

answers²

Användarhandbok

Wireless LAN

Svenska



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.

Utgiven av/Published by
Fujitsu Siemens Computers GmbH

Ordernummer/Order No.: **A26391-K133-Z131-1-5319**

Utgåva/Edition **3**

Tryckt i Förbundsrepubliken Tyskland

AG 0704 07/04

Wireless LAN

Användarhandbok

Wireless LAN allmänt

Installera Odyssey

Använda Odyssey-klienten

Sökregister

Utgåva juli 2004

Microsoft, MS, MS-DOS, Windows och Windows NT är inregistrerade varumärken från Microsoft Corporation.

Odyssey är ett inregistrerat varumärke från Funk Software.

Alla övriga varumärken är varumärken eller inregistrerade varumärken från respektive innehavare och erkänns som skyddade.

Copyright © Fujitsu Siemens Computers GmbH 2004

Alla rättigheter förbehållna, i synnerhet till översättning, eftertryck, duplicering genom kopiering o.dyl. (även delar av dokumentationen).

Alla kränkningar av dessa rättigheter medför skadeståndsskyldighet.

Alla rättigheter förbehållna, i synnerhet till patentsökning eller registrering av mönsterskydd.

Leverans efter tillgänglighet. Rätten till tekniska ändringar förbehålles.

Denna handbok har producerats av
cognitas. Gesellschaft für Technik-Dokumentation mbH
www.cognitas.de

Innehåll

Wireless LAN allmänt	1
Radionätverk enligt IEEE 802.11-standarden	1
Adhoc-läge	2
Infrastruktur-läge	2
Förutsättningar för operativsystemet	2
Namn på radionätverk (SSID)	3
802.11-nätverkssäkerhet	3
Wired-Equivalent Privacy (WEP) med förkonfigurerade kryptonycklar	4
Wi-Fi Protected Access (WPA) och TKIP-kryptering	4
802.1X-standard	5
Extensible Authentication Protocol (EAP)	5
Viktigt att veta	6
Säkerhetsföreskrifter	6
CE-märkning	6
Radiofrekvenser och säkerhetsstandarder	7
Installera Odyssey	9
Installera Odyssey-klienten	9
Configure and Enable Wizard	9
Använda Odyssey-klienten	11
Översikt Odyssey Client Manager	11
Odyssey Client Manager-fönstret	12
Styra nätverksanslutningar - fönstret "Connection"	12
Välja nätverkskort	13
Ansluta till ett nätverk	13
Söka efter radionätverk	13
Ansluta till ett nätverk igen	15
Re-autentisera i nätverket	15
Koppla från nätverksanslutning	15
Titta på anslutningsdata	15
Definiera profiler - fönstret "Profiles"	16
Lägga till eller ändra profil – fönstret "Profile Properties"	17
Flik "Authentication"	20
Konfigurera radionätverk – fönstret "Networks"	27
Lägga till och ändra nätverk – fönstret "Network Properties"	28
Specificera pålitliga servrar – fönstret "Trusted Servers"	34
Enkelt förfarande för Trusted Server-konfiguration	35
Avancerat förfarande för Trusted Server-konfiguration	37
Untrusted server	42
Konfigurera nätverkskort – fönstret "Adapters"	43
Lägga till radionätverkskort	44
Ta bort nätverkskort från listan	45
Odyssey Client Manager - menyn "Settings"	46
Menypunkt "Preferences"	46
Menypunkt "Security settings"	46
Menypunkt "Enable/Disable Odyssey"	49
Menypunkt "Close"	49
Odyssey Client Manager - menyn "Commands"	49
Menypunkt "Forget Password"	50
Menypunkt "Forget Temporary Trust"	50

Innehåll

Odyssey Client Manager - menyn "Help"..... 50

 Menypunkt "Help topics" 50

 Menypunkt "License keys" 51

Kontextmeny "Odyssey" 51

 Menypunkt "Odyssey for Fujitsu Siemens Computers"..... 51

 Menypunkt "Enable Odyssey/Disable Odyssey" 51

 Menypunkt "Help" 52

 Menypunkt "Exit" 52

Features 53

Overview 53

Technical details 54

Declaration of Conformity 57

Sökregister 59

Wireless LAN allmänt

Ett radionätverkskort är integrerat i din enhet. I denna användarmanual beskrivs hur du kan göra inställningar för ditt Wireless LAN.

