

# answers<sup>2</sup>

Guide d'utilisateur

## Wireless LAN

Français



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 sobre papel reciclado.  
Questo manuale è stato stampato su carta da riciclaggio.  
Denna handbok är tryckt på recyclingpapper.  
Dit handboek werd op recycling-papier gedrukt.

Publié par  
Fujitsu Siemens Computers GmbH

No de référence : **A26391-K133-Z131-1-7719**  
Edition **3**  
Printed in the Federal Republic of Germany  
AG 0704 07/04

# Wireless LAN

## Guide d'utilisateur

Wireless LAN -  
Généralités

Installation d'Odyssey

Utilisation d'Odyssey  
Client

Index

Microsoft, MS, MS-DOS, Windows et Windows NT sont des marques déposées de Microsoft Corporation.

Odyssey est une marque commerciale déposée de Funk Software.

Toutes les autres marques commerciales citées sont des marques commerciales ou des marques déposées par leurs propriétaires respectifs et sont protégées comme tel.

Copyright © Fujitsu Siemens Computers GmbH 2004

Tous droits réservés, y compris celui de la traduction, de la reproduction, de la duplication (même partielles) par photocopie ou procédé analogue.

Tout manquement à cette règle expose son auteur au versement de dommages et intérêts.

Tous droits réservés, y compris en cas d'octroi de brevet ou d'enregistrement comme modèle d'utilité.

Sous réserve de disponibilité et de modifications techniques.

Ce manuel a été rédigé par  
cognitas. Gesellschaft für Technik-Dokumentation mbH  
[www.cognitas.de](http://www.cognitas.de)

---

# Sommaire

<b>Wireless LAN - Généralités</b> .....	<b>1</b>
Réseau radio selon la norme IEEE 802.11 .....	1
Mode Adhoc .....	2
Mode Infrastructure.....	2
Système d'exploitation requis .....	2
Noms des réseaux radio (SSID) .....	3
Sécurité réseau 802.11.....	3
Wired-Equivalent Privacy (WEP) avec clés préconfigurées .....	4
Wi-Fi Protected Access (WPA) et chiffrement TKIP .....	4
Norme 802.1X .....	5
Extensible Authentication Protocol (EAP) .....	5
Remarques importantes .....	6
Consignes de sécurité .....	6
Marquage CE.....	6
Fréquences radio et normes de sécurité.....	7
<b>Installation d'Odyssey</b> .....	<b>9</b>
Installation d'Odyssey Client.....	9
Configure and Enable Wizard .....	9
<b>Utilisation d'Odyssey Client</b> .....	<b>11</b>
Aperçu de l'Odyssey Client Manager .....	11
L'écran Odyssey Client Manager .....	12
Utiliser les connexions réseau - Fenêtre "Connection" .....	12
Sélectionner la carte réseau .....	13
Se connecter à un réseau.....	13
Rechercher les réseaux radio .....	13
Se reconnecter à un réseau.....	15
Se ré-authentifier au réseau.....	15
Couper la connexion réseau .....	15
Visualiser les données de connexion.....	15
Définir des profils - Fenêtre "Profiles" .....	16
Ajouter et modifier un profil - Fenêtre "Profile Properties" .....	17
Onglet "Authentication" .....	20
Configurer des réseaux radio - Fenêtre "Networks" .....	27
Ajouter ou modifier des réseaux – Fenêtre "Network Properties".....	28
Spécifier des serveurs dignes de confiance - Fenêtre "Trusted Servers" .....	34
Procédure simple de configuration des serveurs de confiance .....	35
Procédure élargie de configuration des serveurs de confiance .....	37
Untrusted Server.....	42
Configurer des cartes réseau - Fenêtre "Adapters" .....	43
Ajouter une carte réseau sans fil .....	44
Supprimer une carte réseau de la liste.....	45
Odyssey Client Manager - Menu "Settings" .....	46
Option de menu "Preferences".....	46
Option de menu "Security settings".....	47
Option de menu "Enable/Disable Odyssey" .....	49
Option de menu "Close".....	49
Odyssey Client Manager - Menu "Commands" .....	50
Option de menu "Forget Password" .....	50
Option de menu "Forget Temporary Trust" .....	50

Odyssey Client Manager – Menu "Help" ..... 50

    Option de menu "Help topics" ..... 51

    Option de menu "License keys" ..... 51

Menu contextuel "Odyssey" ..... 51

    Option de menu "Odyssey for Fujitsu Siemens Computers" ..... 51

    Option de menu "Enable Odyssey/Disable Odyssey" ..... 52

    Option de menu "Help" ..... 52

    Option de menu "Exit" ..... 52

**Features ..... 53**

    Overview ..... 53

    Technical details ..... 54

**Declaration of Conformity ..... 57**

**Index ..... 59**



# Wireless LAN - Généralités

Votre appareil est équipé d'une carte réseau radio. Vous trouverez dans le présent guide d'utilisateur une description des réglages à effectuer pour votre carte Wireless LAN.

## Symboles

Les symboles suivants sont utilisés dans ce manuel.



signale des instructions à respecter impérativement pour votre propre sécurité, celle de votre appareil et celle de vos données. La garantie s'éteint dès l'instant où vous endommagez l'appareil en ne respectant pas ces consignes.



signale des informations importantes pour la bonne utilisation du système.

► signale une opération que vous devez exécuter.

Les textes en caractères machine correspondent à des affichages écran.

Les caractères en italiques symbolisent des commandes ou des options de menu.

"Entre guillemets" sert à identifier des titres de chapitres, des noms de disquettes et d'autres noms de média et différents concepts à mettre en évidence.

## Réseau radio selon la norme IEEE 802.11

La carte réseau radio intégrée fonctionne selon la norme IEEE 802.11. S'agissant d'un support de communication, elle utilise les fréquences des bandes de fréquences ISM (ISM, Industrial, Scientific, Medical). La carte réseau radio peut s'utiliser gratuitement et sans abonnement. La famille des normes IEEE 802.11 prévoit plusieurs façons d'exploiter les bandes de fréquences ISM :

IEEE 802.11a	Bande 5,0 GHz	54 Mbit/s
IEEE 802.11b	Bande 2,4 GHz	11 Mbit/s
IEEE 802.11g	Bande 2,4 GHz	54 Mbit/s

Les réseaux radio basés sur la norme 802.11 peuvent être facilement reliés à des réseaux Ethernet existants. Les cartes réseau radio basées sur la norme 802.11 sont comparables à une carte Ethernet normale à la seule différence près qu'elles offrent quelques paramètres supplémentaires. Vous pouvez en effet utiliser tous les protocoles sur un réseau radio 802.11 comme sur un réseau Ethernet câblé (IP, IPX, NetBIOS,...). La seule différence réside dans le fait qu'il ne faut pas poser de câbles entre les ordinateurs. On appelle généralement une cellule radio l'ensemble des stations Wireless LAN qui sont en communication directe les unes avec les autres. La norme IEEE offre deux modes d'exploitation, le mode Adhoc ('peer-to-peer' ou point à point) et le mode Infrastructure.

Cette norme non seulement décrit la modulation et le tramage de données ('data framing') mais elle renferme également un procédé d'authentification et de cryptage appelé Wired Equivalent Privacy (WEP). De nombreuses entreprises utilisent des réseaux radio 802.11. Les réseaux radio 802.11 sont à présent proposés également dans des hôtels, des aéroports et autres "hotspots" offrant un accès à Internet.

### Mode Adhoc

Un réseau Wireless LAN en mode Adhoc, appelé aussi 'peer-to-peer', se compose d'une cellule radio fermée unique. On est en présence de réseaux radio Adhoc lorsqu'un groupe de travail se met en place et souhaite interconnecter les systèmes pour procéder à des échanges de données. D'autres systèmes peuvent se rajouter à ce type de réseau puis en être retirés.

Afin d'éviter que plusieurs réseaux radio Adhoc ne se gênent mutuellement lors des communications radio, chacun possède un identifiant de réseau bien défini, le SSID (Service Set Identifier). Le SSID s'utilise pour l'adressage afin qu'un paquet de données puisse toujours être affecté à une cellule radio donnée.

Pour pouvoir participer à un réseau radio en place, vous devez connaître son identifiant (SSID) que vous spécifiez dans les réglages de votre carte réseau. Au démarrage, la carte réseau recherche un réseau radio possédant cette identification SSID. Lorsque la carte réseau trouve un réseau radio, elle se branche sur celui-ci et vous pouvez alors communiquer avec les autres systèmes de ce réseau radio. Lorsque deux cellules radio sont très proches l'une de l'autre, les canaux radio devraient être séparés de 4 à 5 canaux l'un de l'autre. Cette règle s'applique à la norme 802.11b et à la norme 802.11g.

### Mode Infrastructure

En mode Infrastructure, les stations mobiles côtoient une station de base que l'on appelle AccessPoint (relais). Dans ce mode, l'AccessPoint exerce la fonction de "gardien". Contrairement au mode Adhoc, chaque système doit s'annoncer auprès de l'AccessPoint avant d'être autorisé à échanger des données au sein de la cellule radio.

L'autre fonction de l'AccessPoint consiste à relier les cellules radio à un réseau Ethernet câblé. Dans la mesure où l'AccessPoint sait à tout moment - par l'obligation pour les stations de s'annoncer - quelles sont celles qui se trouvent actuellement sur le réseau radio, il peut décider avec précision quelles sont les données à transmettre et à ne pas transmettre. Cette opération s'appelle le "bridging" (pontage).

Pour étendre la portée d'un réseau radio, il est possible d'utiliser plusieurs AccessPoints dotés d'une même SSID.

Lorsqu'un système intègre un réseau radio, il recherche parmi les AccessPoints accessibles celui qui possède le signal radio le plus fort et s'y annonce. Deux systèmes annoncés auprès d'AccessPoints différents peuvent ainsi communiquer l'un avec l'autre même s'ils ne se trouvent pas à portée directe l'un de l'autre. Après s'être annoncé, un système continue à surveiller l'état des signaux radio et peut reconnaître l'affaiblissement des signaux d'un AccessPoint et le renforcement des signaux d'un autre de manière à se désannoncer sans que l'utilisateur ne le remarque. Cette opération s'appelle le "roaming" (itinérance).

### Système d'exploitation requis

Systèmes d'exploitation Windows 2000 et Windows XP

## Noms des réseaux radio (SSID)

Chaque réseau radio possède un nom bien à lui. Vous pouvez sélectionner le réseau radio auquel vous souhaitez vous connecter par son nom. Les noms de réseau permettent à différents réseaux radio de coexister dans un même environnement sans qu'ils interfèrent les uns avec les autres. Si l'entreprise voisine, par exemple, utilise elle aussi des réseaux radio, vous voulez être certain que votre ordinateur est connecté au réseau de votre entreprise et non à celui de l'entreprise voisine même si votre ordinateur est situé à proximité immédiate des AccessPoints (points d'accès). (la rubrique ci-dessous consacrée à la sécurité explique précisément comment empêcher des intrus de se connecter au réseau de votre entreprise.) Un nom de réseau est tout simplement une suite de 32 caractères maximum, comme, p. ex. " Bayonne Office " ou " Acme-Marketronics " ou " BE45789 ". La distinction entre majuscules et minuscules s'applique aux noms de réseau, soyez par conséquent vigilant lorsque vous entrez le nom du réseau. Vous êtes cependant libre de choisir des noms de réseaux déjà disponibles. En sélectionnant le réseau dans une liste, vous éviterez les risques d'erreur survenant pendant la saisie du nom. La norme 802.11 définit les noms de réseau comme, par exemple, le "Service Set Identifier" (SSID).

## Sécurité réseau 802.11

Avec l'apparition des réseaux radio, la sécurité, bien plus qu'avant, joue un rôle critique pour la simple raison que les intrus ont plus de facilité à détourner ces liaisons. Dans le cas de réseaux câblés, la plupart des entreprises ont recours à des appareils pour protéger leurs réseaux. Un intrus devrait entrer dans les bâtiments de l'entreprise pour se connecter au réseau LAN et espionner le trafic du réseau en question.

Pour observer les flux de données d'un réseau radio, il suffit de disposer d'un ordinateur équipé d'une carte réseau et de s'installer sur le parking ou dans le bureau voisin à un endroit approprié. Voici quelques dispositions à prendre afin de garantir une interconnexion sécurisée :

- Un utilisateur doit être authentifié par le réseau avant d'être autorisé à y accéder de manière à protéger le réseau contre toute intrusion.
- L'utilisateur doit authentifier le réseau avant d'autoriser son ordinateur à entrer en communication avec le réseau. Cette précaution empêche qu'un dispositif radio se fasse passer pour un réseau légitime et reçoive l'autorisation d'accéder à l'ordinateur de l'utilisateur.
- L'authentification mutuelle entre utilisateur et réseau doit être protégée par un cryptage des informations échangées. Ce cryptage garantit que vous êtes bien connecté au réseau souhaité.
- La liaison radio entre un ordinateur et l'AccessPoint doit être cryptée pour empêcher d'éventuels intrus d'accéder à des données confidentielles.

Ce type de cryptage sécurisé via un réseau radio repose sur deux mécanismes fondamentaux :

- Information confidentielle préconfigurée et faisant office de clé WEP. Les clés WEP empêchent les utilisateurs non autorisés d'accéder au réseau radio et cryptent les données des utilisateurs légitimes.
- Authentification au moyen d'un protocole 802.1X. Le contrôle d'accès au réseau repose sur de multiples protocoles d'authentification élémentaires. Les protocoles les plus puissants sont en mesure de sécuriser l'authentification mutuelle de l'utilisateur et du réseau et de générer dynamiquement des clés permettant de crypter les données radio.

### Wired-Equivalent Privacy (WEP) avec clés préconfigurées

Grâce aux clés WEP (Wired-Equivalent Privacy) préconfigurées, l'ordinateur client comme l'AccessPoint reçoivent la même clé secrète. Cette clé sert à crypter toutes les informations échangées entre l'ordinateur et l'AccessPoint. La clé WEP peut également servir à authentifier l'ordinateur client sur l'AccessPoint. Si l'ordinateur ne peut pas prouver qu'il connaît la clé WEP, l'accès au réseau lui sera refusé.

- Lorsque l'AccessPoint exige une clé WEP pour l'authentification, vous devez procéder à l'association avec l'AccessPoint en mode partagé (shared). Le mode d'association se règle dans les propriétés du réseau.
- Lorsque l'AccessPoint n'exige pas de clé WEP pour l'authentification, on parle alors de mode ouvert (open). Le mode d'association se règle dans les propriétés du réseau.
- Lorsque l'AccessPoint exige un cryptage WEP pour WPA au lieu de TKIP pour l'authentification, toutes les clés WEP nécessaires sont générées à partir d'une passphrase ASCII que vous configurerez pour votre AccessPoint ainsi que pour Odyssey Client.

Voir les thèmes suivants :

- "Spécifier le mode d'association", avec une explication de la sélection d'un mode d'association dans Odyssey Client
- "Spécifier un mécanisme de cryptage adapté à votre mode d'association", avec une explication de la sélection du cryptage WEP en mode partagé (shared)
- "Clés préconfigurées (WEP)", pour l'utilisation de clés WEP statiques avec Odyssey Client
- "Clés pre-shared (WPA)", pour la configuration du cryptage WEP en mode WPA

### Wi-Fi Protected Access (WPA) et chiffrement TKIP

En tant qu'extension de la norme 802.11, Wi-Fi Protected Access (WPA) intègre une série d'innovations de sécurité qui complètent Wired-Equivalent Privacy. Ces innovations sont les suivantes :

- Cryptage amélioré des données avec TKIP (protocole temporaire d'intégrité de clé). TKIP offre un cryptage plus performant que WEP dans la mesure où les clés sont actualisées dynamiquement tous les 10 000 paquets environ.
- Authentification 802.1X avec EAP. Si le matériel de l'AccessPoint de votre réseau exige que vous procédiez à l'authentification en mode WPA étendu, vous pouvez configurer Odyssey Client de manière à réaliser l'authentification en mode WPA. Si le matériel est configuré pour le cryptage TKIP, vous pouvez aussi configurer Odyssey Client pour ce mécanisme étendu de cryptage des données. En plus du respect des spécifications de la norme 802.1X régissant la génération de clés dynamique (réalisable avec les mécanismes d'authentification les plus performants), WPA propose de générer des clés 'pre-shared' en vue d'un cryptage TKIP (ou WEP) au moyen d'une passphrase (mot de passe alphanumérique). Si vous configurez une passphrase pour la génération des clés sur vos AccessPoints, vous devez générer la même passphrase dans Odyssey Client.

