

answers²

Benutzerhandbuch

Wireless LAN

Deutsch



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.

Herausgegeben von/Published by
Fujitsu Siemens Computers GmbH

Bestell-Nr./Order No.: **A26391-K133-Z131-1-19**
Ausgabe/Edition **3**
Printed in the Federal Republic of Germany
AG 0704 07/04

Wireless LAN

Benutzerhandbuch

Wireless LAN allgemein

Installation von Odyssey

Verwendung von Odyssey
Client

Stichwörter

Microsoft, MS, MS-DOS, Windows und Windows NT sind eingetragene Warenzeichen der Microsoft Corporation.

Odyssey ist ein eingetragenes Warenzeichen von Funk Software.

Alle anderen Warenzeichen sind Warenzeichen oder eingetragene Warenzeichen der jeweiligen Inhaber und werden als geschützt anerkannt.

Copyright © Fujitsu Siemens Computers GmbH 2004

Alle Rechte vorbehalten, insbesondere (auch auszugsweise) die der Übersetzung, des Nachdrucks, der Wiedergabe durch Kopieren oder ähnliche Verfahren.

Zu widerhandlungen verpflichten zu Schadenersatz.

Alle Rechte vorbehalten, insbesondere für den Fall der Patenterteilung oder GM-Eintragung.

Liefermöglichkeiten und technische Änderungen vorbehalten.

Dieses Handbuch wurde erstellt von
cognitas. Gesellschaft für Technik-Dokumentation mbH
www.cognitas.de

Inhalt

Wireless LAN allgemein	1
Funknetzwerk nach dem IEEE 802.11-Standard	1
Adhoc-Modus	2
Infrastruktur-Modus	2
Betriebssystemvoraussetzungen	2
Namen für Funknetzwerke (SSID)	3
802.11-Netzwerksicherheit	3
Wired-Equivalent Privacy (WEP) mit vorkonfigurierten Schlüsseln	4
Wi-Fi Protected Access (WPA) und TKIP-Verschlüsselung	4
802.1X-Standard	5
Extensible Authentication Protocol (EAP)	5
Wichtige Hinweise	6
Sicherheitshinweise	6
CE-Kennzeichnung	6
Funkfrequenzen und Sicherheits-Standards	7
Installation von Odyssey	9
Odyssey Client installieren	9
Configure and Enable Wizard	9
Verwendung von Odyssey Client	11
Übersicht über den Odyssey Client Manager	11
Odyssey Client Manager-Anzeige	12
Netzwerkverbindungen steuern - Fenster "Connection"	12
Netzwerkkarte auswählen	13
Mit einem Netzwerk verbinden	13
Nach Funknetzwerken suchen	13
Mit einem Netzwerk wieder verbinden	15
Im Netzwerk re-authentifizieren	15
Netzwerkverbindung trennen	15
Verbindungsdaten ansehen	15
Profile definieren - Fenster "Profiles"	16
Profil hinzufügen oder ändern - Fenster "Profile Properties"	17
Registerkarte "Authentication"	20
Funknetzwerke konfigurieren - Fenster "Networks"	27
Netzwerke hinzufügen oder ändern – Fenster "Network Properties"	28
Vertrauenswürdige Server spezifizieren - Fenster "Trusted Servers"	34
Einfaches Verfahren zum Konfigurieren von Trusted Servern	35
Erweitertes Verfahren zum Konfigurieren von Trusted Servern	37
Untrusted Server	42
Netzwerkkarten konfigurieren - Fenster "Adapters"	43
Funknetzwerkkarte hinzufügen	44
Netzwerkkarte aus der Liste entfernen	45
Odyssey Client Manager - Menü "Settings"	45
Menüpunkt "Preferences"	46
Menüpunkt "Security settings"	46
Menüpunkt "Enable/Disable Odyssey"	49
Menüpunkt "Close"	49
Odyssey Client Manager - Menü "Commands"	49
Menüpunkt "Forget Password"	50
Menüpunkt "Forget Temporary Trust"	50

Odyssey Client Manager - Menü "Help" 50

 Menüpunkt "Help topics" 50

 Menüpunkt "License keys" 50

Kontextmenü "Odyssey" 51

 Menüpunkt "Odyssey for Fujitsu Siemens Computers" 51

 Menüpunkt "Enable Odyssey/Disable Odyssey" 51

 Menüpunkt "Help" 52

 Menüpunkt "Exit" 52

Features 53

Overview 53

Technical details 54

Declaration of Conformity 57

Stichwörter 59

Wireless LAN allgemein

In Ihrem Gerät ist eine Funknetzwerkarte integriert. In diesem Benutzerhandbuch ist beschrieben, wie Sie die Einstellungen für Ihr Wireless LAN vornehmen.

Darstellungsmittel

In diesem Handbuch werden folgende Darstellungsmittel verwendet.



kennzeichnet Hinweise, bei deren Nichtbeachtung Ihre Gesundheit, die Funktionsfähigkeit Ihres Geräts oder die Sicherheit Ihrer Daten gefährdet ist. Die Gewährleistung erlischt, wenn Sie durch Nichtbeachtung dieser Hinweise Defekte am Gerät verursachen.



kennzeichnet wichtige Informationen für den sachgerechten Umgang mit dem System.

► kennzeichnet einen Arbeitsschritt, den Sie ausführen müssen.

Texte in Schreibmaschinenschrift stellen Bildschirmausgaben dar.

Kursive Schrift kennzeichnet Programmnamen, Befehle oder Menüpunkte.

"Anführungszeichen" markieren Kapitelnamen, Diskettennamen und andere Mediennamen und einzelne Begriffe, die hervorgehoben werden sollen.

Funknetzwerk nach dem IEEE 802.11-Standard

Die integrierte Netzwerkkarte arbeitet nach dem IEEE 802.11-Standard. Als Kommunikationsmedium werden Frequenzen aus den ISM-Frequenzbändern verwendet (ISM, Industrial, Scientific, Medical). Die Funknetzwerkkarte darf ohne Anmeldung und gebührenfrei betrieben werden. Der IEEE 802.11-Standard sieht mehrere Möglichkeiten vor, die ISM-Frequenzbänder zu nutzen:

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

Die nach 802.11 arbeitenden Funknetzwerke lassen sich leicht mit vorhandenen Ethernet-Netzwerken verbinden. Nach 802.11 arbeitende Funknetzwerkkarten sind bis auf ein paar Zusatzparameter ein System mit einer normalen Ethernet-Karte. Das heißt, dass Sie in einem 802.11-Funknetzwerk alle Protokolle verwenden können, wie in einem kabelgebundenes Ethernet (IP, IPX, NetBIOS,...). Der einzige Unterschied ist, dass Sie keine Leitungen zwischen den Computern verlegen müssen. Die Menge aller Wireless-LAN-Stationen, die sich gegenseitig direkt erreichen können, bezeichnet man allgemein als Funkzelle. Der IEEE-Standard bietet zwei Betriebsarten an, den Adhoc-Modus (Peer-to-Peer) und den Infrastruktur-Modus.

Neben der Beschreibung der Modulation und des Data Framing enthält diese Norm ein Authentifizierungs- und Verschlüsselungsverfahren mit der Bezeichnung Wired Equivalent Privacy (WEP). Viele Unternehmen setzen 802.11-Funknetzwerke ein. 802.11-Funknetzwerke findet man jetzt auch in Hotels, auf Flugplätzen und an anderen "Hotspots" mit Zugang zum Internet.

Adhoc-Modus

Ein Wireless LAN im Adhoc-Modus, auch Peer-to-Peer-Modus genannt, besteht aus einer einzelnen abgeschlossenen Funkzelle. Adhoc-Funknetzwerke entstehen, wenn sich eine Arbeitsgruppe mit ihren Systemen zusammenfindet und diese zum Datenaustausch vernetzen möchte. Systeme können zu einem solchen Netzwerk beliebig hinzukommen und es wieder verlassen.

Damit sich mehrere Adhoc-Funknetzwerke nicht gegenseitig im Funkverkehr behindern, gibt es einen eindeutigen Netzwerknamen, die SSID (Service Set Identifier). Die SSID wird zur Adressierung verwendet, sodass sich ein Datenpaket immer einer bestimmten Funkzelle zuordnen lässt.

Wenn Sie sich in ein bestehendes Funknetzwerk einwählen wollen, benötigen Sie den Netzwerknamen (SSID), den Sie in den Einstellungen für die Netzwerkkarte eintragen. Die Netzwerkkarte sucht dann beim Start nach einem Funknetzwerk mit dieser SSID. Wenn die Netzwerkkarte ein Funknetzwerk gefunden hat, klinkt sie sich in dieses ein und Sie können mit den Systemen in diesem Funknetzwerk kommunizieren. Wenn zwei Funkzellen sehr nah beieinander sind, sollten die Funkkanäle dieser Netzwerke 4 bis 5 Kanäle auseinander liegen. Dies gilt für 802.11b und 802.11g.

Infrastruktur-Modus

Im Infrastruktur-Modus existiert neben den beweglichen Stationen eine Basisstation, die als AccessPoint bezeichnet wird. Im Infrastruktur-Modus übernimmt der AccessPoint die Funktion eines "Wächters". Im Gegensatz zum Adhoc-Modus muss sich jedes System bei dem AccessPoint anmelden, bevor es Daten in der Funkzelle austauschen darf.

Eine weitere Aufgabe des AccessPoint ist die Verbindung der Funkzelle mit einem kabelgebundenen Ethernet. Da der AccessPoint durch den Zwang zur Anmeldung jederzeit genau weiß, welche Stationen sich auf der Funkseite befinden, kann er exakt entscheiden, welche Daten durchgereicht werden müssen und welche nicht. Diesen Vorgang bezeichnet man auch als Bridging.

Um die Reichweite eines Funknetzwerks zu vergrößern, können mehrere AccessPoints mit der gleichen SSID verwendet werden.

Geht ein System ins Funknetzwerk, sucht es sich unter den erreichbaren AccessPoints den mit dem stärksten Signal aus und meldet sich dort an. Zwei Systeme, die an unterschiedlichen AccessPoints angemeldet sind, kommunizieren so miteinander, auch wenn sie nicht in direkter Funkreichweite sind. Überwacht ein System auch nach der Anmeldung kontinuierlich die Funksituation, kann es erkennen, wie die Signale von einem AccessPoint schwächer und von einer anderen stärker werden und sich für den Benutzer unmerklich ummelden. Diesen Vorgang bezeichnet man als Roaming.

Betriebssystemvoraussetzungen

Betriebssystem Windows 2000 und Windows XP

Namen für Funknetzwerke (SSID)

Jedes Funknetzwerk verfügt über seinen eigenen Namen. Sie können das Funknetzwerk, mit dem Sie sich verbinden wollen, über seinen Namen auswählen. Netzwerknamen ermöglichen den gleichzeitigen Betrieb verschiedener Funknetzwerke nebeneinander in derselben Umgebung, ohne dass diese sich gegenseitig behindern. Wenn beispielsweise das Unternehmen neben Ihnen ebenfalls Funknetzwerke verwendet, möchten Sie sicherstellen, dass Ihr Computer mit dem Netzwerk Ihrer Firma verbunden ist und nicht mit dem anderen, auch wenn sich Ihr Computer im Bereich der benachbarten AccessPoints (Zugangspunkte) liegt. (Wie verhindert wird, dass Fremde sich in Ihr Firmennetzwerk einwählen, ist Gegenstand der nachfolgenden Sicherheitsdiskussion.) Ein Netzwerkname ist einfach eine Folge aus maximal 32 Zeichen, wie z. B. "Bayonne Office" oder "Acme-Marketronics" oder "BE45789". Für Netzwerknamen gilt die Groß- und Kleinschreibung, darum müssen Sie beim Eingeben sorgsam darauf achten. Es steht Ihnen jedoch frei, Namen bereits verfügbarer Netzwerke auszusuchen. Wenn Sie das Netzwerk aus einer Liste auswählen, werden Fehler bei der Namenseingabe vermieden. Die 802.11-Norm legt Netzwerknamen fest wie beispielsweise den "Service Set Identifier" (SSID).

802.11-Netzwerksicherheit

Seit dem Aufkommen der Funknetzwerke spielt Sicherheit in weit größerem Maße eine kritische Rolle als früher, aus dem einfachen Grund, weil es Angreifer leichter haben, diese Verbindungen anzuzapfen. Bei kabelgebundenen Netzwerken können die meisten Unternehmen den Schutz ihrer Netzwerke gerätetechnisch sichern. Ein Angreifer müsste in die Firmenräume gelangen, um sich in das LAN einzuschalten und den Netzwerkverkehr auszuspiionieren.

Alles was man zum Ausspiionieren von Daten im Funknetzwerk braucht, ist ein Computer mit einer Funknetzwerkkarte und eine geeignete Stelle draußen auf dem Parkplatz oder im Büro nebenan. Nachfolgend werden einige Voraussetzungen für die sichere Vernetzung beschrieben:

- Ein Benutzer muss vom Netzwerk authentifiziert werden, ehe ihm der Zugriff darauf genehmigt wird, damit das Netzwerk vor Eindringlingen sicher ist.
- Das Netzwerk muss durch den Benutzer authentifiziert sein, ehe er seinem Computer die Verbindung mit dem Netzwerk gestattet. Dadurch wird verhindert, dass ein Funkgerät sich als legitimes Netzwerk ausgibt und Zugriff auf den Computer des Benutzers erhält.
- Die gegenseitige Authentifizierung zwischen Benutzer und Netzwerk muss kryptographisch geschützt werden. Damit wird sichergestellt, dass Sie mit Ihrem gewünschten Netzwerk verbunden werden und nicht mit einem falschen.
- Die Funkverbindung zwischen einem Computer und dem AccessPoint muss so verschlüsselt werden, dass Eindringlinge nicht Zugriff auf Daten erhalten, die als vertraulich gelten.

Für diese Art sicherer Verschlüsselung über ein Funknetzwerk gibt es zwei grundlegende Mechanismen:

- Als WEP-Schlüssel bezeichnete, vorkonfigurierte geheime Angaben. WEP-Schlüssel halten nicht zugelassene Benutzer vom Funknetzwerk fern und verschlüsseln die Daten legitimer Benutzer.
- Authentifizierung mit Hilfe eines 802.1X-Protokolls. Hierbei werden vielfältige zugrunde liegende Authentifizierungsprotokolle für die Zugangskontrolle zum Netzwerk verwendet. Die stärksten dieser Protokolle können gegenseitige Authentifizierung von Benutzer und Netzwerk sichern und können dynamisch Schlüssel zur Verschlüsselung von Funkdaten erzeugen.

Wired-Equivalent Privacy (WEP) mit vorkonfigurierten Schlüsseln

Mit vorkonfigurierten WEP-Schlüsseln (Wired-Equivalent Privacy) wird dem Client-Computer sowie dem AccessPoint derselbe Geheimschlüssel zugeordnet. Dieser Schlüssel wird dazu verwendet, alle zwischen dem Computer und dem AccessPoint ausgetauschten Daten zu verschlüsseln. Zusätzlich kann der WEP-Schlüssel zur Authentifizierung des Client-Computer am AccessPoint benutzt werden. Falls der Computer nicht nachweisen kann, dass er den WEP-Schlüssel kennt, wird ihm der Zugang zum Netzwerk verwehrt.

- Wenn der AccessPoint einen WEP-Schlüssel für die Authentifizierung erfordert, müssen Sie die Zuordnung zum AccessPoint im Shared-Modus vornehmen. Den Zuordnungsmodus stellen Sie in den Netzwerk-Eigenschaften ein.
- Wenn der AccessPoint keinen WEP-Schlüssel für die Authentifizierung erfordert, wird dies als offener Modus (open) bezeichnet. Den Zuordnungsmodus stellen Sie in den Netzwerk-Eigenschaften ein.
- Wenn der AccessPoint eine WEP-Verschlüsselung für WPA anstelle von TKIP für die Authentifizierung erfordert, werden alle erforderlichen WEP-Schlüssel aus einer ASCII-Passphrase erzeugt, die Sie für Ihren AccessPoint sowie für Odyssey Client konfigurieren.

Siehe folgende Themen:

- "Zuordnungsmodus angeben", mit Anleitung zur Auswahl eines Zuordnungsmodus in Odyssey Client
- "Ein geeignetes Verschlüsselungsverfahren für Ihren Zuordnungsmodus angeben", mit Anleitung zur Auswahl der WEP-Verschlüsselung im Shared-Modus
- "Vorkonfigurierte Schlüssel (WEP)", zur Verwendung statischer WEP-Schlüssel bei Odyssey Client
- "Pre-shared-Schlüssel (WPA)", zum Konfigurieren der WEP-Verschlüsselung im WPA-Modus

Wi-Fi Protected Access (WPA) und TKIP-Verschlüsselung

Als Erweiterung der 802.11-Norm umfasst Wi-Fi Protected Access (WPA) eine Reihe von Sicherheitszusätzen über Wired-Equivalent Privacy hinaus. Diese Erweiterungen beinhalten Folgendes:

- Verbesserte Datenverschlüsselung durch TKIP (temporäres Schlüsselintegritäts-Protokoll). TKIP bietet eine leistungstärkere Verschlüsselung als WEP, weil Schlüssel nach jeweils 10.000 Paketen dynamisch aktualisiert werden.
- 802.1X-Authentifizierung mit EAP. Wenn die Hardware des AccessPoints in Ihrem Netzwerk erfordert, dass Sie die Authentifizierung über den erweiterten WPA-Modus vornehmen, können Sie Odyssey Client so konfigurieren, dass die Authentifizierung im WPA-Modus erfolgt. Falls die Hardware für die TKIP-Verschlüsselung konfiguriert ist, können Sie Odyssey Client auch für dieses erweiterte Datenverschlüsselungsverfahren konfigurieren. Neben der Übereinstimmung mit den 802.1X-Spezifikationen für die dynamische Schlüsselerzeugung (verfügbar mit den leistungstärksten Authentifizierungsmethoden), ermöglicht WPA das Generieren von Pre-shared-Schlüsseln zur TKIP- (oder WEP-) Verschlüsselung über eine Passphrase. Wenn Sie eine Passphrase für die Schlüsselerzeugung bei Ihren AccessPoints konfigurieren, müssen Sie dieselbe Passphrase bei Odyssey Client konfigurieren.