Symboler och grafiska attribut

Följande symboler och grafiska attribut används i denna manual.



markerar hänvisningar som absolut måste iakttas - i annat fall finns risk för kroppslig skada, för skada på datorn eller att data går förlorade. Garantin gäller inte, om du förorsakar skador på enheten genom att inte följa dessa hänvisningar.



markerar viktig information för lämplig hantering av systemet.

► markerar ett arbetsmoment som du måste utföra.

Text som tryckts med skrivmaskinsstil representerar text som visas på skärmen.

Kursiv stil markerar programnamn, kommandon eller menyobjekt.

"Citationstecken" markerar kapitelrubriker, diskettnamn, andra medienamn och enstaka begrepp som ska framhåvas.

Radionätverk enligt IEEE 802.11-standarden

Det integrerade nätverkskortet arbetar enligt IEEE 802.11-standarden. Som kommunikationsmedium används frekvenser från ISM-frekvensbanden (ISM, Industrial, Scientific, Medical). Radionätverkskortet får användas utan anmälning och avgiftsfritt. I IEEE-standarden 802.11 förutses flera möjligheter att använda ISM-frekvensbanden:

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

Radionätverken som arbetar enligt 802.11 går enkelt att ansluta till befintliga Ethernet-nätverk. Radionätverkskort som arbetar enligt 802.11 är förutom några extra parametrar ett system med ett normalt Ethernet-kort. Detta betyder att du kan använda alla protokoll över ett 802.11-radionätverk på samma sätt som över ett kabelbundet Ethernet (IP, IPX, NetBIOS,...). Den enda skillnaden är att du inte måste dra några kablar mellan datorerna. Mängden av alla Wireless-LAN-stationer, som kan nå varandra direkt, betecknar man allmänt som radiocell. IEEE-standarden erbjuder två driftarter, adhoc-läget (Peer-to-Peer) och infrastruktur-läget.

Förutom beskrivningen av moduleringen och data framing innehåller denna norm ett autentiserings- och krypteringsförfarande med beteckningen Wired Equivalent Privacy (WEP). Många företag använder 802.11-radionätverk. 802.11-radionätverk hittar man nu också på hotell, på flygplatser och andra "hotspots" med internettillgång.

Adhoc-läge

Ett Wireless LAN i adhoc-läge, även kallat Peer-to-Peer-läge, består av en enda sluten radiocell. Adhoc-radionätverk uppstår när en arbetsgrupp träffas med sina system och vill koppla samman dessa för att utbyta data. System kan fritt tillkomma till ett sådant nätverk och lämna det igen.

För att inte flera adhoc-radionätverk ska störa varandra i radiokommunikationen, finns ett entydigt nätverksnamn, SSID (Service Set Identifier). SSID används för adressering så att det alltid går att tilldela ett datapaket till en specifik radiocell.

Om du vill ansluta dig till ett befintligt radionätverk, behöver du nätverksnamnet (SSID), som du matar in i inställningarna för nätverkskortet. Nätverkskortet letar då efter ett radionätverk med detta SSID vid starten. När nätverkskortet hittat ett radionätverk, ansluter det till detta och du kan kommunicera med systemen i det här radionätverket. Om två radioceller är mycket nära varandra, bör radiokanalerna för dessa nätverk ligga 4 till 5 kanaler från varandra. Detta gäller för 802.11b och 802.11g.