Voir les thèmes suivants :

- "Spécifier le mode d'association", pour utiliser le mode WPA dans Odyssey Client
- "Spécifier un mécanisme de cryptage adapté à votre mode d'association", pour utiliser le cryptage TKIP en mode WPA
- "Clés pre-shared (WPA)", pour configurer une passphrase statique

## Norme 802.1X

Le protocole IEEE 802.1X permet un accès authentifié à un réseau LAN. Cette norme vaut autant pour les réseaux câblés que pour les réseaux non câblés. Dans un réseau non-câblé, l'authentification 802.1X est réalisée après la mise en place des associations 802.11. Les réseaux câblés utilisent la norme 802.1X sans association 802.11.

Le protocole WEP qui utilise des clés préconfigurées présente différentes faiblesses tant en matière de gestion des clés que de sécurité. Pour résoudre ces problèmes, l'IEEE a introduit une nouvelle norme : 802.1X. 802.1X propose davantage de sécurité que les clés WEP préconfigurées et est facile à utiliser, en particulier dans les grands réseaux.

Dans le cas de clés WEP préconfigurées, l'ordinateur client sans fil est authentifié par rapport au réseau. Avec la norme 802.1X, l'utilisateur est authentifié par rapport au réseau sur la base des identifiants (mot de passe, certificat ou carte à jeton (token card)). L'authentification n'est pas réalisée par l'AccessPoint mais plutôt par un serveur central. Si ce serveur utilise le protocole RADIUS, on l'appellera serveur RADIUS.

Avec la norme 802.1X, un utilisateur peut s'annoncer sur le réseau depuis l'ordinateur de son choix et plusieurs AccessPoints peuvent faire appel simultanément à un seul serveur RADIUS pour l'authentification. Il devient dès lors plus facile pour l'administrateur réseau de contrôler les accès au réseau.

Vous trouverez plus de détails à ce propos dans les thèmes suivants :

- Protocole EAP (Extensible Authentication Protocol)
- Reprise d'une session (Session resumption)
- Ré-authentification (Reauthentication)

## Extensible Authentication Protocol (EAP)

802.1X utilise le protocole appelé EAP (Extensible Authentication Protocol) pour procéder à l'authentification. EAP n'est pas un mécanisme d'authentification en soi mais plutôt un cadre général pour le transport des protocoles actuels d'authentification. Le protocole EAP présente l'avantage de ne pas devoir modifier le mécanisme EAP de base lors de la mise au point de nouveaux protocoles d'authentification.

## Remarques importantes

### Consignes de sécurité

La plupart des consignes de sécurité vous trouverez dans le manuel "Premiers pas" de votre appareil. Quelques-unes des plus importantes consignes de sécurité sont décrites ci-après.

- Eteignez les composants radio (Bluetooth ou Wireless LAN) de l'appareil lorsque vous entrez dans un hôpital, une salle d'opération ou que vous vous trouvez à proximité d'un système électronique médical. Les ondes radio transmises peuvent perturber le fonctionnement des appareils médicaux.

Le manuel "EasyGuide" fourni avec votre appareil explique comment .v.désactiver le composant radio.

- N'approchez pas l'appareil à moins de 20 cm d'un stimulateur cardiaque car les ondes radio peuvent perturber le fonctionnement normal du stimulateur cardiaque.
- Les ondes radio transmises peuvent provoquer un bourdonnement désagréable dans les appareils auditifs.
- Mettez l'appareil hors tension lorsque vous volez en avion ou conduisez une voiture.
- N'approchez pas l'appareil de gaz inflammables ou d'un environnement explosif (p. ex. un atelier de peinture) avant d'avoir désactivé les composants radio car les ondes radio transmises peuvent provoquer une explosion ou un incendie.

L'entreprise Fujitsu Siemens Computers GmbH n'est pas responsable des parasites radio ou TV provoqués par des modifications non autorisées apportées à cet appareil. Fujitsu Siemens n'assume par ailleurs aucune responsabilité pour le remplacement ou l'échange de câbles de raccordement et d'appareils qui n'ont pas été déclarés par Fujitsu Siemens Computers GmbH. L'utilisateur est seul responsable de la résolution des pannes causées par une modification non autorisée de ce type et du remplacement ou de l'échange des appareils.

### Marquage CE



Tel qu'il est livré, cet appareil satisfait aux exigences de la directive 1999/5/CE du Parlement européen et du Conseil du 9 mars 1999 sur les équipements radio et les dispositifs de télécommunication ainsi qu'à la reconnaissance réciproque de conformité.

Cet appareil peut être utilisé dans les pays suivants : Allemagne, Autriche, Belgique, Danemark, Espagne, Finlande, France, Grande-Bretagne, Grèce, Irlande, Islande, Italie, Liechtenstein, Luxembourg, Norvège, Pays-Bas, Portugal, Suède et Suisse. Vous trouverez des informations actualisées sur d'éventuelles restrictions d'exploitation en vous adressant aux autorités compétentes du pays en question. Si votre pays n'est pas repris dans l'énumération ci-dessus, demandez aux autorités de régulation compétentes si l'utilisation de ce produit est autorisée dans votre pays.

## Restrictions

- France
  - Plage de fréquences limitée : seuls les canaux 10 à 13 (2457 MHz à 2472 MHz) peuvent être utilisés en France. Il est interdit d'utiliser l'appareil à l'extérieur.
- Italie
  - Une autorisation ministérielle est également indispensable pour l'utilisation à l'intérieur des bâtiments. Veuillez prendre contact avec le revendeur pour connaître la procédure à suivre dans ce cas. Il est interdit d'utiliser l'appareil à l'extérieur.
- Pays-Bas
  - Une licence est requise pour l'utilisation à l'extérieur des bâtiments. Veuillez prendre contact avec le revendeur pour connaître la procédure à suivre dans ce cas.

## Fréquences radio et normes de sécurité

Les informations ci-après concernent la situation en vigueur en janvier 2002. Vous trouverez des informations actuelles en vous adressant aux autorités compétentes de votre pays (p. ex. [www.art-tel.com.fr](http://www.art-tel.com.fr)).

### Fréquences de la norme IEEE 802.11a

Pays	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
Autriche	x	x	x	x				
Belgique	x	x	x	x	x	x	x	x
Danemark	x	x	x	x				
Finlande	x	x	x	x	x	x	x	x
France	x	x	x	x				
Allemagne	x	x	x	x				
Grèce								
Italie								
Irlande	x	x	x	x	x	x	x	x
Luxembourg								
Pays-Bas	x	x	x	x				
Norvège	x	x	x	x				
Portugal	x	x	x	x				
Espagne								
Suède	x	x	x	x				
Suisse	x	x	x	x				
Grande-Bretagne	x	x	x	x	x	x	x	x

Fréquences norme IEEE 802.11b (11 Mbits/s) / 802.11g (54 Mbits/s)

Les cartes et adaptateurs pour réseaux radio sont prévus pour fonctionner dans la bande de fréquences ISM (Industrial, Scientific, Medical) comprise entre 2,4 et 2,4835 GHz conformément à la norme IEEE 802.11b. Parce que chacun des 13 canaux radio utilisables exige une largeur de bande de 22 MHz sur la base de la procédure DSSS (Direct Sequence Spread Spectrum), un max. de trois canaux indépendants les uns des autres (p. ex. 1, 6 et 11) sont effectivement disponibles. Vous trouverez dans les tableaux ci-dessous les canaux autorisés dans votre pays :

N° de canal / MHz	Europe, R&TTE	France, R&TTE	US 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		



---

# Installation d'Odyssey

Vous trouverez le logiciel d'installation d'Odyssey Client dans le dossier C:\Add on \Software.

Avant de procéder à l'installation, respectez les points suivants :

- votre carte réseau pour le réseau sans fil et les pilotes sont déjà installés.
- Sous Windows 2000 et Windows XP, vous devez disposer de droits d'administrateur.

## Installation d'Odyssey Client

Pour installer Odyssey Client :

- Double-cliquez sur le fichier *FSC-OdysseyClient.msi* dans le dossier C:\Add on\Software.

L'assistant d'installation démarre pour vous guider pendant la procédure d'installation.

- Cliquez sur *Next* pour continuer.

Les conditions de licence s'affichent à l'écran.

- Cliquez sur l'option *I accept the terms in the license agreement* pour accepter les conditions de licence puis sur *Next* pour continuer.
- Entrez vos données d'utilisateur puis cliquez sur *Next* pour continuer.
- Dans la fenêtre *Setup Type*, choisissez l'option *Complete* pour exécuter l'installation dans le dossier proposé par défaut. Choisissez l'option *Custom* si vous voulez spécifier vous-même le dossier d'installation. Cette option est réservée aux utilisateurs expérimentés. Cliquez sur *Next* pour continuer.

L'assistant d'installation dispose à présent de toutes les informations nécessaires pour commencer l'installation.

- Cliquez sur *Back* si vous souhaitez vérifier ou modifier vos données puis sur *Install* pour lancer l'installation.

L'installation est lancée. Cette opération peut durer quelques minutes. Lorsque l'installation est terminée, la fenêtre *InstallShield Wizard Completed* s'affiche à l'écran. Vous pouvez lancer Odyssey Client directement ou demander l'affichage du fichier *Lisez-moi (readme)*.

- Cliquez sur *Finish* pour terminer l'installation.

Si plusieurs comptes utilisateur ont été créés sur un ordinateur, Odyssey Client est disponible pour tous les utilisateurs après l'installation. Les réglages propres à l'utilisation d'Odyssey Client sont cependant personnels et doivent être réalisés pour chaque compte utilisateur séparément.

## Configure and Enable Wizard

Lorsque vous installez Odyssey Client pour la première fois, le *Configure and Enable Wizard* apparaît automatiquement après l'installation pour configurer et activer Odyssey Client.

Si vous ne souhaitez pas configurer le programme à ce moment-là, vous pourrez le faire plus tard. Démarrez l'Odyssey Client Manager sous *Démarrer – Programmes – Fujitsu Siemens Computers – Odyssey Client for Fujitsu Siemens Computers – Odyssey Client Manager for Fujitsu Siemens Computers*. Le *Configure and Enable Wizard* démarre automatiquement.

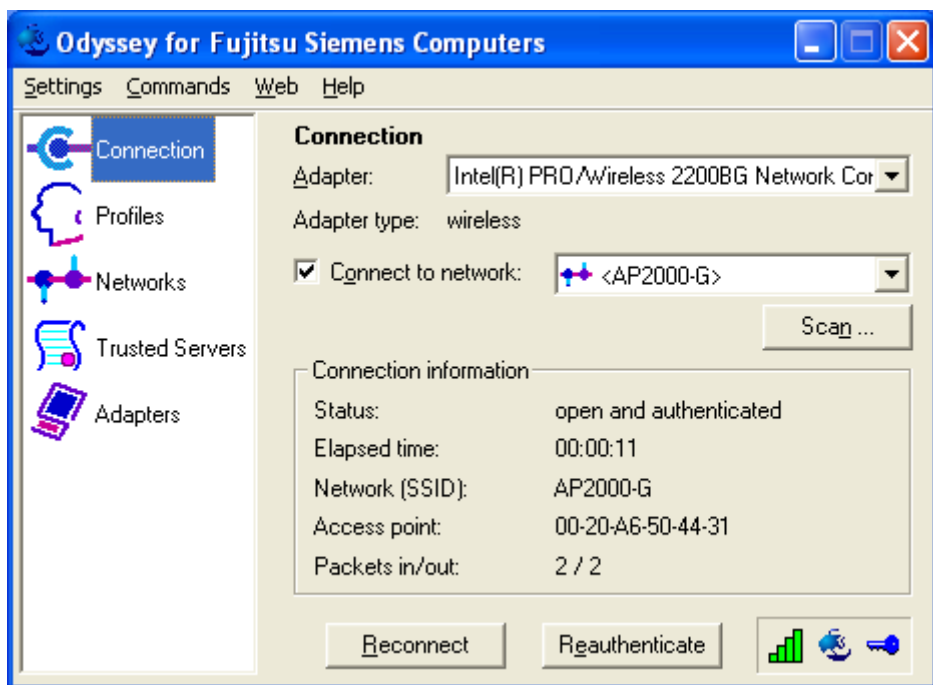


# Utilisation d'Odyssey Client

## Aperçu de l'Odyssey Client Manager

*Odyssey Client for Fujitsu Siemens Computers* est le nom de l'interface Windows de l'Odyssey Client Manager qui vous permettra d'utiliser et de configurer votre Wireless LAN. Cette interface est la même pour toutes les plates-formes Fujitsu Siemens Computer sur lesquelles vous pouvez utiliser le produit.

- Démarrez l'*Odyssey Client Manager* sous *Démarrer – Tous les programmes – Fujitsu Siemens Computers – Odyssey Client for Fujitsu Siemens Computers – Odyssey Client Manager* ou double-cliquez sur l'icône de l'Odyssey Client Manager dans la barre des tâches.



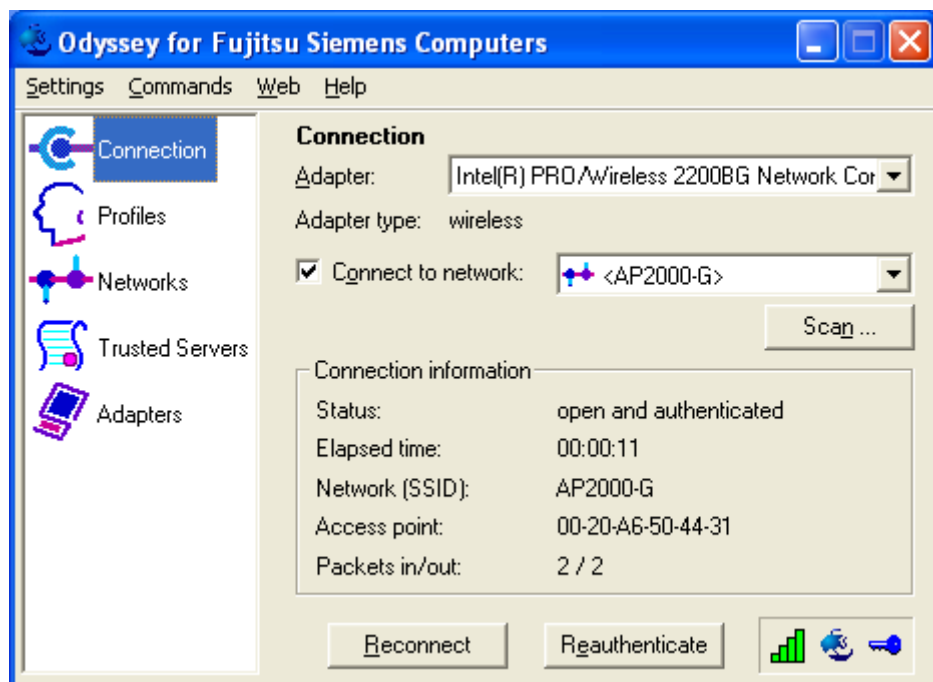
## L'écran Odyssey Client Manager

Pour la plupart des connexions réseau, Odyssey Client Manager se compose d'une série de fenêtres dans lesquelles vous pouvez effectuer différents réglages :

- Dans la fenêtre *Connection*, vous pouvez utiliser votre connexion réseau et visualiser l'état actuel de votre connexion.
- Entrez dans la fenêtre *Profiles* les informations nécessaires pour l'authentification ou l'ouverture d'une session réseau, p. ex. votre mot de passe ou votre certificat.
- La fenêtre *Networks* vous permet de configurer différents réseaux radio et de décider de la façon dont vous voulez les relier.
- La fenêtre *Trusted Servers* vous permet de spécifier les données de certification et d'identification vis-à-vis des serveurs que vous pouvez authentifier au moment de l'établissement de la connexion pour être certain que vous vous connectez au réseau souhaité.
- La fenêtre *Adapters* vous permet de sélectionner une ou plusieurs cartes réseau pour l'interconnexion de réseaux sans fils.