Siehe folgende Themen:

- "Zuordnungsmodus angeben", zur Anwendung des WPA-Modus bei Odyssey Client
- "Ein geeignetes Verschlüsselungsverfahren für Ihren Zuordnungsmodus angeben", zur Verwendung der TKIP-Verschlüsselung im WPA-Modus
- "Pre-shared-Schlüssel (WPA)" zum Konfigurieren einer statischen Passphrase

802.1X-Standard

Das IEEE 802.1X-Protokoll ermöglicht den authentifizierten Zugang zu einem LAN. Diese Norm gilt sowohl für kabellose als auch kabelgebundene Netzwerke. Bei einem Funknetzwerk erfolgt die 802.1X-Authentifizierung, nachdem die 802.11-Zuordnung implementiert ist. Kabelgebundene Netzwerke verwenden die 802.1X-Norm ohne 802.11-Zuordnung.

Das WEP-Protokoll, das vorkonfigurierte Schlüssel verwendet, weist verschiedene Schwächen auf in Bezug auf einfache Verwaltung und Sicherheit. Um diese Probleme zu lösen, hat IEEE eine weitere Norm eingeführt: 802.1X. 802.1X bietet bessere Sicherheit als die vorkonfigurierten WEP-Schlüssel und ist einfach zu handhaben, insbesondere bei großen Netzwerken.

Bei Anwendung vorkonfigurierter WEP-Schlüssel wird der kabellose Client-Computer gegenüber dem Netzwerk authentifiziert. Bei 802.1X wird der Benutzer gegenüber dem Netzwerk mit den Berechtigungsnachweisen authentifiziert (Passwort, Zertifikat oder Token-Karte). Die Authentifizierung wird nicht durch den AccessPoint vorgenommen, sondern vielmehr durch einen zentralen Server. Falls dieser Server das RADIUS-Protokoll benutzt, bezeichnet man ihn als RADIUS-Server.

Bei 802.1X kann ein Benutzer sich bei dem Netzwerk von jedem Computer aus anmelden, und viele AccessPoints können gemeinsam einen einzelnen RADIUS-Server zur Authentifizierung benutzen. Dadurch ist es für den Netzwerkadministrator viel einfacher, den Zugang zum Netzwerk zu kontrollieren.

Einzelheiten können Sie folgenden Themen entnehmen:

- EAP-Protokoll (Extensible Authentication Protocol)
- Wiederaufnahme einer Sitzung (Session resumption)
- Re-Authentifizierung (Reauthentication)

Extensible Authentication Protocol (EAP)

802.1X benutzt das Protokoll mit der Bezeichnung EAP (Extensible Authentication Protocol), um die Authentifizierung vorzunehmen. EAP ist kein Authentifizierungsmechanismus an sich, sondern ein gemeinsamer Rahmen für den Transport aktueller Authentifizierungsprotokolle. Der Vorteil des EAP-Protokolls ist, dass der grundlegende EAP-Mechanismus bei der Entwicklung neuer Authentifizierungsprotokolle nicht geändert werden muss.

Wichtige Hinweise

Sicherheitshinweise

Die meisten Sicherheitshinweise finden Sie im Handbuch "Erste Schritte" Ihres Geräts. Einige der wichtigsten Sicherheitshinweise finden Sie im folgenden Text.

- Schalten Sie die Funkkomponente (Bluetooth oder Wireless LAN) am Gerät aus, wenn Sie sich in einem Krankenhaus, einem Operationssaal oder in der Nähe eines medizinischen Elektroniksystems befinden. Die übertragenen Funkwellen können die medizinischen Geräte in ihrer Funktion beeinträchtigen.
- Wie Sie die Funkkomponente ausschalten, ist in dem mit Ihrem Gerät ausgelieferten Handbuch "EasyGuide" beschrieben.
- Halten Sie das Gerät mindestens 20 cm von einem Herzschrittmacher fern, da sonst die ordnungsgemäßen Funktionen des Herzschrittmachers durch Funkwellen beeinträchtigt werden können.
- Die übertragenen Funkwellen können ein unangenehmes Summen in Hörgeräten verursachen.
- Schalten Sie das Gerät aus, wenn Sie sich in einem Flugzeug befinden oder mit dem Auto fahren.
- Bringen Sie das Gerät nicht mit eingeschalteter Funkkomponente in die Nähe entflammbarer Gase oder in eine explosionsgefährdete Umgebung (z. B. Lackiererei), da die übertragenen Funkwellen eine Explosion oder ein Feuer auslösen können.

Das Unternehmen Fujitsu Siemens Computers GmbH ist nicht für Funk- oder Fernsehstörungen verantwortlich, die durch unerlaubte Änderungen an diesem Gerät verursacht wurden. Fujitsu Siemens übernimmt ferner keine Verantwortung für den Ersatz bzw. den Austausch von Anschlussleitungen und Geräten, die nicht von der Fujitsu Siemens Computers GmbH angegeben wurden. Für die Behebung von Störungen, die durch eine derartige unerlaubte Änderung hervorgerufen wurden, und für den Ersatz bzw. den Austausch der Geräte ist allein der Benutzer verantwortlich.

CE-Kennzeichnung



Dieses Gerät erfüllt in der ausgelieferten Ausführung die Anforderungen der Richtlinie 1999/5/EG des Europäischen Parlamentes und des Rates vom 9. März 1999 über Funkanlagen und Telekommunikationsendeinrichtungen und die gegenseitige Anerkennung der Konformität.

Dieses Gerät darf in Belgien, Dänemark, Deutschland, Finnland, Frankreich, Griechenland, Großbritannien, Irland, Italien, Luxemburg, Niederlanden, Österreich, Portugal, Schweden, Schweiz, Spanien, Island, Liechtenstein und Norwegen verwendet werden. Aktuelle Information über eventuelle Einschränkungen im Betrieb finden Sie bei der entsprechenden Behörde des jeweiligen Landes. Wenn Ihr Land nicht in der Aufzählung dabei ist, dann wenden Sie sich bitte an die entsprechende Aufsichtsbehörde, ob die Nutzung dieses Produkts in Ihrem Land erlaubt ist.

Einschränkungen

- Frankreich
 - Eingeschränkter Frequenzbereich: nur die Kanäle 10 bis 13 (2457 MHz bis 2472 MHz) dürfen in Frankreich verwendet werden. Es ist untersagt, das Gerät draußen zu verwenden.
- Italien
 - Eine ministerielle Genehmigung ist auch für den Gebrauch im Innenbereich notwendig. Bitte setzen Sie sich wegen der diesbezüglichen Verfahrensweise mit dem Verkäufer in Verbindung. Es ist untersagt, das Gerät draußen zu verwenden.
- Niederlande
 - Für den Gebrauch im Freien ist eine Lizenz vorgeschrieben. Bitte setzen Sie sich wegen der diesbezüglichen Verfahrensweise mit dem Verkäufer in Verbindung.

Funkfrequenzen und Sicherheits-Standards

Die folgende Information entspricht dem Stand Januar 2002. Aktuelle Information finden Sie bei der entsprechenden Behörde Ihres Landes (z. B. www.regtp.de).

Frequenzen IEEE-Standard 802.11a

Land	Kanal 36 5180 MHz	Kanal 40 5200 MHz	Kanal 44 5220 MHz	Kanal 48 5240 MHz	Kanal 52 5260 MHz	Kanal 56 5280 MHz	Kanal 60 5300 MHz	Kanal 64 5320 MHz
Österreich	x	x	x	x				
Belgien	x	x	x	x	x	x	x	x
Dänemark	x	x	x	x				
Finnland	x	x	x	x	x	x	x	x
Frankreich	x	x	x	x				
Deutschland	x	x	x	x				
Griechenland								
Italien								
Irland	x	x	x	x	x	x	x	x
Luxemburg								
Niederlande	x	x	x	x				
Norwegen	x	x	x	x				
Portugal	x	x	x	x				
Spanien								
Schweden	x	x	x	x				
Schweiz	x	x	x	x				
Groß-Britannien	x	x	x	x	x	x	x	x

Frequenzen IEEE-Standard 802.11b (11 Mbits/s) / 802.11g (54 Mbits/s)

Funknetzwerkkarten und -adapter sind gemäß dem IEEE-Standard 802.11b für den Betrieb im ISM-Frequenzband (Industrial, Scientific, Medical) zwischen 2.4 und 2.4835 GHz vorgesehen. Weil jeder der 13 verwendbaren Funkkanäle durch das DSSS-Verfahren (Direct Sequence Spread Spectrum) eine Breite von 22 MHz beansprucht, stehen maximal drei voneinander unabhängige Kanäle (z. B. 1, 6 und 11) zur Verfügung. In der folgenden Tabellen finden Sie die in Ihrem Land zulässigen Kanäle:

Kanal-Nr. / MHz	Europa, R&TTE	Frankreich, 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 von Odyssey

Die Installationssoftware für den Odyssey Client befindet sich im Verzeichnis `C:\Add on\Software`.

Vor der Installation beachten Sie bitte Folgendes:

- Ihre Netzwerkkarte für das kabellose Netzwerk sowie die zugehörige Treiber-Software sollten bereits installiert sein.
- Unter Windows 2000 und Windows XP müssen Sie Administratorrechte besitzen.

Odyssey Client installieren

Um Odyssey Client zu installieren:

- ▶ Doppelklicken Sie auf die Datei *FSC-OdysseyClient.msi* im Verzeichnis `C:\Add on\Software`.

Der Installations-Wizard wird aufgerufen, um Sie durch den Installationsprozess zu führen.

- ▶ Klicken Sie auf *Next*, um fortzufahren.

Die Lizenzbedingungen werden angezeigt.

- ▶ Klicken Sie die Option *I accept the terms in the license agreement* an, um die Lizenzbedingungen anzuerkennen und klicken Sie auf *Next*, um fortzufahren.
- ▶ Geben Sie Ihre Benutzerdaten ein und klicken Sie auf *Next*, um fortzufahren.
- ▶ Wählen Sie im Fenster *Setup Type* die Option *Complete* aus, um die Installation im Standardverzeichnis durchzuführen. Wählen Sie die Option *Custom* aus, wenn Sie das Installationsverzeichnis selbst bestimmen wollen. Die Option sollte nur von erfahrenen Benutzern verwendet werden. Klicken Sie auf *Next*, um fortzufahren.

Der Installations-Wizard hat nun alle benötigten Informationen, um mit der Installation zu beginnen.

- ▶ Klicken Sie auf *Back*, wenn Sie Ihre Angaben überprüfen oder ändern wollen, und klicken Sie auf *Install*, um die Installation zu starten.

Die Installation wird gestartet. Das kann einige Minuten dauern. Wenn die Installation abgeschlossen ist, wird das Fenster *InstallShield Wizard Completed* angezeigt. Sie können den Odyssey Client direkt aufrufen oder zuerst die Readme-Datei anzeigen lassen.

- ▶ Klicken Sie auf *Finish*, um die Installation abzuschließen.

Auf einem Computer mit mehreren Benutzerkonten steht Odyssey Client nach der Installation allen Benutzern zur Verfügung. Die Einstellungen zur Steuerung des Odyssey Client-Betriebs sind jedoch benutzerspezifisch und müssen für jedes Benutzerkonto einzeln vorgenommen werden.

Configure and Enable Wizard

Wenn Sie Odyssey Client zum ersten Mal installieren, erscheint nach der Installation automatisch der *Configure and Enable Wizard*, um Odyssey Client abschließend zu konfigurieren und zu aktivieren.

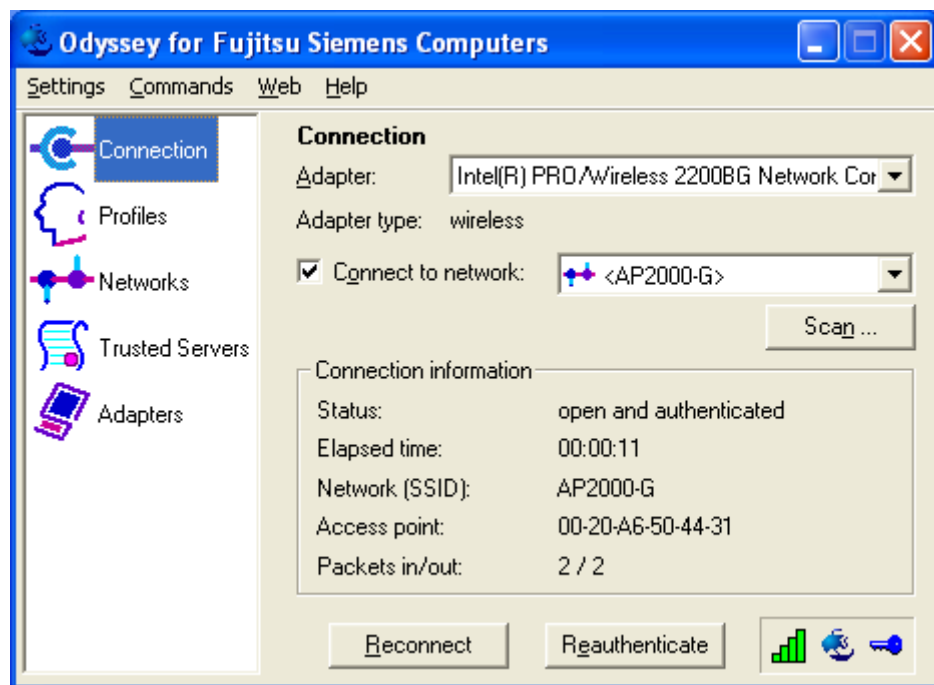
Wenn Sie die Konfigurierung nicht zum aktuellen Zeitpunkt durchführen wollen, können Sie dies später tun. Starten Sie den Odyssey Client Manager unter *Start – Programme – Fujitsu Siemens Computers – Odyssey Client for Fujitsu Siemens Computers – Odyssey Client Manager for Fujitsu Siemens Computers*. Der *Configure and Enable Wizard* startet dann automatisch.

Verwendung von Odyssey Client

Übersicht über den Odyssey Client Manager

Odyssey Client for Fujitsu Siemens Computers heißt die Windows-Oberfläche des Odyssey Client Managers, mit der Sie Ihr Wireless LAN steuern und konfigurieren können. Diese Schnittstelle ist für alle Fujitsu Siemens Computer-Plattformen konsistent, auf denen Sie das Produkt anwenden können.

- ▶ Starten Sie den *Odyssey Client Manager* unter *Start – Alle Programme – Fujitsu Siemens Computers – Odyssey Client for Fujitsu Siemens Computers – Odyssey Client Manager* oder doppelklicken Sie auf das Odyssey Client Manager-Symbol in der Taskleiste.



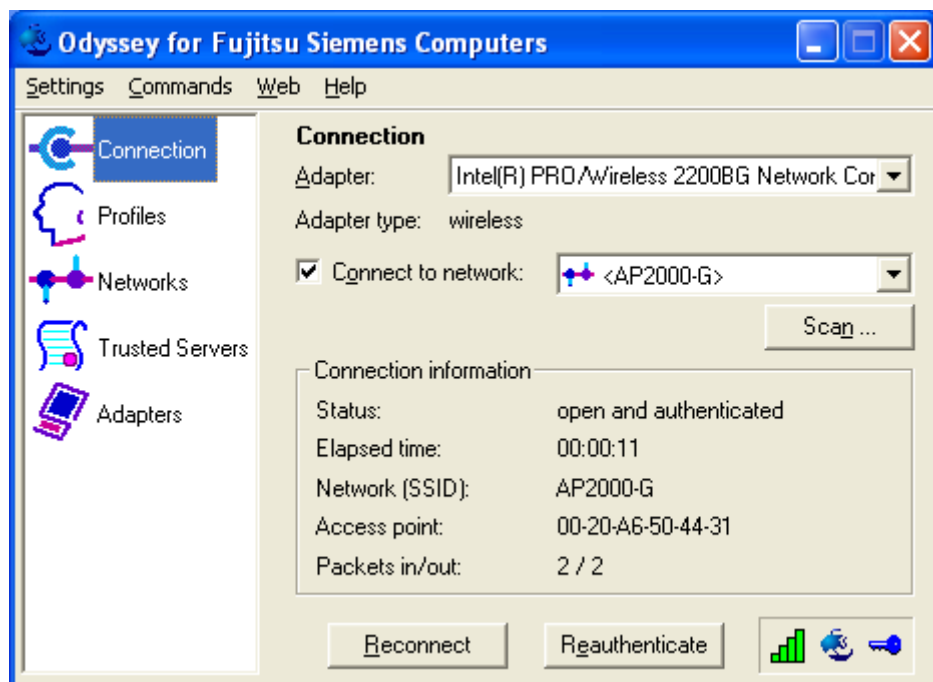
Odyssey Client Manager-Anzeige

Bei den meisten Netzwerkverbindungen besteht Odyssey Client Manager aus einer Anzahl von Fenstern, in denen Sie verschiedene Betriebseinstellungen vornehmen können:

- Im Fenster *Connection* können Sie Ihre Netzwerkverbindung steuern und Ihren derzeitigen Verbindungsstatus sehen.
- Im Fenster *Profiles* geben Sie Informationen ein, die beim Authentifizieren oder beim Anmelden im Netzwerk benötigt werden, z. B. Ihr Passwort oder Zertifikat.
- Im Fenster *Networks* können Sie verschiedene Funknetzwerke konfigurieren und festlegen, wie Sie sie verbinden wollen.
- Im Fenster *Trusted Servers* legen Sie die Zertifizierungs- und Identifizierungsinformationen zu den Servern fest, die Sie authentifizieren können, wenn Sie die Verbindung herstellen, um sicherzustellen, dass Sie sich bei dem gewünschten Netzwerk anmelden.
- Im Fenster *Adapters* können Sie eine oder mehrere Netzwerkkarten für kabellose Netzwerke konfigurieren.