Infrastruktur-läge

I infrastruktur-läget finns förutom de rörliga stationerna en basstation som kallas för accesspunkt (AccessPoint). I infrastruktur-läget övertar accesspunkten funktionen av en "övervakare". I motsats till adhoc-läget måste varje system logga in vid accesspunkten innan den får utbyta data i radiocellen.

Ytterligare en uppgift för accesspunkten är radiocellens anslutning till ett kabelbundet Ethernet. Eftersom accesspunkten alltid exakt vet, genom inloggningstväranget, vilka stationer som befinner sig på radiosidan, kan den exakt avgöra vilka data som måste släppas igenom och vilka inte. Denna procedur kallas även för "bridging".

För att öka räckvidden för ett radionätverk, kan flera accesspunkter med samma SSID användas.

Om ett system går in i radionätverket, letar den, bland de accesspunkter som kan nås, upp den med den starkaste signalen och loggar in sig där. Två system som är inloggade till olika accesspunkter, kommunicerar på så vis med varandra, även om de inte befinner sig inom direkt radioräckvidd.

Övervakar ett system kontinuerligt radioläget även efter inloggningen, kan det identifiera, hur signalerna från en accesspunkt blir svagare och starkare från en annan och logga om sig utan att användaren märker detta. Denna procedur kallas för "roaming".

Förutsättningar för operativsystemet

Operativsystem Windows 2000 och Windows XP

Namn på radionätverk (SSID)

Varje radionätverk har ett eget namn. Du kan välja det radionätverk som du vill ansluta dig till via namnet. Nätverksnamn gör att det går att använda flera radionätverk samtidigt i samma omgivning utan att de stör varandra ömsesidigt. Om exempelvis företaget bredvid också använder radionätverk, vill du vara säker på att din dator är ansluten till ditt företags nätverk och inte med det andra företags, även om din dator befinner sig inom området för närbelägna accesspunkter. (Hur man förhindrar att främmande personer kommer in i ditt företagsnätverk tas upp i den efterföljande säkerhetsdiskussionen.) Ett nätverksnamn är helt enkelt en följd av maximalt 32 tecken, t.ex. "Bayonne Office" eller "Acme-Marketronics" eller "BE45789". För nätverksnamn skiljer man mellan versaler och gemener, därför måste du vara noggrann med detta när du skriver in namnet. Du har dock möjligheten att välja ut namn på redan tillgängliga nätverk. Om du väljer nätverket från en lista undviks fel när namnet skrivs in. 802.11-normen definierar nätverksnamn som exempelvis "Service Set Identifier" (SSID).

802.11-nätverkssäkerhet

Sedan radionätverken började användas spelar säkerhet en avsevärt mer kritisk roll än tidigare, av den enkla anledningen att angripare har det lättare att avlyssna dessa anslutningar. Vid kabelbundna nätverk kan de flesta företag säkra skyddet av sina nätverk på ett apparattekniskt sätt. En angripare skulle vara tvungen att komma in i företagets lokaler, koppla upp sig till LAN och spionera på nätverkstrafiken.

Allt vad man behöver för att spionera på data i radionätverket är en dator med ett radionätverkskort och ett lämpligt ställe på parkeringsplatsen eller kontoret. Nedan beskrivs några förutsättningar för säker nätverksanslutning:

- En användare måste autentiseras av nätverket innan han beviljas åtkomst så att nätverket är skyddat mot inkräktare.
- Nätverket måste vara autentiserat genom användaren innan hans dator tillåter anslutningen till nätverket. Därigenom förhindras att radioutrustning utger sig vara legitimt nätverk och får åtkomstillåtelse till användarens dator.
- Den ömsesidiga autentiseringen mellan användare och nätverk måste skyddas kryptografiskt. Med detta säkerställs att du ansluts till det nätverk du vill och inte till ett felaktigt.
- Radiokommunikationen mellan en dator och accesspunkten måste vara krypterad på ett sätt att inkräktare inte kommer åt konfidentiell data.