Tous les noms de fenêtres sont proposés dans une liste dans la partie gauche de l'écran Odyssey Client Manager. Cliquez sur le nom de la fenêtre que vous voulez visualiser ou modifier.

## Utiliser les connexions réseau - Fenêtre "Connection"



## Sélectionner la carte réseau

Si vous ou votre administrateur avez configuré plus d'une carte réseau pour utiliser Odyssey, vous pouvez utiliser la liste déroulante *Adapters* dans la fenêtre *Connection* pour associer chacune de ces cartes réseau à une connexion réseau.

Dès que vous avez sélectionné une carte réseau, le champ *Adapter type* est actualisé et affiche le type de carte sélectionné.

## Se connecter à un réseau

Si vous établissez la connexion réseau au moyen d'une carte réseau radio, vous devez entrer toutes les informations nécessaires à la connexion à l'aide d'une définition de réseau Odyssey Client. Vous devez au préalable spécifier les données d'authentification que vous avez définies dans un profil Odyssey Client (voir "Ajouter et modifier un profil - Fenêtre "Profile Properties"" dans la section "Définir des profils - Fenêtre "Profiles"").

La case à cocher *Connect to network* vous permet d'établir ou de mettre fin à la connexion au réseau radio. Pour établir une connexion avec un réseau radio, assurez-vous que cette case est bien cochée.

La liste déroulante à droite de la case à cocher *Connect to network* vous permet de sélectionner un réseau radio auquel vous connecter. Cette liste reprend tous les réseaux que vous avez déjà configurés dans la fenêtre *Networks*.

Les noms de réseau apparaissent entre crochets derrière les descriptions de réseau.

Le nom est précédé du symbole suivant :



pour les réseaux

Pour se connecter à un réseau déjà configuré :

- Dans la liste déroulante, sélectionnez le réseau auquel vous souhaitez vous connecter.
- Cochez la case à cocher *Connect to network* si elle ne l'est pas encore.

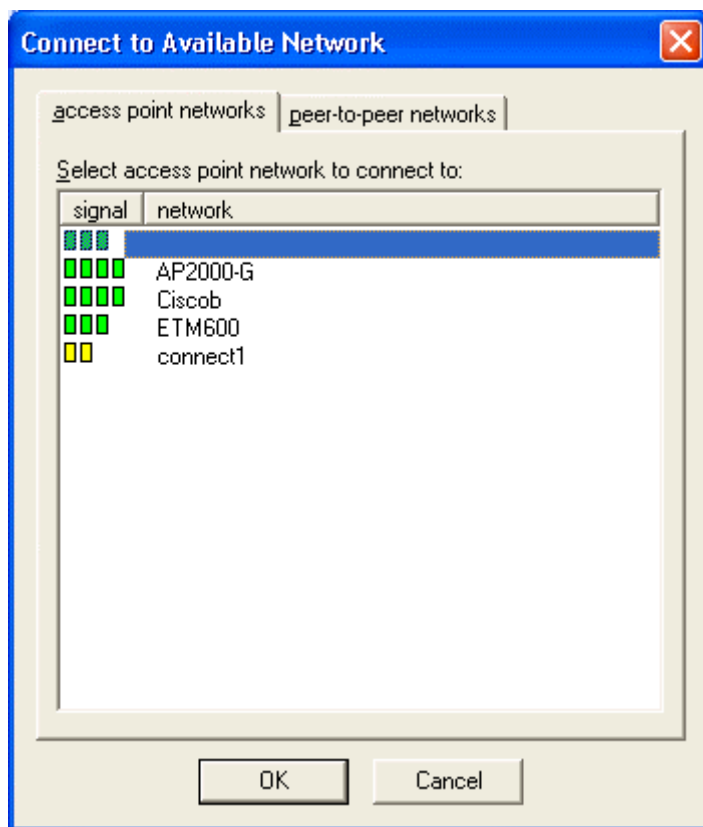
Pour couper la connexion à un réseau, il suffit de décocher la case à cocher *Connect to network*.

## Rechercher les réseaux radio

Si vous voyagez fréquemment, vous pouvez aussi vous faire authentifier par des réseaux radio locaux que vous n'avez pas encore configurés. Pour vous connecter à un réseau radio qui n'est pas encore configuré, procédez comme suit :

- Cliquez sur *Scan* dans la fenêtre *Connection*.

Odyssey Client vérifie les ondes radio et affiche la liste de tous les réseaux radio actuellement accessibles.



- Sélectionnez le réseau auquel vous souhaitez vous connecter et cliquez sur OK.
    - Si vous avez déjà configuré les réglages pour ce réseau, Odyssey Client essaie d'établir la connexion sur la base de ces réglages.
    - Si vous n'avez pas encore configuré les réglages pour ce réseau, la fenêtre *Network Properties* s'affiche d'abord à l'écran. Spécifiez les réglages puis cliquez sur OK.
- Odyssey Client essaie d'établir une connexion avec le réseau.

**i** Seuls les réseaux radio configurés par un administrateur pour envoyer des signaux (SSID visible ou „send beacons“) seront visibles après une recherche. Si l'SSID n'est pas visible, vous devrez entrer le réseau dans la fenêtre *Networks*.

## Se reconnecter à un réseau

Lorsque la connexion radio à un réseau ne fonctionne pas parfaitement, vous pouvez couper la connexion actuelle et établir une nouvelle connexion.

- Cliquez sur *Reconnect* dans la fenêtre *Connection*.

La connexion en cours est coupée et une nouvelle connexion au réseau radio sélectionné est établie. La nouvelle connexion peut être établie avec un autre AccessPoint (au sein du même réseau) que précédemment en fonction de facteurs tels que l'intensité du signal. Si l'authentification est de rigueur sur ce réseau, vous serez à nouveau authentifié lorsque la nouvelle connexion sera établie. Si des clés dynamiques sont utilisées pour le cryptage, elles seront actualisées.

## Se ré-authentifier au réseau

Si vous cliquez sur *Reauthenticate* dans la fenêtre *Connection*, Odyssey Client vous authentifie à nouveau sur la nouvelle connexion en cours qui apparaît dans la fenêtre mais sans établir de nouvelle connexion. Si des clés dynamiques sont utilisées pour le cryptage, elles seront actualisées.

## Couper la connexion réseau

Pour couper une connexion réseau, décochez la case *Connect to network* pour les connexions radio.

## Visualiser les données de connexion

Le champ *Status* dans la fenêtre *Connection* indique l'état actuel de votre connexion au réseau pour cette carte réseau. Un des messages suivants est affiché :

Message d'état	Définition
open and authenticated	La connexion est authentifiée, vous êtes connecté.
open / authenticating	Ré-authentification en cours, vous êtes connecté.
open / requesting authentication	Vous avez demandé une ré-authentification, vous êtes connecté.
open	La connexion n'est pas authentifiée mais vous êtes connecté.
peer-to-peer	Le réseau est de type 'peer-to-peer' (Adhoc), vous êtes connecté.
authenticating	Vous n'êtes pas encore connecté mais l'authentification est en cours.
requesting authentication	Vous n'êtes pas encore connecté mais vous avez demandé l'authentification par l'AccessPoint.
waiting to authenticate	Vous n'êtes pas encore connecté et la dernière authentification a échoué mais vous attendez de pouvoir réessayer.

### Message d'état

### Définition

searching for access point

Vous n'êtes pas encore connecté et la communication avec une AccessPoint du réseau souhaité a échoué. Cela peut arriver si votre carte réseau n'est pas compatible avec la norme 802.1X ou si votre AccessPoint est hors de portée radio.

searching for peer(s)

Vous n'êtes pas connecté et la communication avec d'autres ordinateurs du réseau ,peer-to-peer' n'est pas établie

disconnected

Vous n'êtes pas connecté ; la case à cocher *Connect to network* est peut-être décochée. voir "Se connecter à un réseau"

Odyssey is disabled

Vous n'êtes pas connecté et Odyssey Client est désactivé.

Adapter not present

Vous n'êtes pas connecté et la carte réseau configurée n'est pas disponible pour l'instant. Cela peut arriver si votre carte réseau ne supporte pas la norme 802.1X.

Le champ *Elapsed time* dans la fenêtre *Connection* indique le temps qui s'est écoulé depuis le début de la connexion en cours.

Le champ *Network (SSID)* indique le nom du réseau radio auquel vous êtes connecté. Voyez aussi "Noms des réseaux radio (SSID)".

Le champ *Access point* renferme l'adresse MAC du point d'accès radio auquel vous êtes connecté. (une adresse MAC est un nombre 48 bits unique encodé par le constructeur dans l'appareil.)

Le champ *Packets in/out* indique le nombre total de paquets reçus et émis depuis le début de la connexion en cours.

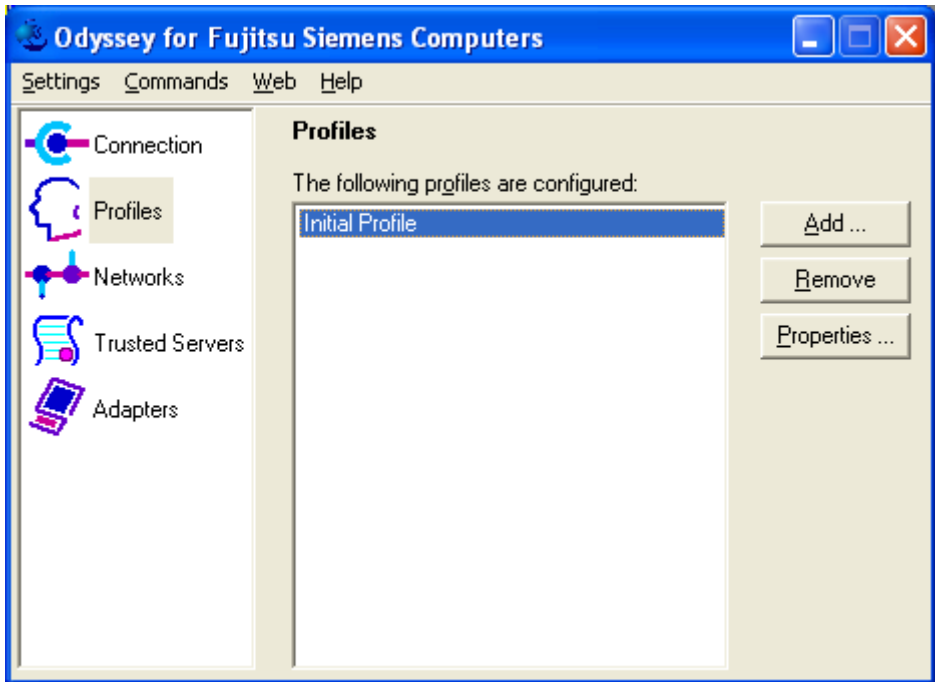
## Définir des profils - Fenêtre "Profiles"

Un profil Odyssey Client renferme toutes les informations indispensables pour vous authentifier sur le réseau. Il s'agit notamment des informations comme votre login, votre mot de passe ou votre certificat ainsi que des protocoles grâce auxquels vous pouvez être authentifié. Votre profil est en fait l'identité que vous présentez au réseau et le moyen que vous utilisez pour prouver cette identité.

Vous pouvez posséder différents profils pour différents réseaux. Vous pouvez, par exemple, utiliser différents logins ou mots de passe sur différents réseaux ou utiliser un mot de passe pour un réseau bien déterminé et un certificat pour un autre.

► Dans l'Odyssey Client Manager, cliquez sur *Profiles* pour afficher la fenêtre à l'écran.





La fenêtre *Profiles* reprend tous les profils configurés. Si vous utilisez *Odyssey Client Manager* pour la première fois, vous trouverez un profil appelé *Initial Profile* qui renferme les réglages les plus courants. D'autre part, votre administrateur réseau a peut-être déjà créé un ou plusieurs profils pour vous.

- Pour ajouter un profil, cliquez sur *Add*. La fenêtre *Profile Properties* s'affiche. Entrez le nom du nouveau profil, configurez les réglages et cliquez sur *OK*.
- Pour supprimer le profil, sélectionnez-le et cliquez sur *Remove*.
- Pour modifier un profil, sélectionnez-le et cliquez sur *Properties* ou double-cliquez sur le profil. La fenêtre *Profile Properties* s'affiche. Modifiez les réglages et cliquez sur *OK*.

## Ajouter et modifier un profil - Fenêtre "Profile Properties"

La fenêtre *Profile Properties* vous permet de configurer un profil. Elle s'affiche lorsque vous cliquez sur *Add* ou *Properties* dans la fenêtre *Profiles*.

Lorsque vous ajoutez un nouveau profil, vous devez entrer dans le champ *Profile Name* un nom univoque. Vous pouvez, par exemple, utiliser le nom "Office" pour désigner votre profil au bureau et "Home" pour désigner votre réseau privé.

Une fois le profil spécifié et enregistré, vous ne pourrez plus modifier son nom lorsque vous éditez les autres propriétés du profil. Vous pouvez en revanche supprimer le profil et en créer un nouveau sous un autre nom.

En plus du nom de profil, vous pouvez configurer (et éditer) les paramètres suivants :

- une identification dans l'onglet *User Info*
- un mot de passe et/ou un certificat dans l'onglet *Authentication*
- les protocoles d'authentification qui sont utilisés pour vous authentifier sur le réseau dans les onglets *TTLS Settings* et *PEAP Setting*

### Onglet "User Info"

L'onglet *User Info* vous permet de configurer le nom que vous utiliserez pour ouvrir une session ainsi que votre mot de passe et/ou vos données de certificat.

The screenshot shows a Windows-style dialog box titled "Add Profile" with a blue title bar and a close button (X) in the top right corner. The dialog has a tabbed interface with four tabs: "User Info" (selected), "Authentication", "TTLS Settings", and "PEAP Settings".

Under the "User Info" tab, there is a "Profile name:" label followed by a text box containing the word "Office". Below this is a "Login name:" label followed by a text box containing "ACME\george".

Below the login name is a "Password" section. It contains a checkbox labeled "Permit login using password" which is checked. Below this checkbox are three radio button options: "use Windows password" (selected), "prompt for password", and "use the following password:". The "use the following password:" option has a corresponding empty text box below it. At the bottom of the password section is an unchecked checkbox labeled "Unmask".

Below the password section is a "Certificate" section. It contains an unchecked checkbox labeled "Permit login using my certificate:". Below this checkbox is an empty text box. At the bottom of the certificate section are two buttons: "View ..." and "Browse ...".

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

## Login

Entrez dans le champ *Login name* votre nom d'utilisateur. Ce nom sera présenté au réseau au moment de votre authentification. Si vous êtes authentifié avec un Windows Active Directory, utilisez la syntaxe nom-de-domaine\nom-d'utilisateur (par exemple Acme\george). Sinon, utilisez une identification conforme à la syntaxe définie par votre administrateur pour les noms d'utilisateur de la base de données d'authentification.

Remarquez les points suivants :

- Si vous êtes annoncé dans le domaine de votre réseau (et non sur votre machine), Odyssey Client indique généralement dans ce champ le nom de domaine et le nom d'utilisateur, le nom d'utilisateur étant votre nom d'utilisateur.
- Si vous êtes annoncé sur votre terminal client local (et non dans le domaine du réseau), Odyssey Client indique dans ce champ uniquement votre nom d'utilisateur.
- Il est possible que vous deviez ajouter le nom de serveur derrière votre login pour que votre authentification puisse être transmise correctement au bon serveur.