Alle Fensternamen sind auf der linken Seite der Odyssey Client Manager-Anzeige aufgelistet. Klicken Sie den Namen des Fensters an, das Sie anzeigen oder modifizieren möchten.

Netzwerkverbindungen steuern - Fenster "Connection"



Netzwerkkarte auswählen

Falls Sie oder Ihr Administrator mehr als eine Netzwerkkarte für die Anwendung von Odyssey konfiguriert haben, können Sie im Auswahlménü *Adapters* im Fenster *Connection* jeder Netzwerkkarte eine Netzwerkverbindung zuordnen.

Sobald Sie eine Netzwerkkarte ausgewählt haben, wird das Feld *Adapter type* aktualisiert und zeigt den ausgewählten Karten-Typ (kabellos).

Mit einem Netzwerk verbinden

Wenn Sie die Netzwerkverbindung mit Hilfe einer Funknetzwerkkarte herstellen, müssen Sie alle erforderlichen Informationen für die Verbindung in einer Odyssey Client-Netzwerkdefinition festlegen. Dabei müssen Sie auch die Authentifizierungsinformationen angeben, die Sie zuvor in einem Odyssey Client-Profil definiert haben (siehe "Profil hinzufügen oder ändern - Fenster "Profile Properties"" im Abschnitt "Profile definieren - Fenster "Profiles"").

Mit dem Kontrollkästchen *Connect to network* können Sie die Verbindung zum Funknetzwerk herstellen oder beenden. Wenn Sie sich mit einem Funknetzwerk verbinden wollen, stellen Sie sicher, dass dieses Kontrollkästchen markiert ist.

Aus dem Auswahlménü rechts von *Connect to network* können Sie ein Funknetzwerk auswählen, mit dem die Verbindung hergestellt werden soll. In dieser Liste erscheinen alle Netzwerke, die Sie bereits mit Hilfe des Fensters *Networks* konfiguriert haben.

Die Netzwerknamen stehen in eckigen Klammern nach der Netzwerkbeschreibung.

Vor dem Namen steht folgendes Symbol:



für Netzwerke

Für die Verbindung mit einem bereits konfigurierten Netzwerk:

- Wählen Sie aus dem Auswahlménü das Netzwerk aus, zu dem Sie die Verbindung wünschen.
- Markieren Sie das Kontrollkästchen *Connect to network*, falls das nicht bereits geschehen ist.

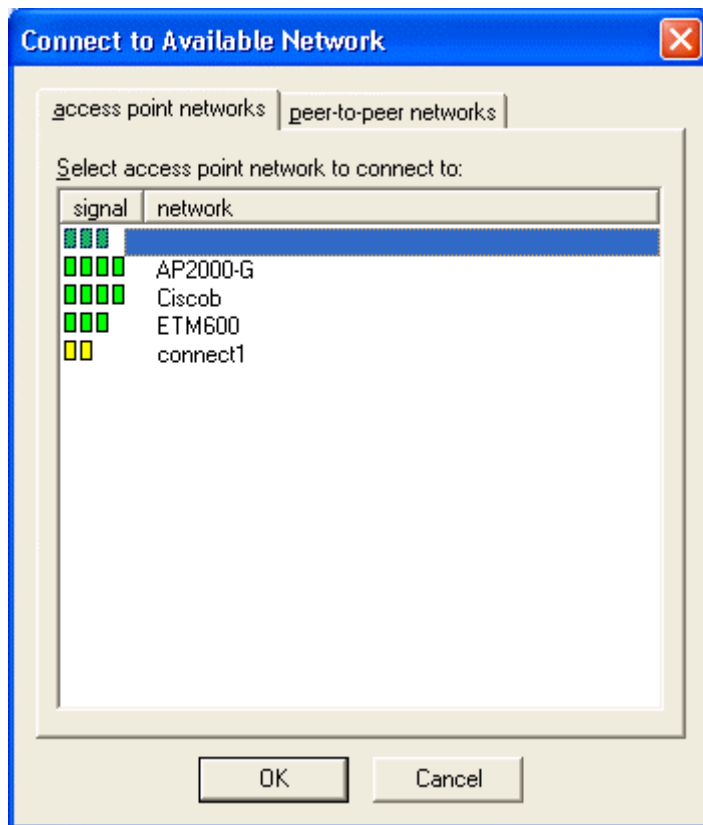
Um die Verbindung zu einem Netzwerk zu beenden, entfernen Sie die Markierung im Kontrollkästchen *Connect to network*.

Nach Funknetzwerken suchen

Falls Sie häufig reisen, können Sie sich auch durch lokal verfügbare Funknetzwerke authentifizieren lassen, die Sie noch nicht konfiguriert haben. Um die Verbindung zu einem noch nicht konfigurierten Funknetzwerk herzustellen, führen Sie folgende Schritte durch:

- Klicken Sie auf *Scan* im Fenster *Connection*.

Odyssey Client überprüft die Funkwellen und zeigt eine Liste aller Funknetzwerke, die derzeit erreichbar sind.



- ▶ Wählen Sie das Netzwerk aus, zu dem Sie die Verbindung herstellen wollen, und klicken Sie auf *OK*.
 - Wenn Sie bereits die Einstellungen für dieses Netzwerk konfiguriert haben, versucht Odyssey Client, die Verbindung mit diesen Einstellungen herzustellen.
 - Wenn Sie die Einstellungen für dieses Netzwerk noch nicht konfiguriert haben, erscheint zuerst das Fenster *Network Properties*. Geben Sie die Einstellungen an und klicken Sie auf *OK*.

Odyssey Client versucht, die Verbindung zum Netzwerk herzustellen.



Es sind nur die Funknetzwerke beim Scannen sichtbar, für die der Administrator SSID (Netzwerkname) sichtbar konfiguriert hat ("send beacons"). Wenn die SSID nicht sichtbar ist, müssen Sie das Netzwerk über das Fenster *Networks* eingeben.

Mit einem Netzwerk wieder verbinden

Wenn die Funkverbindung zu einem Netzwerk nicht einwandfrei funktioniert, können Sie die bestehende Verbindung trennen und eine neue Verbindung aufbauen.

- Klicken Sie auf *Reconnect* im Fenster *Connection*.

Die bestehende Verbindung wird getrennt und eine neue Verbindung mit dem ausgewählten Funknetzwerk wird aufgebaut. Die neue Verbindung kann möglicherweise mit einem anderen AccessPoint (in dem selben Netzwerk) hergestellt werden, abhängig von Faktoren wie der Signalstärke. Falls bei diesem Netzwerk Authentifizierung erforderlich ist, werden Sie erneut authentifiziert, wenn die neue Verbindung beginnt. Falls dynamische Schlüssel für die Verschlüsselung benutzt werden, werden diese aktualisiert.

Im Netzwerk re-authentifizieren

Durch Klicken auf *Reauthenticate* im Fenster *Connection* authentifiziert Odyssey Client Sie erneut über die bestehende Verbindung, die im Fenster angezeigt wird, ohne dass eine neue Verbindung hergestellt wird. Falls dynamische Schlüssel für die Verschlüsselung benutzt werden, werden diese aktualisiert.

Netzwerkverbindung trennen

Um eine Netzwerkverbindung zu trennen, entfernen Sie die Markierung im Kontrollkästchen *Connect to network* für Funkverbindungen.

Verbindungsdaten ansehen

Das Status-Feld im Fenster *Connection* zeigt den aktuellen Status Ihrer Verbindung mit dem Netzwerk über diese Netzwerkkarte an. Eine der folgenden Meldungen erscheint:

Status-Meldung

open and authenticated
open / authenticating
open / requesting authentication

open

peer-to-peer

authenticating

requesting authentication

waiting to authenticate

Definition

Die Verbindung wird authentifiziert, Sie werden verbunden.
Re-Authentifizierung läuft, Sie werden verbunden.
Sie haben Re-Authentifizierung gewünscht, Sie werden verbunden.

Die Verbindung wird nicht authentifiziert, aber Sie werden verbunden.

Der Netzwerktyp ist Peer-to-Peer (Adhoc), Sie werden verbunden.

Sie sind noch nicht verbunden, aber die Authentifizierung läuft.

Sie sind noch nicht verbunden, aber Sie haben die Authentifizierung vom AccessPoint angefordert.

Sie sind noch nicht verbunden, und die letzte Authentifizierung ist missglückt, aber Sie warten einen erneuten Versuch ab.

Status-Meldung

searching for access point

Definition

Sie sind nicht verbunden, und die Kommunikation mit einem AccessPoint im gewünschten Netzwerk ist nicht geglückt. Das kann passieren, wenn Ihre Netzwerkkarte nicht 802.1X unterstützt, oder wenn Ihr AccessPoint nicht im Funkbereich liegt.

searching for peer(s)

Sie sind nicht verbunden, und die Kommunikation mit anderen Computern im Peer-to-Peer-Netzwerk ist nicht hergestellt.

disconnected

Sie sind nicht verbunden; eventuell ist *Connect to network* nicht markiert. Siehe "Mit einem Netzwerk verbinden"

Odyssey is disabled

Sie sind nicht verbunden, und Odyssey Client ist deaktiviert.

Adapter not present

Sie sind nicht verbunden, und die konfigurierte Netzwerkkarte ist derzeit nicht verfügbar. Das kann passieren, wenn Ihre Netzwerkkarte nicht 802.1X unterstützt.

Das Feld *Elapsed time* im Fenster *Connection* zeigt die Zeit an, die seit Beginn der aktuellen Verbindung vergangen ist.

Das Feld *Network (SSID)* zeigt den Namen des Funknetzwerks an, mit dem Sie verbunden sind. Siehe auch "Namen für Funknetzwerke (SSID)".

In dem Feld *Access point* wird die MAC-Adresse des Wireless-AccessPoints dargestellt, mit dem Sie verbunden sind. (Eine MAC-Adresse ist eine eindeutige 48-Bit-Zahl, die der Hersteller als Code in ein Gerät eingegeben hat.)

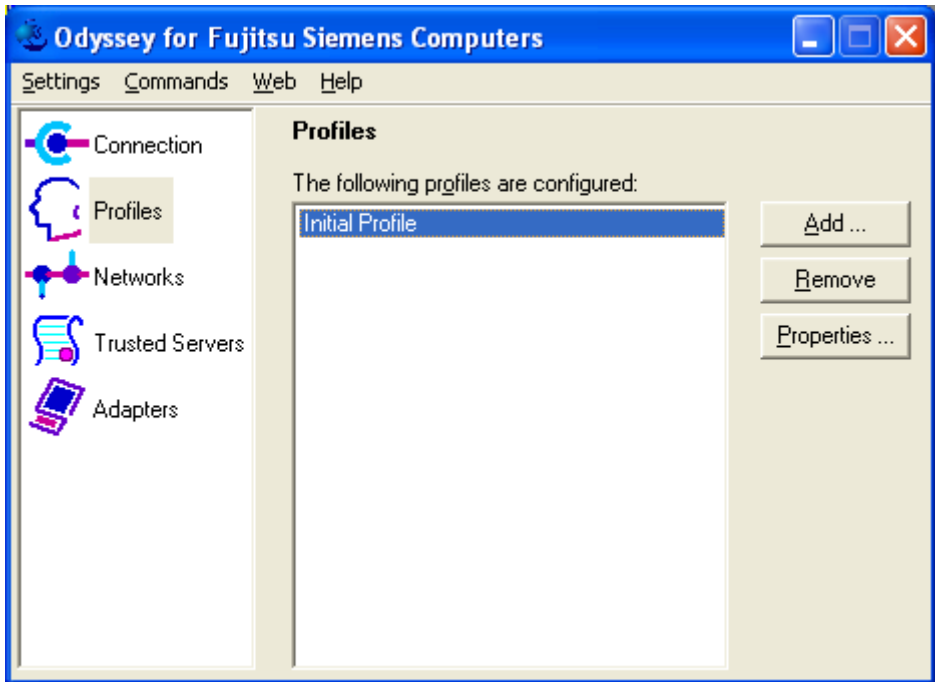
Das Feld *Packets in/out* zeigt die Gesamtanzahl der Netzwerkpakete, die seit Beginn dieser Verbindung empfangen und übertragen wurden.

Profile definieren - Fenster "Profiles"

Ein Odyssey Client-Profil enthält alle Informationen, die notwendig sind, um Sie für das Netzwerk zu authentifizieren. Dazu gehören Angaben wie Ihr Login-Name, Ihr Passwort oder Zertifikat sowie die Protokolle, mittels derer Sie authentifiziert werden können. Ihr Profil ist im Grunde die Identität, die Sie dem Netzwerk gegenüber anzeigen, und das Mittel, mit dem Sie Ihre Identität nachweisen.

Sie können verschiedene Profile für unterschiedliche Netzwerke verwenden. So können Sie beispielsweise verschiedene Login-Namen oder Passwörter bei unterschiedlichen Netzwerken verwenden, oder Sie können ein Passwort in dem einen Netzwerk verwenden und ein Zertifikat in einem andern.

► Klicken Sie im Odyssey Client Manager auf *Profiles*, um das Fenster anzuzeigen.



Im Fenster *Profiles* werden alle Profile aufgelistet, die bisher konfiguriert worden sind. Wenn Sie *Odyssey Client Manager* zum ersten Mal verwenden, finden Sie ein Profil mit der Bezeichnung *Initial Profile* vor, das die allgemeinen Einstellungen enthält. Alternativ dazu kann Ihr Netzwerkadministrator bereits ein oder mehrere Profile für Sie erzeugt haben.

- Um ein Profil hinzuzufügen, klicken Sie auf *Add*. Das Fenster *Profile Properties* erscheint. Geben Sie den Namen für das neue Profil ein, konfigurieren Sie die Einstellungen und klicken Sie auf *OK*.
- Um das Profil zu entfernen, wählen Sie das Profil aus und klicken Sie auf *Remove*.
- Um ein Profil zu verändern, wählen es aus und klicken Sie auf *Properties* bzw. doppelklicken Sie auf das Profil. Das Fenster *Profile Properties* erscheint. Ändern Sie die Einstellungen und klicken Sie auf *OK*.

Profil hinzufügen oder ändern - Fenster "Profile Properties"

Im Fenster *Profile Properties* können Sie ein Profil konfigurieren. Das Fenster wird angezeigt, wenn Sie im Fenster *Profiles* auf *Add* oder *Properties* klicken.

Wenn Sie ein neues Profil hinzufügen, müssen Sie im Feld *Profile Name* einen eindeutigen Namen eingeben. Sie können beispielsweise "Office" für Ihr Profil an Ihrem Arbeitsplatz bzw. "Home" für Ihr Heimnetzwerk verwenden.

Wenn Sie ein Profil definiert und gespeichert haben, haben Sie keine Möglichkeit mehr, den Profilnamen beim Editieren der anderen Profileigenschaften zu verändern. Sie können jedoch das Profil entfernen und ein neues unter anderem Namen erzeugen.

Zusätzlich zum Profilnamen können Sie folgende Parameter in einem Profil konfigurieren (und editieren):

- Login-Name in der Registerkarte *User Info*
- Passwort und/oder Zertifikat in der Registerkarte *Authentication*
- Eine Spezifikation der Authentifizierungsprotokolle, die zur Ihrer Authentifizierung bei dem Netzwerk benutzt werden können, in den Registerkarten *TLS Settings* und *PEAP Setting*

Registerkarte "User Info"

In der Registerkarte *User Info* können Sie den Namen angeben, den Sie zum Anmelden benutzen, sowie Ihr Passwort und/oder Zertifikatsangaben.

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

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

Under the "Login name" section, there is a "Password" section with a checked checkbox "Permit login using password". Below this checkbox are three radio button options: "use Windows password" (selected), "prompt for password", and "use the following password:". Below the "use the following password:" option is an empty text box. There is also an unchecked checkbox labeled "Unmask".

Below the "Password" section is a "Certificate" section with an unchecked checkbox "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 bottom of the dialog box are two buttons: "OK" and "Cancel".

Login-Name

Tragen Sie im Feld *Login name* Ihren Benutzernamen ein. Dieser Name wird dem Netzwerk bei Ihrer Authentifizierung angezeigt. Falls Sie anhand eines Windows Active Directory authentifiziert werden, verwenden Sie die Syntax Domänen\Benutzer-Name (beispielsweise Acme\george). Ansonsten benutzen Sie einen Login-Namen entsprechend der Syntax, die Ihr Administrator für Benutzernamen in der Authentifizierungs-Datenbank festgelegt hat.

Beachten Sie Folgendes:

- Falls Sie bei Ihrer Netzwerkdomäne angemeldet sind (im Gegensatz zur lokalen Anmeldung) gibt Odyssey Client in diesem Feld standardmäßig den Domänen-/Benutzernamen an, wobei der Benutzername Ihr Benutzername ist.
- Wenn Sie lokal bei Ihrem Client angemeldet sind (im Gegensatz zu einer Netzwerkdomäne), gibt Odyssey Client in diesem Feld nur Ihren Benutzernamen ein.
- Es ist möglich, dass Sie den Servernamen nach Ihrem Login-Namen eingeben müssen, damit Ihre Authentifizierung an den richtigen Server geleitet wird.

