
- Reanudación de una sesión (Session resumption)
- Reautenticación (Reauthentication)

Extensible Authentication Protocol (EAP)

802.1X utiliza el protocolo con la denominación EAP (Extensible Authentication Protocol) para realizar la autenticación. EAP no es ningún mecanismo de autenticación en sí, sino un marco común para el transporte de los protocolos de autenticación más actuales. La ventaja del protocolo EAP es que el mecanismo EAP fundamental no debe ser modificado en el desarrollo de nuevos protocolos de autenticación.

Indicaciones importantes

Indicaciones de seguridad

En el manual "Primeros pasos" de su equipo encontrará la mayoría de las indicaciones de seguridad. Encontrará alguna de las principales indicaciones de seguridad en el siguiente texto.

- Desconecte el módulo de radio (Bluetooth o Wireless LAN) en el equipo siempre que se encuentre en un hospital, una sala de operaciones o en la proximidad de equipos médicos electrónicos. La transmisión de ondas de radio pueden afectar la función de los equipos médicos.

En el manual "EasyGuide", que se suministra con el equipo, se describe cómo apagar el módulo de radio.

- Mantenga el equipo alejado al menos a 20 cm de un marcapasos, ya que las ondas radioeléctricas pueden impedir el correcto funcionamiento del marcapasos.
- Las ondas de radio transmitidas podrán provocar un zumbido desagradable en prótesis auditivas.
- Apague el equipo cuando se encuentre en un avión o viaje con el coche.
- No exponga el equipo con el módulo de radio conectado a gases inflamables o en un entorno con riesgo de explosión (p. ej., un taller de barnizado), ya que las ondas de radio transmitidas pueden originar una explosión o un incendio.

La empresa Fujitsu Siemens Computers GmbH no se hace responsable de las interferencias de televisión o de radio que sean provocadas por modificaciones no autorizadas de este equipo. Fujitsu Siemens no aceptará además ninguna responsabilidad para la sustitución o el repuesto de cables de conexión y dispositivos no facilitados por parte de Fujitsu Siemens Computers GmbH. El usuario es el único responsable ante la eliminación de interferencias provocadas por una modificación no autorizada y por la sustitución o el intercambio de los equipos.

Marcado CE



Este equipo, en la versión suministrada, cumple con los requisitos de la directiva 1999/5/EG del Parlamento Europeo y del Consejo del 9. de marzo de 1999 sobre instalaciones de radio e de telecomunicación, así como con el mutuo reconocimiento de la conformidad.

Este dispositivo puede utilizarse en Alemania, Austria, Bélgica, Dinamarca, España, Finlandia, Francia, Grecia, Gran Bretaña, Irlanda, Islandia, Italia, Liechtenstein, Luxemburgo, Noruega, Países Bajos, Portugal, Suecia y Suiza. Podrá obtener información actualizada sobre posibles limitaciones en su funcionamiento en los organismos correspondientes de los respectivos países. En el caso de que su país no sea uno de la lista, diríjase a la correspondiente autoridad competente para comprobar si está permitida la utilización de este producto.

Restricciones

- Francia
 - Margen de frecuencias limitado: en Francia solo pueden utilizarse los canales 10 a 13 (2457 MHz a 2472 MHz). No está permitido emplear el dispositivo al aire libre.
- Italia
 - Para el uso en el área interior se necesita también un permiso de las autoridades. Debido al procedimiento necesario para ello, póngase en contacto con el vendedor. No está permitido emplear el dispositivo al aire libre.
- Holanda
 - Para el uso al aire libre se necesita obligatoriamente una licencia. Debido al procedimiento necesario para ello, póngase en contacto con el vendedor.

Frecuencias de transmisión y normas de seguridad

La siguiente información está actualizada a enero de 2002. Las autoridades correspondientes de su país (p. ej., www.cmt.es) podrán facilitarle información más actualizada.

Frecuencias del estándar IEEE-802.11a

País	Canal 36 5180 MHz	Canal 40 5200 MHz	Canal 44 5220 MHz	Canal 48 5240 MHz	Canal 52 5260 MHz	Canal 56 5280 MHz	Canal 60 5300 MHz	Canal 64 5320 MHz
Austria	X	X	X	X				
Bélgica	X	X	X	X	X	X	X	X
Dinamarca	X	X	X	X				
Finlandia	X	X	X	X	X	X	X	X
Francia	X	X	X	X				
Alemania	X	X	X	X				
Grecia								
Italia								
Irlanda	X	X	X	X	X	X	X	X
Luxemburgo								
Holanda	X	X	X	X				
Noruega	X	X	X	X				
Portugal	X	X	X	X				
España								
Suecia	X	X	X	X				
Suiza	X	X	X	X				
Gran Bretaña	X	X	X	X	X	X	X	X

Frecuencias estándar IEEE 802.11b (11 Mbits/s) / 802.11g (54 Mbits/s)

Las tarjetas de red inalámbrica y los adaptadores están preparados, según la norma IEEE 802.11b, para trabajar en la banda de frecuencias ISM (Industrial, Scientific, Medical = industrial, científica, médica) entre 2,4 y 2,4835 GHz. El procedimiento DSSS (Direct Sequence Spread Spectrum) utilizado para la transmisión requiere un ancho de banda de 22 MHz en cada uno de los 13 canales de radio disponibles, con lo que se podrá contar con un máximo de tres canales simultáneos independientes entre sí (p. ej., 1, 6, y 11). En las siguientes tablas encontrará los canales permitidos en su país:

Nº de canal / MHz	Europa, R&TTE	Francia, R&TTE	EE. UU. FCC	CA RSS-210
1 / 2412	X		X	X
2 / 2417	X		X	X
3 / 2422	X		X	X
4 / 2427	X		X	X
5 / 2432	X		X	X
6 / 2437	X		X	X
7 / 2442	X		X	X
8 / 2447	X		X	X
9 / 2452	X		X	X
10 / 2457	X	X	X	X
11 / 2462	X	X	X	X
12 / 2467	X	X		
13 / 2472	X	X		

Instalación de Odyssey

El software de instalación para Odyssey Client se encuentra en el directorio C:\Add on\Software.

Antes de la instalación tenga en cuenta lo siguiente:

- Su tarjeta de red para red inalámbrica, así como el correspondiente software de controlador ya tienen que estar instalados.
- En Windows 2000 y Windows XP deberá disponer de derechos de administrador.

Instalar Odyssey Client

Para instalar Odyssey Client:

- ▶ Haga doble clic en el archivo *FSC-OdysseyClient.msi* en el directorio C:\Add on\Software.

Se activará el asistente de instalación para guiarle a través del proceso de instalación.

- ▶ Haga clic en *Next* para continuar.

Se mostrarán las condiciones de licencia.

- ▶ Marque en la opción *I accept the terms in the license agreement* para aceptar las condiciones de licencia y haga clic en *Next* para continuar.
- ▶ Introduzca los datos de usuario y haga clic en *Next* para continuar.
- ▶ En la ventana *Setup Type* seleccione la opción *Complete* para ejecutar la instalación en el directorio estándar. Seleccione la opción *Custom* si desea especificar su propio directorio de instalación. Esta opción sólo deberá ser utilizada por usuarios expertos. Haga clic en *Next* para continuar.

El asistente de instalación dispone ahora de toda la información necesaria para proceder con la instalación.

- ▶ Haga clic en *Back* si desea verificar o modificar sus datos y haga clic en *Install* para iniciar la instalación.

Se inicia la instalación. El proceso puede durar algunos minutos. Una vez concluida la instalación aparecerá la ventana *InstallShield Wizard Completed*. Podrá activar directamente Odyssey Client o abrir primero el archivo Readme.

- ▶ Haga clic en *Finish* para completar la instalación.

En un ordenador con varias cuentas de usuario, Odyssey Client estará disponible para todos los usuarios después de la instalación. Sin embargo, los ajustes para el control de funcionamiento de Odyssey Client son específicos para cada usuario y deberán ser determinados individualmente para cada cuenta de usuario.

Configure and Enable Wizard

Cuando instale Odyssey Client por primera vez, aparecerá automáticamente después de la instalación el asistente *Configure and Enable Wizard* para proceder a continuación con la configuración y activación de Odyssey Client.

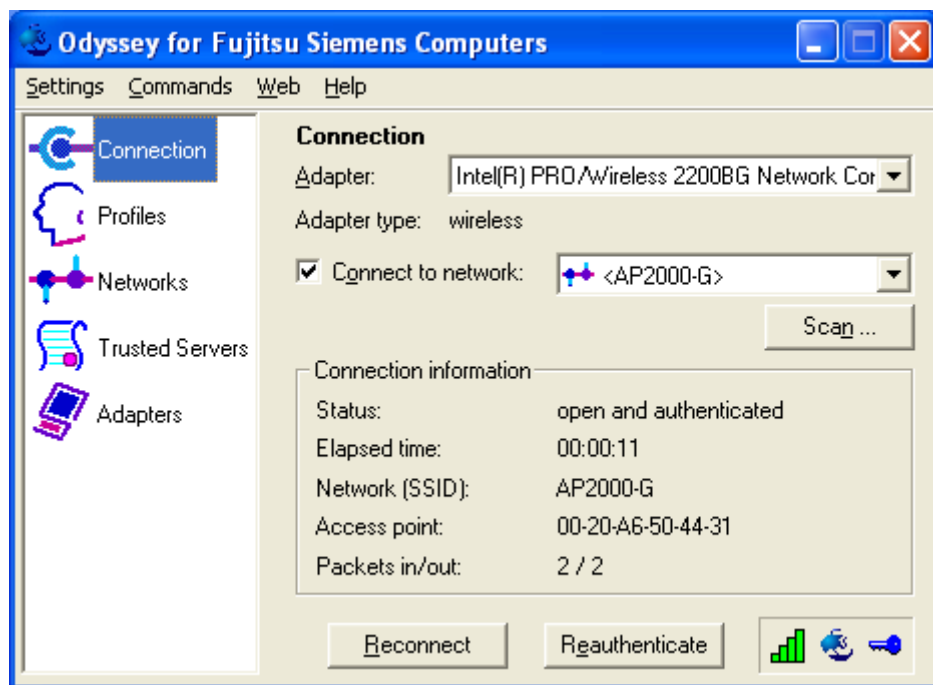
Si no desea realizar la configuración en este momento concreto, podrá hacerlo más tarde. Inicie el Odyssey Client Manager en *Inicio – Programas – Fujitsu Siemens Computers – Odyssey Client for Fujitsu Siemens Computers – Odyssey Client Manager for Fujitsu Siemens Computers*. El asistente *Configure and Enable Wizard* arranca de forma automática.

Empleo de Odyssey Client

Vista general del Odyssey Client Manager

Odyssey Client for Fujitsu Siemens Computers es el nombre de la interfaz de Windows del Odyssey Client Manager con la que puede controlar y configurar su LAN inalámbrica. Esta interfaz es consistente para todas las plataformas de ordenador Fujitsu Siemens, en los cuales usted puede aplicar el producto.

- Inicie el *Odyssey Client Manager* en Inicio – Todos los programas – Fujitsu Siemens Computers – *Odyssey Client for Fujitsu Siemens Computers* – *Odyssey Client Manager* o haga doble clic en el icono del Odyssey Client Manager situado en la barra de tareas.



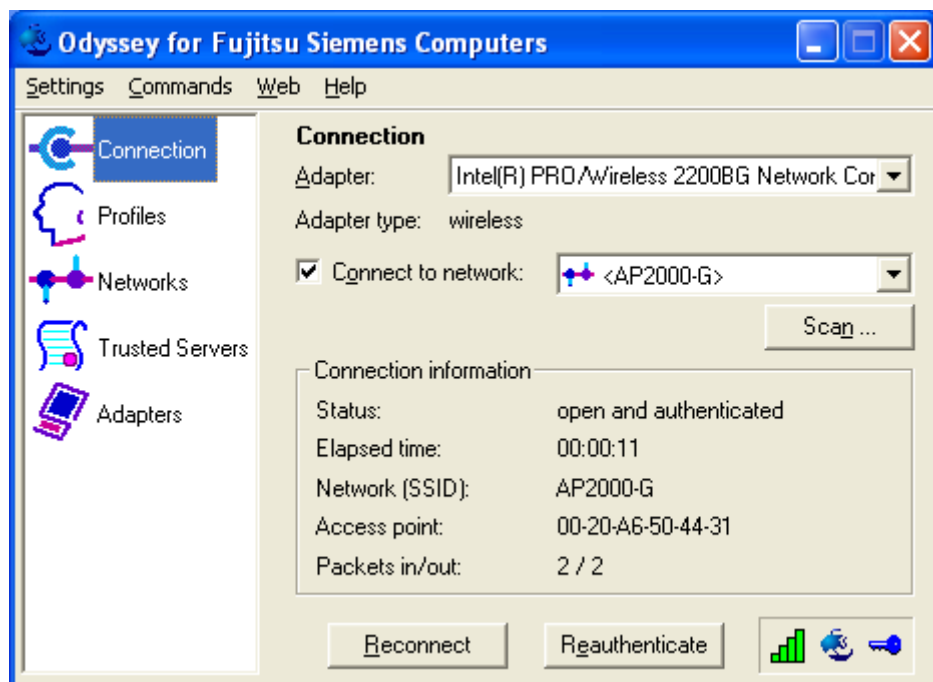
Pantalla Odyssey Client Manager

En la mayoría de las conexiones de red, el Odyssey Client Manager está compuesto por una serie de ventanas, en las que usted puede realizar diferentes ajustes operativos:

- En la ventana *Connection* podrá controlar su conexión de red y visualizar su actual estado de conexión.
- En la ventana *Profiles*, introduzca las informaciones necesarias para la autenticación o para el registro en la red, p. ej. su contraseña o certificado.
- En la ventana *Networks* puede configurar diferentes redes inalámbricas, y determinar como quiere conectarlas.
- En la ventana *Trusted Servers* usted determinará las informaciones de certificación e identificación con el servidor que usted puede autenticar, cuando usted establezca la conexión para asegurar que se está registrando en la red deseada.
- En la ventana *Adapters* usted puede configurar una o varias tarjetas de red para redes inalámbricas.

Todos los nombres de ventanas están relacionados en la parte izquierda de la pantalla del Odyssey Client Manager. Haga clic sobre el nombre de la ventana que desea visualizar o modificar.