Exemple : *acme\george@sales.acme.com*. Votre administrateur réseau peut vous expliquer comment utiliser correctement ce champ.

## Mot de passe

Cochez la case *Permit login using password* pour activer le mécanisme qui utilise votre mot de passe pour vous authentifier. Vous pouvez définir le mot de passe qu'Odyssey Client utilise :

- Sélectionnez *Use Windows password* si vous voulez vous authentifier sur le réseau avec le même mot de passe que pour l'ouverture d'une session Windows.
- Sélectionnez *prompt for password* si vous souhaitez qu'Odyssey Client vous signale qu'il est temps de vous authentifier.
- Sélectionnez *use the following password* et entrez un mot de passe dans le champ situé sous cette option si vous souhaitez qu'Odyssey Client enregistre votre mot de passe et l'utilise chaque fois que vous vous authentifiez avec ce profil.

Si vous avez sélectionné *prompt for password*, vous serez invité la première fois à entrer le mot de passe si vous vous authentifiez après le démarrage. Odyssey Client garde ce mot de passe en mémoire et l'utilise pendant toute la durée de votre session Windows. Le mot de passe que vous avez spécifié ne s'applique qu'à un seul profil. Si vous êtes authentifié avec un autre profil, vous serez à nouveau invité à entrer le mot de passe.

Vous pouvez aussi être invité, dans certains cas, à entrer votre mot de passe Windows lorsque vous vous connectez au réseau :

- Si vous avez par inadvertance entré un mot de passe incorrect ou en présence d'une erreur d'authentification. Cette fonction permet, notamment, d'empêcher un blocage éventuel provoqué par l'utilisation répétée de mots de passe incorrects.
- Si vous devez modifier votre mot de passe Windows régulièrement et que vous accédez au réseau au moyen d'une authentification EAP-TTLS ou PEAP avant l'ouverture de session Windows.

## Certificat

Cochez *Permit login using my certificate* pour activer les mécanismes d'authentification qui utilisent votre certificat d'authentification.

Pour sélectionner un certificat personnel d'authentification, cliquez sur *Browse*. Une liste contenant vos certificats personnels s'affiche. Sélectionnez un certificat et cliquez sur *OK*.



Cette fonction a été améliorée. Adressez-vous si nécessaire à votre administrateur réseau pour savoir quel certificat sélectionner.

## Onglet "Authentication"

Dans l'onglet *Authentication*, vous pouvez spécifier les protocoles avec lesquels vous vous authentifiez sur le réseau.

The screenshot shows the 'Add Profile' dialog box with the 'Authentication' tab selected. The 'Profile name' field contains 'Office'. Below the tabs, the 'Authentication protocols, in order of preference:' section shows a list box with 'EAP / TTLS'. To the right of the list box are buttons for 'Add ...' and 'Remove'. Below the list box is a checked checkbox labeled 'Validate server certificate'. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

**Add Profile**

Profile name:

User Info   **A**uthentication   ITLS Settings   PEAP Settings

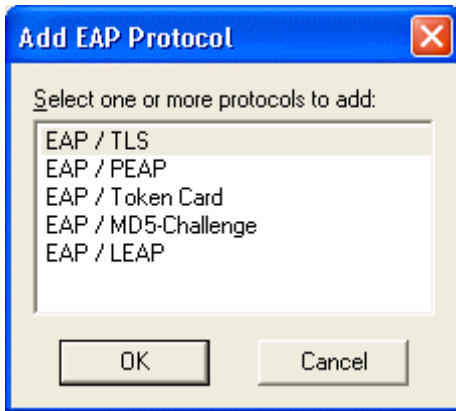
Authentication protocols, in order of preference:

☒ Validate server certificate

## Sélectionner les protocoles d'authentification

La liste des protocoles d'authentification renferme les protocoles que vous avez activés pour l'authentification. Cette liste peut ne contenir qu'un seul protocole d'authentification ou plusieurs. Si vous avez plusieurs protocoles d'authentification, vous pouvez leur attribuer des priorités. La séquence détermine le protocole qu'utilisera le serveur lorsqu'il disposera de plus d'un protocole commun.

- Pour modifier l'ordre des protocoles, sélectionnez un protocole et déplacez-le à l'aide des boutons fléchés.
- Pour supprimer un protocole, sélectionnez-le et cliquez sur *Remove*.
- Pour ajouter un protocole, cliquez sur *Add*. La fenêtre *Add EAP Protocol* s'affiche. Sélectionnez un ou plusieurs protocoles à ajouter et cliquez sur *OK*. Vous pouvez sélectionner plusieurs protocoles à la fois en maintenant la touche **Ctrl** de votre clavier enfoncée tout en sélectionnant les protocoles avec la souris. N'oubliez que tous les protocoles que vous avez déjà sélectionnés n'apparaissent pas dans cette fenêtre.



## Validation du certificat du serveur

Certains protocoles tels EAP-TTLS, PEAP et EAP-TLS vous permettent de vérifier l'identité du serveur d'authentification pendant que le serveur vérifie votre identité. Cette procédure est appelée authentification mutuelle.

Cochez la case *Validate Server Certificate* pour vérifier l'identité du serveur d'authentification sur la base de son certificat lorsque vous utilisez les protocoles EAP-TTLS, PEAP et EAP-TLS. (ce champ est coché par défaut.) Vous pouvez sélectionner les certificats des 'Trusted Authentication Server' dans la fenêtre *Trusted Servers*. Voir "Spécifier des serveurs dignes de confiance - Fenêtre "Trusted Servers"".

En règle générale, vous devez cocher la case *Validate server certificate*. Vous pouvez en option désactiver cette importante mesure de sécurité mais uniquement lorsqu'aucun certificat n'est exigé côté serveur. N'agissez que si votre administrateur réseau vous y invite.

## Onglet "TTLS Settings"

L'onglet *TTLS Settings* vous permet de configurer l'utilisation d'EAP-TTLS en tant que protocole d'authentification. Ces réglages sont uniquement valables si vous faites d'EAP-TTLS un de vos protocoles d'authentification dans l'onglet *Authentication*.

The screenshot shows the 'Add Profile' dialog box with the 'TTLS Settings' tab selected. The 'Profile name' field contains 'Office'. The 'Inner authentication protocol' dropdown is set to 'MS-CHAP-V2'. Below this, there is a list box for 'Inner EAP protocols, in order of preference' which is currently empty, accompanied by up/down arrow buttons, an 'Add...' button, and a 'Remove' button. A text box explains that when using EAP-TTLS exclusively, an anonymous name can be used instead of a login name, with examples like 'anonymous' or 'anonymous@myisp.com'. The 'Anonymous name' field at the bottom contains the text 'anonymous'. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

**Add Profile**

Profile name:

User Info | Authentication | **TTLS Settings** | PEAP Settings

Inner authentication protocol:

Inner EAP protocols, in order of preference:

↑ ↓

Add...

Remove

Anonymous name

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".

Anonymous name:

OK Cancel

EAP-TTLS crée un tunnel sécurisé et crypté par l'intermédiaire duquel vous présentez vos identifiants au serveur d'authentification. Il existe encore à l'intérieur du protocole EAP-TTLS un autre protocole d'authentification interne (Inner Authentication Protocol) que vous devez configurer.

## Sélection du protocole d'authentification interne

Sélectionnez dans la liste déroulante *Inner Authentication Protocol* le protocole d'authentification interne souhaité. Les protocoles suivants vous sont proposés :

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

Le protocole le plus couramment utilisé est MS-CHAP-V2. Ce protocole vous permet de vous authentifier à un contrôleur de domaine Windows (Windows Domain Controller) ainsi qu'à d'autres bases de données utilisateur ne tournant pas sous Windows.

CHAP est le protocole le plus fréquemment utilisé pour une authentification vis-à-vis de bases de données utilisateur qui ne tournent pas sous Windows.



Vous ne pouvez pas faire de CHAP la méthode d'authentification interne avec un domaine Windows NT ou avec un Active Directory. N'utilisez donc pas CHAP pour l'authentification avec un serveur Odyssey car il s'authentifie uniquement auprès d'un domaine Windows ou d'un Active Directory.

PAP/Token est le protocole à utiliser avec les cartes à jeton (token card). Si vous utilisez PAP/Token, le mot de passe que vous aurez spécifié dans la boîte de dialogue Mot de passe ne sera jamais enregistré en mémoire cache parce que chaque mot de passe à base de jeton n'est valable que pour une seule utilisation.

Consultez votre administrateur réseau pour savoir quel protocole d'authentification interne est utilisé sur votre réseau.

## EAP en tant que protocole d'authentification interne

Si vous utilisez EAP en tant que protocole d'authentification interne, vous devez configurer la liste des protocoles EAP internes en y ajoutant un ou plusieurs protocoles.

- Pour ajouter un protocole, cliquez sur *Add*. La fenêtre *Add EAP Protocol* s'affiche. Sélectionnez un ou plusieurs protocoles à ajouter et cliquez sur *OK*. Vous pouvez sélectionner plusieurs protocoles à la fois en maintenant la touche **Ctrl** de votre clavier enfoncée tout en sélectionnant les protocoles avec la souris. N'oubliez que tous les protocoles que vous avez déjà ajoutés n'apparaissent pas dans cette fenêtre.
- Pour supprimer un protocole, sélectionnez-le et cliquez sur *Remove*.
- Pour modifier l'ordre des protocoles, sélectionnez un protocole et déplacez-le à l'aide des boutons fléchés.

### Spécification d'un nom anonyme

EAP-TTLS possède une fonction unique que les autres protocoles n'ont pas. Etant donné qu'EAP-TTLS crée un tunnel crypté pour vos identifiants, il est aussi possible de transmettre votre login au travers de ce tunnel. Cela signifie que non seulement vos identifiants mais aussi votre identité sont protégés contre les risques d'écoute.

Avec EAP-TTLS, vous possédez donc deux identités : une interne et une externe. L'identité interne est votre login actuel, elle est extraite du champ login de l'onglet *User Info*. Votre identité externe peut être parfaitement anonyme. Spécifiez votre identité externe dans le champ *Anonymous name* ein.

En règle générale, réglez le champ *Anonymous name* est réglé sur sa valeur par défaut *anonymous*. Dans certains cas, vous devrez entrer du texte supplémentaire. Cette identité externe, par exemple, pourra être utilisée pour présenter votre authentification au serveur correspondant et vous pourrez être invité à utiliser „anonymous@acme.com“. Votre administrateur réseau peut vous expliquer comment configurer ce champ correctement.



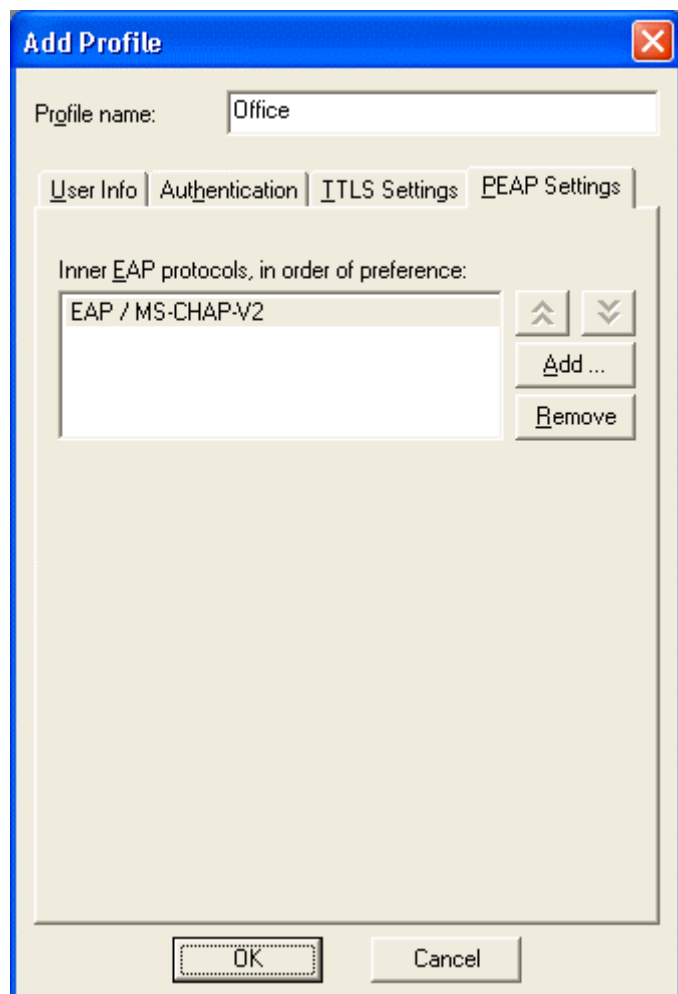
Votre identité externe peut uniquement être anonyme si EAP-TTLS est le seul protocole d'authentification configuré dans l'onglet *Authentication Protocols*. Si d'autres protocoles sont également activés, Odyssey Client ne peut cacher votre identité et le champ *Anonymous name* est désactivé. Si vous souhaitez l'anonymat offert par EAP-TTLS, vous devez configurer EAP-TTLS comme étant le seul protocole d'authentification.

### Onglet "PEAP Settings"

Si vous spécifiez dans l'onglet *Authentication* qu'EAP/PEAP est le mécanisme d'authentification souhaité, vous pouvez utiliser jusqu'à trois mécanismes d'authentification EAP internes:

- EAP/MS-CHAP-V2
  - EAP/carte à jeton (token card)
  - EAP/MD5-Challenge. Pour ajouter ou supprimer des mécanismes d'authentification internes utilisés avec PEAP :
- Sélectionnez l'onglet *PEAP Settings*.

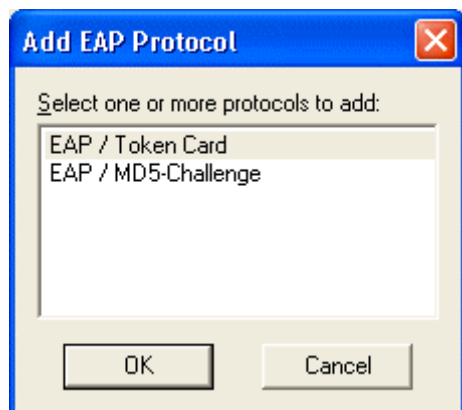




- Sélectionnez les protocoles que vous souhaitez supprimer et cliquez sur *Remove*.
- Cliquez sur *Add* pour ajouter un protocole.

La fenêtre *Add EAP Protocol* s'affiche.

- Sélectionnez un ou plusieurs protocoles à ajouter et cliquez sur *OK*.



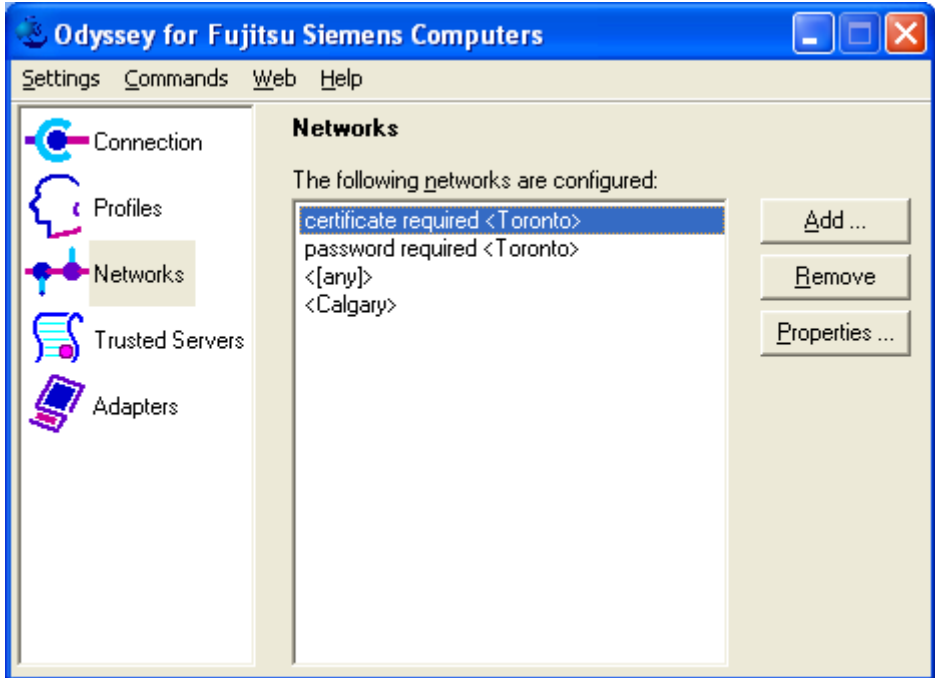
N'oubliez que tous les protocoles que vous avez déjà sélectionnés n'apparaissent pas dans cette fenêtre.