Beispiel: *acme\george@sales.acme.com*. Ihr Netzwerkadministrator kann Ihnen mitteilen, wie dieses Feld korrekt zu benutzen ist.

Password

Markieren Sie *Permit login using password*, um die Verfahren zur Authentifizierung mit Passwort zu aktivieren. Sie können festlegen, welches Passwort Odyssey Client verwendet:

- Wählen Sie *use Windows password*, wenn Sie zur Authentifizierung beim Netzwerk dasselbe Passwort verwenden wollen wie bei der Windows-Anmeldung.
- Wählen Sie *prompt for password*, wenn Odyssey Client Sie zur Passwort-Eingabe auffordern soll, wenn der Zeitpunkt zur Authentifizierung da ist.
- Wählen Sie *use the following password* und geben Sie ein Passwort in das nachfolgende Feld ein, wenn Odyssey Client Ihr Passwort speichern soll und es jedes Mal für Ihre Authentifizierung mit diesem Profil benutzt.

Falls Sie *prompt for password* gewählt haben, werden Sie allgemein nur beim ersten Mal zur Eingabe aufgefordert, wenn Sie nach dem Start authentifiziert werden. Odyssey Client erinnert sich an dieses Passwort und verwendet es während der ganzen Dauer Ihrer Windows-Sitzung. Das von Ihnen angegebene Passwort gilt nur für ein Profil. Falls Ihre Authentifizierung mit einem anderen Profil erfolgte, werden Sie erneut zur Eingabe aufgefordert.

Sie können bei einigen Gelegenheiten auch aufgefordert werden, Ihr Windows-Passwort einzugeben, wenn Sie die Verbindung zum Netzwerk herstellen:

- Falls Sie versehentlich ein falsches Passwort angegeben haben oder ein anderer Authentifizierungsfehler vorliegt. Diese Funktion wird auch dazu verwendet, ein versehentliches Aussperren wegen wiederholter Verwendung falscher Passwörter zu verhindern.
- Falls Sie Ihr Windows-Passwort periodisch ändern müssen und Sie auf das Netzwerk mittels EAP-TTLS oder PEAP-Authentifizierung vor dem Windows-Login zugreifen.

Zertifikat

Markieren Sie *Permit login using my certificate*, um die Authentifizierungsverfahren zu aktivieren, bei denen Ihr Zertifikat zum Authentifizieren dient.

Zum Auswählen eines persönlichen Zertifikats für die Authentifizierung klicken Sie auf *Browse*. Es erscheint eine Liste Ihrer persönlichen Zertifikate. Wählen Sie ein Zertifikat und klicken Sie auf *OK*.



Das ist eine erweiterte Funktion. Wenden Sie sich bei Auswahl Ihres benötigten Zertifikats gegebenenfalls an Ihren Netzwerkadministrator.

Registerkarte "Authentication"

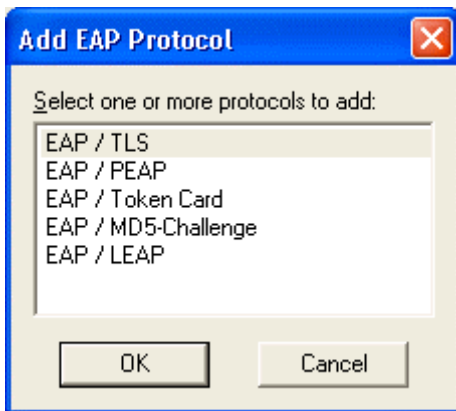
In der Registerkarte *Authentication* können Sie Protokolle spezifizieren, mit denen Sie sich beim Netzwerk authentifizieren.

The screenshot shows a Windows-style dialog box titled "Add Profile" with a blue title bar and a red close button. The "Profile name:" text box contains the word "Office". Below this are four tabs: "User Info", "Authentication" (which is selected), "TLS Settings", and "PEAP Settings". The "Authentication" tab contains the text "Authentication protocols, in order of preference:" above a list box. The list box currently contains the entry "EAP / TTLS". To the right of the list box are four buttons: an up arrow, a down arrow, an "Add ..." button, and a "Remove" button. At the bottom left of the tab area is a checked checkbox labeled "Validate server certificate". At the very bottom of the dialog are "OK" and "Cancel" buttons.

Auswählen von Authentifizierungsprotokollen

Die Liste der Authentifizierungsprotokolle zeigt die Protokolle, die zum Authentifizieren aktiviert sind. Die Liste kann nur ein Authentifizierungsprotokoll oder auch mehrere enthalten. Wenn Sie mehr als ein Authentifizierungsprotokoll haben, können Sie ihnen Prioritäten zuordnen. Die Reihenfolge bestimmt das Protokoll, das der Server benutzt, wenn mehr als ein gemeinsames Protokoll zur Verfügung stehen.

- Um die Reihenfolge der Protokolle zu verändern, wählen Sie ein Protokoll aus und verschieben Sie es mit Hilfe der Pfeiltasten.
- Um ein Protokoll zu entfernen, wählen Sie das Protokoll aus und klicken Sie auf *Remove*.
- Um ein Protokoll hinzuzufügen, klicken Sie auf *Add*. Das Fenster *Add EAP Protocol* erscheint. Wählen Sie ein oder mehrere Protokolle aus, die hinzugefügt werden sollen, und klicken Sie auf *OK*. Sie können mehr als ein Protokoll auswählen, wenn Sie die Taste **Strg** Ihrer Tastatur beim Auswählen mit der Maus gedrückt halten. Beachten Sie, dass alle Protokolle, die Sie bereits ausgewählt haben, in diesem Fenster nicht aufgeführt werden.



Validierung des Server-Zertifikats

Bestimmte Protokolle wie beispielsweise EAP-TTLS, PEAP und EAP-TLS ermöglichen Ihnen das Verifizieren der Identität des Authentifizierungsservers, während der Server Ihre Identität prüft. Dieses Verfahren wird als gegenseitiges Authentifizieren bezeichnet.

Markieren Sie *Validate Server Certificate*, um die Identität des Authentifizierungs-Servers auf der Grundlage seines Zertifikats zu prüfen, wenn EAP-TTLS, PEAP und EAP-TLS verwendet wird. (Dieses Feld ist standardmäßig markiert.) Im Fenster *Trusted Servers* können Sie die Zertifikate der Trusted Authentication Server ansehen. Siehe "Vertrauenswürdige Server spezifizieren - Fenster "Trusted Servers".

In der Regel sollten Sie *Validate server certificate* markieren. Optional können Sie diese wichtige Sicherheitsmaßnahme abstellen, aber nur, wenn beim Server kein Zertifikat erforderlich ist. Das sollten Sie nur auf Anweisung Ihres Netzwerkadministrators tun.

Registerkarte "TTLS Settings"

In der Registerkarte *TTLS Settings* können Sie EAP-TTLS als Authentifizierungsprotokoll einstellen. Diese Einstellungen sind nur relevant, wenn Sie EAP-TTLS als eines Ihrer Authentifizierungsprotokolle in der Registerkarte *Authentication* verwenden.

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, with 'Add...', 'Remove', and arrow buttons to its right. 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 below this text contains 'anonymous'. At the bottom are 'OK' and 'Cancel' buttons.

Add Profile [X]

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 erzeugt einen sicheren, verschlüsselten Tunnel, über den Sie Ihren Berechtigungsnachweis an den Authentifizierungsserver übergeben. Innerhalb EAP-TTLS existiert noch ein anderes inneres Authentifizierungsprotokoll (Inner Authentication Protocol), das Sie konfigurieren müssen.

Auswahl des inneren Authentifizierungsprotokolls

Wählen Sie im Auswahlmenü *Inner Authentication Protocol* das gewünschte innere Authentifizierungsprotokoll aus. Folgende Protokolle stehen zur Verfügung:

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

Das am häufigsten verwendete Protokoll ist MS-CHAP-V2. Das Protokoll ermöglicht die Authentifizierung bei einem Windows Domain Controller sowie anderen, nicht unter Windows laufenden Benutzer-Datenbanken.

CHAP ist das am häufigsten verwendete Protokoll für die Authentifizierung bei nicht unter Windows laufenden Benutzer-Datenbanken.



Sie können CHAP nicht als Verfahren für die innere Authentifizierung bei einer Windows NT-Domäne oder Active Directory verwenden. Verwenden Sie CHAP daher nicht für die Authentifizierung beim Odyssey-Server, da er sich nur bei einer Windows-Domäne oder einem Active Directory authentifiziert.

PAP/Token ist das bei Token-Karten anzuwendende Protokoll. Wenn Sie PAP/Token verwenden, wird der von Ihnen im Passwort-Dialog eingetragene Passwort-Wert niemals im Cache-Speicher abgespeichert, weil jedes Token-basierte Passwort nur für den einmaligen Gebrauch bestimmt ist.

Erkundigen Sie sich bei Ihrem Netzwerkadministrator, welches innere Authentifizierungsprotokoll in Ihrem Netzwerk zum Einsatz kommt.

EAP als inneres Authentifizierungsprotokoll

Wenn Sie EAP als Ihr inneres Authentifizierungsprotokoll verwenden, müssen Sie die Liste der inneren EAP- Protokolle mit einem oder mehreren Protokollen konfigurieren.

- Um ein Protokoll hinzuzufügen, klicken Sie auf *Add*. Das Fenster *Add EAP Protocol* erscheint. Wählen Sie ein oder mehrere Protokolle aus, die hinzugefügt werden sollen, und klicken Sie auf *OK*. Sie können mehr als ein Protokoll auswählen, wenn Sie die Taste **Strg** Ihrer Tastatur beim Auswählen mit der Maus gedrückt halten. Beachten Sie, dass die von Ihnen bereits hinzugefügten Protokolle in diesem Fenster nicht aufgeführt werden.
- Um ein Protokoll zu entfernen, wählen Sie das Protokoll aus und klicken Sie auf *Remove*.
- Um die Reihenfolge zu verändern, wählen Sie ein Protokoll aus und verschieben Sie es mit Hilfe der Pfeiltasten.

Festlegen eines anonymen Namens

EAP-TTLS bietet gegenüber anderen Protokollen eine einmalige Funktion. Weil EAP-TTLS einen verschlüsselten Tunnel für Ihren Berechtigungsnachweis einrichtet, ist es auch möglich, Ihren Login-Namen durch diesen Tunnel zu übermitteln. Damit ist nicht nur Ihr Berechtigungsnachweis vor einem Lauschangriff sicher, sondern auch Ihre Identität.

Somit haben Sie mit EAP-TTLS zwei Identitäten: eine innere und eine äußere. Die innere Identität ist Ihr aktueller Login-Name und wird dem Login-Namensfeld in der Registerkarte *User Info* entnommen. Ihre äußere Identität kann vollständig anonym sein. Stellen Sie Ihre äußere Identität im Feld *Anonymous name* ein.

Ganz allgemein ist *Anonymous name* auf *anonymous* als Standardwert eingestellt. In einigen Fällen müssen Sie zusätzlichen Text eintragen. So kann beispielsweise diese äußere Identität benutzt werden, um Ihre Authentifizierung zum entsprechenden Server zu leiten, und Sie können aufgefordert werden, *anonymous@acme.com* zu verwenden. Ihr Netzwerkadministrator kann Ihnen sagen, wie dieses Feld korrekt konfiguriert wird.

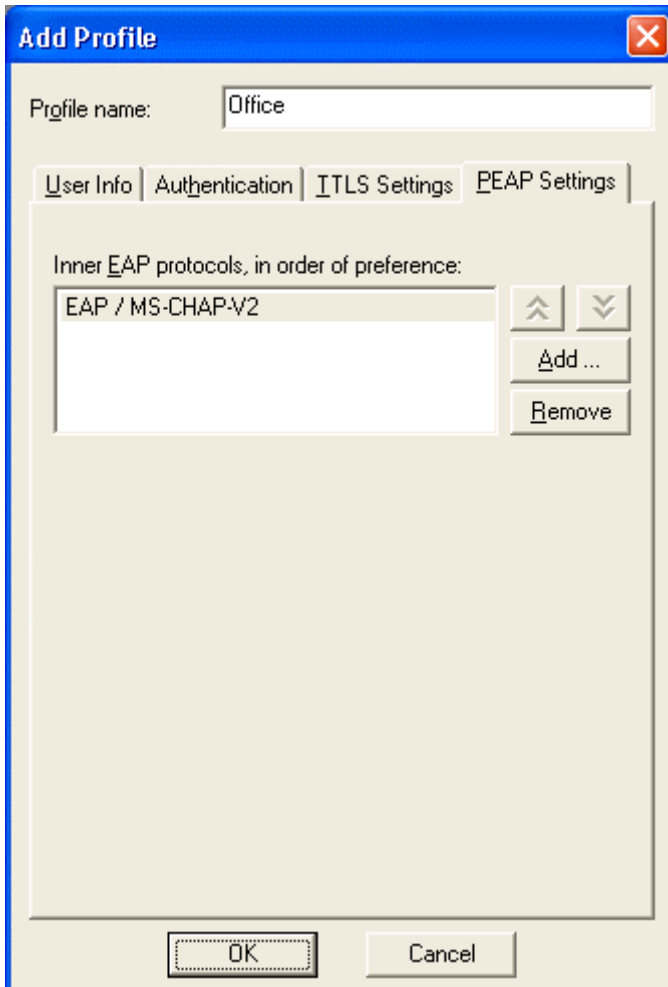


Ihre äußere Identität kann nur anonym sein, wenn EAP-TTLS das einzige Authentifizierungsprotokoll ist, das in der Registerkarte *Authentication Protocols* konfiguriert ist. Falls auch andere Protokolle aktiviert sind, kann Odyssey Client Ihre Identität nicht geheim halten, und das Feld *Anonymous name* ist deaktiviert. Wenn Sie die von EAP-TTLS angebotene Anonymität wünschen, müssen Sie EAP-TTLS als einziges Authentifizierungsprotokoll einrichten.

Registerkarte "PEAP Settings"

Falls Sie EAP/PEAP als Authentifizierungsverfahren auf der Registerkarte *Authentication* bestimmen, können Sie bis zu drei innere EAP-Authentifizierungsverfahren nutzen:

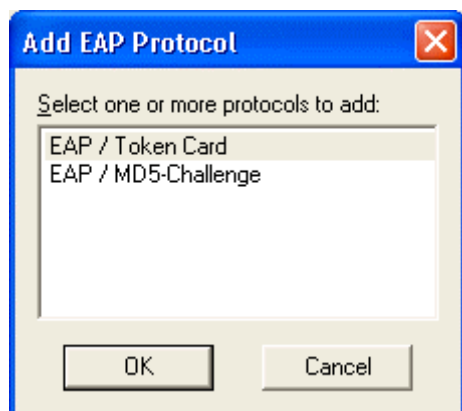
- EAP/MS-CHAP-V2
 - EAP/Token-Karte
 - EAP/MD5-Challenge zum Hinzufügen oder Entfernen von inneren Authentifizierungsverfahren, die bei PEAP benutzt werden:
- Wählen Sie die Registerkarte *PEAP Settings*.



- ▶ Wählen Sie die Protokolle aus, die Sie löschen wollen, und klicken Sie auf *Remove*.
- ▶ Klicken Sie auf *Add*, um ein Protokoll hinzuzufügen.

Das Fenster *Add EAP Protocol* erscheint.

- Wählen Sie ein oder mehrere Protokolle aus, die hinzugefügt werden sollen, und klicken Sie auf *OK*.



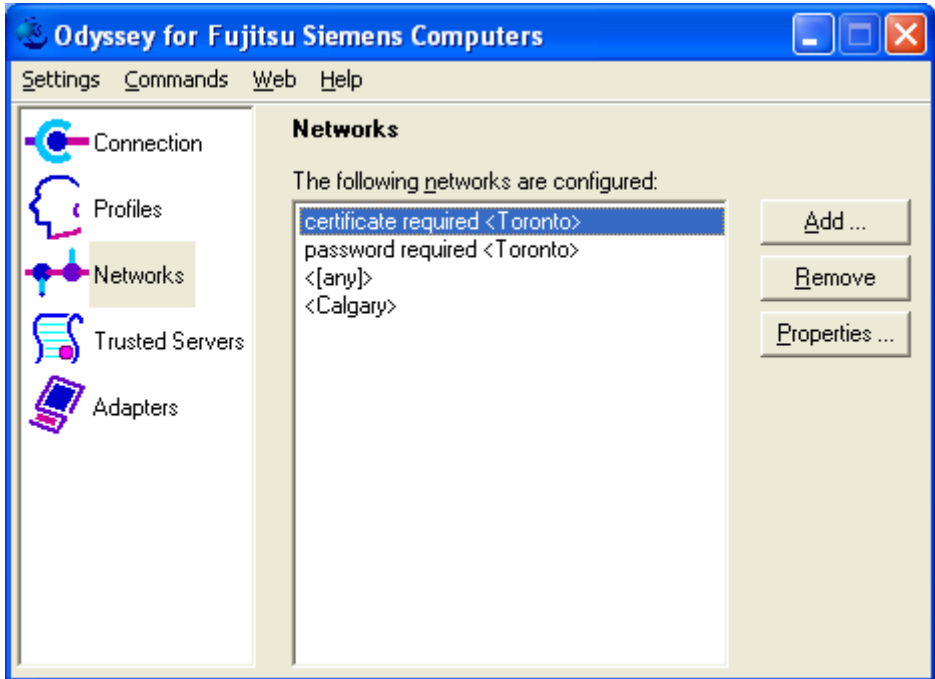
Beachten Sie, dass alle Protokolle, die Sie bereits ausgewählt haben, in diesem Fenster nicht aufgeführt werden.