Controlar las conexiones de red – Ventana "Connection"



Seleccionar tarjeta de red

En caso de que usted o su administrador hayan configurado más de una tarjeta de red para la aplicación de Odyssey, podrán asignar a cada tarjeta de red una conexión de red en el menú de selección *Adapters* de la ventana *Connection*.

Tan pronto como usted haya seleccionado una tarjeta de red, se actualizará el campo *Adapter type* y mostrará los tipos de tarjetas seleccionados (inalámbrica)

Conectar con una red

Cuando usted establece la conexión de red con ayuda de una tarjeta inalámbrica, deberá determinar todas las informaciones necesarias para la conexión en una definición de red Odyssey Client. Para ello deberá indicar asimismo la información de autenticación que ha definido previamente en un perfil de Odyssey Client (véase "Añadir o modificar un perfil – Ventana "Profile Properties"" en el apartado "Definir perfiles – Ventana "Profiles"").

Con la casilla de verificación *Connect to network* usted puede establecer o finalizar la conexión con la red inalámbrica. Cuando usted desee conectarse con una red inalámbrica, asegúrese de que esta casilla de verificación esté activada.

Desde el menú de selección a la derecha de *Connect to network* usted puede seleccionar una red inalámbrica, con la que debe establecerse la conexión. En esta lista aparecerán todas las redes que haya configurado ya con ayuda de la ventana *Networks*.

Los nombres de red aparecen entre corchetes después de la descripción de red.

Delante del nombre aparecerá el siguiente icono:



para redes

Para la conexión con una red ya configurada:

- Del menú de selección, seleccione la red con la que desee realizar la conexión.
- Seleccione usted la casilla de verificación *Connect to network*, en el caso de que no lo estuviera.

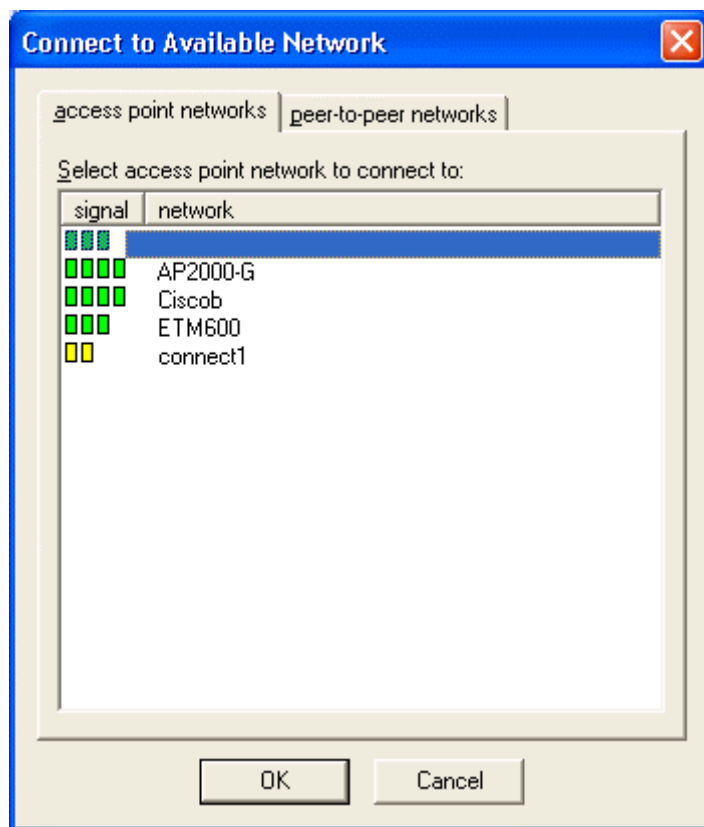
Para finalizar la conexión con una red, quite la marca en la casilla de verificación *Connect to network*.

Buscar redes inalámbricas

En caso de que viaje con frecuencia, podrá realizar la autenticación a través de redes inalámbricas locales que aún no haya configurado. Para establecer la conexión con una red inalámbrica todavía no configurada, ejecute usted los siguientes pasos:

- Haga clic sobre *Scan* en la ventana *Connection*.

Odyssey Client comprueba las ondas de radio y muestra una lista de todas las redes inalámbricas que actualmente están disponibles.



- ▶ Seleccione usted la red con la que desee establecer la conexión y haga clic sobre OK.
 - Cuando usted ya haya configurado los ajustes para esta red, Odyssey Client intentará establecer la conexión con estos ajustes.
 - Si usted todavía no ha configurado los ajustes para esta red, aparecerá en primer lugar la ventana *Network Properties*. Indique los ajustes y haga clic sobre *OK*.
- Odyssey Client intentará establecer la conexión con la red.

i Al escanear sólo son visibles las redes inalámbricas para las que el administrador ha configurado el SSID de manera visible ("send beacons"). Si el SSID no es visible, usted deberá introducir la red a través de la ventana *Networks*.

Conectar de nuevo con una red

Si la conexión inalámbrica con una red no funciona correctamente, podrá desconectar la conexión existente y establecer una nueva.

- Haga clic sobre *Reconnect* en la ventana *Connection*.

La conexión existente quedará anulada y se establecerá una conexión nueva con la red inalámbrica seleccionada. La nueva conexión puede establecerse posiblemente con otro punto de acceso (AccessPoint) (en la misma red), dependiendo de factores como la intensidad de señal. En caso de que sea necesaria la autenticación para dicha red, usted será autenticado de nuevo cuando comience la nueva conexión. En caso de que se utilicen claves dinámicas para la codificación, estas serán actualizadas.

Reautenticar en la red

Haciendo clic sobre *Reauthenticate* en la ventana *Connection*, Odyssey Client le autentifica de nuevo por medio de la conexión existente que se muestra en la ventana, sin que se establezca una nueva conexión. En caso de que se utilicen claves dinámicas para la codificación, estas serán actualizadas.

Desconectar la conexión de red

Para desconectar una conexión de red, elimine la marca de la casilla de verificación *Connect to network* para conexiones inalámbricas.

Visualizar datos de conexión

El campo de estado en la ventana *Connection* muestra el estado actual de su conexión con la red a través de esa tarjeta de red. Aparece una de los siguientes mensajes:

Aviso de estado	Definición
open and authenticated	Autenticando la conexión, usted está siendo conectado.
open / authenticating	Reautenticación en curso, usted está siendo conectado.
open / requesting authentication	Usted desea reautenticación, usted está siendo conectado.
open	La conexión no se autentifica, pero usted está siendo conectado.
peer-to-peer	El tipo de red está Peer-to-Peer (Adhoc), usted está siendo conectado.
authenticating	Usted todavía no ha sido conectado, pero la autenticación esta en curso.
requesting authentication	Usted todavía no ha sido conectado, pero ha solicitado la autenticación del punto de acceso (AccessPoint).
waiting to authenticate	Usted todavía no ha sido conectado y la última autenticación ha fallado, pero está esperando un nuevo intento.

Aviso de estado

searching for access point

Definición

Usted no ha sido conectado, y la comunicación con un punto de acceso (AccessPoint) en la red deseada no ha sido posible. Esto puede ocurrir cuando su tarjeta de red no soporta 802.1X, o cuando su punto de acceso (AccessPoint) no está situado en la zona de radio.

searching for peer(s)

Usted no ha sido conectado y la comunicación con otro ordenador en red Peer-to-Peer no está establecida.

disconnected

Usted no está conectado; eventualmente *Connect to network* no está activado. Véase "Conectar con una red"

Odyssey is disabled

Usted no está conectado y Odyssey Client está desactivado.

Adapter not present

Usted no está conectado y la tarjeta de red configurada no está disponible actualmente. Esto puede ocurrir cuando su tarjeta de red no soporta 802.1X.

El campo *Elapsed time* en la ventana *Connection* muestra el tiempo que ha pasado desde el comienzo de la conexión actual.

El campo *Network (SSID)* muestra los nombres de la red inalámbrica con la que usted está conectado. Véase también "Nombres para redes inalámbricas (SSID)".

En el campo *Access point* se representa la dirección MAC del punto de acceso Wireless (Wireless-AccessPoint), con el que usted está conectado. (Una dirección MAC es un número único de 48 bit que ha sido introducido en el aparato como código por el fabricante.)

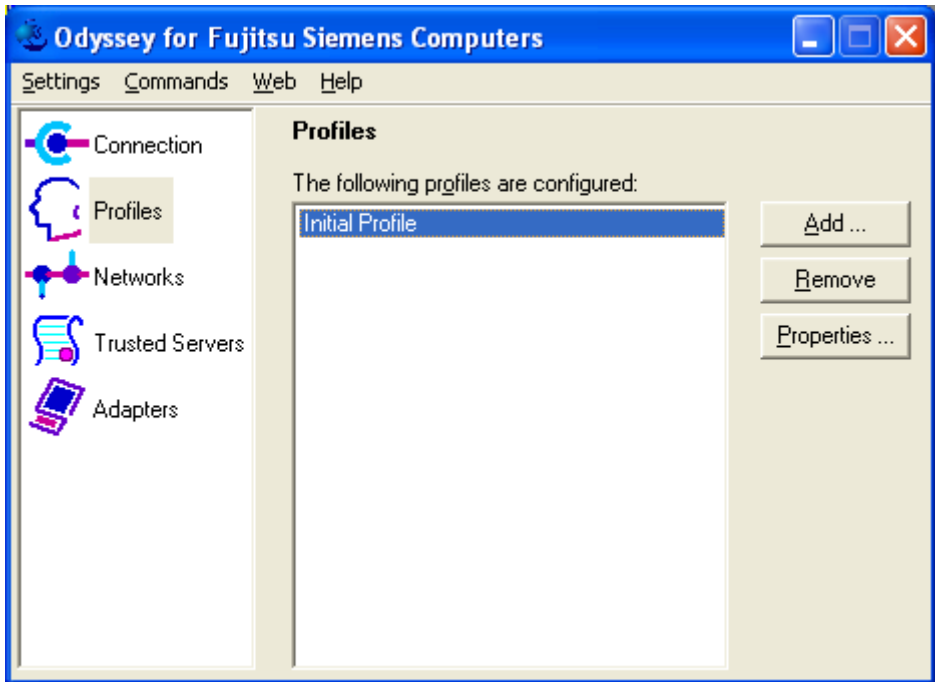
El campo *Packets in/out* muestra la cantidad total de los paquetes de red que han sido recibidos y transmitidos desde el comienzo de esta conexión.

Definir perfiles – Ventana "Profiles"

Un perfil Odyssey Client contiene todas las informaciones que son necesarias para autentificarle a usted para la red. De estas informaciones forma parte indicaciones como su nombre login, su contraseña o certificado, así como los protocolos por medio de los cuales usted puede ser autenticado. Su perfil es básicamente la identidad que usted muestra frente a la red y el medio con el que usted demuestra su identidad.

Usted puede utilizar varios perfiles para diferentes redes. De este modo usted puede utilizar por ejemplo diferentes nombres login o contraseñas en redes diferentes o usted puede utilizar una contraseña en una red y un certificado en otra.

► En el Odyssey Client Manager, haga clic en *Profiles* para abrir la ventana.



En la ventana *Profiles* se relacionan todos los perfiles que han sido configurados hasta ahora. Cuando usted utilice el *Odyssey Client Manager* por primera vez, encontrará un perfil con la denominación *Initial Profile* que contiene los ajustes generales. Alternativamente su administrador de red puede haber generado ya uno o varios perfiles para usted.

- Para añadir un perfil haga clic sobre *Add*. Aparece la ventana *Profile Properties*. Introduzca el nombre para el nuevo perfil, configure los ajustes y haga clic sobre *OK*.
- Para eliminar el perfil seleccione usted el perfil y haga clic sobre *Remove*.
- Para modificar un perfil selecciónelo y haga clic en *Properties* o doble clic sobre el perfil. Aparece la ventana *Profile Properties*. Modifique los ajustes y haga clic en *OK*.

Añadir o modificar un perfil – Ventana "Profile Properties"

En la ventana *Profile Properties* usted puede configurar un perfil. La ventana se muestra cuando usted en la ventana *Profiles* hace clic sobre *Add* o *Properties*.

Para añadir un nuevo perfil, deberá indicar un nombre unívoco en el campo *Profile Name*. Usted puede por ejemplo utilizar el nombre "Office" para su perfil en su lugar de trabajo o "Home" para su red privada.

Si usted ha definido y guardado un perfil, ya no tendrá ninguna posibilidad más de modificar el nombre del perfil al editar las otras propiedades del perfil. No obstante usted podrá eliminar el perfil y crear otro nuevo bajo otro nombre.

Además del nombre de perfil, podrá configurar (y editar) los siguientes parámetros en un perfil:

- Nombre login en la ficha *User Info*
- Contraseña y/o certificado en la ficha *Authentication*
- Una especificación de los protocolos de autenticación que puedan ser empleados para su autenticación en la red, en las fichas *TTLS Settings* y *PEAP Setting*

Ficha "User Info"

En la ficha *User Info* usted puede indicar el nombre que usted utiliza para registrarse, así como su contraseña y/o indicaciones del certificado.

The screenshot shows the 'Add Profile' dialog box with the 'User Info' tab selected. The 'Profile name' field contains 'Office'. The 'Login name' field contains 'ACME\george'. Under the 'Password' section, the 'Permit login using password' checkbox is checked, and the 'use Windows password' radio button is selected. There is an empty text field for a password and an 'Unmask' checkbox. Under the 'Certificate' section, the 'Permit login using my certificate:' checkbox is unchecked, and there is an empty text field. At the bottom of the certificate section are 'View ...' and 'Browse ...' buttons. The dialog has 'OK' and 'Cancel' buttons at the bottom.

Add Profile

Profile name:

User Info | Authentication | TTLS Settings | PEAP Settings

Login name:

Password

☒ Permit login using password

☒ use Windows password

☐ prompt for password

☐ use the following password:

☐ Unmask

Certificate

☐ Permit login using my certificate:

Nombre login

Introduzca su nombre de usuario en el campo *Login name*. Este nombre se mostrará a la red al realizar su autenticación. En caso de que usted se autentique mediante un directorio Windows Active, utilice el formato nombre de dominio\nombre de usuario (por ejemplo Acme\george). En caso contrario, emplee un nombre login según el formato establecido por su administrador para los nombres de usuario en el banco de datos de autenticación.