För denna typ av säker kryptering via ett radionätverk finns två grundläggande mekanismer:

- Förkonfigurerade hemliga uppgifter med beteckningen WEP-kryptonyckel. WEP-kryptonycklar håller inte ej tillåtna användare borta från radionätverket och krypterar datan från legitima användare.
- Autentisering med hjälp av ett 802.1X-protokoll. Här ligger mångfaldiga autentiseringsprotokoll till grund för åtkomstkontrollen till nätverket. De starkaste av dessa protokoll kan säkra autentisering av användare och nätverk ömsesidigt och kan skapa kryptonycklar för kryptering av radiodata dynamiskt.

Wired-Equivalent Privacy (WEP) med förkonfigurerade kryptonycklar

Klientdatorn och accesspunkten tilldelas samma hemliga kryptonyckel med förkonfigurerade WEP-kryptonycklar (Wired-Equivalent Privacy). Denna kryptonyckel används för att kryptera alla data mellan datorn och accesspunkten. Dessutom kan WEP-kryptonyckeln användas för att autentisera klientdatorn vid accesspunkten. Om datorn inte kan bevisa att den känner till WEP-kryptonyckeln förvägras den åtkomst till nätverket.

- Om accesspunkten kräver en WEP-kryptonyckel för autentiseringen, måste anslutningen till accesspunkten göras i Shared-läget. Anslutningsläget ställer du in i nätverksegenskaperna.
- Om accesspunkten inte kräver någon WEP-kryptonyckel för autentiseringen, betecknas detta som öppet läge (open). Anslutningsläget ställer du in i nätverksegenskaperna.
- Om accesspunkten kräver en WEP-kryptering för WPA istället för TKIP för autentiseringen, genereras alla nödvändiga WEP-kryptonycklar från en ASCII-lösenfras, som du konfigurerar för din accesspunkt och för Odyssey-klienten.

Se följande teman:

- "Ange anslutningsläge", med anvisning för att välja ett anslutningsläge i Odyssey-klienten
- "Ange ett lämpat krypteringsförfarande för ditt anslutningsläge", med anvisning för att välja WEP-kryptering i Shared-läge
- "Förkonfigurerade kryptonycklar (WEP)", för användningen av statiska WEP-kryptonycklar för Odyssey-klienten
- "Pre-shared-kryptonycklar (WPA)", för konfiguration av WEP-krypteringen i WPA-läge

Wi-Fi Protected Access (WPA) och TKIP-kryptering

Som uppgradering av 802.11-normen omfattar Wi-Fi Protected Access (WPA) en rad säkerhetstillägg utöver Wired-Equivalent Privacy. Dessa uppgraderingar innehåller följande:

- Förbättrad datakryptering genom TKIP (temporärt kryptonyckelintegritets-protokoll). TKIP erbjuder en prestationsstark kryptering som WEP, eftersom kryptonycklar uppdateras dynamiskt efter var 10 000:e paket.
- 802.1X-autentisering med EAP. Om accesspunktens hårdvara begär att du gör autentiseringen via det avancerade WPA-läget, kan du konfigurera Odyssey-klienten så att autentiseringen görs i WPA-läge. Om hårdvaran är konfigurerad för TKIP-krypteringen, kan du även konfigurera Odyssey-klienten för detta avancerade datakrypteringsförfarande. Förutom överensstämmelsen med 802.1X-specifikationen för att generera kryptering dynamiskt (tillgängligt med de prestationsstarka autentiseringsmetoderna), möjliggör WPA generering av pre-shared-kryptonycklar för TKIP- (eller WEP-) kryptering via en lösenfras. Om du konfigurerar en lösenfras för kryptonyckelgenereringen för dina accesspunkter måste du konfigurera samma lösenfras för Odyssey-klienten.