- Klicken Sie auf *OK*, wenn Sie die Änderung der Profilkonfiguration ganz abgeschlossen haben.

Funknetzwerke konfigurieren - Fenster "Networks"

Im Fenster *Networks* können Sie Einstellungen zur Verbindung mit einer beliebigen Anzahl von Funknetzwerken vornehmen.

- Klicken Sie im Odyssey Client Manager auf *Networks*, um das Fenster anzuzeigen.



Alle konfigurierten Netzwerke werden aufgelistet. Sie können folgende Aufgaben im Fenster *Networks* durchführen:

- Um ein Netzwerk hinzuzufügen, klicken Sie auf *Add*. Das Fenster *Network Properties* erscheint. Konfigurieren Sie die Einstellungen für das neue Netzwerk und klicken Sie auf *OK* (siehe Abschnitt "Netzwerke hinzufügen oder ändern – Fenster "Network Properties"").
- Um ein Netzwerk zu entfernen, wählen Sie das Netzwerk aus und klicken Sie auf *Remove*.
- Um die Einstellungen für ein Netzwerk zu ändern, wählen Sie das Netzwerk aus und klicken Sie auf *Properties* oder doppelklicken Sie auf den Netzwerk-Namen. Das Fenster *Network Properties* erscheint. Ändern Sie die Einstellungen und klicken Sie auf *OK* (siehe Abschnitt "Netzwerke hinzufügen oder ändern – Fenster "Network Properties"").

Netzwerk-Bezeichnungen

Die Netzwerk-Bezeichnungen im Fenster *Networks* sind wie folgt aufgebaut:

- Der Name des Netzwerks steht in eckigen Klammern.
- Die Beschreibung des Netzwerks steht vor dem Namen. Diese Beschreibung wird dem Feld *Description* im Fenster *Network Properties* entnommen. Sie können Ihre eigene Beschreibung zu jedem konfigurierten Netzwerk hinzufügen. Das hilft Ihnen, zwischen den Netzwerken zu unterscheiden.

Das Feld zur Netzwerkbeschreibung ist nützlich in Situationen, in denen Sie zwischen unterschiedlichen "Persönlichkeiten" in ein und demselben Netzwerk umschalten möchten. Sie können beispielsweise unterschiedliche Berechtigungsnachweise zu verschiedenen Zeiten benutzen. Das Beschreibungsfeld ermöglicht auch die Unterscheidung zwischen zwei verschiedenen Netzwerken mit denselben Netzwerknamen.

Die Netzwerknamen sind wahlfreier Text, der vom Administrator gewählt wird. Daher ist es möglich, dass zwei voneinander unabhängige Netzwerke denselben Namen haben. In der Darstellung des Fensters *Networks* gibt es zwei Netzwerke "Toronto". Die konfigurierten Beschreibungen zeigen an, dass der Passwort-Berechtigungsnachweis bei dem einen Netzwerk verwendet wird, und der Zertifikat-Nachweis bei dem anderen.

Netzwerke hinzufügen oder ändern – Fenster "Network Properties"

Im Fenster *Network Properties* können Sie die Einstellungen für das Funknetzwerk konfigurieren. Klicken Sie im Fenster *Networks* auf *Add* oder *Properties*, um die Netzwerkeigenschaften anzuzeigen. Das Fenster *Add Network* bzw. *Network Properties* wird angezeigt.

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

Hier können Sie die folgenden Parameter konfigurieren:

- Netzwerkeigenschaften im Abschnitt *Network*
- Authentifizierungsfelder im Abschnitt *Authentication*
- Vorkonfigurierte Schlüssel (WEP oder WPA) im Abschnitt *Pre-configured keys*

Network

In diesem Abschnitt im Fenster *Network Properties* können Sie die folgenden Aufgaben ausführen:

- Netzwerknamen angeben
- Netzwerk suchen
- Odyssey zum Anschluss an ein verfügbares Netzwerk konfigurieren
- Netzwerkbeschreibung angeben
- Netzwerktyp angeben
- Zuordnungsmodus angeben
- Ein geeignetes Verschlüsselungsverfahren für den Zuordnungsmodus angeben

Netzwerknamen angeben

Stellen Sie *Network name (SSID)* auf den Namen des Funknetzwerks ein. Der Netzwerkname kann bis zu 32 Zeichen lang sein. Zwischen Groß- und Kleinbuchstaben wird unterschieden. Dieser Name muss korrekt eingegeben werden, damit die Verbindung erfolgreich hergestellt werden kann.

Netzwerk suchen

Sie können den Namen des Netzwerks direkt eingeben oder auf *Scan* klicken, um aus einer Liste aller momentan sichtbaren Netzwerke auszuwählen.

Wenn Sie sich in der Nachbarschaft des Netzwerks befinden, das Sie konfigurieren, ist das Benutzen der Schaltfläche *Scan* nicht nur einfacher als das Eintippen, es garantiert auch, dass der Netzwerkname korrekt angegeben ist.

Beachten Sie, dass nur AccessPoints, die Richtstrahlen senden, für Sie sichtbar sind, wenn Sie die Schaltfläche *Scan* benutzen.

Odyssey für die Verbindung mit einem beliebigen Netzwerk konfigurieren

Odyssey Client Manager bietet ein spezielles Netzwerk unter der Bezeichnung *[any]*. Das Netzwerk *[any]* stellt die Verbindung zu einem beliebigen Netzwerk her, unabhängig von seinem Namen. Das Netzwerk *[any]* ist nützlich für Sie in Konferenzen, Hotels oder an anderen Orten, bei denen Netzwerkzugang besteht. Wenn Sie das Netzwerk *[any]* im Fenster *Connection* wählen, können Sie sich mit solchen Netzwerken verbinden, ohne sie individuell konfigurieren zu müssen.

Um ein Netzwerk *[any]* zu konfigurieren, markieren Sie *Connect to any available network* und klicken Sie auf *OK*.

Obleich Sie WEP-Schlüssel und -Profile mit *[any]* benutzen können, besteht die üblichere Praxis darin, *[any]* ohne die 802.11- oder 802.1X-Authentifizierung zu benutzen.

Netzwerkbeschreibung angeben

Netzwerkbeschreibungen sind nützlich, um zwischen Netzwerken mit gleichen oder ähnlichen Namen zu unterscheiden. Die Netzwerkbeschreibung können Sie im Feld *Description* eingeben.

Netzwerktyp angeben

Falls Sie die Schaltfläche *Scan* nicht zur Auswahl Ihres Netzwerks verwendet haben, müssen Sie den Netzwerktyp spezifizieren, indem Sie eine der Optionen aus dem Auswahlménú auswählen.

- Wählen Sie *Access point (infrastructure mode)*, wenn dieses Netzwerk AccessPoints verwendet, um die Verbindungsmöglichkeit für das Unternehmensnetzwerk oder das Internet zu sichern. Das ist die üblichste Einstellung.
- Wählen Sie *Peer-to-peer (ad-hoc mode)*, um ein Privatnetzwerk mit einem oder mehreren Computern einzurichten.

Zuordnungsmodus angeben

Vor dem Authentifizieren müssen Sie Ihren Client einem AccessPoint zuordnen. Der von Ihnen geforderte Zuordnungsmodus ist abhängig von Ihrer AccessPoint-Hardware und davon, wie sie konfiguriert ist. Ihr Netzwerkadministrator kann Ihnen beim Konfigurieren des Zuordnungsmodus behilflich sein, der für Ihr Netzwerk erforderlich ist.

Weitere Informationen zu den Wahlmöglichkeiten dieser Verschlüsselung und den Zuordnungsmodus finden Sie unter "Wired-Equivalent Privacy (WEP) mit vorkonfigurierten Schlüsseln" und "Wi-Fi Protected Access (WPA) und TKIP-Verschlüsselung".

Sie können unter drei Zuordnungsmodi auswählen:

- *Open* für die Verbindung mit einem Netzwerk durch einen AccessPoint oder Switch mit 802.1X-Authentifizierung. Wählen Sie diesen Modus, wenn Sie keinen Shared-Modus oder WPA wählen müssen.
- *Shared* für die Verbindung mit einem Netzwerk über einen AccessPoint, der WEP-Schlüssel zum Authentifizieren und zur Datenverschlüsselung erfordert.
- *WPA* für die Verbindung mit einem Netzwerk über einen AccessPoint mit WPA (Wi-Fi Protected Access).

Ein geeignetes Verschlüsselungsverfahren für Ihren Zuordnungsmodus angeben

Die Auswahl des Verschlüsselungsverfahrens hängt auch von den Bedingungen des AccessPoints ab. Ihre Wahlmöglichkeiten unterscheiden sich entsprechend dem gewählten Zuordnungsmodus. Weitere Informationen finden Sie unter "Wired-Equivalent Privacy (WEP) mit vorkonfigurierten Schlüsseln und "Wi-Fi Protected Access (WPA) und TKIP-Verschlüsselung".

Sie haben folgende Optionen:

- *none* bei Verwendung der 802.1X-Authentifizierung ohne WEP- Schlüssel. Diese Option ist nur verfügbar, wenn Sie den Zuordnungsmodus *open* gewählt haben.
- *WEP* bei Verwendung des WEP-Schlüssels zur Datenverschlüsselung. Diese Option steht bei allen Zuordnungsmodi zur Verfügung und ist erforderlich im Shared-Modus. Wenn Sie diese Option auswählen, müssen Sie den WEP-Schlüssel im Abschnitt *Pre-configured keys* des Fensters *Network Properties* eingeben. Sie müssen diese Option wählen, wenn die AccessPoints in Ihrem Netzwerk WEP-Schlüssel für die Authentifizierung erfordern (Shared-Modus).
- *TKIP* bei Verwendung des Protokolls für temporäre Schlüsselintegrität. Wählen Sie diese Option, wenn die AccessPoints in Ihrem Netzwerk WPA-Authentifizierung erfordern und für TKIP-Datenverschlüsselung verschlüsselt sind.
- *AES* bei Verwendung des erweiterten Standard-Verschlüsselungsprotokolls. Wählen Sie diese Option, wenn die AccessPoints in Ihrem Netzwerk WPA-Authentifizierung erfordern und für die AES-Datenverschlüsselung konfiguriert sind.

Authentifizierungs-Felder

Im Abschnitt *Authentication* können Sie die Netzwerk-Authentifizierung mit folgenden Merkmalen konfigurieren:

- Authentifizierung mit Profil
- Automatische Schlüsselerzeugung

Authentifizierung mit Profil

Falls es bei dem von Ihnen konfigurierten Funknetzwerk notwendig ist, dass Sie sich mit Ihrem persönlichen Berechtigungsnachweis authentifizieren, markieren Sie *Authenticate using profile* und wählen Sie das entsprechende Profil aus dem Auswahlménü. **Sie müssen bereits ein Profil konfiguriert haben, das sich zum Authentifizieren bei diesem Netzwerk eignet.**

Wenn Sie *Authenticate using profile* markieren, führt Odyssey Client eine 802.1X-Authentifizierung mit Ihrem Passwort, Zertifikat oder anderen Mitteln durch, so wie es im ausgewählten Profil konfiguriert ist.

Automatische Schlüsselerzeugung

Markieren Sie *Keys will be generated automatically for data privacy*, wenn das im Profil angegebene Authentifizierungsverfahren zur Erzeugung von dynamischen WEP-Schlüsseln für die Verwendung zwischen Ihrem Computer und dem AccessPoint ausgelegt ist. Bestimmte Authentifizierungsverfahren wie EAP-TTLS, PEAP und EAP-TLS erzeugen Schlüssel. Andere Authentifizierungsverfahren erzeugen keine Schlüssel. Falls Sie EAP-TTLS, PEAP oder EAP-TLS zum Authentifizieren verwenden, markieren Sie dieses Feld. Sie können jedes dieser Authentifizierungsverfahren verwenden für AccessPoints mit 802.1x-Authentifizierung. Diese Option bietet mehr Sicherheit als die Verwendung statischer (vorkonfigurierter) Schlüssel. Lassen Sie diese Option unmarkiert, wenn Sie aufgefordert werden, vorkonfigurierte WEP-Schlüssel, oder im Fall der WPA-Authentifizierung, einen Pre-shared-Schlüssel zu verwenden.

Vorkonfigurierte Schlüssel (WEP oder WPA)

Das Funknetzwerk kann es erfordern, dass Sie WEP-Schlüssel vorkonfigurieren oder dass Sie im Fall der WPA-Authentifizierung eine Passphrase zuvor gemeinsam benutzen (Pre-share). Schlüssel können Sie im unteren Teil von *Network Properties* eingeben.

Pre-shared-Schlüssel (WPA)

Wenn Sie den WPA-Modus gewählt haben und den Schlüssel nicht automatisch erzeugen, wenn Sie ein Authentifizierungsprofil zur Netzwerkverbindung zuordnen, müssen Sie eine Pre-shared-ASCII-Passphrase im Feld *Passphrase* eingeben. Diese Passphrase wird als Basis beim Erzeugen des erforderlichen Schlüssels verwendet.

Vorkonfigurierte Schlüssel (WEP)

Wenn Sie den Shared-Modus gewählt haben, müssen Sie mindestens einen WEP-Schlüssel konfigurieren. Sie müssen auch mindestens einen WEP-Schlüssel konfigurieren, wenn Sie WEP-Verschlüsselung für den offenen Modus auswählen, und die Schlüssel nicht automatisch erzeugt werden, wenn Sie ein Authentifizierungsprofil zur Netzwerkverbindung zuordnen. WEP-Schlüssel dienen folgenden Zwecken:

- Zuordnen zu einem AccessPoint, ehe eine Verbindung hergestellt werden kann (Shared-Modus).
- Verschlüsselung von Daten zwischen Ihrem Computer und dem AccessPoint (oder anderen Computern in einem Peer-to-Peer-Netzwerk) (siehe "Wired-Equivalent Privacy (WEP) mit vorkonfigurierten Schlüsseln").

Falls das Funknetzwerk 802.1X-Authentifizierung verwendet und dynamische WEP-Schlüssel erzeugt werden (d. h. Sie haben *Authenticate using profile* und *Keys will be generated automatically for data privacy* markiert), dann brauchen Sie keine vorkonfigurierten WEP-Schlüssel zum Datenschutz einzugeben. Es ist jedoch notwendig, wenn auch nicht typisch, vorkonfigurierte WEP-Schlüssel zum Authentifizieren zusätzlich zu 802.1X zu verwenden. EAP-MD5 erzeugt beispielsweise keine WEP-Schlüssel zur Datenverschlüsselung, sodass Sie einen Schlüssel bereitstellen müssen, wenn Ihr Profil zur Authentifizierung mit dieser Methode eingestellt ist.

Falls Sie eine dieser Anwendungen von vorkonfigurierten WEP-Schlüsseln implementieren, müssen Sie die entsprechenden Felder markieren und einen oder mehrere WEP-Schlüssel entsprechend einstellen:

- Markieren Sie *authenticate to access points (shared mode)*, falls vorkonfigurierte WEP-Schlüssel zum Authentifizieren bei einem AccessPoint vor der Verbindung mit dem Funknetzwerk erforderlich sind.
- Markieren Sie *Keys will be generated automatically for data privacy*, um vorkonfigurierte WEP-Schlüssel zur Verschlüsselung von Daten über das Funknetzwerk zu verwenden. Tragen Sie den WEP-Schlüssel in den Feldern *Key 0* bis *Key 3* ein. Die hier eingetragenen Werte müssen denen der AccessPoints oder Peer-Computer entsprechen, zu denen Sie die Verbindung herstellen. Allgemein wird *Key 0* verwendet, obgleich Ihr Netzwerk auch andere Schlüssel erfordern kann. Sie können Schlüssel entweder als gewöhnliche Textzeichen (ASCII) oder hexadezimale Zeichen eingeben.

WEP-Schlüssel sind 40 oder 104 Bit lang. Das entspricht entweder 5 oder 13 Zeichen, wenn Sie sie als ASCII-Zeichen eingeben bzw. 10 oder 26 Zeichen, wenn Sie sie als hexadezimale Zeichen eingeben.

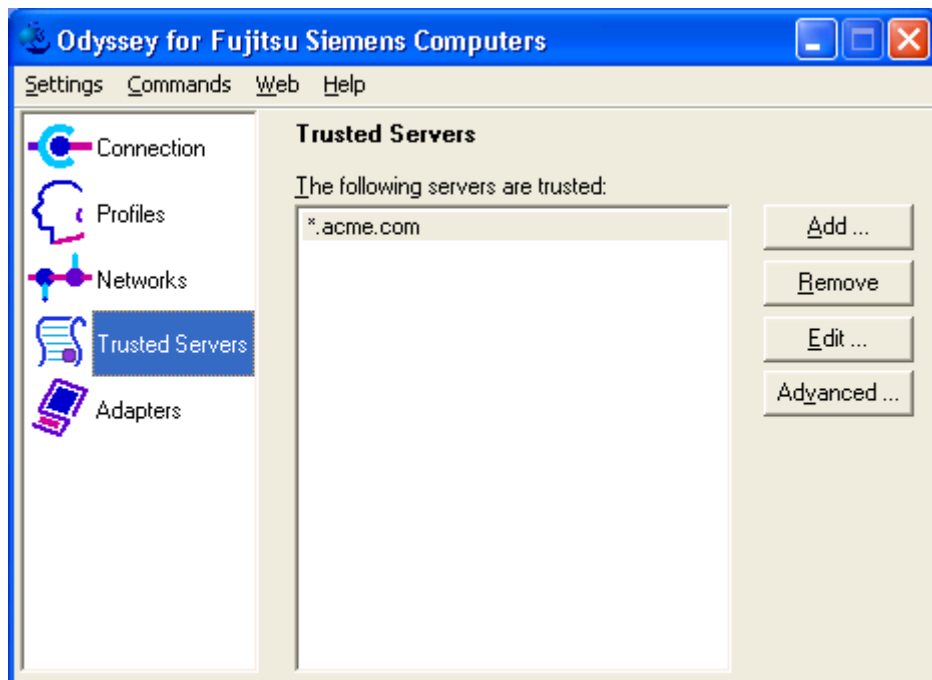
Eingabe eines vorkonfigurierten WEP-Schlüssels:

- ▶ In der Auswahlliste *Format for entering keys* wählen Sie entweder ASCII-Zeichen oder hexadezimale Zeichen, je nachdem wie Sie die Schlüssel eingeben wollen.
- ▶ Geben Sie in den Textfeldern *Key 0* bis *Key 3* jeden Schlüssel an, den Sie vorkonfigurieren wollen.