- Cliquez sur *OK* lorsque vous avez réalisé tous les changements dans la configuration du profil.

## Configurer des réseaux radio - Fenêtre "Networks"

La fenêtre *Networks* vous permet de configurer les réglages pour vous connecter à un nombre quelconque de réseaux radio.

- Dans l'Odyssey Client Manager, cliquez sur *Networks* pour afficher la fenêtre à l'écran.



Tous les réseaux configurés sont affichés. Vous pouvez effectuer les tâches suivantes dans la fenêtre *Networks* :

- Pour ajouter un réseau, cliquez sur *Add*. La fenêtre *Network Properties* s'affiche. Configurez les réglages pour le nouveau réseau et cliquez sur *OK* (voir la section "Ajouter ou modifier des réseaux – Fenêtre "Network Properties"").
- Pour supprimer un réseau, sélectionnez-le et cliquez sur *Remove*.
- Pour modifier les réglages d'un réseau, sélectionnez-le et cliquez sur *Properties* ou double-cliquez sur le nom du réseau. La fenêtre *Network Properties* s'affiche. Modifiez les réglages et cliquez sur *OK* (voir la section "Ajouter ou modifier des réseaux – Fenêtre "Network Properties"").

### Désignations des réseaux

Les désignations des réseaux dans la fenêtre *Networks* sont structurées comme suit :

- Le nom du réseau apparaît entre crochets.
- La description du réseau précède son nom. Cette description provient du champ *Description* dans la fenêtre *Network Properties*. Vous pouvez ajouter votre description personnelle à chaque réseau configuré. Vous serez en mesure de distinguer les réseaux plus facilement.

Le champ réservé à la description du réseau est utile dans les situations où vous souhaitez changer de "personnalités" au sein du même réseau. Vous pouvez, par exemple, utiliser des identifiants différents à différents moments. Le champ de description permet aussi de faire la distinction entre deux réseaux différents mais portant le même nom de réseau.

Les noms de réseau sont des intitulés libres choisis par l'administrateur. Il est donc possible que deux réseaux indépendants l'un de l'autre portent le même nom. La représentation de la fenêtre *Networks* affiche deux réseaux "Toronto". Les descriptions qui précèdent le nom du réseau indiquent que l'identifiant par mot de passe est utilisé pour l'un des réseaux et l'identifiant par certificat pour l'autre.

### Ajouter ou modifier des réseaux – Fenêtre "Network Properties"

Vous pouvez configurer les réglages du réseau radio dans la fenêtre *Network Properties*. Cliquez sur *Add* ou *Properties* dans la fenêtre *Networks* pour visualiser les propriétés du réseau. La fenêtre *Add Network* ou *Network Properties* s'affiche à l'écran.

**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

Vous pouvez configurer ici les paramètres suivants :

- Propriété du réseau dans la zone *Network*
- Champs d'authentification dans la zone *Authentication*
- Clés pré-configurées (WEP ou WPA) dans la zone *Pre-configured keys*

### Reseau

Dans la zone *Network* de la fenêtre *Network Properties*, vous pouvez réaliser les tâches suivantes :

- Entrer le nom du réseau
- Rechercher un réseau
- Configurer Odyssey pour se connecter à un réseau disponible
- Spécifier la description du réseau
- Spécifier le type de réseau
- Spécifier le mode d'association
- Spécifier un mécanisme de cryptage adapté à votre mode d'association

#### Entrer le nom du réseau

Entrez dans le champ *Network name (SSID)* le nom du réseau radio. Le nom de réseau peut renfermer jusqu'à 32 caractères. Une distinction est faite entre majuscules et minuscules. Ce nom doit être spécifié correctement pour pouvoir se connecter avec succès.

#### Rechercher un réseau

Vous pouvez entrer le nom du réseau directement ou cliquer sur *Scan* pour le sélectionner dans une liste de tous les réseaux actuellement visibles.

Si vous vous situez à proximité immédiate du réseau que vous configurez, il est non seulement plus facile d'utiliser le bouton de commande *Scan* que d'entrer le nom du réseau, mais il est certain que le nom du réseau sera entré correctement.

N'oubliez pas que seuls les AccessPoints qui envoient des balises sont visibles à vos yeux lorsque vous utilisez le bouton de commande *Scan*.

#### Configurer Odyssey pour se connecter à n'importe quel réseau

*Odyssey Client Manager* propose une configuration de réseau spéciale appelée *[any]*. Le réseau *[any]* se connecte à n'importe quel réseau, quel que soit son nom. Le réseau *[any]* est très utile lorsque vous vous déplacez dans des salles de conférence, des hôtels ou dans d'autres endroits proposant des accès réseau. Si vous sélectionnez le réseau *[any]* dans la fenêtre *Connection*, vous pouvez vous connecter à de tels réseaux sans avoir à les configurer individuellement.

Pour configurer un réseau *[any]*, cochez la case *Connect to any available network* et cliquez sur *OK*.

Même si vous pouvez utiliser des clés WEP ou des profils WEP avec un réseau *[any]*, il est courant d'utiliser *[any]* sans authentification 802.11 ou 802.1X.

#### Spécifier la description du réseau

Des descriptions de réseau sont utiles pour distinguer les réseaux ayant des noms identiques ou similaires. Vous pouvez entrer la description du réseau dans le champ *Description*.

## Spécifier le type de réseau

Si vous n'avez pas utilisé le bouton de commande *Scan* pour sélectionner votre réseau, vous devez spécifier le type de réseau en sélectionnant l'une des options de la liste déroulante.

- Sélectionnez *Access point (infrastructure mode)* si ce réseau utilise des AccessPoints pour offrir des possibilités de connexion au réseau de l'entreprise ou à Internet. Il s'agit du réglage le plus courant.
- Sélectionnez *Peer-to-peer (ad-hoc mode)* pour configurer un réseau privé avec un ou plusieurs ordinateurs.

## Spécifier le mode d'association

Avant l'authentification, vous devez associer votre Client à un AccessPoint. Le mode d'association que vous demandez est fonction du matériel de votre AccessPoint et de la façon dont il est configuré. Votre administrateur réseau peut vous aider à configurer le mode d'association requis par votre réseau.

Vous trouverez d'autres informations sur les possibilités de sélection de ce mécanisme de cryptage et sur le mode d'association sous "Wired-Equivalent Privacy (WEP) avec clés préconfigurées" et "Wi-Fi Protected Access (WPA) et chiffrement TKIP".

Vous avez le choix entre trois modes d'association :

- *Open* pour se connecter à un réseau via un AccessPoint ou un commutateur avec authentification 802.1X. Sélectionnez ce mode si vous ne devez pas sélectionner de mode partagé ou WPA.
- *Shared* pour se connecter à un réseau via un AccessPoint qui exige des clés de sécurité WEP pour l'association et le cryptage des données.
- *WPA* pour se connecter à un réseau via un AccessPoint mettant en œuvre WPA (Wi-Fi Protected Access).

## Spécifier un mécanisme de cryptage adapté à votre mode d'association

Le choix du mécanisme de cryptage dépend également des conditions imposées par l'AccessPoint. Vos possibilités varient en fonction du mode d'association sélectionné. Vous trouverez d'autres informations dans "Wired-Equivalent Privacy (WEP) avec clés préconfigurées" et "Wi-Fi Protected Access (WPA) et chiffrement TKIP".

Les options suivantes s'offrent à vous :

- *none* pour utiliser l'authentification 802.1X sans clé WEP. Cette option est uniquement disponible si vous avez opté pour le mode d'association *open*.
- *WEP* pour utiliser la clé WEP pour le cryptage des données. Cette option est proposée pour tous les modes d'association et est requis si vous configurez l'association en mode partagé (*Shared*). Si vous sélectionnez cette option, vous devez entrer la clé WEP dans la partie *Pre-configured keys* de l'onglet *Network Properties*. Vous devez sélectionner cette option si les AccessPoints de votre réseau requièrent l'association en mode partagé (*Shared*) avec une clé WEP.
- *TKIP* pour utiliser le protocole d'intégrité temporaire des clés. Sélectionnez cette option si les AccessPoints de votre réseau requièrent l'authentification WPA et sont configurés pour le cryptage de données TKIP.
- *AES* pour utiliser le protocole étendu de cryptage par défaut. Sélectionnez cette option si les AccessPoints de votre réseau requièrent l'authentification WPA et sont configurés pour le cryptage de données AES.

### Champs d'authentification

Dans la partie *Authentication* vous pouvez configurer l'authentification au réseau avec les caractéristiques suivantes :

- Authentification avec un profil
- Génération automatique de clés

#### Authentification avec un profil

Si le réseau radio que vous avez configuré exige que vous vous authentifiiez avec votre identifiant personnel, cochez la case *Authenticate using profile* et sélectionnez dans la liste déroulante le profil à utiliser pour l'authentification. **Vous devez avoir déjà configuré un profil adapté à l'authentification sur ce réseau.**

Si vous cochez la case *Authenticate using profile*, Odyssey Client effectue une authentification 802.1X avec votre mot de passe, votre certificat ou d'autres moyens conformément à la configuration du profil sélectionné.

#### Génération automatique de clés

Cochez la case *Keys will be generated automatically for data privacy* si la méthode d'authentification spécifiée dans le profil est configurée pour créer des clés WEP dynamiques à utiliser entre votre ordinateur et l'AccessPoint. Certaines méthodes d'authentification comme EAP-TTLS, PEAP et EAP-TLS génèrent des clés. D'autres méthodes d'authentification n'en génèrent pas. Si vous utilisez EAP-TTLS, PEAP ou EAP-TLS pour vous authentifier, cochez cette case. Vous pouvez utiliser chacune de ces méthodes d'authentification pour les AccessPoints avec authentification 802.1x. Cette option offre davantage de sécurité que l'utilisation de clés statiques (préconfigurées). Ne cochez pas cette option si vous êtes invité à utiliser des clés WEP préconfigurées ou, dans le cas d'une authentification WPA, une clé pre-shared.

### Clés préconfigurées (WEP ou WPA)

Le réseau radio peut exiger que vous préconfiguriez des clés WEP ou que vous partagiez (pre-share) une passphrase en cas d'authentification WPA. Vous pouvez spécifier les clés dans la zone *Pre-configured keys* de l'onglet *Network Properties*.

#### Clés pre-shared (WPA)

Si vous avez sélectionné le mode WPA sans générer automatiquement la clé lorsque vous associez un profil d'authentification à la connexion réseau, vous devez entrer une passphrase ASCII pre-shared dans le champ *Passphrase*. Cette passphrase servira de base à la génération de la clé requise.



## Clés préconfigurées (WEP)

Si vous avez sélectionné le mode partagé, vous devez configurer au moins une clé WEP. Vous devez aussi configurer au moins une clé WEP si vous sélectionnez le cryptage WEP pour le mode ouvert et que vous ne générez pas les clés automatiquement lorsque vous associez un profil d'authentification à la connexion réseau. Les clés WEP jouent les rôles suivants :

- Association à un AccessPoint avant l'établissement d'une connexion (mode partagé).
- Cryptage de données entre votre ordinateur et l'AccessPoint (ou d'autres ordinateurs dans un réseau peer-to-peer)  
voir "Wired-Equivalent Privacy (WEP) avec clés préconfigurées".

Si le réseau radio utilise l'authentification 802.1X et que des clés WEP dynamiques sont générées (ce qui signifie que vous avez coché les cases *Authenticate using profile* et *Keys will be generated automatically for data privacy*), vous ne devez spécifier aucune clé WEP préconfigurée pour protéger les données. Il est cependant possible mais peu courant d'utiliser des clés WEP préconfigurées pour une authentification en plus de 802.1X. EAP-MD5, par exemple, ne génère pas de clé WEP pour le cryptage des données, ce qui signifie que vous devez préparer une clé si votre profil est configuré pour l'authentification avec cette méthode.

Si vous utilisez l'une de ces clés WEP préconfigurées, vous devez cocher les cases correspondantes et régler en conséquence une ou plusieurs clés WEP :

- Cochez la case *authenticate to access points (shared mode)* si des clés WEP préconfigurées sont requises pour vous authentifier sur un AccessPoint avant l'établissement de la connexion avec le réseau radio.
- Cochez la case *for data privacy* pour utiliser des clés WEP préconfigurées pour crypter les données sur le réseau radio. Entrez la clé WEP dans les champs *Key 0* à *Key 3*. Les valeurs de ces champs doivent correspondre à celles des AccessPoints ou des ordinateurs homologues (peer) auxquels vous voulez vous connecter. Il est courant d'utiliser *Key 0* même si votre réseau peut exiger d'autres clés. Vous pouvez entrer des clés sous la forme soit de caractères normaux (ASCII) soit de caractères hexadécimaux.

Les clés WEP ont une longueur de 40 ou 104 bits. Cette longueur correspond à 5 ou 13 caractères si vous les entrez en tant que caractères ASCII ou à 10 ou 26 caractères si vous les entrez en tant que caractères hexadécimaux.

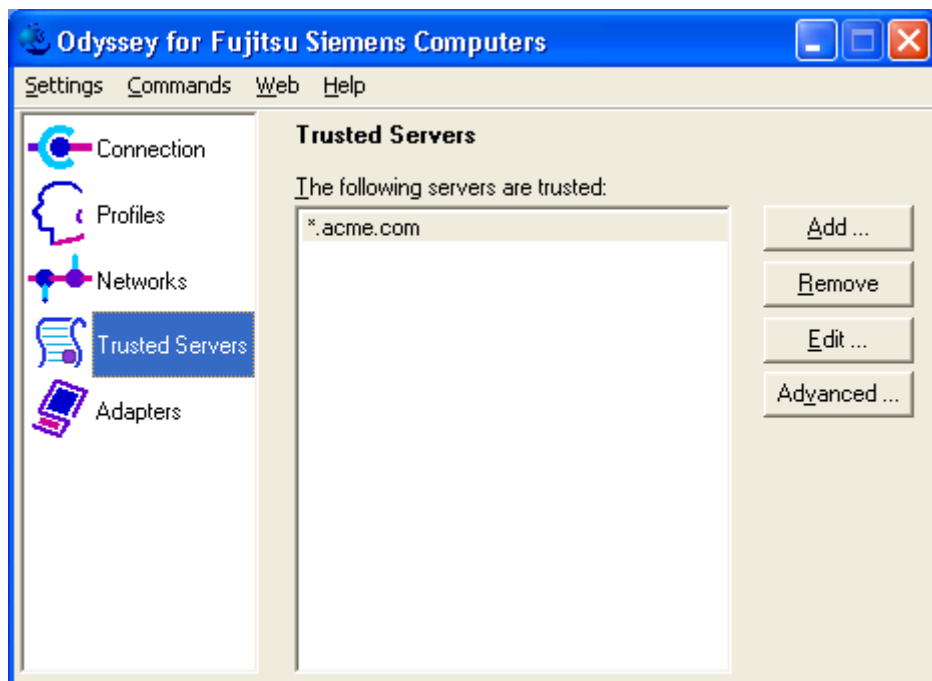
Pour entrer une clé WEP préconfigurée :

- Pour *Format for entering keys*, sélectionnez soit *ASCII characters* soit *Hexadecimal digits* en fonction de la manière dont vous voulez entrer les clés.
- Entrez dans les champs texte *Key 0* à *Key 3* chaque clé que vous voulez préconfigurer.