Tenga en cuenta lo siguiente:

- En el caso de que usted esté registrado en su dominio de red (a diferencia del registro local), Odyssey Client indicará en este campo de forma estándar el nombre de dominio / nombre de usuario, donde el nombre de usuario es su propio nombre de usuario.
- Si está registrado de manera local en su cliente (a diferencia de un dominio de red), Odyssey Client indicará en este campo sólo su nombre de usuario.
- Es posible que usted tenga que introducir el nombre del servidor después de su nombre login, para que con ello su autenticación sea dirigida al servidor correcto.
Ejemplo: `acme\george@sales.acme.com`. Su administrador de red puede comunicarle como debe utilizarse correctamente este campo.

Contraseña

Marque usted *Permit login using password* para activar el procedimiento para la autenticación con contraseña. Podrá especificar qué contraseña debe emplear Odyssey Client:

- Seleccionar *use Windows password* cuando usted quiera utilizar para la autenticación en la red la misma contraseña que la que usa para el registro de Windows.
- Seleccionar *prompt for password* en el caso de que Odyssey Client deba exigirle la introducción de una contraseña llegado el momento de la autenticación.
- Seleccione *use the following password* e introduzca una contraseña en el siguiente campo en el caso de que Odyssey Client deba almacenar su contraseña y emplearla siempre para su autenticación con este perfil.

En el caso de que usted haya seleccionado *prompt for password*, sólo será requerida por lo general la introducción de la contraseña la primera vez que sea autenticado después del inicio. Odyssey Client recuerda esta contraseña y la utiliza durante toda la duración de su sesión de Windows. La contraseña indicada por usted sólo es válida para un perfil. En caso de que su autenticación fuera realizada con otro perfil, usted será requerido nuevamente para la indicación.

En alguna ocasión usted también puede ser requerido para introducir su contraseña de Windows cuando usted establece la conexión con la red:

- En el caso de que usted por error haya introducido una contraseña errónea o exista cualquier otro fallo de autenticación. Esta función se utiliza también para impedir un bloqueo por error a causa de la utilización repetida de contraseñas erróneas.
- En caso de que usted tenga que cambiar periódicamente su contraseña de Windows y acceda a la red por medio de EAP-TTLS o autenticación PEAP antes del logon de Windows.

Certificado

Marque usted *Permit login using my certificate* para activar el procedimiento de autenticación en el que su certificado sirve para autenticarse.

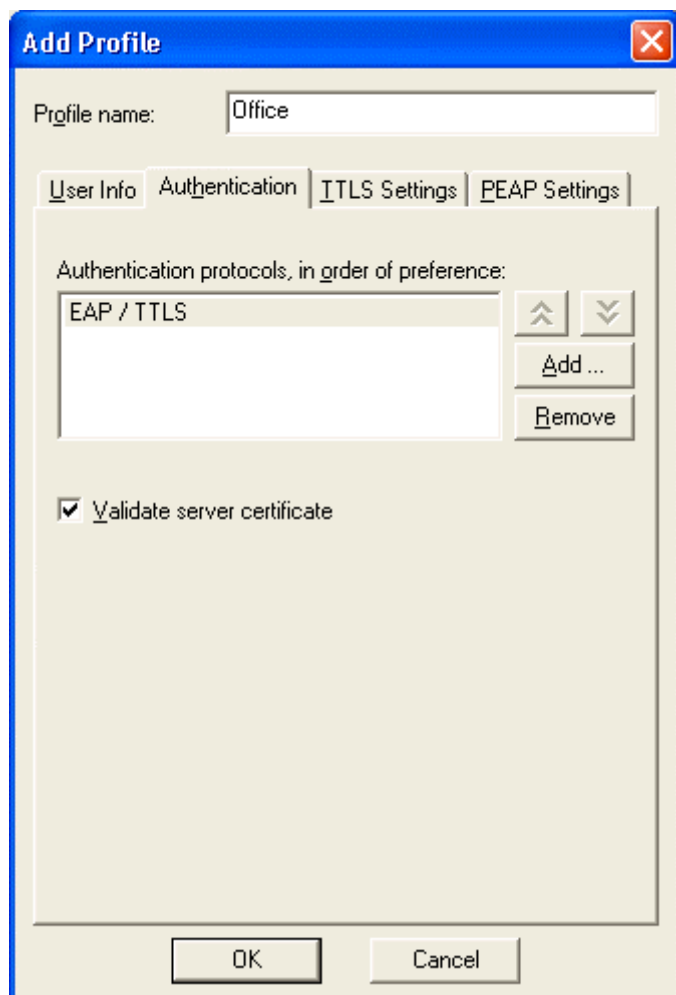
Para seleccionar un certificado personal para la autenticación haga usted clic sobre *Browse*. Aparece una lista de sus certificados personales. Seleccione un certificado y haga clic sobre *OK*.



Esta es una función avanzada. En caso dado dirijase usted a su administrador de red al seleccionar su certificado necesario.

Ficha "Authentication"

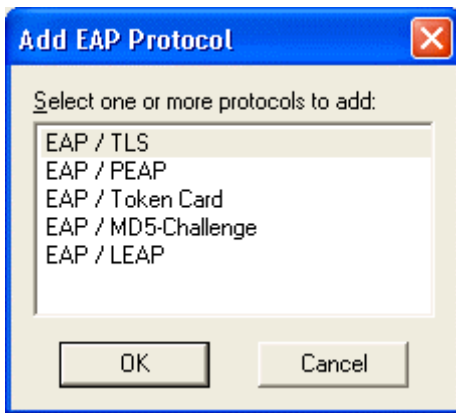
En la ficha *Authentication* podrá especificar protocolos con los que autenticarse en la red.



Selección de protocolos de autenticación

La lista de los protocolos de autenticación muestra los protocolos que están activados para la autenticación. La lista puede contener uno o varios protocolos de autenticación. Si usted tiene más de un protocolo de autenticación, usted podrá asignarles prioridades. El orden determinará el protocolo que deberá emplear el servidor cuando se encuentre disponible más de un protocolo común.

- Para variar el orden de protocolos seleccione un protocolo y desplácelo con ayuda de las teclas de flechas.
- Para eliminar un protocolo, selecciónelo y haga clic sobre *Remove*.
- Para añadir un protocolo haga usted clic sobre *Add*. Aparece la ventana *Add EAP Protocol*. Seleccione uno o varios protocolos que deban ser añadidos y haga clic sobre *OK*. Usted puede seleccionar más de un protocolo si usted mantiene presionada la tecla **Ctrl** de su teclado al seleccionar con el ratón. Tenga en cuenta que todos los protocolos que usted ya haya seleccionado no estén relacionados en esta ventana.



Validación del certificado de servidor

Determinados protocolos como por ejemplo EAP-TTLS, PEAP y EAP-TLS le permiten la verificación de la identidad del servidor de autenticación mientras el servidor compruebe su identidad. Este procedimiento es identificado como autenticación recíproca.

Marque la opción *Validate Server Certificate* para verificar la identidad del servidor de autenticación en base a su certificado cuando se emplee EAP-TTLS, PEAP y EAP-TLS. (Este campo está marcado de forma estándar.) En la ventana *Trusted Servers* podrá visualizar los certificados del servidor de autenticación Trusted. Véase "Especificar servidores fiables - Ventana "Trusted Servers"".

Por regla general usted debe marcar *Validate server certificate*. De forma opcional podrá desactivar esta importante medida de seguridad, pero sólo cuando no sea necesario ningún certificado para el servidor. Usted sólo debería hacer esto a petición de su administrador de red.

Ficha "TTLS Settings"

En la ficha *TTLS Settings* usted puede ajustar EAP-TTLS como protocolo de autenticación. Estos ajustes sólo son relevantes cuando usted utiliza EAP-TTLS como uno de sus protocolos de autenticación en la ficha *Authentication*.

The screenshot shows a window titled "Add Profile" with a close button (X) in the top right corner. The window has a tabbed interface with four tabs: "User Info", "Authentication", "TTLS Settings" (which is selected), and "PEAP Settings".

Under the "TTLS Settings" tab, the "Profile name:" field contains the text "Office".

Below the tabs, there is a section for "Inner authentication protocol:" with a dropdown menu currently set to "MS-CHAP-V2".

Below that is a section titled "Inner EAP protocols, in order of preference:" which contains an empty list box. To the right of the list box are four buttons: an up arrow, a down arrow, an "Add..." button, and a "Remove" button.

At the bottom of the dialog is a text box labeled "Anonymous name:" containing the text "anonymous". Above this text box is a paragraph of explanatory text: "When using EAP-TTLS exclusively, you can keep your login name private and reveal only an anonymous name on the network; for example, 'anonymous' or 'anonymous@myisp.com'."

At the very bottom of the window are two buttons: "OK" and "Cancel".

EAP-TTLS genera un túnel seguro y codificado, a través del cual usted transmite su demostración de autorización al servidor de autenticación. Dentro de EAP-TTLS existe todavía otro protocolo interior de autenticación (Inner Authentication Protocol), que usted tiene que configurar.

Selección del protocolo interior de autenticación

En el menú de selección *Inner Authentication Protocol*, seleccione el protocolo interior de autenticación deseado. Se encuentran disponibles los siguientes protocolos:

- PAP
- CHAP
- MS-CHAP
- MS-CHAP-V2
- PAP/Token
- EAP

El protocolo utilizado más frecuentemente es MS-CHAP-V2. El protocolo permite la autenticación en un controlador de dominio de Windows así como en otros bancos de datos de usuarios que no funcionen en Windows.

CHAP es el protocolo más empleado para la autenticación en bancos de datos de usuarios que no funcionen en Windows.



No puede emplear CHAP como procedimiento para la autenticación interna en un dominio Windows NT o directorio Active. Por lo tanto, no emplee CHAP para la autenticación en el servidor Odyssey porque éste sólo se identifica en un dominio Windows o en un directorio Active.

PAP/Token es el protocolo a utilizar en caso de tarjetas Token. Si usted utiliza PAP/Token, el valor de contraseña introducido por usted en el diálogo de contraseña no será nunca guardado en la memoria caché, ya que toda contraseña basada en Token está determinada para un solo uso.

Consulte a su administrador de red, qué protocolo interior de autenticación se aplica en su red.

EAP como protocolo interior de autenticación

Cuando usted utilice EAP como protocolo interior de autenticación, usted tiene que configurar la lista de los protocolos interiores EAP con uno o varios protocolos.

- Para añadir un protocolo haga usted clic sobre *Add*. Aparece la ventana *Add EAP Protocol*. Seleccione uno o varios protocolos que deban ser añadidos y haga clic sobre *OK*. Usted puede seleccionar más de un protocolo si usted mantiene presionada la tecla **Ctrl** de su teclado al seleccionar con el ratón. Tenga en cuenta que los protocolos ya añadidos por usted no aparecerán relacionados en esta ventana.
- Para eliminar un protocolo, selecciónelo y haga clic sobre *Remove*.
- Para variar el orden seleccione un protocolo y desplácelo con ayuda de las teclas de flechas.

Determinar un nombre anónimo

EAP-TTLS ofrece frente a otros protocolos una única función. Como EAP-TTLS configura un túnel codificado para su demostración de autorización, también es posible transmitir su nombre login a través de este túnel. Con ello no sólo su demostración de autorización queda protegida contra una vigilancia secreta, sino también su identidad.

De este modo usted tiene con EAP-TTLS dos identidades: una interior y una exterior. La identidad interior es su actual nombre login y se encuentra en el campo de nombre login en la ficha *User Info*. Su identidad exterior puede ser totalmente anónima. Ajuste usted su identidad externa en el campo *Anonymous name*.

Por lo general *Anonymous name* está ajustado de forma estándar en *anonymous*. En algunos casos usted deberá introducir texto adicional. De esta forma puede utilizarse por ejemplo esta identidad exterior para dirigir su autenticación hacia el servidor correspondiente y usted puede ser requerido a utilizar *anonymous@acme.com*. Su administrador de red puede decirle cómo se configura este campo correctamente.

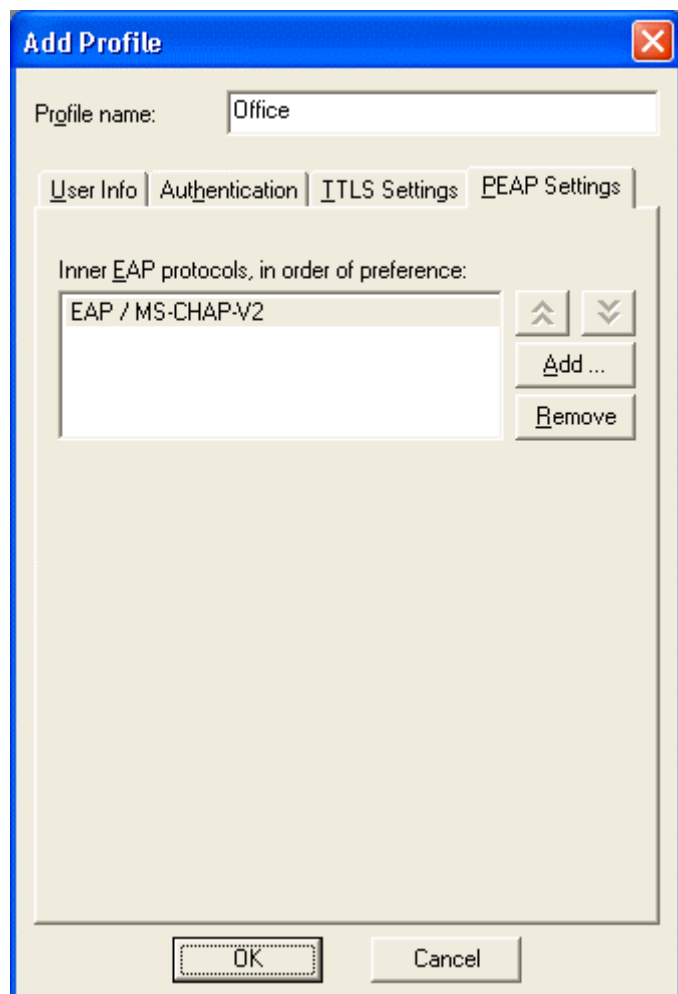


Su identidad exterior sólo puede ser anónima cuando EAP-TTLS es el único protocolo de autenticación que está configurado en la ficha *Authentication Protocols*. En el caso de que también estén activados otros protocolos, Odyssey Client no puede mantener su identidad en secreto y el campo *Anonymous name* está desactivado. Cuando usted desea el anonimato ofrecido por EAP-TTLS, deberá establecer a EAP-TTLS como único protocolo de autenticación.