Vertrauenswürdige Server spezifizieren - Fenster "Trusted Servers"

Im Fenster *Trusted Servers* können Sie konfigurieren, welchen Authentifizierungs-Servern Sie für Ihre Netzwerkanmeldung als Trusted Server (Vertrauenswürdiger Server) vertrauen.

- Klicken Sie im Odyssey Client Manager auf *Trusted Servers*, um das Fenster anzuzeigen.



Wenn Sie einen Trusted Server konfigurieren, müssen Sie nicht nur den Namen des Servers angeben, sondern auch die Zertifikatkette, zu der er gehört. Odyssey Client ist sehr flexibel und bietet ein einfaches und ein höher entwickeltes Verfahren zum Konfigurieren von Trusted Servern.

Weitere Informationen finden Sie unter "Extensible Authentication Protocol (EAP)"

Einfaches Verfahren zum Konfigurieren von Trusted Servern

In den meisten Fällen können Sie ein einfaches Verfahren zum Konfigurieren von Trusted Servern verwenden. Bei diesem Verfahren müssen Sie zwei Elemente bestimmen:

- Name der Server-Domäne oder das Ende des Domänen-Namens (beispielsweise *acme.com*)
- Das Zertifikat einer Certificate Authority in der Kette. Das könnte das Zertifikat einer Root- oder Intermediate Certificate Authority sein.

Domännennamen

Jeder Server verfügt über einen Domännennamen, der ihn eindeutig identifiziert, und dieser Domänenname ist gewöhnlich im Feld "Subject CN" des Server-Zertifikats enthalten.

Der Domänenname eines Servers endet mit dem Namen einer größeren administrativen Domäne, zu welcher der Server gehört. So kann beispielsweise das Acme-Unternehmen einen Domännennamen wie *acme.com* haben. Die Gesellschaft könnte auch verschiedene Authentifizierungsserver mit den Namen *auth1.acme.com*, *auth2.acme.com* und *auth3.acme.com* haben.

Wie aus diesem Beispiel ersichtlich ist, können Sie durch die Angabe der verbindlichen Endung des Domännennamens des Servers das Vertrauen in alle Server in einem Unternehmen mit einem einzelnen Eintrag festlegen.

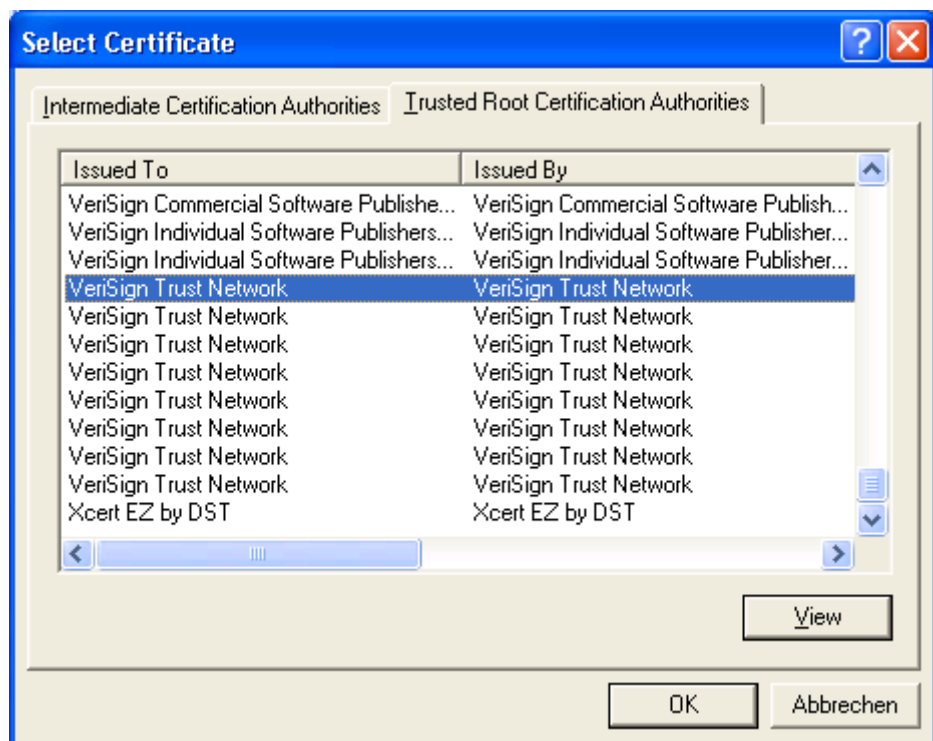
Hinzufügen eines Trusted Server-Eintrags

Um der Liste der Trusted Server einen Eintrag hinzuzufügen, führen Sie die folgenden Schritte aus:

- Klicken Sie auf *Add*. Das Fenster *Add Trusted Servers Entry* erscheint.

- In dem Feld *Server domain name must end with* tragen Sie den Namen (oder die End-Elemente des Namens) der Domäne ein, zu welcher der Trusted Server gehören soll. Dieses Feld darf nicht frei bleiben.

- Stellen Sie das Feld *Server certificate must be issued by* auf das Zertifikat der Certificate Authority ein, die direkt oder indirekt das Server-Zertifikat erteilt hat. Zum Zuordnen eines Zertifikats führen Sie folgende Schritte aus:
 - Klicken Sie auf *Browse*, um eine Liste der Zertifikate zu erhalten.
 - Wählen Sie ein Zertifikat aus der Liste und klicken Sie auf *OK*.



Sie können als Zertifikat eine Root- oder Intermediate Certificate Authority wählen. Es braucht nicht das Zertifikat zu sein, das direkt als Server-Zertifikat erteilt wurde. Es kann jegliches Zertifikat in der Kette sein.

Löschen eines Trusted Server-Eintrags

Um einen Eintrag aus der Liste der Trusted Server zu löschen, wählen Sie den Eintrag aus und klicken Sie auf *Remove*.

Editieren eines Trusted Server-Eintrags

Um einen Eintrag aus der Liste der Trusted Server zu bearbeiten, wählen Sie den Eintrag aus und klicken Sie auf *Edit*. Das Fenster *Edit Trusted Servers Entry* erscheint und ermöglicht Ihnen, die Server-Domäne und das Zertifikat der erteilenden Stelle zu editieren.

Erweitertes Verfahren zum Konfigurieren von Trusted Servern

Falls Sie mehr Vertrauenskontrolle benötigen, können Sie das erweiterte Verfahren benutzen.



Falls Sie keine praktischen Erfahrungen mit Zertifikaten und Zertifikatketten haben, sollten Sie keine Konfiguration mit dem erweiterten Verfahren versuchen. Erkundigen Sie sich bei Ihrem Netzwerkadministrator über das Konfigurieren von Trusted Servern.

Bei diesem Verfahren wird der gesamte Trust-Baum dargestellt. Der Trust-Baum zeigt alle konfigurierten Trusted Server.

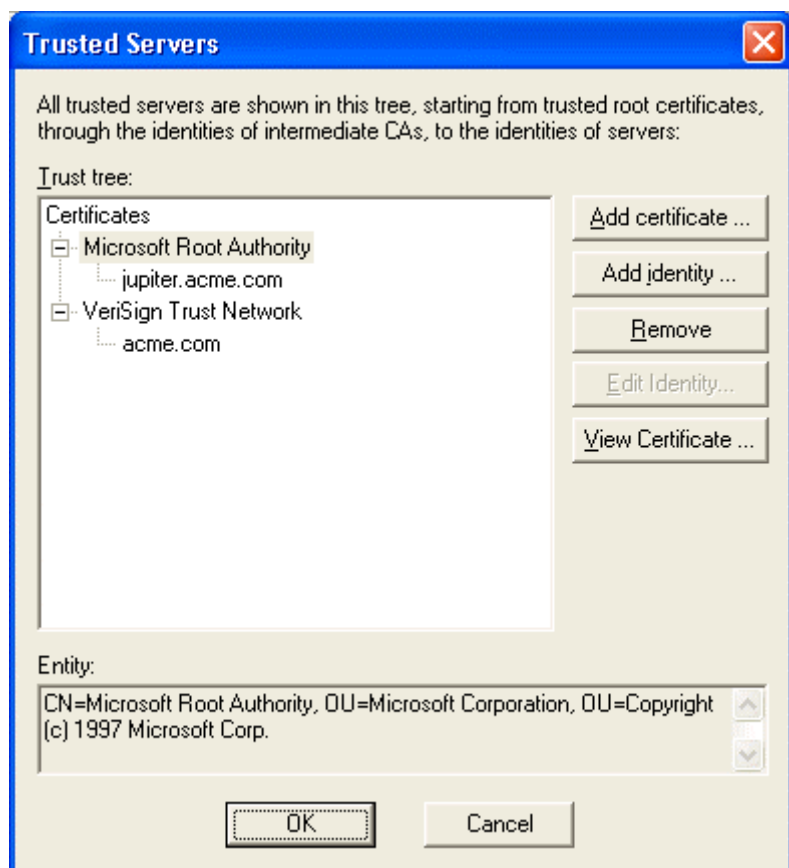
Jeder Pfad durch den Trust-Baum bestimmt eine Regelmenge zur Abstimmung einer Zertifikatkette. Odyssey Client vertraut einem Authentifizierungs-Server nur dann, wenn seine Zertifikat-Kette mindestens in einem Pfad durch Trust-Baum übereinstimmt.

Ein Pfad durch den Trust-Baum besteht aus zwei oder mehreren Knoten:

- Jeder Knoten auf oberster Ebene ist das Zertifikat einer Root oder Intermediate Certificate Authority.
- Jeder Zwischenknoten (sofern vorhanden) ist der Name einer Intermediate Certificate Authority in der Kette.
- Jeder Endknoten ist der Name eines Servers, dem Sie die Authentifizierung anvertrauen. Die Namen der Certificate Authorities und Server können als Subjektnamen oder Domännennamen angegeben werden. Zusätzlich können Sie festlegen, dass der Name in einem Zertifikat dem konfigurierten Namen genau entsprechen muss oder dass er mit dem konfigurierten Namen enden muss.

Anzeige des Trust-Baums

Um den Trust-Baum anzuzeigen, klicken Sie auf *Advanced*. Das Fenster *Trusted Servers* erscheint, in dem Sie die Trust-Regeln anzeigen und ändern können.

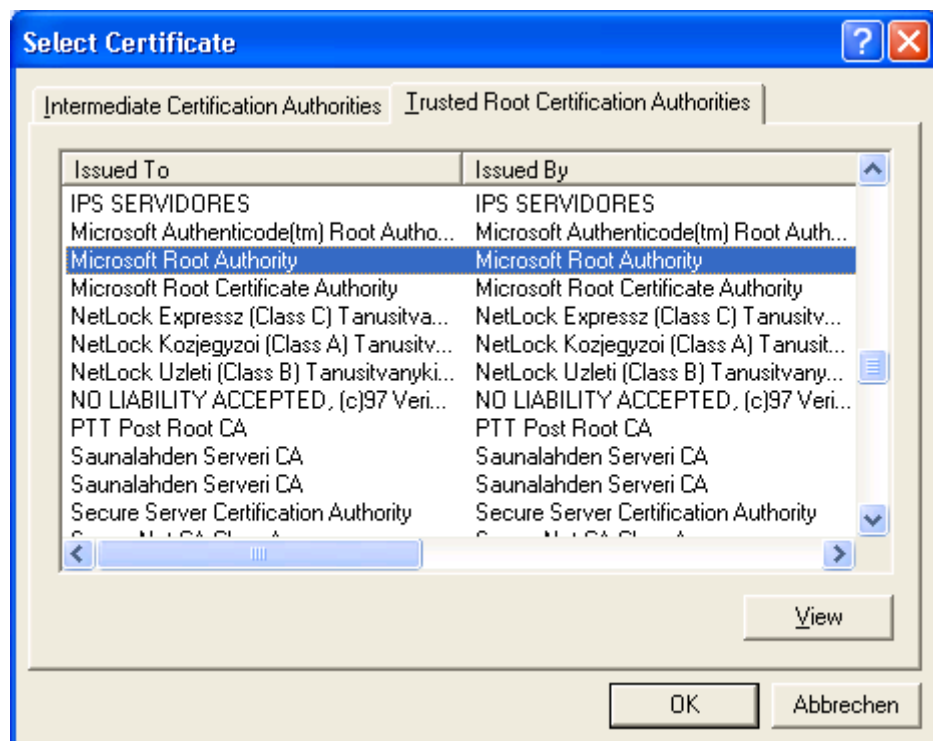


Hinzufügen von Zertifikat-Knoten

Um ein neues Zertifikat am Anfang des Trust-Baums hinzuzufügen:

- ▶ Klicken Sie auf *Add certificate*. Das Fenster *Select Certificate* erscheint.
- ▶ Wählen Sie ein Zertifikat und klicken Sie auf *OK*. Sie können entweder aus der Liste der Intermediate oder der Trusted Root-Zertifikate auswählen.

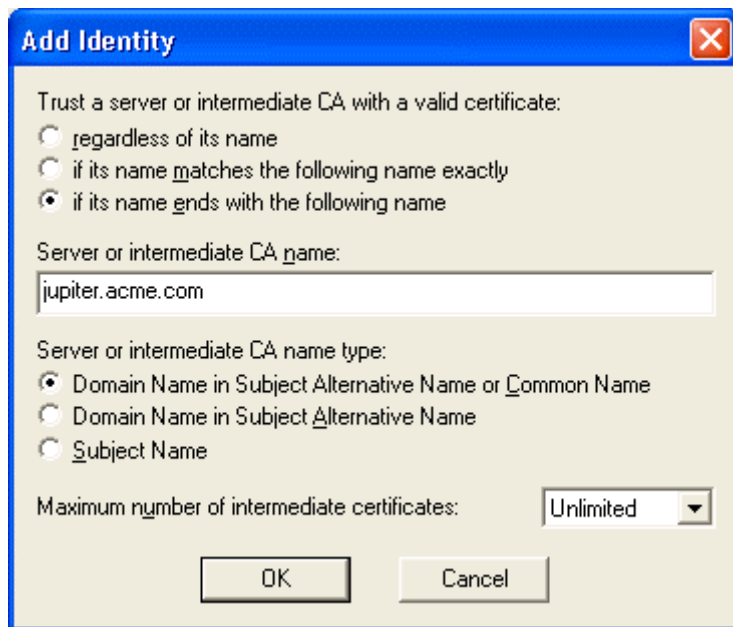
Um ausführliche Angaben über ein Zertifikat vor dem Hinzufügen zu bekommen, wählen Sie das Zertifikat aus und klicken Sie auf *View*.



Hinzufügen von Authentifizierungs-Servern oder Intermediate CA-Knoten

Alle Knoten unterhalb der oberen Ebene bezeichnen entweder Authentifizierungs-Server oder Intermediate Certificate Authorities. Bei einem Endknoten wird davon ausgegangen, dass er einen Authentifizierungs-Server bezeichnet. Anderenfalls wird davon ausgegangen, dass er eine Intermediate Certificate Authority bezeichnet. Zum Hinzufügen eines Authentifizierungs-Servers oder einer Intermediate Certificate Authority zum Baum:

- ▶ Wählen Sie den Knoten bei dem Baum aus, unter dem Sie das neue Element hinzufügen wollen.
- ▶ Klicken Sie auf *Add Identity*. Das Fenster *Add Identity* erscheint.
- ▶ Geben Sie die Informationen ein, welche die Regeln bestimmen, die Odyssey Client zum Anpassen eines Zertifikats in der Server-Zertifikat-Kette an diesen Knoten verwendet.
- ▶ Klicken Sie auf *OK*.



Mit Hilfe des Fensters *Add Identity* können Sie die Anpassungsregeln für einen einzelnen Knoten des Trust-Baums einstellen.

Zur Bestimmung eines Trusted Servers oder Intermediate CA mit gültigem Zertifikat wählen Sie:

- *regardless of its name*, um ein Zertifikat, unabhängig von seinem Namen anzupassen, vorausgesetzt, es trägt das Signum der Certificate Authority in dem Knoten oberhalb.
- *if its name matches the following name exactly* um festzulegen, dass der Name in dem Zertifikat genau dem von Ihnen angegebenen Namen entspricht.
- *if its name ends with the following name* um festzulegen, dass der Name im Zertifikat dem von Ihnen angegebenen Namen untergeordnet ist. Ein Zertifikat beispielsweise mit dem Namen "sales.acme.com" würde einem Eintrag "acme.com" entsprechen.

Für *Name of Server or intermediate CA* geben Sie den Namen (oder die End-Elemente eines Namens ein) mit dem Sie die Übereinstimmung wünschen. (Dieses Feld wird nicht benötigt, wenn Sie die Auswahl unabhängig vom Namen treffen.). Die Form des Namens hängt ab von Ihrer Wahl des Namentyps.