## Spécifier des serveurs dignes de confiance - Fenêtre "Trusted Servers"

La fenêtre *Trusted Servers* vous permet de configurer les serveurs d'authentification auxquels vous faites confiance pour vous connecter au réseau.

- Dans l'Odyssey Client Manager, cliquez sur *Trusted Servers* pour afficher la fenêtre à l'écran.



Si vous faites confiance à un serveur, vous devez non seulement spécifier son nom mais aussi la chaîne de certificats à laquelle il appartient. Odyssey Client est très souple et propose une méthode simple et sophistiquée de configuration des serveurs de confiance.

Vous trouverez d'autres informations dans "Extensible Authentication Protocol (EAP)".

## Procédure simple de configuration des serveurs de confiance

Dans la plupart des cas, vous pouvez utiliser une méthode simple pour configurer la confiance. Avec cette méthode, vous devez définir deux éléments :

- Le nom de domaine du serveur ou le suffixe du nom de domaine (par exemple, acme.com)
- Le certificat d'une autorité de certification dans la chaîne. Il peut s'agir du certificat d'une autorité de certification de base ou intermédiaire („Root or Intermediate Certificate Authority").

### Noms de domaine

Chaque serveur dispose d'un nom de domaine qui l'identifie clairement et ce nom de domaine est généralement repris dans le champ "Subject CN" du certificat du serveur.

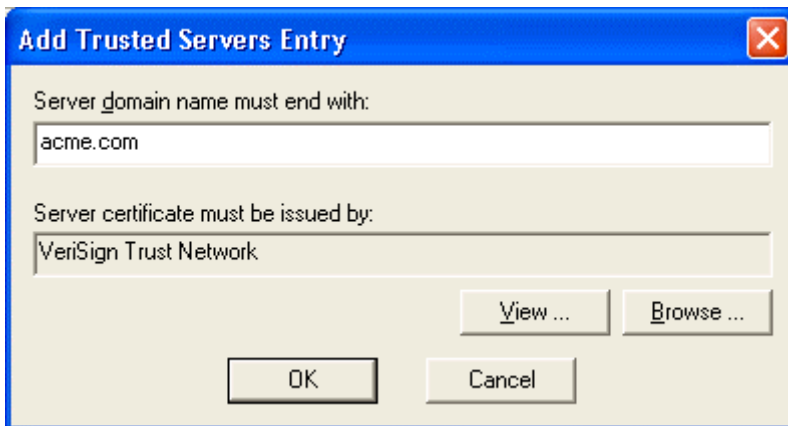
Le nom de domaine d'un serveur se termine par le nom d'un domaine administratif plus important auquel le serveur appartient. L'entreprise Acme, par exemple, peut avoir un nom de domaine comme acme.com. L'entreprise pourrait aussi avoir différents serveurs d'authentification portant les noms auth1.acme.com, auth2.acme.com et auth3.acme.com.

Comme le montre cet exemple, vous pouvez - par une seule entrée - définir la confiance que vous avez dans tous les serveurs d'une entreprise en spécifiant la terminaison du nom de domaine du serveur.

### Ajouter une entrée ‚Trusted Server'

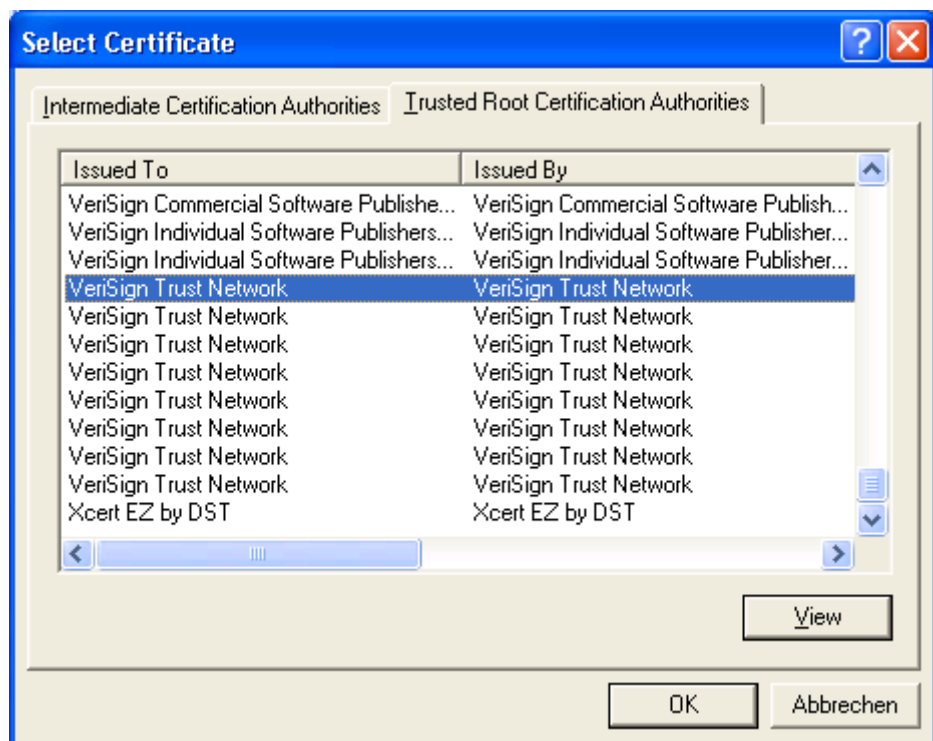
Pour ajouter une entrée dans la liste des serveurs de confiance, procédez comme suit :

- Cliquez sur *Add*. La fenêtre *Add Server* s'affiche.



- Dans le champ *Server domain name must end with*, entrez le nom (ou le suffixe du nom) de domaine auquel doit appartenir le serveur de confiance. Vous devez compléter ce champ.

- Réglez le champ *Server certificate must be issued by* sur le certificat de l'autorité de certification qui a émis directement ou indirectement le certificat du serveur. Pour attribuer un certificat, procédez comme suit :
  - Cliquez sur *Browse* pour obtenir une liste des certificats.
  - Sélectionnez le certificat dans la liste et cliquez sur *OK*.



Il peut s'agir du certificat d'une autorité de certification de base ou intermédiaire (.Root or Intermediate Certificate Authority'). Il ne doit pas s'agir du certificat qui a directement émis le certificat du serveur. Il peut s'agir de n'importe quel certificat de la chaîne.

### Supprimer une entrée ,Trusted Server'

Pour supprimer une entrée de la liste des Trusted Server, sélectionnez l'entrée et cliquez sur *Remove*.

### Editer une entrée ,Trusted Server'

Pour éditer une entrée de la liste des serveurs de confiance, sélectionnez l'entrée et cliquez sur *Edit*. La fenêtre *Edit Trusted Servers Entry* s'affiche et vous permet d'éditer le domaine de serveur et le certificat de l'émetteur.

## Procédure élargie de configuration des serveurs de confiance

Si vous avez besoin de plus de contrôle de confiance, vous pouvez utiliser la procédure avancée.



Si vous n'avez aucune expérience pratique des certificats et des chaînes de certificats, n'essayez pas de configurer la confiance avec la procédure avancée. Renseignez-vous auprès de votre administrateur réseau sur la configuration de serveurs de confiance.

Cette procédure permet de visualiser toute la structure de confiance. La structure de confiance montre tous les serveurs de confiance configurés.

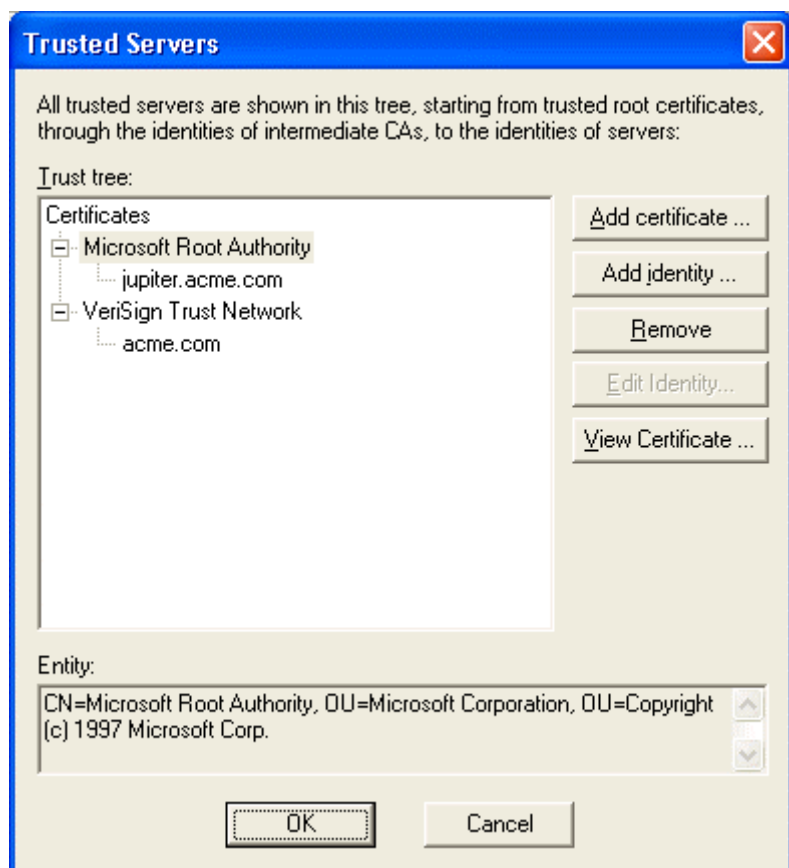
Chaque branche de la structure de confiance détermine une série de règles pour apparier une chaîne de certificats. Odyssey Client fait uniquement confiance à un serveur d'authentification si sa chaîne de certificats correspond au moins à une branche de la structure de confiance.

Une branche de la structure de confiance se compose de deux ou plusieurs nœuds :

- Chaque nœud de niveau supérieur est le certificat d'une autorité de certification de base ou intermédiaire.
- Chaque nœud intermédiaire (pour autant qu'il existe) est le nom d'une autorité de certification intermédiaire au sein de la chaîne.
- Chaque nœud de fin est le nom d'un serveur auquel vous confiez l'authentification. Les noms des autorités et serveurs de certification peuvent être spécifiés sous la forme de noms d'objet ou de noms de domaine. Par ailleurs, vous pouvez décider que le nom dans un certificat doit correspondre précisément au nom configuré ou qu'il doit se terminer par le nom configuré.

## Visualiser la structure de confiance

Pour visualiser la structure de confiance, cliquez sur *Advanced*. La fenêtre *Trusted Servers* s'affiche dans laquelle vous pouvez afficher et modifier les règles de confiance.

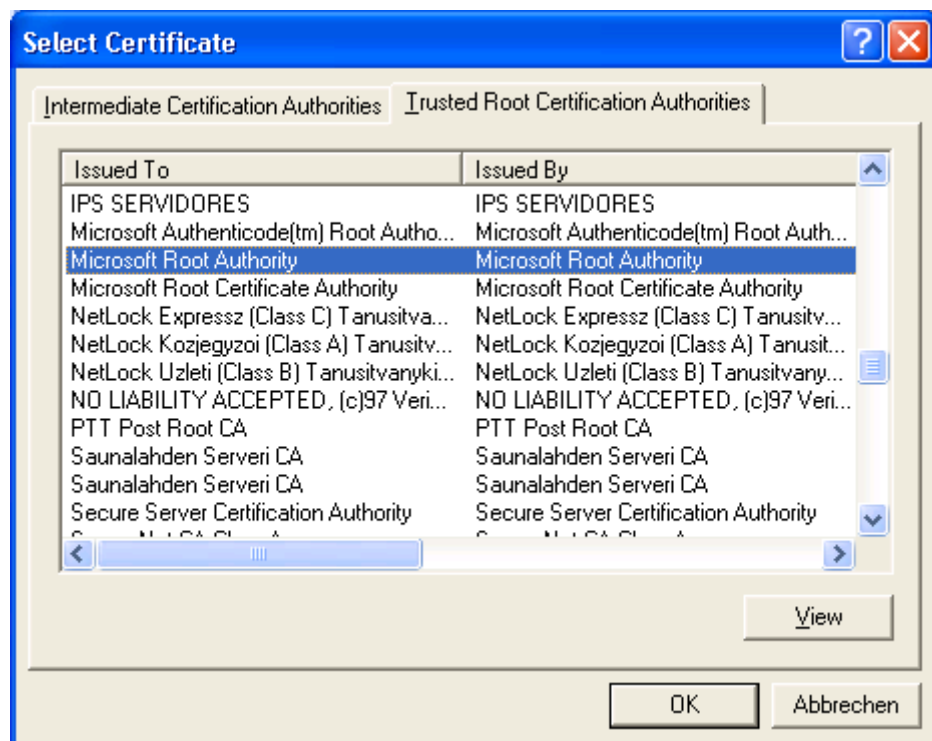


## Ajouter des nœuds de certificat

Pour ajouter un nouveau certificat au début de la structure de confiance :

- ▶ Cliquez sur *Add certificate*. La fenêtre *Select Certificate* s'affiche.
- ▶ Sélectionnez un certificat et cliquez sur *OK*. Vous pouvez faire votre choix dans la liste des certificats intermédiaires ou des certificats de base homologués.

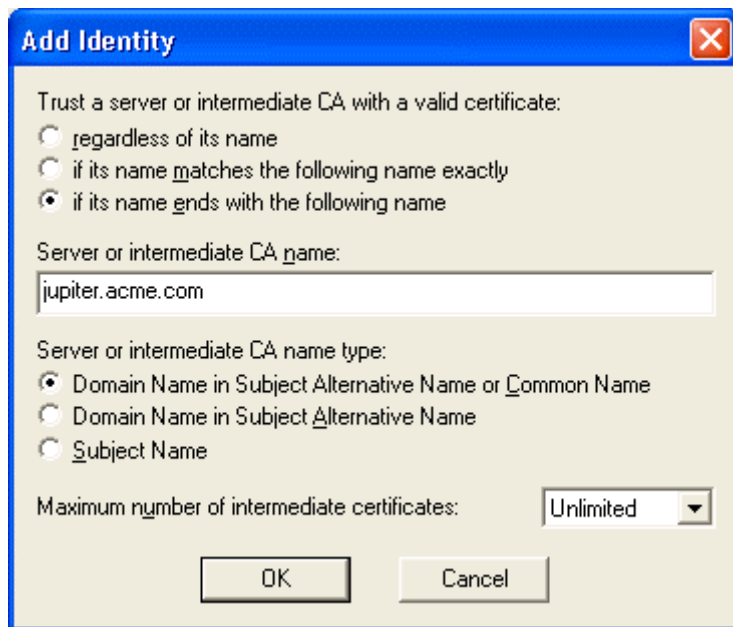
Pour obtenir plus d'informations sur un certificat avant de l'ajouter, sélectionnez le certificat et cliquez sur *View*.



## Ajouter des serveurs d'authentification ou des nœuds CA intermédiaires

Tous les nœuds situés sous le niveau supérieur désignent soit des serveurs d'authentification soit des autorités de certification intermédiaires. Un nœud final désignera un serveur d'authentification. Si ce n'est pas le cas, il partira du principe qu'il désigne une autorité de certification intermédiaire. Pour ajouter à la structure un serveur d'authentification ou une autorité de certification intermédiaire :

- ▶ Sélectionnez le nœud dans la structure sous laquelle vous voulez ajouter le nouvel élément.
- ▶ Cliquez sur *Add Identity*. La fenêtre *Add Identity* s'affiche.
- ▶ Entrez les informations qui définissent les règles qu'Odyssey Client utilise pour adapter un certificat de la chaîne de certificats du serveur à ce nœud.
- ▶ Cliquez sur *OK*.



La fenêtre *Add Identity* vous permet de configurer les règles d'adaptation pour un seul nœud de la structure de confiance.