Ficha "PEAP Settings"

En el caso de que usted determine EAP/PEAP como protocolo de autenticación en la ficha *Authentication*, usted podrá utilizar hasta tres procedimientos de autenticación internos EAP:

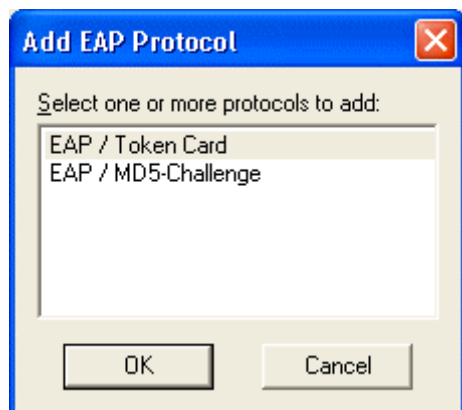
- EAP/MS-CHAP-V2
 - EAP/Tarjeta Token
 - EAP/MD5-Challenge para añadir o eliminar procedimientos de autenticación interiores, que se utilizan en PEAP:
- Seleccione la ficha *PEAP Settings*.



- ▶ Seleccione los protocolos que desee borrar y haga clic sobre *Remove*.
- ▶ Haga usted clic sobre *Add* para añadir un protocolo.

Aparece la ventana *Add EAP Protocol*.

- Seleccione uno o varios protocolos que deban ser añadidos y haga clic sobre *OK*.



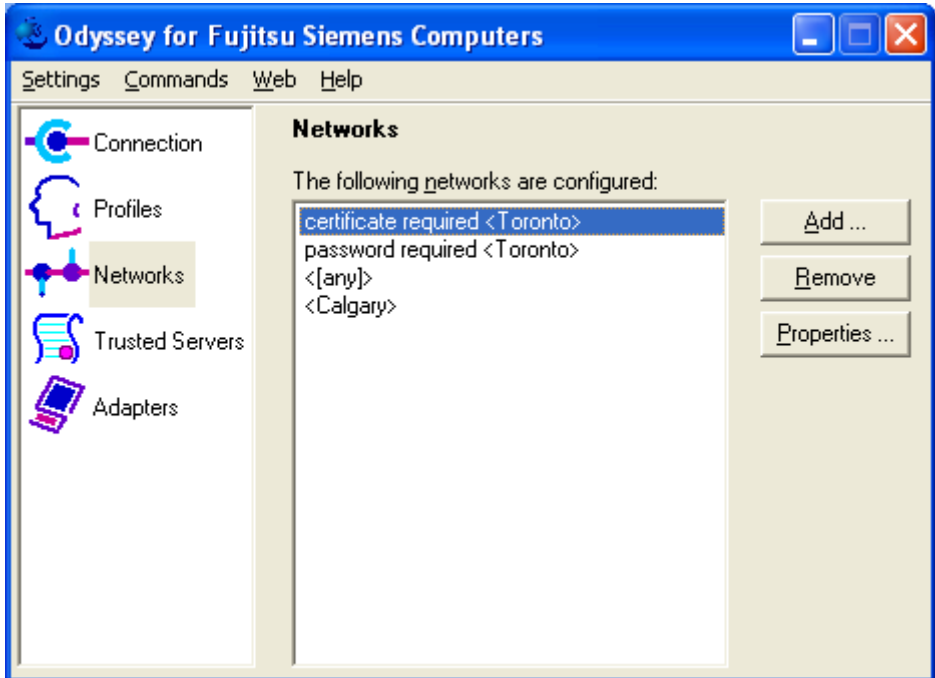
Tenga en cuenta que todos los protocolos que usted ya haya seleccionado no estén relacionados en esta ventana.

- Haga clic sobre *OK* cuando usted haya concluido por completo la modificación de la configuración de perfil.

Configurar las redes inalámbricas – Ventana "Networks"

En la ventana *Networks* usted puede realizar ajustes para la conexión con una cantidad cualquiera de redes inalámbricas.

- En el Odyssey Client Manager, haga clic en *Networks* para abrir la ventana.



Aparecerán enumeradas todas las redes configuradas. Usted puede realizar las siguientes tareas en la ventana *Network*:

- Para añadir una red haga clic sobre *Add*. Aparece la ventana *Network Properties*. Configure los ajustes para la nueva red y haga clic sobre *OK* (véase el apartado "Añadir o modificar redes – Ventana "Network Properties"").
- Para eliminar una red, selecciónela y haga clic sobre *Remove*.
- Para modificar los ajustes para una red, selecciónela y haga clic sobre *Properties* o haga doble clic sobre el nombre de la red. Aparece la ventana *Network Properties*. Modifique los ajustes y haga clic en *OK* (véase el apartado "Añadir o modificar redes – Ventana "Network Properties"").

Denominaciones de red

Las denominaciones de red en la ventana *Networks* están estructuradas de la siguiente forma:

- El nombre de la red aparece entre corchetes.
- La descripción de la red se encuentra delante del nombre. Esta descripción se extrae del campo *Description* de la ventana *Network Properties*. Usted puede añadir su propia descripción para cada red configurada. Esto le ayuda a diferenciar entre las diferentes redes.

El campo de la descripción de red es útil en situaciones en las que desee cambiar entre varias "Personalidades" dentro de la misma red. Usted puede por ejemplo utilizar demostraciones de autorización diferentes en diferentes momentos. El campo de descripción le permite, asimismo, diferenciar entre dos redes diferentes con el mismo nombre de red.

Los nombres de red son texto de libre elección que es seleccionado por el administrador. Por ello es posible que dos redes independientes una de otra tengan el mismo nombre. En la presentación de la ventana *Networks* hay dos redes "Toronto". Las descripciones configuradas muestran que en una red se utiliza la contraseña como demostración de autorización y en la otra la demostración con certificado.

Añadir o modificar redes – Ventana "Network Properties"

En la ventana *Network Properties* puede configurar los ajustes para la red inalámbrica. En la ventana *Networks* haga clic sobre *Add* o *Properties* para visualizar las propiedades de red. Se abrirá la ventana *Add Network* o *Network Properties*.

Network Properties

Network

Network name (SSID): Toronto

☐ Connect to any available network Scan ...

Description (optional):

Network type: Access point (infrastructure mode)

Channel: default channel

Association mode: open

Encryption method: WEP

Authentication

☒ Authenticate using profile: Office

☒ Keys will be generated automatically for data privacy

Pre-configured keys [WEP]

Format for entering keys: ASCII characters

Key 0:

Key 1:

Key 2:

Key 3:

OK Cancel

Aquí usted puede configurar los siguientes parámetros:

- Propiedades de red en la sección *Network*
- Campos de autenticación en la sección *Authentication*
- Claves preconfiguradas (WEP o WPA) en la sección *Pre-configured keys*

Network

En esta sección en la ventana *Network Properties* usted puede ejecutar las siguientes tareas:

- Indicar el nombre de red
- Buscar una red
- Configurar Odyssey para la conexión a una red disponible
- Indicar descripción de red
- Indicar tipo de red
- Indicar el modo de asignación
- Indicar un procedimiento de codificación adecuado para el modo de asignación

Indicar el nombre de red

Ajuste usted *Network name (SSID)* al nombre de la red inalámbrica. El nombre de red puede ser de hasta 32 caracteres. Se diferencia entre escritura en mayúscula y minúscula. Este nombre deberá ser introducido correctamente para que con ello puede establecerse la conexión con éxito.

Buscar una red

Usted puede introducir directamente el nombre de la red o hacer clic sobre *Scan* para seleccionar de una lista con todas las redes visibles en ese momento.

Si usted se encuentra en las cercanías de la red que está configurando, la utilización del botón *Scan* no sólo es más sencilla que la introducción por teclado, sino que también garantiza que el nombre de red está indicado correctamente.

Tenga en cuenta que si utiliza el botón *Scan*, para usted sólo son visible aquellos puntos de acceso (AccessPoints) que emiten radiación direccional.

Configurar Odyssey para la conexión con cualquier red

Odyssey Client Manager ofrece una red especial bajo la denominación *[any]*. La red *[any]* establece la conexión con cualquier red, independientemente de su nombre. La red *[any]* es útil para usted en conferencias, hoteles u otros lugares en los que existe acceso a la red. Cuando usted selecciona la red *[any]* en la ventana *Connection*, se podrá conectar a estas redes, sin tener que configurarlas de forma individual.

Para configurar una red *[any]*, marque usted *Connect to any available network* y haga clic sobre *OK*.

Aunque usted pueda utilizar clave y perfil WEP con *[any]*, existe la práctica habitual de utilizar *[any]* sin la autenticación 802.11 o 802.1X.

Indicar descripción de red

Las descripciones de red son útiles para diferenciar entre redes con el mismo nombre o un nombre similar. Puede introducir la descripción de red en el campo *Description*.

Indicar tipo de red

En el caso que usted no haya utilizado el botón *Scan* para la selección de su red, deberá especificar el tipo de red seleccionando una de las opciones del menú de selección.

- Seleccione *Access point (infrastructure mode)* si esta red utiliza puntos de accesos (AccessPoints), para asegurar la posibilidad de conexión para la red corporativa o para Internet. Este es el ajuste más habitual.
- Seleccione *Peer-to-peer (ad-hoc mode)* para crear una red privada con uno o varios ordenadores.

Indicar el modo de asignación

Antes de autenticar deberá usted asignar su cliente a un punto de acceso (AccessPoint). El modo de asignación exigido por usted depende de su hardware de punto de acceso (AccessPoint) y de como esté configurado. Su administrador de red le podrá ayudar al configurar el modo de asignación que es necesario para su red.

Podrá encontrar más información sobre las posibilidades de elección de esta codificación y sobre el modo de asignación en "Wired-Equivalent Privacy (WEP) con claves preconfiguradas" y "Wi-Fi Protected Access (WPA) y codificación TKIP".

Usted puede seleccionar entre tres modos de asignación:

- *Open* para la conexión con una red a través de un punto de acceso (AccessPoint) o conmutador con autenticación 802.1X. Seleccione este modo cuando usted no pueda seleccionar ningún modo Shared o WPA.
- *Shared*, para la conexión a una red a través de un punto de acceso (AccessPoint) que exija una clave WEP para la autenticación y para la codificación de datos.
- *WPA*, para la conexión a una red a través de un punto de acceso (AccessPoint) con WPA (Wi-Fi Protected Access).

Indicar un procedimiento de codificación adecuado para su modo de asignación

La elección del procedimiento de codificación depende también de las condiciones del punto de acceso (AccessPoint). Sus posibilidades de elección son diferentes dependiendo del modo de asignación elegido. Podrá encontrar más información en "Wired-Equivalent Privacy (WEP) con claves preconfiguradas" y "Wi-Fi Protected Access (WPA) y codificación TKIP".

Usted dispone de las siguientes opciones:

- *none* para la utilización de la autenticación 802.1X sin clave WEP. Esta opción sólo estará disponible cuando haya seleccionado el modo de asignación *open*.
- *WEP* para la utilización de la clave WEP a fin de llevar a cabo la codificación de datos. Esta opción está disponible con todos los modos de asignación y es necesaria en modo Shared. Si usted selecciona esta opción, deberá introducir la clave WEP en la sección *Network Properties* en el ventana *Network Properties*. Deberá seleccionar esta opción cuando los puntos de acceso (AccessPoints) en su red exijan claves WEP para la autenticación (modo Shared).
- *TKIP* para la utilización del protocolo para integridad temporal de la clave. Seleccione esta opción cuando los puntos de acceso (AccessPoints) en su red exigen autenticación WPA y estén codificados para codificación de datos TKIP.
- *AES* para la utilización del protocolo de codificación estándar extendido. Seleccione esta opción cuando los puntos de acceso (AccessPoints) en su red exigen autenticación WPA y estén configurados para la codificación de datos AES.

Campos de autenticación

En la sección *Authentication* puede configurar la autenticación de red con las siguientes características:

- Autenticación con perfil
- Generación automática de claves

Autenticación con perfil

En caso de que en la red configurada por usted sea necesario que usted se autentique con su demostración personal de autorización, marque *Authenticate using profile* y seleccione en el menú de selección el perfil correspondiente. **Usted ya ha tenido que configurar un perfil que es apropiado para la autenticación en esta red.**

Si usted marca *Authenticate using profile*, Odyssey Client realiza una autenticación 802.1X con su contraseña, certificado u otro medio, tal y como está configurado en el perfil seleccionado.

Generación automática de claves

Marque *Keys will be generated automatically for data privacy*, cuando el procedimiento de autenticación indicado en el perfil está determinado para la creación de claves dinámicas WEP para la utilización entre su ordenador y el punto de acceso (AccessPoint). Determinados procedimientos de autenticación como EAP-TTLS, PEAP y EAP-TLS generan claves. Otros procedimientos de autenticación no generan ninguna clave. En el caso de que se utilicen EAP-TTLS, PEAP o EAP-TLS para la autenticación, seleccione este campo. Podrá emplear cada uno de estos procedimientos de autenticación para puntos de acceso (AccessPoints) con autenticación 802.1x. Esta opción ofrece más seguridad que la utilización de claves estáticas (preconfiguradas). Deje usted esta opción sin marcar cuando usted sea requerido a utilizar claves WEP preconfiguradas, o en el caso de la autenticación WPA, una clave Pre-shared.

Clave preconfigurada (WEP o WPA)

La red inalámbrica puede exigir que usted configure previamente claves WEP o que en el caso de autenticación WPA usted utilice previamente una frase de acceso (Pre-share). Usted puede introducir claves en la parte inferior de *Network Properties*.

Claves Pre-shared (WPA)

Si ha seleccionado el modo WPA y la clave no se genera automáticamente al asignar un perfil de autenticación para la conexión de red, deberá introducir una frase de acceso ASCII Pre-shared en el campo *Password*. Esta frase de acceso se utiliza como base al generar la clave necesaria.

Clave preconfigurada (WEP)

Cuando usted ha seleccionado el modo Shared, tendrá que configurar como mínimo una clave WEP. También deberá configurar como mínimo una clave WEP si selecciona la codificación WEP para el modo abierto y no se generan las claves de manera automática al asignar un perfil de autenticación a la conexión de red. Las claves WEP tienen las siguientes finalidades:

- Asignación a un punto de acceso (AccessPoint) antes de que pueda ser establecida una conexión (modo Shared).
- Codificación de datos entre su ordenador y el punto de acceso (AccessPoint) (u otro ordenador en una red Peer-to-Peer) (véase "Wired-Equivalent Privacy (WEP) con claves preconfiguradas").