Se följande teman:

- "Ange anslutningsläge", för användning av WPA-läget för Odyssey-klient
- "Ange ett lämpat krypteringsförfarande för ditt anslutningsläge", för användning av TKIP-krypteringen i WPA-läge
- "Pre-shared-kryptonycklar (WPA)" för att konfigurera en statisk lösenfras

802.1X-standard

IEEE 802.1X-protokollet möjliggör autentiserad åtkomst till ett LAN. Denna norm gäller både för trådlösa och kabelbundna nätverk. För ett radionätverk sker 802.1X-autentiseringen efter att 802.11-anslutningen har implementerats. Kabelbundna nätverk använder 802.1X-normen utan 802.11-anslutning.

WEP-protokollet som använder förkonfigurerade kryptonycklar, har vissa svagheter avseende enkel förvaltning och säkerhet. För att lösa dessa problem har IEEE infört ännu en norm: 802.1X. 802.1X erbjuder bättre säkerhet än de förkonfigurerade WEP-kryptonycklarna och är enkel att hantera, i synnerhet för stora nätverk.

När förkonfigurerade WEP-kryptonycklar används autentiseras den trådlösa klientdatorn gentemot nätverket. Vid 802.1X autentiseras användaren gentemot nätverket med behörighetsbevisen (lösenord, certifikat eller Token-kort). Autentiseringen görs inte genom accesspunkten utan tvärtom genom en central server. Om denna server använder RADIUS-protokollet betecknar man den RADIUS-server.

För 802.1X kan en användare logga in sig till nätverket från varje dator och många accesspunkter kan använda en enskild RADIUS-server gemensamt för autentiseringen. Därigenom är det mycket enklare för nätverksadministratören att kontrollera åtkomsten till nätverket.

Detaljer hittar du bland följande teman:

- EAP-protokoll (Extensible Authentication Protocol)
- Återuppta en session (Session resumption)
- Re-autentisering (Reauthentication)

Extensible Authentication Protocol (EAP)

802.1X använder protokollet med beteckningen EAP (Extensible Authentication Protocol) för att genomföra autentiseringen. EAP är ingen autentiseringsmekanism i sig, utan en gemensam ram för transporten av aktuella autentiseringsprotokoll. Fördelen med EAP-protokollet är att den grundläggande EAP-mekanismen inte måste ändras vid utvecklingen av nya autentiseringsprotokoll.

Viktigt att veta

Säkerhetsföreskrifter

De flesta säkerhetsföreskrifterna hittar du i handboken "Komma i gång" till din enhet. Några av de viktigaste säkerhetsföreskrifterna hittar du i följande text.

- Stäng av radiomodulen (Bluetooth eller Wireless LAN) på enheten, när du befinner dig på ett sjukhus, i en operationssal eller i närheten av medicinska elektroniska system. De överförda radiovågorna kan påverka funktionen av de medicinska apparaterna.
Hur du kopplar från radiomodulen beskrivs i handboken "EasyGuide" som följer med vid leveransen av enheten.
- Håll enheten på ett avstånd på minst 20 cm från en pacemaker eftersom den felfria funktionen av pacemakern kan inskränkas genom radiovågor.
- De överförda radiovågorna kan förorsaka ett obehagligt surrande ljud i hörapparater.
- Stäng av enheten när du är ombord på ett flygplan och medan du åker bil.
- Ställ inte enheten med påkopplad radiomodul i närheten av brännbara gaser eller i explosionsfarliga miljöer (t.ex. lackeringsverkstad), eftersom de överförda radiovågorna kan utlösa en explosion eller en brand.

Företaget Fujitsu Siemens Computers GmbH ansvarar inte för radio- eller tv-störningar som förorsakas av otillåtna ändringar på enheten. Fujitsu Siemens ansvarar inte heller för ersättning eller utbyte av kopplingsledningar eller enheter som inte uppgivits av Fujitsu Siemens Computers GmbH. Användaren ansvarar ensamt för åtgärd av störningar som beror på sådana otillåtna ändringar och för utbyte eller ersättning av enheter.