Pour définir un serveur de confiance ou une autorité de certification intermédiaire avec certificat valide, sélectionnez :

- *regardless of its name* pour adapter un certificat indépendamment de son nom pour autant qu'il porte la signature de l'autorité de certification dans le nœud supérieur.
- *if its name matches the following name exactly* pour décider que le nom dans le certificat correspond précisément à celui que vous avez indiqué.
- *if its name ends with the following name* pour décider que le nom dans le certificat est subordonné au nom que vous avez indiqué. Un certificat portant, par exemple, le nom "sales.acme.com" correspondrait à une entrée "acme.com".

Pour *Name of Server or intermediate CA*, entrez le nom (ou le suffixe d'un nom) avec lequel vous voulez établir la correspondance. (ce champ n'est pas nécessaire si vous sélectionnez *regardless of its name*). La forme du nom dépend du type de nom que vous avez choisi.

Pour l'autorité de certification *Name type*, vous devez indiquer la manière dont le nom sera interprété et où il se trouve dans le certificat. Sélectionnez l'une des options suivantes :

- *Domain name in Subject Alternative Name or Common Name* lorsque le nom de domaine (p. ex. acme.com) se trouve dans le champ *Subject Alternative Name* du certificat ou, si ce n'est pas le cas, le *Common Name* dans le champ *Subject* du certificat (ceci est le choix le plus courant).
- *Domain name in Subject Alternative Name* lorsque le nom de domaine se trouve dans le champ "Subject Alternative Name" du certificat. Ce qui correspond approximativement à la sélection précédente.



- *Subject Name* lorsque le nom est un nom X.500 et qu'il se trouve dans le champ *Subject* du certificat. Lorsque vous entrez intégralement ou partiellement un nom de rubrique, vous devez le faire au format X.500. Il correspond à chaque nom de rubrique d'un certificat de même niveau ou de niveau inférieur.

- Lorsque vous indiquez, par exemple, ceci :

`OU=acme.com, C=US`

le nom correspond à l'un des noms de rubrique suivants :

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



Si vous entrez du texte contenant des virgules, chaque virgule doit être précédée et suivie de guillemets simples.

Pour *Maximum number of Intermediate Certificates*, fixez le nombre maximum de certificats qui sont susceptibles d'apparaître dans la chaîne entre ce nœud et le nœud directement supérieur à ce nœud. Vous pouvez sélectionner un nombre entre 0 et 5 ou encore *unlimited* (illimité) :

- Si vous choisissez 0, le certificat qui correspond à ce nœud doit être signé avec le certificat qui correspond au nœud supérieur.
- Si vous choisissez 1, le certificat qui correspond à ce nœud peut être signé avec le certificat qui correspond au nœud supérieur ou par un certificat qui a été signé à son tour par le certificat qui correspond au nœud supérieur.
- Si vous choisissez *unlimited*, n'importe quel nombre de certificats de la chaîne peut apparaître entre le certificat qui correspond à ce nœud et un certificat qui correspond au nœud supérieur.

## Supprimer des nœuds

Pour supprimer un nœud, sélectionnez dans la structure le nœud à supprimer et cliquez sur *Remove*. Le nœud sélectionné et chaque nœud en-dessous seront supprimés dans la structure.

Les nœuds suivants peuvent être supprimés :

- Nœud Top-Level Certificate
- Nœud Intermediate CA
- Nœud de serveur

## Affichage des informations de certificats

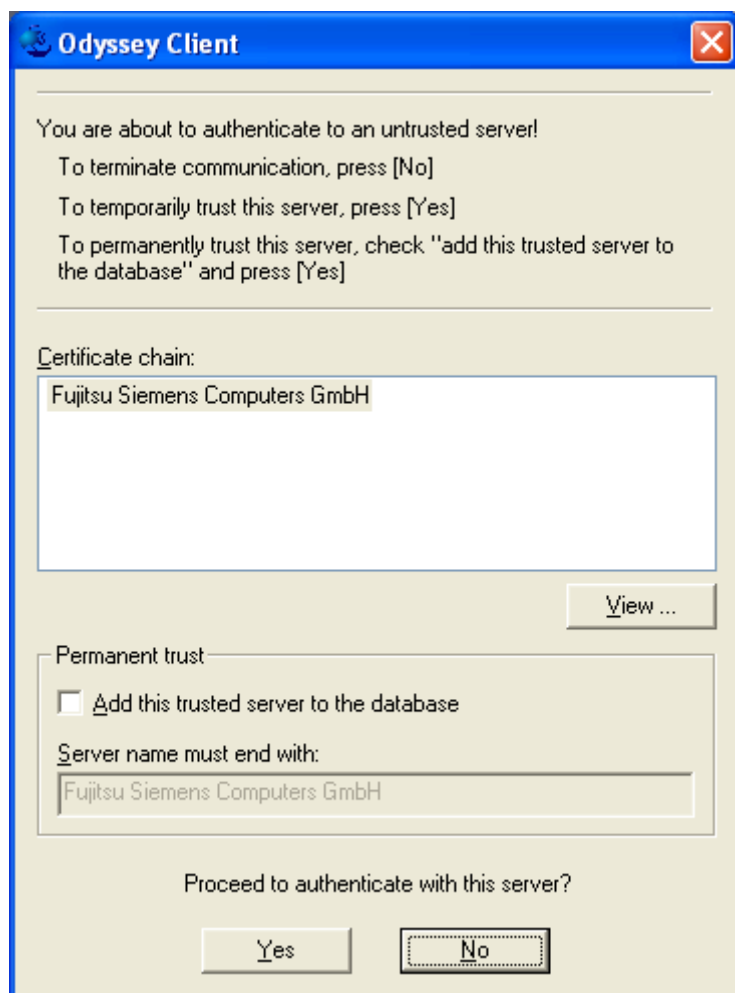
Pour obtenir des informations détaillées sur un certificat du niveau supérieur de la structure de confiance, sélectionnez le certificat et cliquez sur *View Certificate*.

## Untrusted Server

Pendant la phase d'authentification du réseau et dans les conditions suivantes, vous avez la possibilité de faire confiance à un serveur qui n'était pas sécurisé auparavant ("Untrusted Server") :

- Vous avez choisi l'option de confiance provisoire (*Enable Server temporary trust*) dans le menu *Security Settings*.
- Le profil d'authentification requiert une validation du serveur.
- L'autorité de certification de base sécurisée (Trusted Root Certificate Authority) du certificat du serveur (il s'agit du certificat "ACMERootCA" dans l'exemple reproduit ci-dessous) est installée sur votre client.

La fenêtre suivante s'affiche pendant que vous vous authentifiez au réseau.



La fenêtre montre toute la chaîne de certificats entre le serveur d'authentification et une 'Trusted Root Certificate Authority'. Vous obtiendrez d'autres informations sur un certificat de la chaîne en sélectionnant le certificat en question et en cliquant sur *View*.

Si ce serveur doit être temporairement utilisé comme serveur de confiance (c'est-à-dire jusqu'à ce qu'Odyssey soit relancé) pour l'authentification et la connexion au réseau, cliquez sur *Yes*. Si ce n'est pas le cas, cliquez sur *No*. Vous pouvez être invité à entrer votre mot de passe en fonction du profil que vous avez défini pour cette connexion.

Si vous souhaitez faire toujours confiance à ce serveur et l'ajouter dans la liste des serveurs de confiance (Trusted Servers), cochez la case *Add this trusted Server to the database* et cliquez sur *Yes*. Le serveur est ajouté dans la liste des serveurs de confiance sous le nom de serveur utilisé dans le champ *Server name must end with*. Vous pouvez éditer le nom de serveur. Vous pouvez, par exemple, transformer un nom de serveur "auth2.acme.com" en "acme.com" si vous voulez faire de tous les serveurs d'authentification du domaine "acme.com" des serveurs de confiance.

## Configurer des cartes réseau - Fenêtre "Adapters"

La fenêtre *Adapters* vous permet de sélectionner une ou plusieurs cartes réseau pour l'interconnexion de réseaux sans fils. Vous pouvez sélectionner plusieurs cartes réseau en maintenant la touche **Ctrl** de votre clavier enfoncée pendant que vous faites votre choix avec la souris.

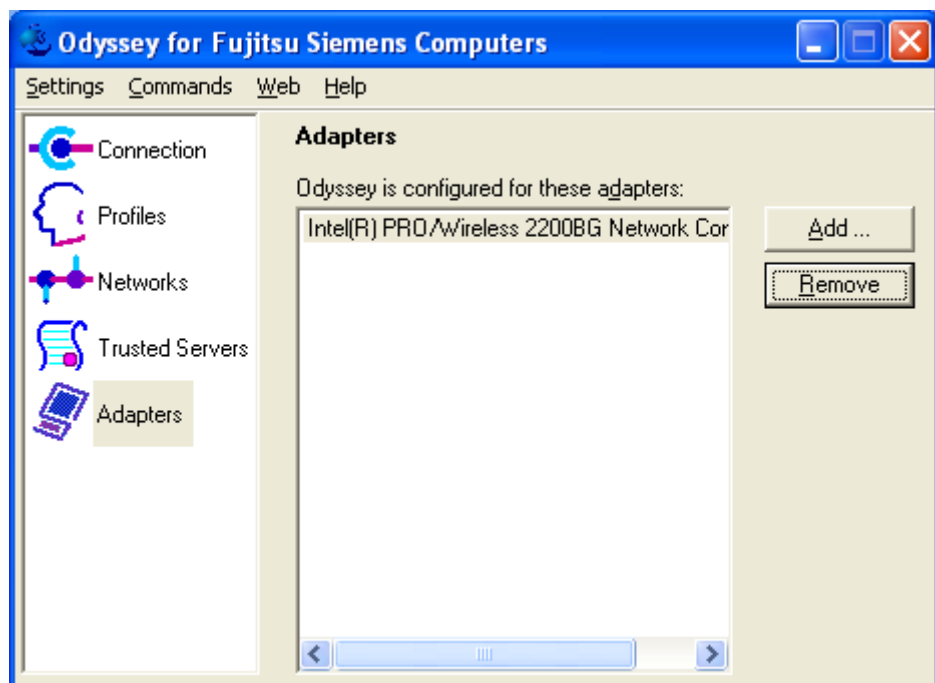
La fenêtre *Adapters* propose une liste de toutes les cartes réseau sans fil qui sont configurées dans Odyssey Client. Vous avez probablement configuré une seule carte réseau. Vous pouvez cependant en configurer plusieurs. Vous pouvez utiliser la fenêtre *Adapters* pour les tâches suivantes :

- Ajouter une carte réseau sans fil
- Supprimer une carte réseau de la liste



Vous devez avoir installé votre carte réseau sur votre système avant de pouvoir configurer Odyssey Client pour l'utiliser.

- Cliquez dans l'Odyssey Client Manager sur *Adapters* pour afficher la fenêtre.



## Ajouter une carte réseau sans fil

Pour ajouter une carte réseau sans fil qu'Odyssey Client n'a pas encore reconnue, procédez comme suit dans la fenêtre *Adapters* de l'Odyssey Client Manager :

- Cliquez sur *Add*. La fenêtre *Add Adapter* apparaît et affiche la liste de toutes les cartes réseau qui sont installées sur votre ordinateur (à l'exception de celles pour lesquelles Odyssey Client est configuré).



- Choisissez l'onglet *Wireless*.
- Sélectionnez la carte réseau voulue dans la liste et cliquez sur *OK*.

N'oubliez pas que seules sont affichées les cartes réseau que vous n'avez pas encore ajoutées. Si votre carte réseau sans fil ne figure pas dans la liste, sélectionnez *All Adapters*.



Assurez-vous que toutes les cartes réseau que vous avez sélectionnées dans l'onglet *Wireless* sont effectivement des cartes réseau sans fil.

## Supprimer une carte réseau de la liste

Pour supprimer une carte réseau de la liste des cartes réseau dans la fenêtre *Adapters*, sélectionnez la carte réseau à supprimer et cliquez sur *Remove*.

Odyssey Client n'utilisera plus cette carte réseau. La carte réseau est toujours installée sur votre système mais elle se comporte comme si Odyssey Client n'existait pas.

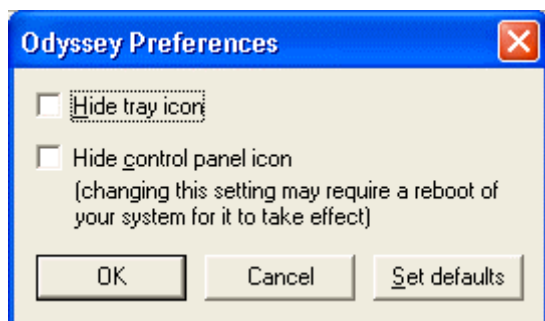
## Odyssey Client Manager - Menu "Settings"

Le menu *Settings* dans la fenêtre *Odyssey Client Manager* propose les options de menu suivantes :

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

### Option de menu "Preferences"

Vous pouvez modifier la façon dont Odyssey Client fonctionne avec l'option de menu *Preferences*. La fenêtre *Odyssey Preferences* s'affiche.



Réglez vos préférences et cliquez sur *OK* pour activer ce réglage :

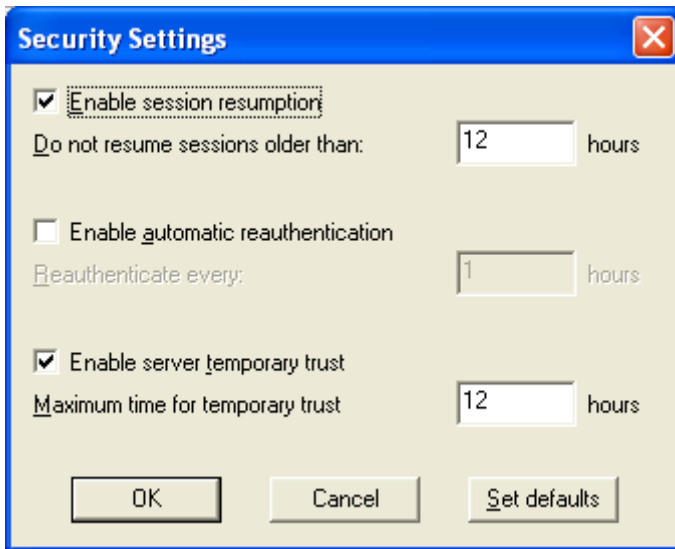
- Si vous sélectionnez *Hide tray icon*, l'icône Odyssey n'apparaît pas dans la barre de tâches (en bas à droite de votre écran).
- Si vous sélectionnez *Hide control panel icon*, l'icône Odyssey n'apparaît pas dans le panneau de configuration Windows.



Si le panneau de configuration Windows est ouvert au moment où vous sélectionnez *Hide control panel icon* et cliquez sur *OK*, le panneau de configuration est réactualisé. (Appuyez sur la touche **F5** pour voir le résultat). Dans certains cas, il sera nécessaire de redémarrer l'ordinateur.

## Option de menu "Security settings"

Pour configurer des options de sécurité avancées pour l'authentification, sélectionnez *Security Settings*. La fenêtre *Security Settings* s'affiche.



Les options de sécurité affichent par défaut des valeurs standard qui conviennent dans la plupart des cas. Vous pouvez réactiver les valeurs par défaut à tout moment en sélectionnant *Set defaults*.

Les champs de temps sont exprimés en heures et peuvent compter jusqu'à maximum deux décimales. Pour indiquer une heure et quinze minutes, par exemple, vous devez entrer *1.25*.

### Reprise d'une session

La fenêtre *Security Settings* vous permet d'activer la reprise de la session.

Pour activer la reprise de la session :

- Cochez la case *Enable session resumption*.
- Réglez le champ *Do not resume sessions older than* sur le nombre d'heures maximum pendant lequel une authentification initiale peut être utilisée pour accélérer l'authentification. Lorsque la limite est dépassée, le système procède à une nouvelle authentification la prochaine fois que vous vous ré-authentifiez. Le nombre d'heures peut compter jusqu'à deux décimales. Pour indiquer une heure et quinze minutes, par exemple, vous devez entrer *1.25*.