En caso de que la red inalámbrica utilice autenticación 802.1X y se generen claves dinámicas WEP (es decir, usted ha marcado *Authenticate using profile* y *Keys will be generated automatically for data privacy*), entonces usted no necesita introducir ninguna clave WEP preconfigurada para la protección de datos. No obstante es necesario, aunque no es frecuente, utilizar claves WEP preconfiguradas para la autenticación de forma adicional a 802.1X. EAP-MD5 no genera por ejemplo ninguna clave WEP para la codificación de datos, de forma que usted deberá preparar una clave cuando su perfil esté ajustado para la autenticación con este método.

En el caso que usted implemente una de estas aplicaciones de clave preconfigurada WEP, tendrá que marcar los campos correspondientes y ajustar correspondientemente una o varias claves WEP:

- Marque usted *authenticate to access points (shared mode)* en caso de que sean necesarias claves WEP preconfiguradas para la autenticación en un punto de acceso (AccessPoint) antes de la conexión con la red inalámbrica.
- Marque usted *Keys will be generated automatically for data privacy*, para utilizar claves WEP preconfiguradas para la codificación de datos a través de la red inalámbrica. Introduzca la clave WEP en los campos *Key 0* hasta *Key 3*. Los valores introducidos aquí tienen que corresponder con los de los puntos de acceso (AccessPoints) u ordenador Peer, con los que usted establece la conexión. Por lo general se utiliza *Key 0*, aunque su red puede exigir también otra clave. Usted puede introducir claves o bien como caracteres de texto habituales (ASCII) o como caracteres hexadecimales.

Una clave WEP tiene una longitud de 40 ó 104 bit. Esto corresponde o bien 5 o 13 caracteres, cuando usted los introduce como caracteres ASCII ó 10 o 26 caracteres, cuando usted los introduce como caracteres hexadecimales.

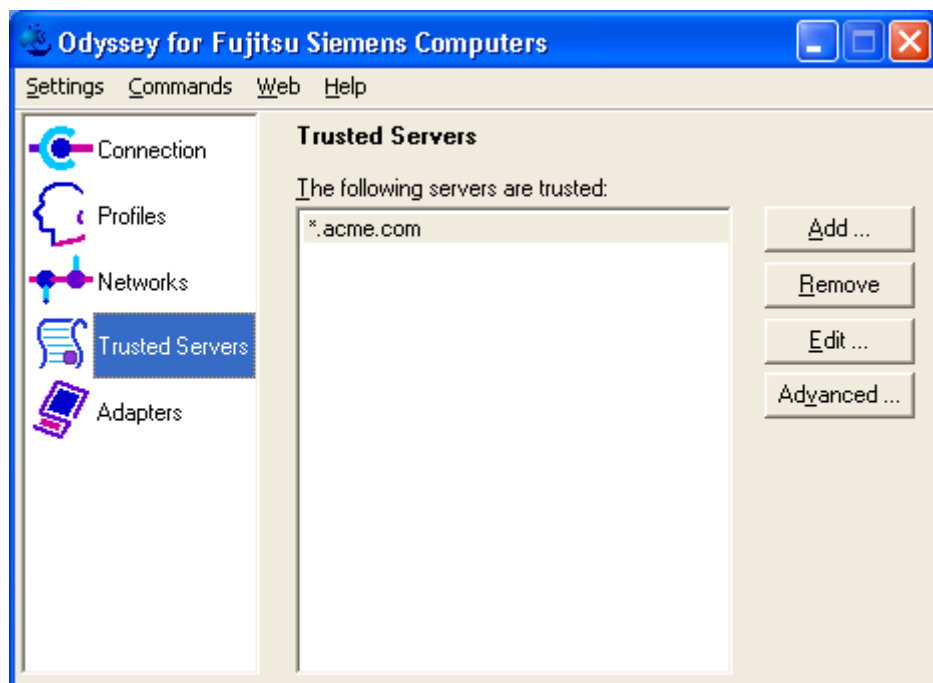
Introducción de una clave WEP preconfigurada:

- ▶ En la lista de selección *Format for entering keys* seleccione bien caracteres ASCII o caracteres hexadecimales, dependiendo del formato en que desee introducir las claves.
- ▶ Indique en los campos de texto *Key 0* hasta *Key 3* cada clave que usted quiera preconfigurar.

Especificar servidores fiables - Ventana "Trusted Servers"

En la ventana *Trusted Servers* podrá configurar en qué servidor de autenticación confía para su registro de red como servidor Trusted (servidor fiable).

- En el Odyssey Client Manager, haga clic en *Trusted Servers* para abrir la ventana.



Cuando usted configura un servidor Trusted, usted no sólo necesita indicar el nombre del servidor, sino también la cadena de certificados a la que este pertenece. El Odyssey Client es muy flexible y ofrece un procedimiento sencillo y un procedimiento avanzado para la configuración de servidores Trusted.

Encontrará información adicional bajo "Extensible Authentication Protocol (EAP)".

Procedimiento sencillo para la configuración de servidores Trusted

En la mayoría de los casos usted puede utilizar un sencillo procedimiento para la configuración de servidores Trusted. En este procedimiento usted tiene que determinar dos elementos:

- Nombre del dominio del servidor o el final del nombre del dominio (por ejemplo *acme.com*)
- El certificado de un Certificate Authority en la cadena. Esto podría ser el certificado de un Certificate Authority Root o Intermediate.

Nombre de dominio

Cada servidor dispone de un nombre de dominio que le identifica claramente, y este nombre de dominio está contenido habitualmente en el campo "Subject CN" del certificado del servidor.

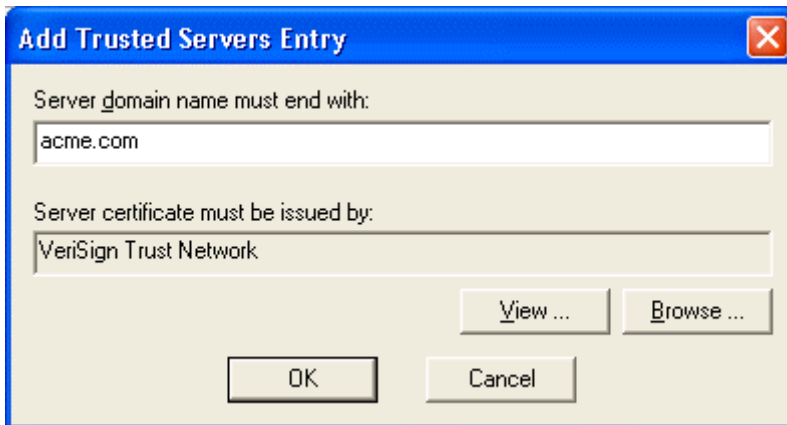
El nombre de dominio de un servidor finaliza con el nombre de un dominio administrativo superior, al que pertenece este servidor. Así por ejemplo la empresa Acme puede tener un nombre de dominio como *acme.com*. La compañía podría tener también diferentes servidores de autenticación con los nombres *auth1.acme.com*, *auth2.acme.com* y *auth3.acme.com*.

Tal y como se ve en este ejemplo, usted puede determinar, a través de la indicación de la terminación vinculante del nombre de dominio del servidor, la confianza en todos los servidores en una empresa con un sólo registro.

Añadir un registro Trusted Server

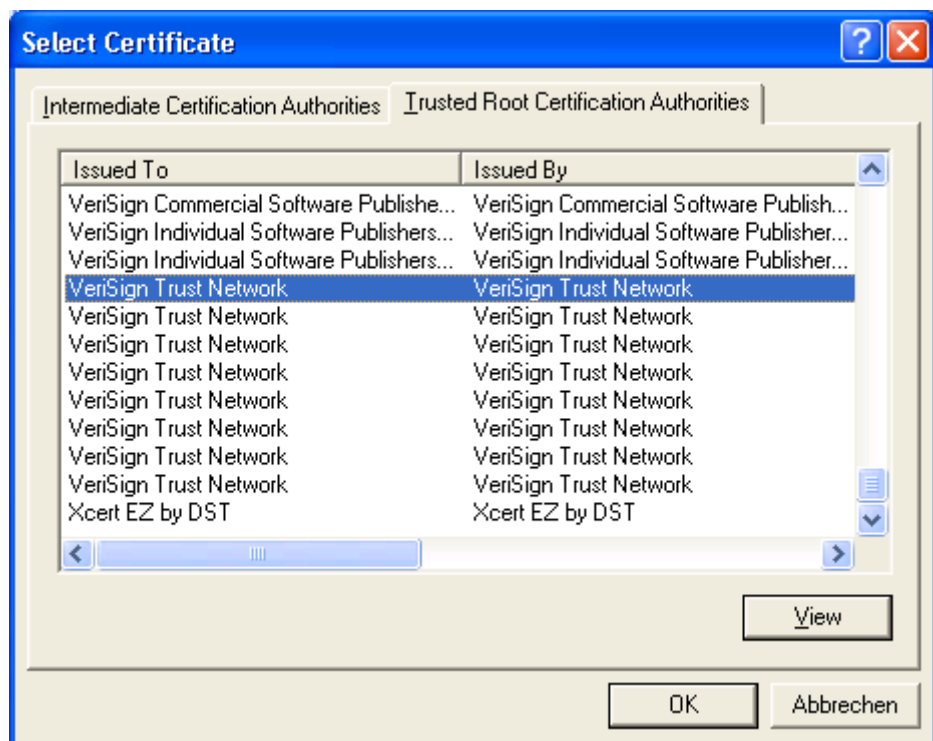
Para añadir un registro a la lista de los servidores Trusted, siga usted los siguientes pasos:

- Haga clic sobre *Add*. Aparece la ventana *Add Trusted Servers Entry*.



- En el campo *Server domain name must end with* introduzca usted el nombre (o los elementos finales del nombre) del dominio al que debe pertenecer el servidor Trusted. Este campo no puede permanecer libre.

- Ajuste el campo *Server certificate must be issued by* al certificado del Certificate Authority, que directa o indirectamente ha emitido el certificado de servidor. Para asignar un certificado realice los siguientes pasos:
 - Haga clic sobre *Browse* para obtener una lista de los certificados.
 - Seleccione un certificado de la lista y haga clic sobre *OK*.



Como certificado, podrá seleccionar un Certificate Authority Root o Intermediate. No necesita ser el certificado que fue emitido directamente como certificado de servidor. Puede ser cualquier certificado en la cadena.

Borrar un registro de servidor Trusted

Para borrar un registro de la lista de servidores Trusted seleccione el registro y haga clic sobre *Remove*.

Editar un registro de servidor Trusted

Para procesar un registro de la lista de servidores Trusted, selecciónelo y haga clic sobre *Edit*. Aparece la ventana *Edit Trusted Servers Entry* y le permite editar el dominio de servidor y el certificado de la instancia otorgadora.

Procedimiento avanzado para la configuración de servidores Trusted

En el caso de que usted necesite más controles de confianza, puede utilizar el procedimiento avanzado.



En el caso de que usted no tenga ninguna experiencia práctica con certificados y cadenas de certificados, no deberá intentar una configuración con el procedimiento avanzado. Diríjase a su administrador de red e infórmese sobre la configuración de servidores Trusted.

En este procedimiento se representa la estructura Trust completa. La estructura Trust muestra todos los servidores Trusted configurados.

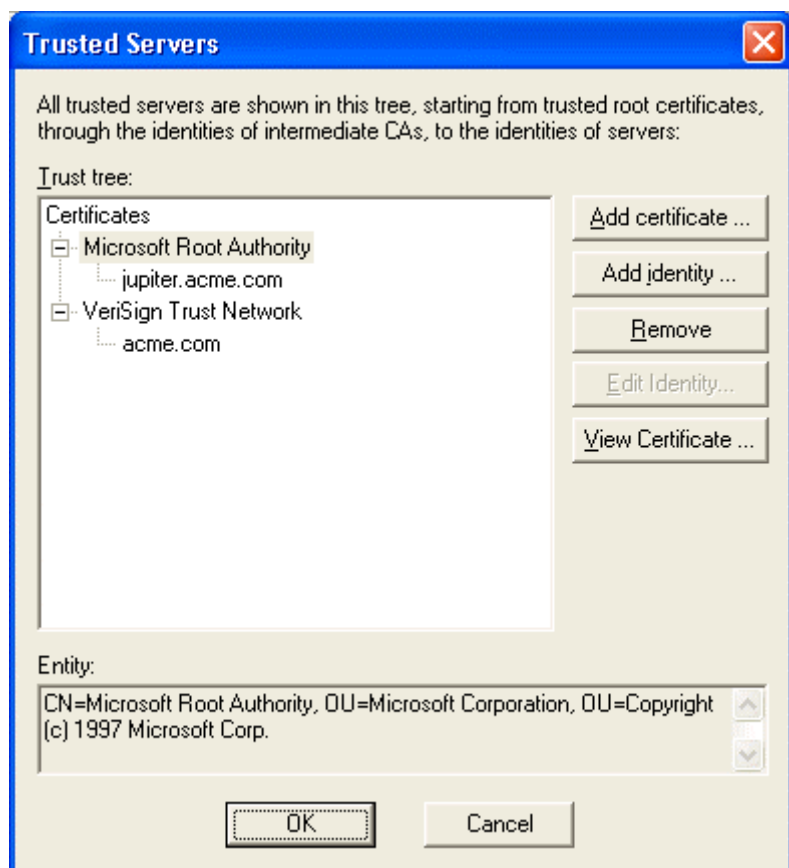
Cada ruta a través de la estructura Trust determina una cantidad de reglas para la determinación de una cadena de certificados. Odyssey Client confía en un servidor de autenticación sólo cuando su cadena de certificados coincide al menos con una ruta de la estructura Trust.

Una ruta a través de la estructura Trust está compuesta de dos o varios nodos:

- Cada nodo en el nivel más alto es el certificado de un Certificate Authority Root o Intermediate.
- Cada nodo intermedio (si existen) es el nombre de un Certificate Authority Intermediate en la cadena.
- Cada nodo final es el nombre de un servidor al que confía su autenticación. Los nombres de los Certificate Authorities y servidores pueden ser indicados como nombres de sujetos o nombres de dominios. Adicionalmente usted puede determinar que el nombre en un certificado debe corresponder exactamente con el nombre configurado o que este debe finalizar con el nombre configurado.