CE-märkning



Apparaten uppfyller som den levereras kraven i riktlinje 1999/5/EG utgiven av Europeiska parlamentet och rådet den 9. mars 1999 ang. radioanläggningar och telekommunikationssändare och den ömsesidiga acceptansen av överensstämmelsen.

Denna enhet får användas i Belgien, Danmark, Tyskland, Finland, Frankrike, Grekland, Storbritannien, Irland, Italien, Luxemburg, Nederländerna, Österrike, Portugal, Sverige, Schweiz, Spanien, Island, Liechtenstein och Norge. Aktuell information om eventuella begränsningar av driften finns hos motsvarande myndighet i respektive land. Om ditt land inte är med i uppräknningen, vänd dig till motsvarande kontrollerande myndighet huruvida användningen av den här produkten är tillåten.

Begränsningar

- Frankrike
 - Begränsat frekvensområde: endast kanalerna 10 till 13 (2457 MHz till 2472 MHz) får användas i Frankrike. Det är förbjudet att använda enheten utomhus.
- Italien
 - Ministeriellt tillstånd krävs även för användning inomhus. Kontakta försäljaren gällande detta tillvägagångssätt. Det är förbjudet att använda enheten utomhus.
- Nederländerna
 - För användning utomhus krävs licens. Kontakta försäljaren gällande detta tillvägagångssätt.

Radiofrekvenser och säkerhetsstandarder

Följande information var aktuell i januari 2002. Aktuell information hittar du hos motsvarande myndighet i ditt land (t.ex. www.regtp.de).

Frekvenser 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
Österrike	x	x	x	x				
Belgien	x	x	x	x	x	x	x	x
Danmark	x	x	x	x				
Finland	x	x	x	x	x	x	x	x
Frankrike	x	x	x	x				
Tyskland	x	x	x	x				
Grekland								
Italien								
Irland	x	x	x	x	x	x	x	x
Luxemburg								
Nederländerna	x	x	x	x				
Norge	x	x	x	x				
Portugal	x	x	x	x				
Spanien								
Sverige	x	x	x	x				
Schweiz	x	x	x	x				
Storbritannien	x	x	x	x	x	x	x	x

Frekvenser IEEE-standard 802.11b (11 Mbits/s) / 802.11g (54 Mbits/s)

Radionätverkkort och -adaptrar är, enligt IEEE-standarden 802.11b, avsedda för drift på ISM-frekvensbandet (Industrial, Scientific, Medical) mellan 2,4 och 2,4835 GHz. Eftersom var och en av de 13 användbara radiokanalerna, kräver en bredd på 22 MHz genom DSSS-förfarandet (Direct Sequence Spread Spectrum), står maximalt tre av varandra oberoende kanaler (t. ex. 1, 6 och 11) till förfogande. I följande tabeller hittar du de kanaler som är tillåtna i ditt land:

Kanalnr. / MHz	Europa, R&TTE	Frankrike, 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		

Installera Odyssey

Installationsprogramvaran för Odyssey-klienten finns i katalogen C:\Add on \Software.

Observera följande innan installationen:

- Ditt nätverkskort för det trådlösa nätverket samt hithörande programvara med drivrutiner bör redan vara installerade.
- För Windows 2000 och Windows XP måste du ha administratörsbehörighet.

Installera Odyssey-klienten

För att installera Odyssey-klienten:

- ▶ Dubbelklicka på filen *FSC-OdysseyClient.msi* i katalogen C:\Add on\Software.

Installationsguiden startas för att föra dig igenom installationsprocessen.

- ▶ Klicka på *Next* för att fortsätta.

Licensvillkoren visas.

- ▶ Klicka på alternativet *I accept the terms in the license agreement* för att godkänna licensvillkoren och klicka på *Next* för att fortsätta.
- ▶ Mata in ditt användarnamn och klicka på *Next* för att fortsätta.
- ▶ I fönstret *Setup Type* väljer du alternativet *Complete* för att genomföra installationen i standardkatalogen. Välj alternativet *Custom* om du själv vill bestämma installationskatalogen. Alternativet bör endast användas av erfarna användare. Klicka på *Next* för att fortsätta.