Le réglage *Session resumption* est activé par défaut et l'authentification recommence pendant un maximum de 12 heures.

Pour désactiver cette fonction, décochez la case d'option *Enable session resumption*.

### Ré-authentification automatique

Vous pouvez aussi activer ou désactiver la fonction *Automatic reauthentication* d'Odyssey Client.

Cochez la case *Enable automatic reauthentication* dans la fenêtre *Security Settings* pour qu'Odyssey Client effectue périodiquement une nouvelle authentification avec le serveur.

Réglez l'intervalle de temps en heures dans le champ *Reauthenticate every* pour que la ré-authentification s'effectue automatiquement.

Décochez la case *Enable automatic reauthentication* dans la fenêtre *Security Settings* pour désactiver cette fonction.

Par défaut, le réglage *Automatic reauthentication* n'est pas activé. En effet, votre administrateur réseau a peut-être configuré vos AccessPoints ou votre serveur d'authentification pour qu'ils relancent l'authentification à intervalles réguliers. Demandez à votre administrateur réseau quel est le bon réglage pour cette option.

### Server temporary trust

Normalement, vous configurez votre serveur d'authentification dans la fenêtre *Trusted Servers*. Il peut arriver, cependant, que vous visitiez un réseau dont le serveur d'authentification ne soit pas encore été configuré comme serveur de confiance dans la fenêtre *Trusted Servers*. Dans ce cas, vous pouvez activer l'option *Temporary Trust* (confiance provisoire) pour cet „Untrusted Server“ (serveur non sécurisé).

Cochez l'option *Enable Server temporary trust* dans la fenêtre *Security Settings* pour activer l'option *Temporary Trust*. Décochez l'option pour désactiver la fonction. Lisez attentivement ce qui suit :

- Si vous avez activé *Temporary Trust*, vous avez la possibilité de faire temporairement confiance à un "Untrusted Server" lorsque vous essayerez de vous authentifier auprès d'un "Untrusted Server". Voyez aussi "Untrusted Server".
- La fenêtre *Untrusted Server* qui s'affiche au moment de la tentative d'authentification d'un serveur pour lequel vous n'avez pas configuré de confiance vous permet d'ajouter définitivement le serveur dans votre structure de confiance. Vous pouvez par conséquent utiliser l'option *Temporary trust* en tant qu'alternative à la fenêtre *Trusted Servers* et configurer des serveurs de confiance lorsque vous en rencontrez.
- Si l'option *Temporary trust* n'est pas activée, toute tentative d'authentification qui exige la validation d'un certificat de serveur échouera si le serveur n'est pas explicitement un serveur de confiance.

Réglez l'option *Maximum time for temporary trust* sur le nombre maximum d'heures pendant lequel Odyssey Client doit continuer à utiliser un serveur comme serveur de confiance une fois que vous l'avez accepté.

Par défaut, l'option *Temporary trust* est activée et la durée maximale pendant laquelle un serveur est temporairement considéré comme serveur de confiance une fois que vous l'avez accepté est de 12 heures.



Ces réglages ne s'appliquent pas si vous décidez en permanence de considérer le serveur comme un serveur de confiance en cochant l'option *Add this trusted Server to the database* dans la fenêtre *Untrusted Server*.



## Option de menu "Enable/Disable Odyssey"

Sélectionnez *Enable Odyssey* ou *Disable Odyssey* pour activer ou désactiver l'Odyssey Client. Au départ, l'Odyssey Client est activé et il n'est normalement pas nécessaire de le désactiver. Si vous sélectionnez *Disable Odyssey Client*, vous débranchez toutes les cartes réseau sans changer les réglages de la fenêtre *Connection*. Le programme Odyssey Client tourne toujours mais il est complètement séparé des connexions réseau radio.

Ne désactivez Odyssey Client que si vous rencontrez des problèmes avec votre configuration Odyssey actuelle. Vous pourriez par exemple désactiver Odyssey Client parce que vous craignez qu'il soit devenu instable et que vous voulez vous assurer que vous êtes bien déconnecté du réseau avant de pouvoir vérifier les réglages.

Odyssey Client peut aussi être activé et désactivé à partir du menu contextuel qui apparaît si vous cliquez avec le bouton droit de la souris sur l'icône Odyssey dans la barre de tâches.



Pour arrêter Odyssey Client complètement, sélectionnez l'option de menu *Exit* après avoir cliqué avec le bouton droit de la souris sur l'icône Odyssey dans la barre de tâches.

## Option de menu "Close"

Sélectionnez *Close* pour fermer la fenêtre Odyssey Client Manager. Bien que l'interface utilisateur ne soit plus visible, Odyssey Client continue de fonctionner.

Vous pouvez relancer Odyssey Client Manager à tout moment en procédant comme suit :

- à partir de la barre de tâches : double-cliquez sur l'icône Odyssey ou cliquez dessus avec le bouton droit de la souris et sélectionnez *Odyssey for Fujitsu Siemens Computers*.
- à partir du panneau de configuration : double-cliquez sur l'icône *Odyssey for Fujitsu Siemens Computers*.
- à partir du menu de démarrage Windows : sélectionnez *Démarrer – Programmes – Fujitsu Siemens Computers – Odyssey Client for Fujitsu Siemens Computers – Odyssey Client Manager for Fujitsu Siemens Computers*.



Pour arrêter Odyssey Client complètement, sélectionnez l'option de menu *Exit* après avoir cliqué avec le bouton droit de la souris sur l'icône Odyssey dans la barre de tâches.

## Odyssey Client Manager - Menu "Commands"

Les options de menu suivantes sont proposées dans le menu *Commands* :

- *Forget Password*
- *Forget Temporary Trust*

### Option de menu "Forget Password"

Lorsque vous vous authentifiez pour la première fois avec un profil réglé sur *prompt for password*, vous êtes invité à entrer votre mot de passe. Odyssey Client mémorise ce mot de passe pour l'utiliser lors des prochaines authentifications avec ce profil sans que vous deviez le réintroduire. Ce mot de passe reste normalement en mémoire jusqu'au redémarrage de l'ordinateur ou d'Odyssey Client.

Si Odyssey Client ne doit pas mémoriser les mots de passe introduits, sélectionnez *Forget Password*. Lorsqu'il aura à nouveau besoin de votre mot de passe, il vous invitera à l'entrer une nouvelle fois.

Cette option de menu vous sera également utile si vous avez mal entré votre mot de passe ou si votre mot de passe a été modifié sur le serveur d'authentification.

### Option de menu "Forget Temporary Trust"

Si vous activez *Temporary trust* au moyen des réglages *Settings - Security Settings*, une fenêtre s'ouvrira chaque fois que vous rencontrez un serveur d'authentification *Untrusted*. Cette fenêtre vous permet d'utiliser temporairement le serveur en question comme serveur de confiance. Odyssey Client se rappelle ce serveur de confiance pendant la période de temps configurée dans *Security Settings*.

Pour effacer immédiatement la liste des serveurs de confiance, sélectionnez *Forget Temporary Trust*.

Cette option de menu vous sera également utile si vous acceptez qu'un serveur soit temporairement *Trusted* avant de décider de couper votre connexion avec lui. Pour s'assurer que la connexion est coupée immédiatement, vous devez désactiver *Session resumption* puis cliquer sur *Reconnect* dans la fenêtre *Connection*.

## Odyssey Client Manager – Menu "Help"

Le menu *Help* propose les options de menu suivantes :

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

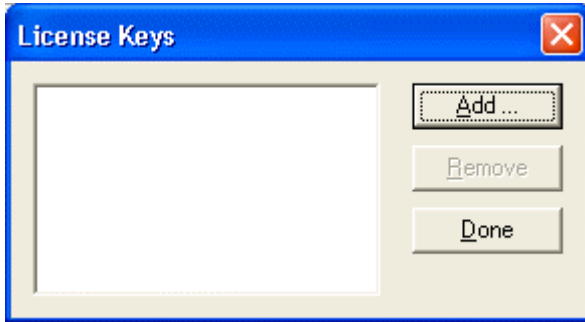
## Option de menu "Help topics"

Sélectionnez *Help Topics* pour accéder au système d'aide d'Odyssey Client.

Vous pouvez aussi obtenir à tout moment une aide contextuelle en appuyant sur la touche **F1**. Le système d'aide s'ouvre au chapitre qui explique le mieux la situation dans laquelle vous vous trouvez à cet instant.

## Option de menu "License keys"

Sélectionnez *License Keys* dans le menu d'aide pour gérer votre clé de licence Odyssey Client.



Une clé de licence est une séquence de texte qui représente votre licence d'utilisation d'Odyssey Client.

## Menu contextuel "Odyssey"

Si vous cliquez avec le bouton droit de la souris sur l'icône Odyssey dans la barre de tâches, vous voyez apparaître les options de menu suivantes :

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

## Option de menu "Odyssey for Fujitsu Siemens Computers"

Lorsque vous sélectionnez l'option de menu *Odyssey for Fujitsu Siemens Computers*, l'Odyssey Client Manager (l'interface utilisateur de l'Odyssey Client) s'affiche à l'écran.

### Option de menu "Enable Odyssey/Disable Odyssey"

Sélectionnez *Enable Odyssey* ou *Disable Odyssey* pour activer ou désactiver l'Odyssey Client.

Au départ, l'Odyssey Client est activé et il n'est normalement pas nécessaire de le désactiver. Si vous sélectionnez *Disable Odyssey Client*, vous débranchez toutes les cartes réseau sans changer les réglages de la fenêtre *Connection*. Le programme Odyssey Client tourne toujours mais il est complètement séparé des connexions réseau radio.

Ne désactivez Odyssey Client que si vous rencontrez des problèmes avec votre configuration Odyssey actuelle. Vous pourriez par exemple désactiver Odyssey Client parce que vous craignez qu'il soit devenu instable et que vous voulez vous assurer que vous êtes bien déconnecté du réseau avant de pouvoir vérifier les réglages.

Odyssey Client peut aussi être activé et désactivé à partir de l'Odyssey Client Manager.

### Option de menu "Help"

Une des options de menu qui apparaît lorsque vous cliquez avec le bouton droit de la souris sur l'icône Odyssey dans la barre de tâches est *Help*. Deux options sont proposées : *Help Topics* et *About*.

Si vous sélectionnez *Help Topics*, le système d'aide apparaît dans une fenêtre ouverte sur la table des matières.

Si vous sélectionnez *About*, la version du produit et les informations de copyright sont affichées.

### Option de menu "Exit"

Si vous sélectionnez *Exit*, Odyssey Client arrête immédiatement de fonctionner en arrière-plan. Vous pouvez sélectionner cette option si vous n'utilisez pas le réseau radio pendant une longue période.

Vous pouvez redémarrer Odyssey Client au moyen de l'*Odyssey Client Manager* sous *Démarrer – Programmes – 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-)einrichtung  
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)...



---

# Index

- A**
- Access point (infrastructure mode) 31
  - AccessPoint 2
  - Adapters 12
  - Afficher les informations des certificats 41
  - Ajouter des nœuds de certificat 38
  - Anonymous name 24
  - Authentification 4
    - avec profil 32
    - clé WEP 4, 31
    - génération automatique de clés 32
    - indiquer le mode d'association 31
    - mode Open 31
    - mode Shared 31
    - mode WPA 31
    - options de sécurité étendue 47
    - ré-authentification automatique 48
  - Authentication 802.1X 33
    - description 4
    - mode Open 31
    - sans clé WEP 31
  - Authentication WPA 31
    - AES 31
    - clé pre-shared 32
    - passphrase 32
- C**
- Carte réseau
    - activer 44
    - configurer 43
    - désactiver 45
  - Certificat 19, 35
  - Certificate Authority 35
  - Chaîne de certificats 37
  - CHAP 23
  - Clé de licence Odyssey Client 51
  - Clé pre-shared
    - description 4
    - entrer 33
  - Clé WEP 4
    - entrer 33
  - Clés de licence 51
  - Close 49
  - Configure and Enable Wizard 9
  - Configurer
    - Odyssey Client 11
  - Configurer carte réseau radio 44
  - Connect to any available network 30
  - Connection 12
    - affichage de l'état de la connexion 15
  - Connexion radio
    - afficher l'état 15
    - couper 15
    - établir (avec n'importe quel réseau) 30
    - ré-authentifier 15
  - Connexion réseau
    - établir 13
    - utiliser 12
  - Consignes de sécurité 6
  - Cryptage de données AES 31
  - Cryptage TKIP 4, 31
- D**
- Définir des profils 16
  - Définir un nom anonyme 24
  - Description de réseau 30
  - Désignation du réseau 28
  - Directive 1999/5/EG 6
  - Domaine de serveur 35
- E**
- EAP 5
  - EAP/PEAP 24
  - EAP-TLS 32
  - EAP-TTLS 22, 32
    - définir un nom anonyme 24
  - Enable Odyssey/Disable Odyssey 52
  - Enable Server temporary trust 42
  - Enable session resumption 47
  - Enable/Disable Odyssey 49
  - Extensible Authentication Protocol 5
- F**
- Fenêtre
    - Adapters 12, 43
    - Connection 12, 15
    - Networks 12, 27
    - Profiles 12, 16
    - Trusted Servers 12, 34
  - Forget Password 50
  - Forget Temporary Trust 50
  - Fréquences radio 7
- I**
- Icône Odyssey
    - afficher dans la barre des tâches 46
    - supprimer dans la barre des tâches 46
  - Identifiant 5
  - Inner Authentication Protocol 23

Installer, Odyssey Client 9  
Intermediate Certificates  
    ajouter à la structure de confiance 39  
    nombre maximum 41

**L**  
Login 19

**M**  
marquage CE 6  
Mauvaise connexion radio 15  
Menu  
    Commands 50  
    Help 50  
    Settings 46  
Menu contextuel Odyssey 51  
Mode Adhoc 2  
Mode Infrastructure 2  
Mode peer-to-peer 2  
Mot de passe  
    ne pas mémoriser 50  
Mot de passe  
    saisie 19  
MS-CHAP-V2. 23

**N**  
Network name (SSID) 30  
Networks 12, 27  
Nom d'utilisateur 19  
Nom de réseau 28  
Norme 802.1X 5  
Norme IEEE 802.11a, fréquences 7  
Norme IEEE 802.11b, fréquences 8

**O**  
Odyssey Client  
    configurer 11  
    installer 9  
    quitter 50, 52  
Odyssey Client Manager 11  
    afficher 51  
Open  
    mode 31

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

Protocole d'authentification 21  
    EAP 5  
    EAP-TLS 21  
    EAP-TTLS 22  
    interne 23  
    PEAP 21

**R**  
Ré-authentification automatique 48  
Reprendre la session Odyssey 47  
Réseau  
    chercher 30  
Réseau radio  
    configurer 27, 28  
    établir une connexion réseau 13  
    Nom 3  
    norme IEEE 802.11 1  
    rechercher 13  
    Reconnect 15  
    Service Set Identifier (SSID) 3

**S**  
Sécurité réseau  
    802.11 3  
    authentification 3  
    clé WEP 3  
Server temporary trust 48  
Serveur d'authentification 21  
    ajouter à la structure de confiance 39  
    Enable Server temporary trust 42  
    Server temporary trust 48  
    Trusted Server 34  
    vérifier l'identité 21  
Serveurs dignes de confiance  
    voir Trusted Servers 34  
Shared  
    mode 31  
Structure de confiance 37  
    afficher 38  
    ajouter des nœuds de certificat 38  
    supprimer les nœuds du certificat 41  
Symboles 1

**T**  
Trusted Root Certificate Authority 43  
Trusted Servers 12, 34  
    ajouter 35  
    contrôle de confiance étendu 37  
    contrôle simple de la confiance 35  
    éditer 36  
    effacer 36  
    structure de confiance 37

Type de réseau  
Adhoc 2  
indiquer 31  
Infrastructure 2

**U**  
Untrusted Server 42

**W**  
Wi-Fi Protected Access (WPA) 4  
Wired-Equivalent Privacy (WEP) 4  
WPA  
description 4