Indicación de la estructura Trust

Para mostrar la estructura Trust haga clic sobre *Advanced*. Aparece la ventana *Trusted Servers*, en la que podrá visualizar y modificar las reglas Trust.

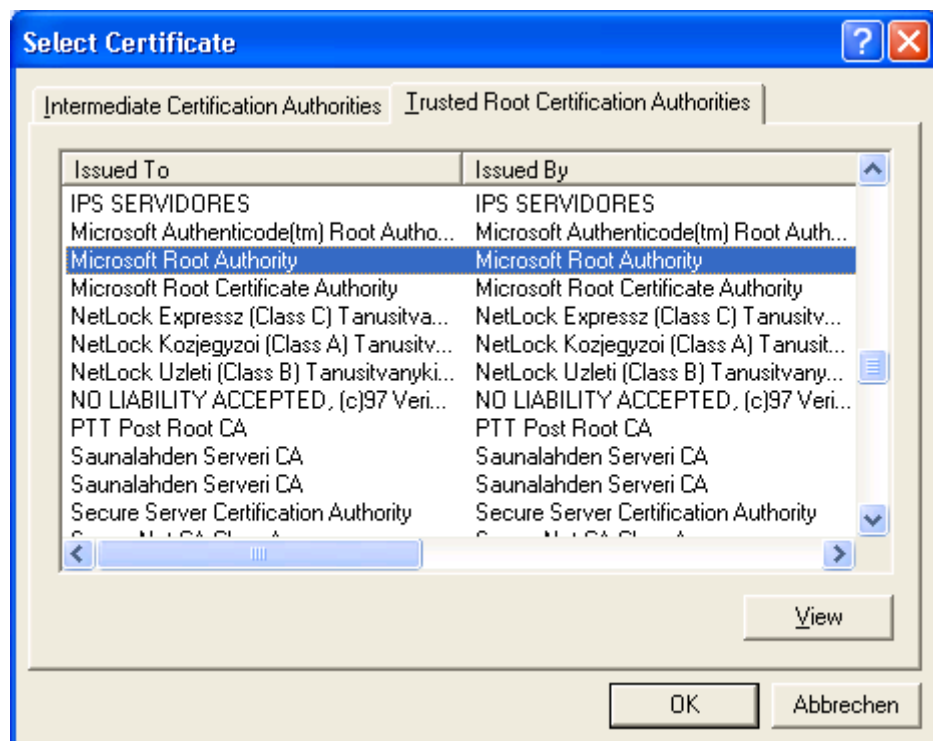


Añadir nodos de certificado

Para añadir un nuevo certificado al principio de la estructura Trust:

- ▶ Haga clic sobre *Add certificate*. Aparece la ventana *Select Certificate*.
- ▶ Seleccione un certificado y haga clic sobre *OK*. Podrá elegir o bien de la lista de los certificados Intermediate o de la de Trusted Root.

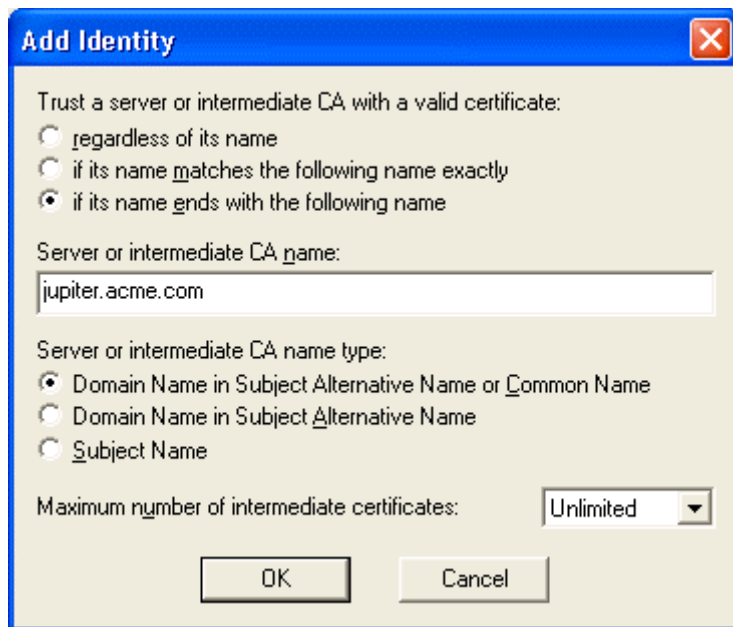
Para recibir indicaciones más detalladas sobre un certificado antes de añadirlo, seleccione el certificado y haga clic sobre *View*.



Añadir servidores de autenticación o nodos Intermediate CA

Todos los nodos por debajo del nivel superior identifican o bien servidores de autenticación o Certificate Authorities Intermediate. En caso de un nodo final, se parte de la base de que no denomina a ningún servidor de autenticación. En caso contrario se parte de la base de que este denomina a un Certificate Authority Intermediate. Para añadir un servidor de autenticación o un Certificate Authority Intermediate a la estructura:

- ▶ Seleccione el nodo en la estructura debajo del cual quiere añadir usted el nuevo elemento.
- ▶ Haga clic sobre *Add Identity*. Aparece la ventana *Add Identity*.
- ▶ Introduzca las informaciones que determinen las reglas que utiliza el Odyssey Client para la adaptación de un certificado en la cadena de certificados de servidor en estos nodos.
- ▶ Haga clic sobre *OK*.



Con ayuda de la ventana *Add Identity* usted puede ajustar las reglas de adaptación para un nodo individual de la estructura Trust.

Para la determinación de un servidor Trusted o Intermediate CA con certificado válido seleccione:

- *regardless of its name*, para adaptar un certificado independientemente de su nombre, suponiendo que este lleva el signo de Certificate Authority en el nodo superior.
- *if its name matches the following name exactly* para determinar que el nombre en el certificado debe corresponder exactamente con el nombre indicado por usted.
- *if its name ends with the following name* para determinar que el nombre en el certificado está subordinado al nombre indicado por usted. Un certificado por ejemplo con el nombre "sales.acme.com" correspondería con un registro "acme.com".

Para *Name of Server or intermediate CA* introduzca el nombre (o los elementos finales de un nombre) con los que usted desea la correspondencia. (Este campo no se necesita cuando la selección se realice independientemente del nombre.). La forma del nombre depende de su elección del tipo de nombre.

Para *Name type* usted tiene que indicar como se interpreta el nombre y dónde se puede encontrar el nombre en el certificado. Seleccione una de las siguientes opciones:

- *Domain name in Subject Alternative Name or Common Name*, cuando el nombre de dominio (p. ej.: *acme.com*) se encuentre en el campo *Subject Alternative Name* en el certificado, o en el caso de que no exista, el *Common Name* en el campo *Subject* del certificado (esta es la elección más usual).
- *Domain name in Subject Alternative Name*, cuando el nombre de dominio se encuentra en el campo *Subject Alternative Name* en el certificado. Es similar a la elección anterior, pero con restricciones.

- *Subject Name*, cuando el nombre es un nombre X.500 y se encuentra en el campo *Subject* del certificado. Cuando introduzca un nombre sujeto, completo o en parte, deberá hacerlo en el formato X.500. Se corresponderá con todos los nombres sujeto de Certificate equivalentes o subordinados.

- Si, por ejemplo, introduce lo siguiente:

`OU=acme.com, C=US`

el nombre corresponde con uno de los siguientes nombres sujeto:

`O=sales, OU=acme.com, C=USCN=george, O=sales, OU=acme.com, C=US`



Cuando usted introduce texto que contiene comas, cada coma deberá encontrarse entre comillas simples.

Como cantidad máxima de Intermediate Certificates, determine la cantidad máxima de certificados que puedan aparecer en la cadena entre este nodo y el nodo inmediatamente superior. Usted puede seleccionar un número entre 0 y 5 ó *unlimited* (ilimitado):

- Si usted selecciona 0, el certificado que corresponde con este nodo tiene que estar firmado, donde se utiliza el certificado que corresponde con el nodo por encima de este nodo.
- Si usted selecciona 1, el certificado que corresponde con este nodo puede estar firmado por el certificado que corresponde con el nodo superior, o por un certificado que de nuevo está firmado por el certificado que corresponde con el nodo superior.
- Si usted selecciona *unlimited*, puede aparecer cualquier cantidad de certificados en la cadena entre el certificado que corresponde con este nodo y uno que corresponde con el nodo superior.

Eliminar nodos

Para eliminar un nodo, seleccione el nodo que quiere eliminar en la estructura y haga clic sobre *Remove*. El nodo seleccionado y cada nodo a un nivel inferior serán eliminados de la estructura.

Será posible eliminar los siguientes nodos:

- Nodo Top-Level Certificate
- Nodo Intermediate CA
- Nodo de servidor

Visualizar información sobre un certificado

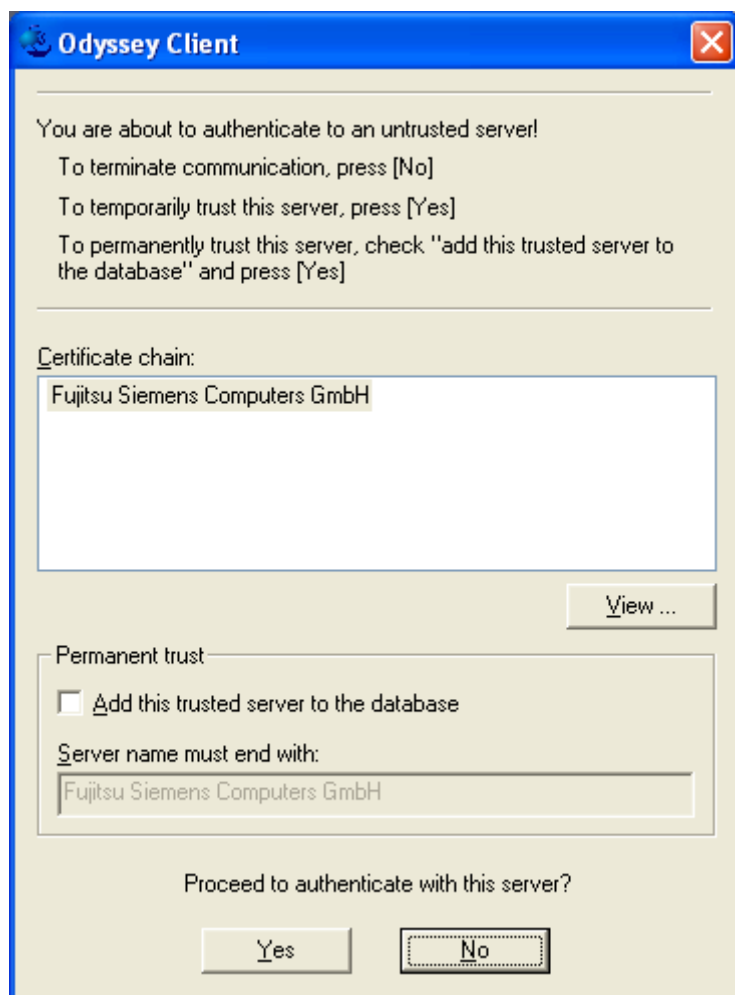
Para tener información más detallada sobre un certificado en el nivel superior de la estructura Trust, seleccione el certificado y haga clic sobre *View Certificate*.

Untrusted Server

Bajo las siguientes condiciones, usted tendrá la opción de seleccionar un anterior "Untrusted Server" durante la autenticación de red como servidor Trusted:

- Ha configurado Trust temporal (*Enable Server temporary trust*) en el menú *Security Settings*.
- El perfil de autenticación exige validación de servidor.
- El Trusted Root Certificate Authority del certificado de servidor (en el ejemplo presentado en la parte inferior el certificado "ACMERootCA") se instala en su cliente.

Aparece la siguiente ventana mientras usted autentifica la red.



La ventana muestra la cadena total de certificados entre el servidor de autenticación y un Trusted Root Certificate Authority. Recibirá más informaciones sobre un certificado en la cadena, seleccionando el certificado y haciendo clic sobre *View*.

En el caso de que este servidor deba ser utilizado temporalmente como Trusted Server (es decir, hasta que Odyssey se inicie de nuevo), para autenticar y establecer la conexión con la red haga clic sobre *Yes*. De lo contrario haga clic sobre *No*. Usted puede ser requerido a introducir su contraseña, dependiendo del perfil que usted ajuste para esta conexión.

Si usted desea este servidor como servidor Trusted permanente y quiere añadirlo a la lista de servidores Trusted, marque *Add this trusted Server to the database* y haga clic sobre *Yes*. El servidor será añadido a la lista de los servidores Trusted empleando como nombre de servidor el mismo que aparece en el campo *Server name must end with*. Usted puede editar el nombre del servidor. Por ejemplo usted puede, si el nombre del servidor es "auth2.acme.com", modificarlo a "acme.com" en el caso de que usted quiera utilizar como servidores Trusted todos los servidores de autenticación que pertenecen al dominio "acme.com".

Configurar tarjetas de red – Ventana "Adapters"

En la ventana *Adapters* usted puede seleccionar una o varias tarjetas de red para el servicio con redes inalámbricas. Usted puede determinar más de una tarjeta de red, si mantiene presionada la tecla **Ctrl** en su teclado mientras que usted realiza la selección con el ratón.