Installationsguiden har nu all nödvändig information för att påbörja installationen.

- ▶ Klicka på *Back* om du vill kontrollera eller ändra dina uppgifter och klicka på *Install* för att starta installationen.

Installationen startas. Detta kan ta några minuter. När installationen är avslutad, visas fönstret *InstallShield Wizard Completed*. Du kan starta Odyssey-klienten direkt eller först titta på Readme-filen.

- ▶ Klicka på *Finish* för att avsluta installationen.

På en dator med flera användarkonton står Odyssey-klienten till förfogande för alla användare efter installationen. Inställningarna för att styra användningen av Odyssey-klienten är dock användarspecifika och måste göras separat för varje användarkonto.

Configure and Enable Wizard

När du installerar Odyssey-klienten första gången, visas *Configure and Enable Wizard* automatiskt efter installationen för att man skall kunna konfigurera och aktivera Odyssey-klienten.

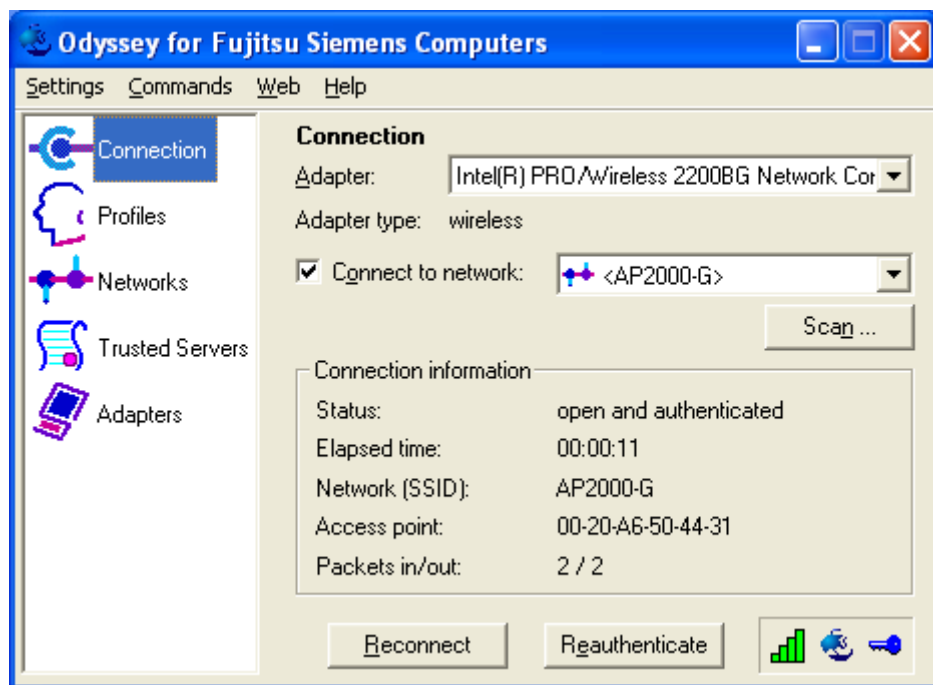
Om du inte vill göra konfigurationen just då kan du vänta till senare. Starta Odyssey Client Manager under *Start – Program – Fujitsu Siemens Computers – Odyssey Client for Fujitsu Siemens Computers – Odyssey Client Manager for Fujitsu Siemens Computers*. *Configure and Enable Wizard* startar då automatiskt.

Använda Odyssey-klienten

Översikt Odyssey Client Manager

Odyssey Client for Fujitsu Siemens Computers heter Windows-gränssnittet för Odyssey Client Managers, med vilket du kan styra och konfigurera ditt Wireless LAN. Detta gränssnitt är oföränderligt för alla Fujitsu Siemens datorplattformar som du kan använda produkten med.