Für *Name type* müssen Sie angeben, wie der Name interpretiert wird und wo der Name im Zertifikat zu finden ist. Wählen Sie eine der folgenden Optionen aus:

- *Domain name in Subject Alternative Name or Common Name*, wenn der Domänenname (z. B. *acme.com*) im Feld *Subject Alternative Name* im Zertifikat zu finden ist, oder falls das nicht vorhanden ist, der *Common Name* in dem Feld *Subject* des Zertifikats (das ist die üblichste Wahl).
- *Domain name in Subject Alternative Name*, wenn der Domänenname sich im Feld *Subject Alternative Name* im Zertifikat befindet. Das ist der vorhergehenden Auswahl m.E. ähnlich.

- *Subject Name*, wenn der Name ein X.500-Name ist und sich im Feld *Subject* des Zertifikats befindet. Wenn Sie einen Subject-Namen vollständig oder teilweise eingeben, müssen Sie dies in der X.500-Form tun. Er entspricht jedem gleich- oder untergeordneten Certificate Subject-Namen.

- Wenn Sie beispielsweise folgendes eingeben:

`OU=acme.com, C=US`

entspricht der Name einem der folgenden Subject-Namen:

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



Wenn Sie Text eingeben, der Kommata enthält, so muss jedes Komma in einfache Anführungszeichen eingeschlossen sein.

Als Höchstanzahl der Intermediate Certificates legen Sie die maximale Anzahl der Zertifikate fest, die in der Kette zwischen diesem Knoten und dem direkt darüberliegenden Knoten auftreten können. Sie können eine Zahl zwischen 0 und 5 auswählen bzw. *unlimited* (unbegrenzt):

- Wenn Sie 0 wählen, muss das Zertifikat, das diesem Knoten entspricht, signiert sein, wobei das Zertifikat verwendet wird, das dem Knoten über diesem Knoten entspricht.
- Wenn Sie 1 auswählen, kann das Zertifikat, das diesem Knoten entspricht, von dem Zertifikat signiert sein, das dem Knoten darüber entspricht, oder von einem Zertifikat, das wiederum von dem Zertifikat signiert ist, das dem Knoten darüber entspricht.
- Wenn Sie *unlimited* wählen, kann jede Anzahl von Zertifikaten in der Kette zwischen dem Zertifikat erscheinen, das diesem Knoten entspricht und einem, das dem Knoten darüber entspricht.

Entfernen von Knoten

Um einen Knoten zu entfernen, wählen Sie im Baum den Knoten aus, den Sie entfernen wollen und klicken Sie auf *Remove*. Der gewählte Knoten und jeder Knoten darunter wird aus dem Baum entfernt.

Folgende Knoten können entfernt werden:

- Top-Level Certificate-Knoten
- Intermediate CA-Knoten
- Server-Knoten

Anzeigen von Zertifikatinformationen

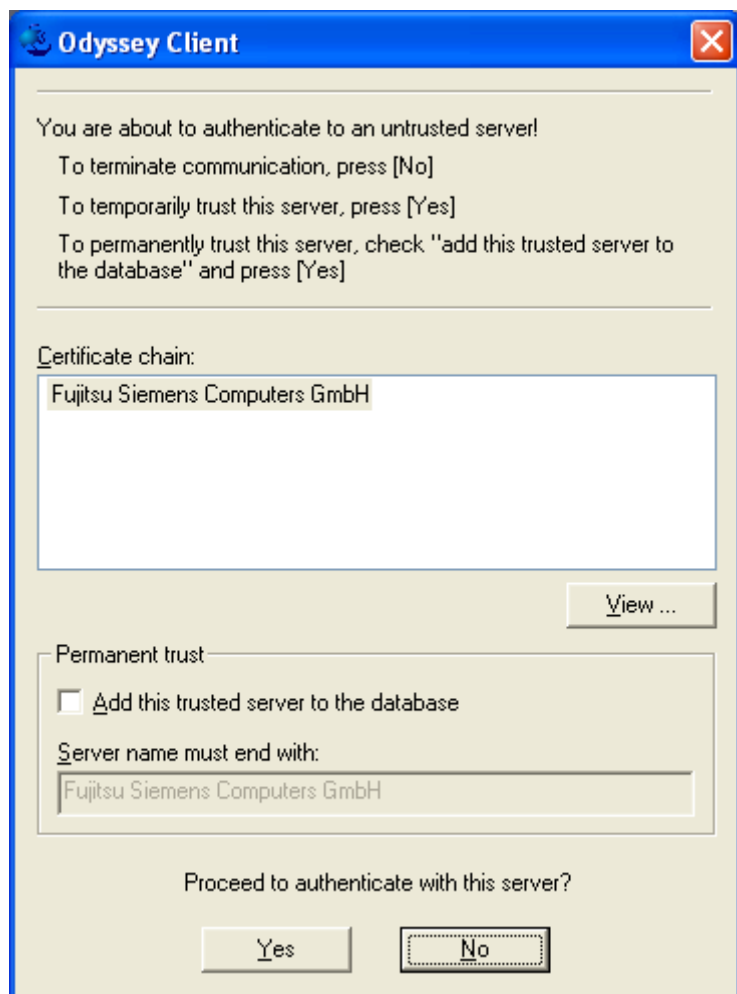
Um ausführliche Information über ein Zertifikat auf der oberen Ebene des Trust-Baums zu erhalten, wählen Sie das Zertifikat und klicken Sie auf *View Certificate*.

Untrusted Server

Unter folgenden Bedingungen erhalten Sie die Option, einen zuvor "Untrusted Server" während der Netzwerk-Authentifizierung als Trusted Server zu wählen:

- Sie haben im Menü *Security Settings* auf temporäres Trust (*Enable Server temporary trust*) eingestellt.
- Das Authentifizierungs-Profil erfordert Server-Validation.
- Die Trusted Root Certificate Authority des Server-Zertifikats (im unten dargestellten Beispiel das Zertifikat "ACMERootCA") wird auf Ihrem Client installiert.

Das folgende Fenster erscheint, während Sie das Netzwerk authentifizieren.



Das Fenster zeigt die gesamte Zertifikatkette zwischen dem Authentifizierungs-Server und einer Trusted Root Certificate Authority. Weitere Informationen zu einem Zertifikat in der Kette erhalten Sie, indem Sie das Zertifikat wählen und auf *View* klicken.

Falls dieser Server zeitweilig als Trusted Server benutzt werden soll (d. h. bis Odyssey erneut gestartet wird), um zu authentifizieren und die Verbindung zum Netzwerk herzustellen, klicken Sie auf *Yes*. Anderenfalls klicken Sie auf *No*. Sie können aufgefordert werden, Ihr Passwort einzugeben, je nach dem Profil, das Sie für diese Verbindung einstellen.

Wenn Sie diesen Server permanent als Trusted Server wünschen und ihn zur Liste der Trusted Servers hinzufügen wollen, markieren Sie *Add this trusted Server to the database* und klicken Sie auf *Yes*. Der Server wird der Liste der Trusted Server hinzugefügt, wobei als Servername derselbe Name wie im Feld *Server name must end with* verwendet wird. Sie können den Servernamen editieren. Beispielsweise können Sie, wenn der Servername "auth2.acme.com" ist, ihn in "acme.com" ändern, falls Sie alle Authentifizierungs-Server, die zur Domäne "acme.com" gehören, als Trusted Server benutzen wollen.

Netzwerkkarten konfigurieren - Fenster "Adapters"

Im Fenster *Adapters* können Sie eine oder mehrere Netzwerkkarten für kabellosen Netzwerkbetrieb wählen. Sie können mehr als eine Netzwerkkarte bestimmen, wenn Sie die Taste **[Strg]** auf Ihrer Tastatur gedrückt halten, während Sie mit Ihrer Maus die Auswahl treffen.

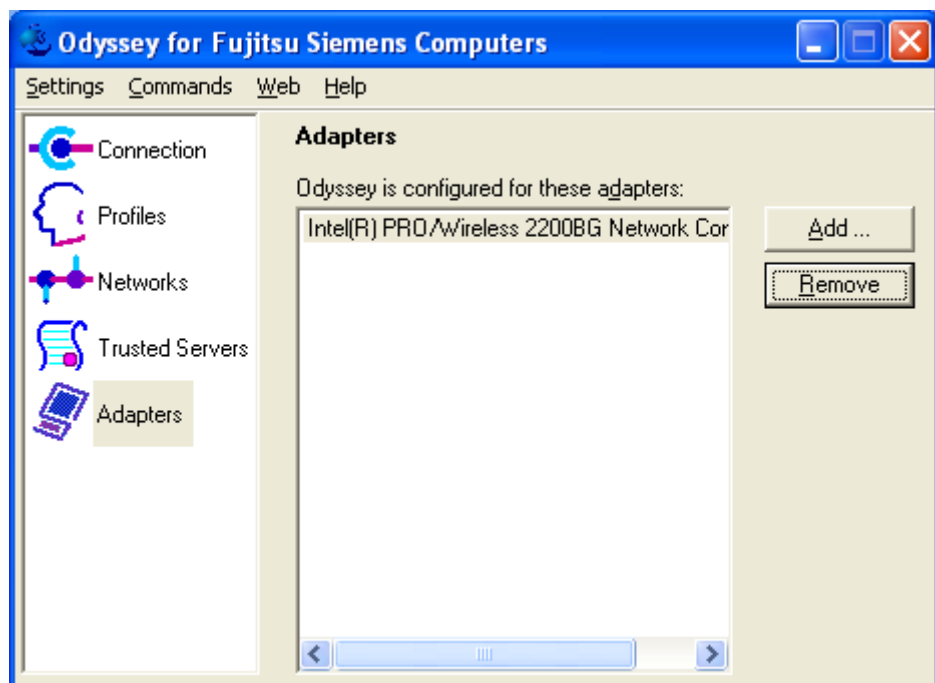
Im Fenster *Adapters* werden alle kabellosen Netzwerkkarten aufgelistet, die bei Odyssey Client konfiguriert sind. Wahrscheinlich haben Sie nur eine Netzwerkkarte konfiguriert. Sie können jedoch auch mehr als eine Netzwerkkarte konfigurieren. Sie können das Fenster *Adapters* für folgende Aufgaben verwenden:

- Funknetzwerkkarte hinzufügen
- Netzwerkkarte aus der Liste entfernen



Ihre Netzwerkkarte muss bereits in Ihrem System installiert worden sein, ehe Sie sie in Odyssey Client konfigurieren können.

- Klicken Sie im Odyssey Client Manager auf *Adapters*, um das Fenster anzuzeigen.



Funknetzwerkkarte hinzufügen

Um eine kabellose Netzwerkkarte hinzuzufügen, die Odyssey Client noch nicht erkannt hat, führen Sie die folgenden Schritte im Fenster *Adapters* des Odyssey Client Manager aus:

- Klicken Sie auf *Add*. Das Fenster *Add Adapter* erscheint und zeigt eine Liste aller Netzwerkkarten an, die auf Ihrem Computer installiert sind (außer denjenigen, für die Odyssey Client bereits konfiguriert ist).



- ▶ Wählen Sie die Registerkarte *Wireless*.
- ▶ Wählen Sie Ihre gewünschte Netzwerkkarte aus der Liste aus und klicken Sie auf *OK*.

Beachten Sie, dass nur Netzwerkkarten angezeigt werden, die Sie noch nicht hinzugefügt haben. Falls Sie Ihre Funknetzwerkkarte nicht in der Liste sehen, wählen Sie *All Adapters*.



Achten Sie darauf, dass alle von Ihnen in der Registerkarte *Wireless* ausgewählten Netzwerkkarten tatsächlich kabellos sind.

Netzwerkkarte aus der Liste entfernen

Um eine Netzwerkkarte aus der Liste der Netzwerkkarten im Fenster *Adapters* zu entfernen, wählen Sie die Netzwerkkarte aus, die Sie entfernen wollen, und klicken Sie auf *Remove*.

Odyssey Client benutzt diese Netzwerkkarte nicht länger. Die Netzwerkkarte ist immer noch in Ihrem System installiert, sie verhält sich jedoch so, als ob Odyssey Client nicht vorhanden ist.

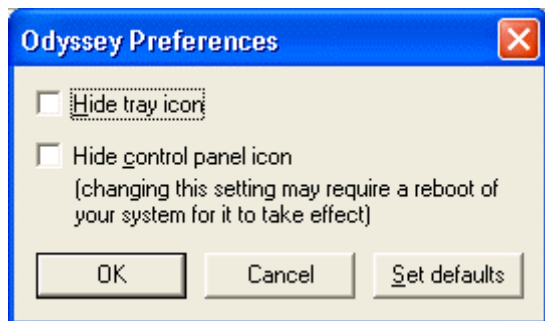
Odyssey Client Manager - Menü "Settings"

Im Menü *Settings* des Fensters *Odyssey Client Manager* stehen die folgenden Menüpunkte zur Verfügung:

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

Menüpunkt "Preferences"

Sie können die Arbeitsweise von Odyssey Client mit Hilfe des Menüpunkts *Preferences* ändern. Das Fenster *Odyssey Preferences* erscheint.



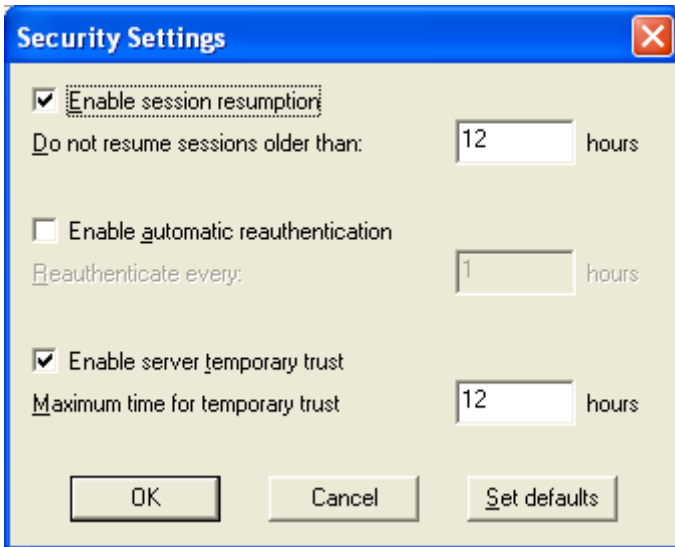
Legen Sie Ihre Präferenzen fest und klicken Sie auf *OK*, damit die Festlegung wirksam wird:

- Wenn Sie *Hide tray icon* auswählen, wird das Odyssey-Symbol nicht in der Task-Leiste angezeigt (unten rechts auf Ihrem Bildschirm).
- Wenn Sie *Hide control panel icon* auswählen, wird das Odyssey-Symbol nicht in der Windows Systemsteuerung angezeigt.

i Wenn Sie die Windows Systemsteuerung geöffnet haben, während Sie *Hide control panel icon* auswählen, und danach auf *OK* klicken, wird die Systemsteuerung aktualisiert. (Drücken Sie die Taste **F5**, um die Aktualisierung zu sehen). In einigen Fällen ist die Aktualisierung erst nach einem Neustart des Computers sichtbar.

Menüpunkt "Security settings"

Um erweiterte Sicherheitsoptionen für die Authentifizierung zu konfigurieren, wählen Sie *Security Settings*. Das Fenster *Security Settings* erscheint.



Die Sicherheitsoptionen weisen ursprünglich Standardwerte auf, die sich für die meisten Zwecke eignen sollten. Sie können diese Standardwerte jederzeit wiederherstellen, indem Sie *Set defaults* wählen.

Die Zeitfelder geben Stundenwerte mit bis zu zwei Dezimalstellen an. Wenn Sie beispielsweise eine Stunde und fünfzehn Minuten angeben wollen, geben Sie *1.25* ein.

Wiederaufnahme einer Sitzung

Mit dem Fenster *Security Settings* können Sie die Wiederaufnahme der Sitzung aktivieren.

Um die Wiederaufnahme der Sitzung zu aktivieren:

- Markieren Sie *Enable session resumption*.
- Stellen Sie *Do not resume sessions older than* auf die Höchstanzahl der Stunden ein, die eine Authentifizierung verwendet werden kann, um die erneute Authentifizierung zu beschleunigen. Wenn das Zeitlimit abgelaufen ist, wird eine vollständig aktualisierte Authentifizierung bei Ihrer nächsten Re-Authentifizierung vorgenommen. Die Anzahl der Stunden kann bis zu zwei Dezimalstellen aufweisen. Wenn Sie beispielsweise eine Stunde und fünfzehn Minuten angeben wollen, geben Sie *1.25* ein.

Als Standardeinstellung ist *Session resumption* aktiviert, und die Authentifizierung wird für bis zu 12 Stunden vorgenommen.

Um diese Funktion zu deaktivieren, entfernen Sie die Markierung für *Enable session resumption*.

Automatische Re-Authentifizierung

Sie können die Funktion *Automatic reauthentication* bei Odyssey Client auch aktivieren bzw. deaktivieren.

Markieren Sie *Enable automatic reauthentication* im Fenster *Security Settings*, damit Odyssey Client periodisch die Re-Authentifizierung beim Server einleitet.

Stellen Sie im Feld *Reauthenticate every* den Zeitraum in Stunden ein, damit die Re-Authentifizierung automatisch erfolgt.

Entfernen Sie die Markierung von *Enable automatic reauthentication* im Fenster *Security Settings*, um diese Funktion zu deaktivieren.

Als Standardeinstellung ist *Automatic reauthentication* nicht aktiviert. Der Grund dafür ist, dass Ihr Netzwerkadministrator eventuell Ihre AccessPoints oder Authentifizierungs-Server so konfiguriert hat, dass periodisch die Authentifizierung erneuert werden muss. Fragen Sie Ihren Netzwerkadministrator nach der richtigen Einstellung für diese Option.