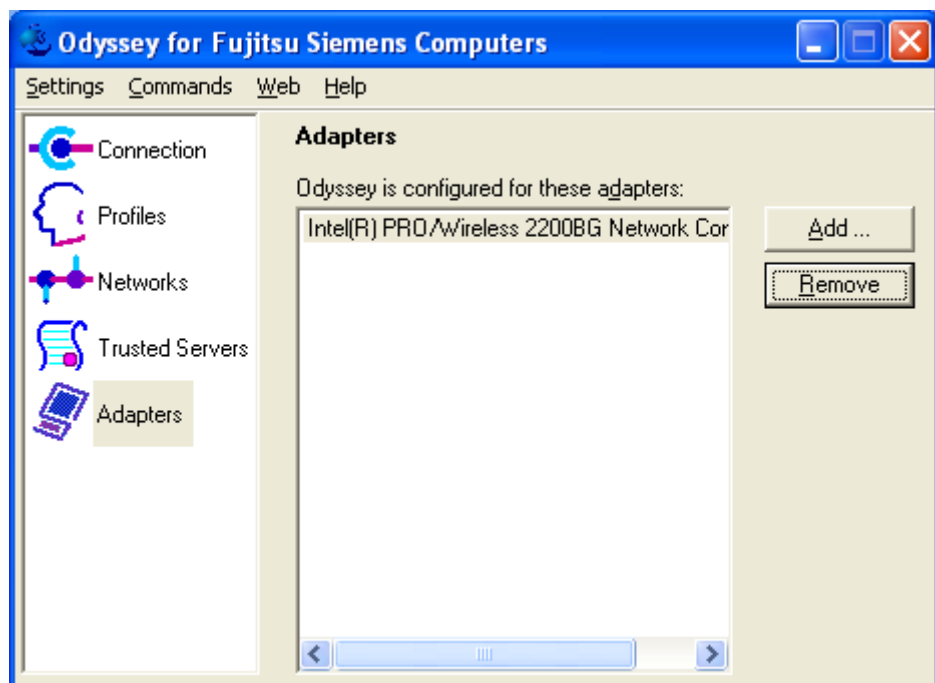
En la ventana *Adapters* se relacionan todas las tarjetas de red inalámbricas que están configuradas para Odyssey Client. Probablemente usted ha configurado una sola tarjeta de red. No obstante usted también puede configurar más de una tarjeta de red. Puede utilizar la ventana *Adapters* para las siguientes tareas:

- Añadir tarjeta de red inalámbrica
- Eliminar tarjeta de red de la lista



Su tarjeta de red ya ha tenido que ser instalada en su sistema antes de que usted pueda configurarla en Odyssey Client.

- En el Odyssey Client Manager, haga clic en *Adapters* para abrir la ventana.



Añadir tarjeta de red inalámbrica

Para añadir una tarjeta de red inalámbrica, que Odyssey Client todavía no ha reconocido, realice usted los siguientes pasos en la ventana *Adapters* del Odyssey Client Manager:

- Haga clic sobre *Add*. Aparece la ventana *Add Adapter* y muestra una lista de todas las tarjetas de red que están instaladas en su ordenador (excepto aquellas para las que Odyssey Client ya está configurado).



- Seleccione la ficha *Wireless*.
- Seleccione la tarjeta de red deseada de la lista y haga clic sobre *OK*.

Tenga en cuenta que sólo se muestran aquellas tarjetas de red que usted todavía no ha añadido. En caso de que sus tarjetas de red inalámbricas no aparezcan en la lista, seleccione *All Adapters*.



Preste atención a que todas las tarjetas de red seleccionadas por usted en la ficha *Wireless* realmente sean inalámbricas.

Eliminar tarjeta de red de la lista

Para eliminar una tarjeta de red de la lista en la ventana *Adapters*, seleccione la tarjeta de red que desee eliminar y haga clic sobre *Remove*.

Odyssey Client no utilizará más esta tarjeta de red. La tarjeta de red sigue estando instalada en su sistema, no obstante esta se comporta como si Odyssey Client no existiese.

Odyssey Client Manager - Menú "Settings"

En el menú *Settings* de la ventana *Odyssey Client Manager* están disponibles las siguientes opciones de menú:

- *Preferences*
- *Security settings*
- *Enable/Disable Odyssey*
- *Close*

Opción de menú "Preferences"

Usted puede variar el modo de trabajo de Odyssey Client con ayuda de la opción de menú *Preferences*. Aparece la ventana *Odyssey Preferences*.



Determine usted sus preferencias y haga clic sobre *OK* para que esta determinación sea efectiva:

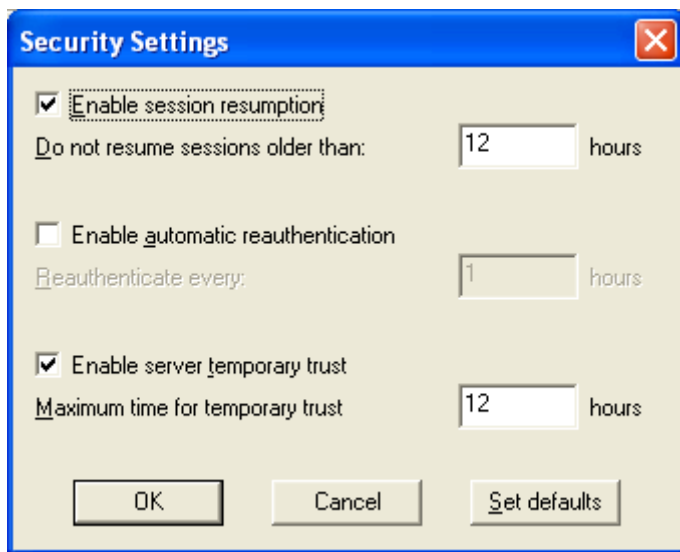
- Si usted selecciona *Hide tray icon*, el icono Odyssey no será mostrado en la barra de tareas (parte inferior derecha de su pantalla).
- Si usted selecciona *Hide control panel icon*, el icono Odyssey no se mostrará en el panel de control de Windows.



Cuando usted haya abierto el panel de control de Windows mientras usted selecciona *Hide control panel icon*, y después pulsa sobre *OK*, se actualiza el panel de control. (Presione la tecla **F5** para ver la actualización). En algunos casos la actualización será visible después de reiniciar el equipo.

Opción de menú "Security settings"

Para configurar opciones de seguridad avanzadas para la autenticación, seleccione *Security Settings*. Aparece la ventana *Security Settings*.



Las opciones de seguridad muestran valores estándar originales, que deberían ser apropiadas para la mayoría de las finalidades. Usted puede establecer de nuevo estos valores estándar en cualquier momento seleccionando *Set defaults*.

Los campos de tiempo indican valores por horas con un máximo de dos decimales. Cuando usted por ejemplo quiere indicar una hora y quince minutos, introduzca *1.25*.

Reanudación de una sesión

Con la ventana *Security Settings* usted puede activar la reanudación de la sesión.

Para activar la reanudación de la sesión:

- Active *Enable session resumption*.
- Ajuste *Do not resume sessions older than* al número máximo de horas que puede utilizar una autenticación para acelerar la autenticación renovada. Cuando el límite de tiempo haya transcurrido se realiza una autenticación completamente actualizada en su próxima reautenticación. La cantidad de las horas puede tener hasta dos cifras decimales. Cuando usted por ejemplo quiere indicar una hora y quince minutos, introduzca *1.25*.

Como ajuste estándar está activado *Session resumption*, y la autenticación se realiza para hasta 12 horas.

Para desactivar esta función, elimine usted la activación de *Enable session resumption*.

Reautenticación automática

Usted también puede activar o desactivar la función *Automatic reauthentication* en el Odyssey Client.

Marque *Enable automatic reauthentication* en la ventana *Security Settings* para que el Odyssey Client active la reautenticación periódica en el servidor.

Ajuste en el campo *Reauthenticate every* el espacio de tiempo en horas para que la reautenticación se realice automáticamente.

Elimine la activación de *Enable automatic reauthentication* en la ventana *Security Settings* para desactivar esta función.

Como ajuste estándar, *Automatic reauthentication* no está activado. La razón para ello es que su administrador de red puede haber configurado eventualmente sus puntos de acceso (AccessPoints) o servidor de autenticación de tal forma que la autenticación deba ser renovada periódicamente. Consulte a su administrador de red el ajuste correcto para esta opción.

Server temporary trust

Normalmente configurará su servidor de autenticación en la ventana *Trusted Servers*. No obstante puede ocurrir que usted busque una red cuyo servidor de autenticación todavía no haya sido configurado como servidor Trusted en la ventana *Trusted Servers*. En este caso podrá activar la opción *Temporary Trust* (fiabilidad temporal) para este servidor Untrusted (servidor no fiable).

Active *Enable Server temporary trust* en la ventana *Security Settings* para activar *Temporary Trust*. Cuando usted elimina esta marca, la función se desactiva de nuevo. Tenga en cuenta lo siguiente en esta función:

- En el caso que *Temporary Trust* este activado, tiene usted la opción de confiar en un servidor Untrusted temporalmente en el intento de autenticar un servidor Untrusted. Véase también "Untrusted Server".
- En la ventana *Untrusted Server*, que se abre al intentar autenticar un servidor sin la propiedad Trust configurada, usted puede añadir el servidor a su estructura Trust de forma permanente. Por lo tanto, podrá emplear *Temporary trust* como alternativa a la ventana *Trusted Servers* para configurar servidores fiables en caso necesario.
- En el caso que *Temporary trust* no este conectado, fracasa cada intento de autenticación que exija la validación de un certificado de servidor cuando el servidor no es explícitamente un servidor Trusted.

Ajuste *Maximum time for temporary trust* a la cantidad máxima de horas durante las cuales el Odyssey Client debe seguir utilizando un servidor como servidor Trusted después de que usted lo haya aceptado.

Como ajuste estándar, *Temporary trust* está activado y 12 horas es el tiempo máximo para un servidor Trusted especialmente temporal después de que usted lo haya aceptado.



Estos ajustes no son relevantes cuando usted decide tratar el servidor como servidor Trusted de forma permanente, marcando el campo *Add this trusted Server to the database* en la ventana *Untrusted Server*.

Opción de menú "Enable/Disable Odyssey"

Seleccione *Enable Odyssey* o *Disable Odyssey* para conectar o desconectar el Odyssey Client. Al principio el Odyssey Client está activado y normalmente no necesita desactivarlo. En el caso de que usted seleccione *Disable Odyssey Client*, se separarán todas las tarjetas de red sin que se modifiquen los ajustes en la ventana *Connection*. El programa Odyssey Client todavía funciona, pero está separado por completo de las conexiones de la tarjeta de red de inalámbrica.

Sólo deberá desactivar el Odyssey Client cuando tenga problemas con su actual configuración Odyssey. Por ejemplo usted podría desactivar Odyssey Client cuando usted tema que este se encuentra en un estado inseguro y usted solo quiera asegurar que está separado de la red hasta que reciba la posibilidad de comprobar sus ajustes.

Odyssey Client también puede ser activado y desactivado a través del menú de contexto, que aparece cuando usted hace clic con el botón derecho del ratón sobre el icono de Odyssey en la barra de tareas.



Para finalizar por completo Odyssey Client, seleccione la opción de menú *Exit* haciendo clic con el botón derecho del ratón sobre el icono de Odyssey en la barra de tareas.

Opción de menú "Close"

Seleccione *Close* para cerrar la ventana de Odyssey Client Manager. A pesar de que la superficie de usuario ya no es visible, Odyssey Client continúa normalmente con su servicio de red.

Usted puede reiniciar Odyssey Client Manager en cualquier momento del siguiente modo:

- en la barra de tareas: haga doble clic sobre el icono Odyssey o haga clic sobre él con el botón derecho del ratón y seleccione *Odyssey for Fujitsu Siemens Computers*.
- en el panel de control: haga doble clic sobre el icono *Odyssey for Fujitsu Siemens Computers*.
- del menú de Inicio del Windows: seleccione *Inicio – Programas – Fujitsu Siemens Computers – Odyssey Client for Fujitsu Siemens Computers – Odyssey Client Manager for Fujitsu Siemens Computers*.



Para finalizar por completo Odyssey Client, seleccione la opción de menú *Exit* haciendo clic con el botón derecho del ratón sobre el icono de Odyssey en la barra de tareas.

Odyssey Client Manager - Menú "Commands"

Las siguientes opciones de menú están disponibles en el menú *Commands*:

- *Forget Password*
- *Forget Temporary Trust*

Opción de menú "Forget Password"

Cuando se autentifique por primera vez con un perfil que esté configurado con *prompt for password*, se le solicitará la introducción de su contraseña. Odyssey Client almacenará esta contraseña y la empleará para cualquier autenticación posterior mediante este perfil, sin que tenga que volver a introducirla de nuevo. Esta contraseña permanecerá almacenada normalmente hasta que arranque de nuevo su ordenador o el Odyssey Client.

Si no desea que Odyssey Client almacene las contraseñas introducidas, seleccione *Forget Password*. Cuando su contraseña se necesite de nuevo, usted será requerido a introducirla nuevamente.

Usted podría volver a utilizar esta opción de menú cuando usted introduce su contraseña erróneamente o cuando su contraseña fue modificada en el servidor de autenticación.

Opción de menú "Forget Temporary Trust"

En caso que usted active *Temporary trust* a través de los ajustes *Settings - Security Settings*, se abrirá una ventana siempre que usted encuentre un servidor de autenticación no fiable. En esta ventana usted puede utilizar este servidor como servidor Trusted temporal. Odyssey Client recuerda este servidor Trusted mientras esto se encuentre configurado en *Security Settings*.

Si desea que la lista de servidores Trusted temporales sea borrada inmediatamente, seleccione *Forget Temporary Trust*.

Usted puede utilizar esta opción de menú cuando usted acepte un servidor como servidor Trusted temporal y después decida interrumpir su conexión con él. Cuando usted quiera asegurar que la conexión se interrumpa de inmediato, desactiva *Session resumption* y hace clic sobre *Reconnect* en la ventana *Connection*.

Odyssey Client Manager - Menú "Help"

El menú *Help* comprende las siguientes opciones de menú:

- *Help topics*
- *License keys*
- *View Readme File*
- *About*

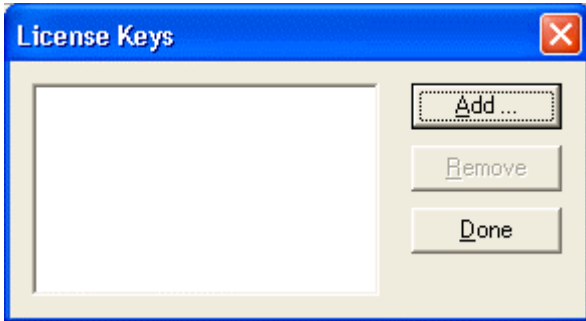
Opción de menú "Help topics"

Seleccione *Help Topics* para llegar al sistema de ayuda de Odyssey Client.

Usted puede recibir ayuda contextual en cualquier momento presionando la tecla **F1**. El sistema de ayuda se abre en el capítulo en el que mejor se puede explicar su situación momentánea.

Opción de menú "License keys"

Seleccione *License Keys* en el menú de ayuda para administrar su clave de licencia Odyssey Client.



Una clave de licencia es una secuencia de texto que representa su licencia para la utilización de Odyssey Client.

Menú de contexto "Odyssey"

Cuando usted hace clic con el botón derecho del ratón sobre el icono Odyssey en la barra de tareas, aparecen las siguientes opciones de menú:

- *Odyssey for Fujitsu Siemens Computers*
- *Enable Odyssey* o *Disable Odyssey*
- *Help*
- *Exit*

Opción de menú "Odyssey for Fujitsu Siemens Computers"

Si selecciona la opción de menú *Odyssey for Fujitsu Siemens Computers*, aparecerá el Odyssey Client Manager (la interfaz de usuario para Odyssey Client).

Opción de menú "Enable Odyssey/Disable Odyssey"

Seleccione *Enable Odyssey* o *Disable Odyssey* para conectar o desconectar el Odyssey Client.

Al principio el Odyssey Client está activado y habitualmente no necesita desactivarlo. En el caso de que usted seleccione *Disable Odyssey Client*, se separarán todas las tarjetas de red sin que se modifiquen los ajustes en la ventana *Connection*. El programa Odyssey Client todavía funciona, pero está separado por completo de las conexiones de la tarjeta de red de inalámbrica.

Sólo deberá desactivar el Odyssey Client cuando tenga problemas con su actual configuración Odyssey. Por ejemplo usted podría desactivar Odyssey Client cuando usted tema que este se encuentra en un estado inseguro y usted solo quiera asegurar que está separado de la red hasta que reciba la posibilidad de comprobar sus ajustes.

Odyssey Client también puede activarse o desactivarse por medio del Odyssey Client Manager.

Opción de menú "Help"

Help es una de las opciones de menú que aparecen cuando usted hace clic sobre el icono de Odyssey de la barra de tareas con el botón derecho del ratón. Hay dos opciones disponibles: *Help Topics* y *About*.

Si usted selecciona *Help Topics*, aparece el sistema de ayuda en una ventana con el índice de contenido abierto.

Si usted selecciona *About*, se muestran las informaciones sobre la versión de producto y Copyright.

Opción de menú "Exit"

Si usted selecciona *Exit*, Odyssey Client detiene de inmediato su funcionamiento en el fondo. Utilice esta opción eventualmente cuando no realice ningún servicio de red durante un espacio de tiempo prolongado.

Podrá iniciar de nuevo el Odyssey Client con ayuda del *Odyssey Client Manager* en *Inicio – Programas – Fujitsu Siemens Computers – Odyssey Client for Fujitsu Siemens Computers – Odyssey Client Manager for Fujitsu Siemens Computers*.

Features

Overview

Standard

- IEEE802.11g
- IEEE802.11b
- IEEE802.11 legacy

Baseband MAC

- GlobespanVirata / Intersil: Cohiba
- Wireless LAN Integrated Medium Access Controller with Baseband Processor
- ISL3887IK 192pin BGA

Memory

- 64 kBit Serial I2C bus EEPROM
- On Baseband MAC SRAM

RF Frontend

- GlobespanVirata / Intersil: Cohiba
- VCO: 5GHz Voltage Controlled Oscillator ISL3084IR
- TX/RX Direct Down Conversion Transceiver ISL3686BIR
- Low Cost Zero IF architecture
- TX: Power Amplifier ISL3980
- Transmit Power Control
- Frequency Range: 2412 to 2472 MHz (EU)

RF I/O Power

- RF Output Power: max: +19 dBm
- RF Receive Sensitivity : min -96 dBm

Communication

- Interface: USB 2.0
- RF Link: omni antenna 2.4 GHz
- Channels: 1 to 13 (EU) selectable
- Time access: CSMA/CA

Data Rates

- 802.11g-Prism Nitro: 100 Mbps OFDM
- 802.11g: 54, 48, 36, 24, 18, 12, 9 and 6 Mbps OFDM
- 802.11b: 11 and 5,5 Mbps CCK
- 802.11 legacy: 2 and 1 Mbps

Modulation

- RF modulations: OFDM and CCK
- Baseband modulations: BPSK, QPSK, 16QAM and 64 QAM
- Convolutional Coding and Interleaving
- Targeted for Multipath Delayed Spreads of 120 ns at 54 Mbps

Features

Regulatory Approvals

- Compliance to ETSI (EU)
- Compliance to FCCI (US)
- Quality: WIFI (tested without label)
- Software Driver: WHQL

Power Supply

- U = 5V (from USB)
- I < 495 mA

Basic security features

- WLAN security By WIN Software
- Internal 64 or 128 bit WEP engine
- Encryption protocol is RSA RC4

Software drivers

- Supported Operating Systems: WIN 98/ME/2k/XP and follower

Software Access Point

- Soft AP with PC-Tel Segue SAM (when required)

Wake On WLAN

- Supported (depends from Software)

Form factor

- 54 x 88,8 mm

Technical details

RF Output Power

Typical Output Power

Transmitter Specifications	Condition	Power [dBm]
IEEE802.11g	6 Mbps OFDM	19
	9 Mbps OFDM	19
	12 Mbps OFDM	18.2
	18 Mbps OFDM	18.3
	24 Mbps OFDM	17
	36 Mbps OFDM	17
	48 Mbps OFDM	13.9
	54 Mbps OFDM	13.9
IEEE802.11b	1 Mbps BPSK	18.7
	2 Mbps QPSK	
	5.5 Mbps CCK	
	11 Mbps CCK	

RF Input Sensitivity

Typical Input Sensitivity

Transmitter Specifications	Condition	Power [dBm]
IEEE802.11g @ 10 % PERI	6 Mbps OFDM	-91.1
	9 Mbps OFDM	-89.2
	12 Mbps OFDM	-87.7
	18 Mbps OFDM	-85
	24 Mbps OFDM	-81.1
	36 Mbps OFDM	-77.3
	48 Mbps OFDM	-72.1
	54 Mbps OFDM	-70.2
IEEE802.11b @ 8% PER	1 Mbps BPSK	-96.0
	2 Mbps QPSK	-92.5
	5.5 Mbps CCK	-91.0
	11 Mbps CCK	-86.7

Communication Range

Typical communication range:

Please note that this is valid for typical environment!

Data Rate [Mbps]	Indoor Range [m]	Outdoor Range [m]
54	9,5	116
48	12	180
36	19	270
24	25	370
18	30	480
12	36	570
9	44	650
6	55	700

Communication

Channels

Channel Number	Channel Frequency	Geographic Usage
1	2412 MHz	US, EU, J
2	2417 MHz	US, EU, J
3	2422 MHz	US, EU, J
4	2427 MHz	US, EU, J
5	2432 MHz	US, EU, J
6	2437 MHz	US, EU, J
7	2442 MHz	US, EU, J
8	2447 MHz	US, EU, J
9	2452 MHz	US, EU, J
10	2457 MHz	US, EU, FR, J
11	2462 MHz	US, EU, FR, J
12	2467 MHz	EU, FR, J
13	2472 MHz	EU, FR, J
14	2484 MHz	J (802.11b only)

Regulatory Approvals

Compliance:

Country	Approval	Notes
USA	FCC part 15, sec 15.107, 15.109. 15.207, 15.209, 15.247	Yes
EU	EN60950 incl. A1 - A4 ETSI EN300328 P1 V1.2.2 ETSI EN300328 P2 V1.1.1 ETSI EN301893 V1.2.1 ETSI EN301489-1 V1.4.1 ETSI EN301489-17 V1.1.1	Yes
Japan	ARIB STD-T71 V1.0, 14 ARIB RCR STD-T33 ARIB STD-T66 V2.0	No

Declaration of Conformity

Konformitätserklärung gemäß dem Gesetz über Funkanlagen und Telekommunikationsendeinrichtungen (FTEG) und der Richtlinie 1999/5/EG (R&TTE)

Declaration of Conformity in accordance with the Radio and Telecommunications Terminal Equipment Act (FTEG) and Directive 1999/5/EC (R&TTE Directive)

Fujitsu Siemens Computers GmbH
Bürgermeister-Ulrich-Str. 100
86199 Augsburg, Germany

Hersteller /Verantwortliche Person // The manufacturer / responsible person

erklärt, dass das Produkt WLAN Module D1700
declares that the product

Type (ggf. Anlagenkonfiguration mit Angabe der Module): D1700 B/ D1700 D/ D1700 E
Type (if applicable, configuration including the modules)

☐ Telekommunikations(Tk-)endeinrichtung
Telecommunications terminal equipment

☒ Funkanlage
Radio equipment

Verwendungszweck: 802.11g WLAN USB Adapter.
Intended purpose

Gerätekategorie
Equipment class

bei bestimmungsgemäßer Verwendung den grundlegenden Anforderungen des § 3 und den übrigen einschlägigen Bestimmungen des FTEG (Artikel 3 der R&TTE) entspricht.
complies with the essential requirements of §3 and the other relevant provisions of the FTEG (Article 3 of the R&TTE Directive), when used for its intended purpose.

Gesundheit und Sicherheit gemäß § 3 (1) 1. (Artikel 3 (1) a))
Health and safety requirements pursuant to § 3 (1) 1. (Article 3(1) a))

angewendete harmonisierte Normen ...
Harmonised standards applied...
EN 60950-1 : 2001

Einhaltung der grundlegenden Anforderungen auf andere Art und Weise (hierzu verwendete Standards/ Spezifikationen) ...
Other means of proving conformity with the essential requirements (standards/specifications used)...

Schutzanforderungen in Bezug auf die elektromagn. Verträglichkeit § 3 (1) 2, Artikel 3 (1) b))
Protection requirements concerning electromagnetic compatibility § 3(1)(2), (Article 3(1)(b))

angewendete harmonisierte Normen
Harmonised standards applied...
EN 301 489-17 : 2002

Einhaltung der grundlegenden Anforderungen auf andere Art und Weise (hierzu verwendete Standards/ Spezifikationen) ...

Other means of proving conformity with the essential requirements (standards/specifications used)...

Índice de materias

A

- Access point (infrastructure mode) 31
- AccessPoint 2
- Adapters 12
- Anonymous name 24
- Autenticación 4
 - 802.1X 33
 - descripción 4
 - modo Open 31
 - sin clave WEP 31
 - clave WEP 4, 31
 - con perfil 32
 - generación automática de claves 32
 - modo de asignación, indicar 31
 - modo Open 31
 - modo Shared 31
 - modo WPA 31
 - opciones de seguridad avanzadas 47
 - reautenticación automática 48
- WPA 31
 - AES 31
 - clave pre-shared 32
 - frase de acceso 32

C

- Cadena de certificados 37
- Certificación de autorización 5
- Certificado 19, 35
- Certificate Authority 35
- Clave de licencia Odyssey Client 51
- Clave pre-shared
 - descripción 4
 - introducir 33
- Clave WEP 4
 - introducir 33
- Close 49
- Codificación
 - de datos AES 31
 - TKIP 4, 31
- Conexion de red
 - controlar 12
 - desconectar 15
 - establecer 13
 - establecer (con cualquier red) 30
 - reautenticar 15
 - visualizar estado 15
- Conexión inalámbrica, deficiente 15
- Configuración, Odyssey Client 11
- Configure and Enable Wizard 10
- Connect to any available network 30

- Connection 12
 - indicación del estado de conexión 15
- Contraseña
 - entrada 19
 - no almacenar 50
- Convenciones 1

Ch

- CHAP 23

D

- Denominación de red 28
- Descripción de red 30
- Directiva 1999/5/CE 6
- Dominio de servidor 35

E

- EAP 5
- EAP/PEAP 24
- EAP-TLS 32
- EAP-TTLS 22, 32
 - nombre anónimo, determinar 24
- Enable Odyssey/Disable Odyssey 51
- Enable Server temporary trust 42
- Enable session resumption 47
- Enable/Disable Odyssey 49
- Estándar
 - 802.1X 5
 - IEEE 802.11b, frecuencias 8
 - IEEE-Standard 802.11, frecuencias 7
- Estructura Trust 37
 - añadir nodo de certificado 38
 - eliminar nodo de certificado 41
 - indicar 38
- Extensible Authentication Protocol 5

F

- Forget Password 50
- Forget Temporary Trust 50
- Frecuencias radioeléctricas 7

I

- Icono Odyssey
 - no se muestra en la barra de tareas 46
 - se muestra en la barra de tareas 46
- Indicaciones de seguridad 6
- Información sobre un certificado, visualizar 41

Inner Authentication Protocol 23
Instalación, Odyssey Client 9
Intermediate Certificates
 añadir a la estructura Trust 39
 número máximo 41

L

License keys 51

M

Marcado CE 6
Menú
 Commands 49
 de contexto Odyssey 51
 Help 50
 Settings 46

Modo

Adhoc 2
de infraestructura 2
Peer-to-Peer 2

MS-CHAP-V2. 23

N

Network name (SSID) 30
Networks 12, 27
Nodo de certificado, añadir 38
Nombre
 anónimo, determinar 24
 de red 28
 de usuario 19
 login 19

O

Odyssey Client
 configurar 11
 finalizar 49, 52
 instalar 9
 Manager 11
 visualizar 51
Open, modo 31

P

PAP/Token 23
PEAP 32
PEAP Settings 25
Peer-to-peer (ad-hoc mode) 31
Perfiles, definir 16
Profiles 12, 16

Protocolo de autenticación 21
 EAP 5
 EAP-TLS 21
 EAP-TTLS 22
 interior 23
 PEAP 21

R

Reautenticación automática 48
Red inalámbrica
 buscar 13
 configurar 27, 28
 establecer conexión de red 13
 nombre 3
 norma IEEE 802.11 1
 Reconnect 15
 Service Set Identifier (SSID) 3
Red, buscar 30

S

Seguridad de red
 802.11 3
 autenticación 3
 clave WEP 3
Server temporary trust 48
Servidor de autenticación 21
 añadir a la estructura Trust 39
 Enable Server temporary trust 42
 Server temporary trust 48
 Trusted Server 34
 verificación de la identidad 21
Servidores fiables, véase Trusted
 Servers 34
Sesión Odyssey, reanudación 47
Shared, modo 31

T

Tarjeta de red
 activar 44
 configurar 43
 desactivar 45
 inalámbrica, configurar 44
Tipo de rec
 Adhoc 2
Tipo de red
 indicar 31
 infraestructura 2
Trusted Root Certificate Authority 43

Trusted Servers 12, 34
 añadir 35
 borrar 36
 editar 36
 estructura Trust 37
 procedimiento avanzado para controles
 de confianza 37
 procedimiento sencillo para controles
 de confianza 35

U

Untrusted Server 42

V

Ventana

 Adapters 12, 43
 Connection 12, 15
 Networks 12, 27
 Profiles 12, 16
 Trusted Servers 12, 34

W

Wi-Fi Protected Access (WPA) 4
Wired-Equivalent Privacy (WEP) 4
WPA, descripción 4