Server temporary trust

Normalerweise konfigurieren Sie Ihre Authentifizierungs-Server im Fenster *Trusted Servers*. Es kann jedoch vorkommen, dass Sie ein Netzwerk aufsuchen, dessen Authentifizierungs-Server noch nicht als Trusted Server im Fenster *Trusted Servers* konfiguriert ist. In diesen Fall können Sie die Option *Temporary Trust* (Zeitweilige Vertrauenswürdigkeit) für diesen Untrusted Server (nicht-vertrauenswürdigen Server) aktivieren.

Markieren Sie *Enable Server temporary trust* im Fenster *Security Settings*, um *Temporary Trust* zu aktivieren. Wenn Sie diese Markierung entfernen, wird die Funktion wieder deaktiviert. Beachten Sie bei dieser Funktion Folgendes:

- Falls *Temporary Trust* aktiviert ist, haben Sie die Option, einem Untrusted Server zeitweilig zu vertrauen bei dem Versuch, einen Untrusted Server zu authentifizieren. Siehe auch "Untrusted Server".
- Im Fenster *Untrusted Server*, das sich bei dem Versuch öffnet, einen Server ohne die konfigurierte Trust-Eigenschaft zu authentifizieren, können Sie den Server permanent zu Ihrem Trust-Baum hinzuzufügen. Daher können Sie *Temporary trust* als Alternative zu dem Fenster *Trusted Servers* verwenden, um bei Bedarf vertrauenswürdige Server zu konfigurieren.
- Falls *Temporary trust* nicht eingeschaltet ist, misslingt jeder Authentifizierungsversuch, der die Validierung eines Server-Zertifikats erfordert, wenn der Server nicht explizit ein Trusted Server ist.

Stellen Sie *Maximum time for temporary trust* auf die Höchstanzahl der Stunden ein, während der Odyssey Client einen Server weiterhin als Trusted Server benutzen soll, nachdem Sie ihn akzeptiert haben.

Als Standardeinstellung ist *Temporary trust* aktiviert, und 12 Stunden ist die maximale Zeit für einen speziellen zeitweiligen Trusted Server, nachdem Sie ihn akzeptiert haben.



Diese Einstellungen sind nicht relevant, wenn Sie beschließen, den Server permanent als Trusted Server zu behandeln, indem Sie das Feld *Add this trusted Server to the database* im Fenster *Untrusted Server* markieren.

Menüpunkt "Enable/Disable Odyssey"

Wählen Sie *Enable Odyssey* oder *Disable Odyssey*, um den Odyssey Client ein- oder auszuschalten. Anfangs ist der Odyssey Client aktiviert und normalerweise brauchen Sie ihn nicht zu deaktivieren. Falls Sie *Disable Odyssey Client* auswählen, werden alle Netzwerkkarten getrennt, ohne dass Einstellungen im Fenster *Connection* verändert werden. Das Odyssey Client-Programm läuft noch, aber es ist vollständig von den Funknetzwerk-Verbindungen getrennt.

Sie sollten den Odyssey Client nur deaktivieren, wenn Sie Probleme mit Ihrer aktuellen Odyssey-Konfiguration haben. Sie könnten Odyssey Client beispielsweise deaktivieren, wenn Sie befürchten, dass er sich in einem unsicheren Zustand befindet und Sie nur sicherstellen wollen, dass Sie vom Netzwerk getrennt sind, bis Sie die Möglichkeit erhalten, Ihre Einstellungen zu überprüfen.

Odyssey Client kann auch über das Kontextmenü aktiviert und deaktiviert werden, das erscheint, wenn Sie mit der rechten Maustaste auf das Odyssey-Symbol in der Task-Leiste klicken.



Um Odyssey Client vollständig zu beenden, wählen Sie den Menüpunkt *Exit*, wenn Sie mit der rechten Maustaste auf das Odyssey-Symbol in der Task-Leiste klicken.

Menüpunkt "Close"

Wählen Sie *Close* zum Schließen des Odyssey Client Manager-Fensters. Obwohl die Benutzeroberfläche nicht mehr sichtbar ist, setzt Odyssey Client seinen Netzwerkbetrieb normal fort.

Sie können Odyssey Client Manager jederzeit erneut auf folgende Weise starten:

- aus der Task-Leiste: Doppelklicken Sie auf das Odyssey-Symbol bzw. klicken Sie mit der rechten Maustaste darauf und wählen Sie *Odyssey for Fujitsu Siemens Computers*.
- aus der Systemsteuerung: Doppelklicken Sie auf das Symbol *Odyssey for Fujitsu Siemens Computers*.
- aus dem Windows-Startmenü: Wählen Sie *Start – Programme – Fujitsu Siemens Computers – Odyssey Client for Fujitsu Siemens Computers – Odyssey Client Manager for Fujitsu Siemens Computers*.



Um Odyssey Client vollständig zu beenden, wählen Sie den Menüpunkt *Exit*, wenn Sie mit der rechten Maustaste auf das Odyssey-Symbol in der Task-Leiste klicken.

Odyssey Client Manager - Menü "Commands"

Folgende Menüpunkte sind im Menü *Commands* verfügbar:

- *Forget Password*
- *Forget Temporary Trust*

Menüpunkt "Forget Password"

Wenn Sie sich erstmals mit einem Profil authentifizieren, das auf *prompt for password* eingestellt ist, werden Sie aufgefordert, Ihr Passwort einzugeben. Odyssey Client speichert dieses Passwort und benutzt es für jede nachfolgende Authentifizierung mit Hilfe dieses Profils, ohne dass Sie wieder zu dieser Eingabe aufgefordert werden. Dieses Passwort bleibt normalerweise gespeichert, bis Sie Ihren Computer oder Odyssey Client erneut starten.

Wenn Odyssey Client die eingegebenen Passwörter nicht speichern soll, wählen Sie *Forget Password*. Wenn Ihr Passwort erneut benötigt wird, werden Sie aufgefordert, es wieder einzugeben.

Sie könnten diesen Menüpunkt wieder gebrauchen, wenn Sie Ihr Passwort falsch eingeben oder wenn Ihr Passwort auf dem Authentifizierungs-Server geändert wurde.

Menüpunkt "Forget Temporary Trust"

Falls Sie *Temporary trust* über die Einstellungen *Settings - Security Settings* aktivieren, öffnet sich jedes Mal ein Fenster, wenn Sie einen nicht-vertrauenswürdigen Authentifizierungs-Server antreffen. In diesem Fenster können Sie den jeweiligen Server als zeitweiligen Trusted Server verwenden. Odyssey Client erinnert sich an diesen Trusted Server so lange, wie er in *Security Settings* konfiguriert ist.

Wenn die Liste temporärer Trusted Server sofort gelöscht werden soll, wählen Sie *Forget Temporary Trust*.

Sie können diesen Menüpunkt gebrauchen, wenn Sie einen Server als temporären Trusted Server akzeptieren und danach beschließen, Ihre Verbindung damit abzubrechen. Wenn Sie sicherstellen wollen, dass die Verbindung sofort unterbrochen wird, deaktivieren Sie *Session resumption* und klicken Sie auf *Reconnect* im Fenster *Connection*.

Odyssey Client Manager - Menü "Help"

Das Menü *Help* umfasst die folgenden Menüpunkte:

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

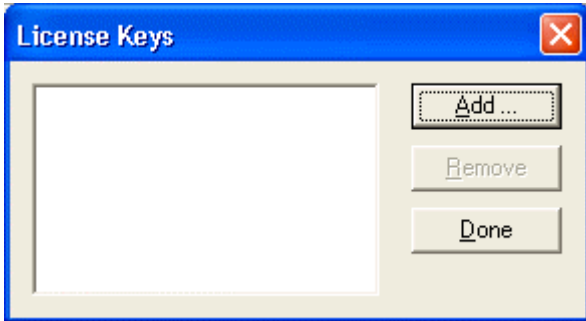
Menüpunkt "Help topics"

Wählen Sie *Help Topics* aus, um zum Odyssey Client-Hilfesystem zu gelangen.

Sie können auch kontextsensitive Hilfe jederzeit erhalten, indem Sie die Taste **F1** drücken. Das Hilfesystem öffnet sich bei dem Kapitel, in dem Ihre momentane Situation am besten erläutert wird.

Menüpunkt "License keys"

Wählen Sie *License Keys* aus dem Hilfemenü, um Ihren Odyssey Client-Lizenz-Schlüssel zu verwalten.



Ein Lizenzschlüssel ist eine Textfolge, die Ihre Lizenz für die Benutzung von Odyssey Client darstellt.

Kontextmenü "Odyssey"

Wenn Sie mit der rechten Maustaste auf das Odyssey-Symbol in der Task-Leiste klicken, erscheinen die folgenden Menüpunkte:

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

Menüpunkt "Odyssey for Fujitsu Siemens Computers"

Wenn Sie den Menüpunkt *Odyssey for Fujitsu Siemens Computers* auswählen, wird der Odyssey Client Manager (die Benutzeroberfläche für Odyssey Client) angezeigt.

Menüpunkt "Enable Odyssey/Disable Odyssey"

Wählen Sie *Enable Odyssey* oder *Disable Odyssey*, um den Odyssey Client ein- oder auszuschalten.

Anfangs ist der Odyssey Client aktiviert und gewöhnlich brauchen Sie ihn nicht zu deaktivieren. Falls Sie *Disable Odyssey Client* auswählen, werden alle Netzwerkkarten getrennt, ohne dass Einstellungen im Fenster *Connection* verändert werden. Das Odyssey Client-Programm läuft noch, aber es ist vollständig von den Funknetzwerk-Verbindungen getrennt.

Sie sollten den Odyssey Client nur deaktivieren, wenn Sie Probleme mit Ihrer aktuellen Odyssey-Konfiguration haben. Sie könnten Odyssey Client beispielsweise deaktivieren, wenn Sie befürchten, dass er sich in einem unsicheren Zustand befindet und Sie nur sicherstellen wollen, dass Sie vom Netzwerk getrennt sind, bis Sie die Möglichkeit erhalten, Ihre Einstellungen zu überprüfen.

Odyssey Client lässt sich auch über den Odyssey Client Manager aktivieren und deaktivieren.

Menüpunkt "Help"

Einer der Menüpunkte, die erscheinen, wenn Sie mit der rechten Maustaste auf das Odyssey-Symbol in der Task-Leiste klicken, ist *Help*. Zwei Optionen stehen zur Verfügung: *Help Topics* und *About*.

Wenn Sie *Help Topics* wählen, erscheint das Hilfe-System in einem Fenster mit dem geöffneten Inhaltsverzeichnis.

Wenn Sie *About* wählen, werden die Produktversion und Copyright-Informationen angezeigt.

Menüpunkt "Exit"

Wenn Sie *Exit* wählen, stoppt Odyssey Client sofort seinen Betrieb im Hintergrund. Diese Option wünschen Sie eventuell, wenn Sie längere Zeit keinen Funknetzwerkbetrieb durchführen.

Sie können Odyssey Client mit Hilfe des *Odyssey Client Manager* erneut starten unter *Start – Programme – Fujitsu Siemens Computers – Odyssey Client for Fujitsu Siemens Computers – Odyssey Client Manager for Fujitsu Siemens Computers*.

Features

Overview

Standard

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

Baseband MAC

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

Memory

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

RF Frontend

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

RF I/O Power

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

Communication

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

Data Rates

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

Modulation

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

Features

Regulatory Approvals

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

Power Supply

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

Basic security features

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

Software drivers

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

Software Access Point

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

Wake On WLAN

- Supported (depends from Software)

Form factor

- 54 x 88,8 mm

Technical details

RF Output Power

Typical Output Power

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

RF Input Sensitivity

Typical Input Sensitivity

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

Communication Range

Typical communication range:

Please note that this is valid for typical environment!

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

Communication

Channels

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

Regulatory Approvals

Compliance:

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

Declaration of Conformity

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

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

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

Hersteller /Verantwortliche Person // The manufacturer / responsible person

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

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

☐ Telekommunikations(Tk-)endeinrichtung
Telecommunications terminal equipment

☒ Funkanlage
Radio equipment

Verwendungszweck: 802.11g WLAN USB Adapter.
Intended purpose

Geräteklasse
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)...

Stichwörter

802.11-Netzwerksicherheit 3
802.1X-Authentifizierung 33
 Beschreibung 4
 Modus Open 31
 ohne WEP- Schlüssel 31
802.1X-Standard 5

A

Access point (infrastructure mode) 31
AccessPoint 2
Adapters 12
Adhoc-Modus 2
AES-Datenverschlüsselung 31
Anonymen Namen festlegen 24
Anonymous name 24
Authentifizierung 4
 automatische Re-Authentifizierung 48
 automatische Schlüsselerzeugung 32
 erweiterte Sicherheitsoptionen 46
 mit Profil 32
 Modus Open 31
 Modus Shared 31
 Modus WPA 31
 WEP-Schlüssel 4, 31
 Zuordnungsmodus angeben 31
Authentifizierungsprotokoll 21
 EAP 5
 EAP-TLS 21
 EAP-TTLS 22
 inneres 23
 PEAP 21
Authentifizierungs-Server 21
 dem Trust-Baum hinzufügen 39
 Enable Server temporary trust 42
 Identität verifizieren 21
 Server temporary trust 48
 Trusted Server 34
Automatische Re-Authentifizierung 48

B

Benutzername 19
Berechtigungsnachweis 5

C

CE-Kennzeichnung 6
Certificate Authority 35
CHAP 23
Close 49
Configure and Enable Wizard 9
Connect to any available network 30

Connection 12
 Anzeige des Verbindungsstatus 15

D

Darstellungsmittel 1

E

EAP 5
EAP/PEAP 24
EAP-TLS 32
EAP-TTLS 22, 32
 anonymen Namen festlegen 24
Enable Odyssey/Disable Odyssey 51
Enable Server temporary trust 42
Enable session resumption 47
Enable/Disable Odyssey 49
Extensible Authentication Protocol 5

F

Fenster
 Adapters 12, 43
 Connection 12, 15
 Networks 12, 27
 Profiles 12, 16
 Trusted Servers 12, 34
Forget Password 50
Forget Temporary Trust 50
Funkfrequenzen 7
Funknetzwerk
 IEEE 802.11-Standard 1
 konfigurieren 27, 28
 Name 3
 Netzwerkverbindung herstellen 13
 Reconnect 15
 Service Set Identifier (SSID) 3
 suchen nach 13
Funknetzwerkkarte konfigurieren 44

I

IEEE-Standard 802.11a, Frequenzen 7
IEEE-Standard 802.11b, Frequenzen 8
Infrastruktur-Modus 2
Inner Authentication Protocol 23
Installieren, Odyssey Client 9
Intermediate Certificates
 dem Trust-Baum hinzufügen 39
 Höchstanzahl 41

K

Konfigurieren
 Odyssey Client 11
Kontextmenü Odyssey 51

L

License keys 50
Login-Name 19

M

Menü
 Commands 49
 Help 50
 Settings 45
MS-CHAP-V2. 23

N

Network name (SSID) 30
Networks 12, 27
Netzwerk
 suchen 30
Netzwerk-Beschreibung 30
Netzwerk-Bezeichnung 28
Netzwerkkarte
 aktivieren 44
 deaktivieren 45
 konfigurieren 43
Netzwerkname 28
Netzwerksicherheit
 Authentifizierung 3
 WEP-Schlüssel 3
Netzwerktyp
 Adhoc 2
 angeben 31
 Infrastruktur 2
Netzwerkverbindung
 herstellen 13
 herstellen (zu beliebigem
 Netzwerk) 30
 re-authentifizieren 15
 Status anzeigen 15
 steuern 12
 trennen 15

O

Odyssey Client
 beenden 49, 52
 installieren 9
 konfigurieren 11
Odyssey Client Manager 11
 anzeigen 51
Odyssey Client-Lizenz-Schlüssel 50
Odyssey-Sitzung wiederaufnehmen 47

Odyssey-Symbol
 aus Taskliste ausblenden 46
 in Taskliste anzeigen 46
Open
 Modus 31

P

PAP/Token 23
Passwort
 Eingabe 19
 nicht speichern 50
PEAP 32
PEAP Settings 25
Peer-to-peer (ad-hoc mode) 31
Peer-to-Peer-Modus 2
Pre-shared Schlüssel
 Beschreibung 4
 eingeben 33
Profile definieren 16
Profiles 12, 16

R

Richtlinie 1999/5/EG 6

S

Schlechte Funkverbindung 15
Server temporary trust 48
Server-Domäne 35
Shared
 Modus 31
Sicherheitshinweise 6

T

TKIP-Verschlüsselung 4, 31
Trust-Baum 37
 anzeigen 38
 Zertifikat-Knoten entfernen 41
 Zertifikat-Knoten hinzufügen 38
Trusted Root Certificate Authority 43
Trusted Servers 12, 34
 editieren 36
 einfache Vertrauenskontrolle 35
 erweiterte Vertrauenskontrolle 37
 hinzufügen 35
 löschen 36
 Trust-Baum 37

U

Untrusted Server 42

V

Vertrauenswürdige Server
 siehe Trusted Servers 34

W

WEP-Schlüssel 4
 eingeben 33
Wi-Fi Protected Access (WPA) 4
Wired-Equivalent Privacy (WEP) 4
WPA
 Beschreibung 4

WPA-Authentifizierung 31

 AES 31
 Passphrase 32
 pre-shared Schlüssel 32

Z

Zertifikat 19, 35
Zertifikatinformationen anzeigen 41
Zertifikatkette 37
Zertifikat-Knoten hinzufügen 38