- Starta *Odyssey Client Manager* under *Start – Alla program – Fujitsu Siemens Computers – Odyssey Client for Fujitsu Siemens Computers – Odyssey Client Manager* eller dubbelklicka på symbolen för Odyssey Client Manager i aktivitetsfältet.



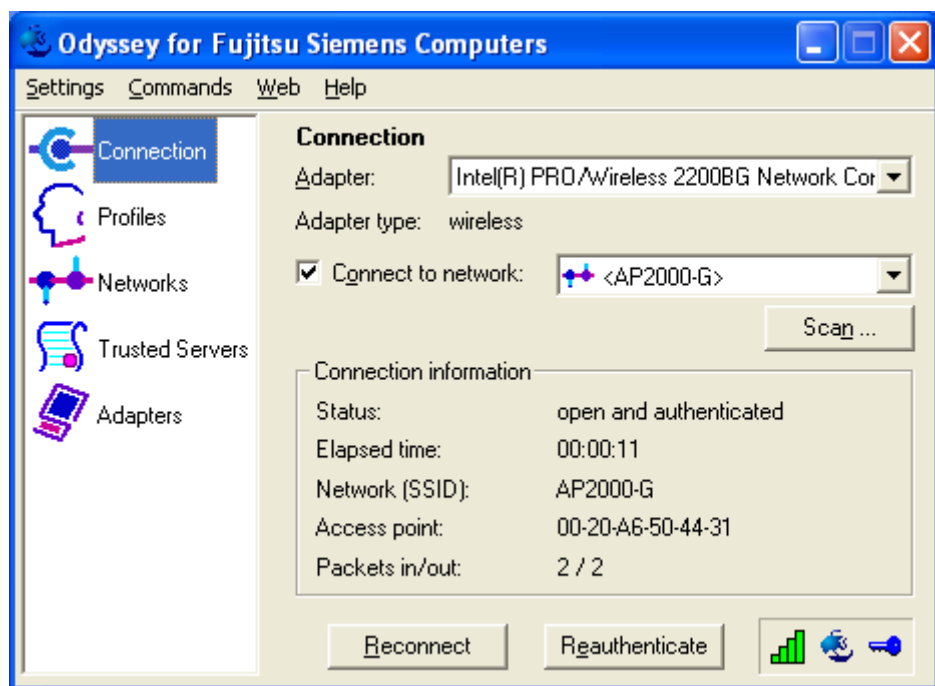
Odyssey Client Manager-fönstret

Vid de flesta nätverksanslutningar består Odyssey Client Manager av ett antal fönster där du kan göra olika driftinställningar:

- I fönstret *Connection* kan du styra din nätverksanslutning och se din aktuella anslutningsstatus.
- I fönstret *Profiles* matar du in information som behövs för att autentisera eller logga in i nätverket, t.ex. ditt lösenord eller certifikat.
- I fönstret *Networks* kan du konfigurera olika radionätverk och definiera hur du vill ansluta dem.
- I fönstret *Trusted Servers* definierar du certifierings- och identifieringsinformation om servrarna, som du kan autentisera när du skapar anslutningen, för att säkerställa att du loggar in på det önskade nätverket.
- I fönstret *Adapters* kan du konfigurera ett eller flera nätverkskort för trådlösa nätverk.

Alla fönsternamn finns listade på vänster sida av Odyssey Client Manager-fönstret. Klicka på namnet för det fönster som du vill visa eller modifiera.

Styra nätverksanslutningar - fönstret "Connection"



Välja nätverkskort

Om du eller din administratör har konfigurerat mer än ett nätverkskort för användningen av Odyssey, kan du ansluta vart och ett av dessa nätverkskort till en nätverksanslutning i urvalsmenyn *Adapters* i fönstret *Connection*.

Så snart du har valt ut ett nätverkskort, uppdateras fältet *Adapter type* och visar den valda korttypen (trådlös).

Ansluta till ett nätverk

Om du skapar nätverksanslutningen med hjälp av ett radionätverkskort, måste du fastlägga all information som krävs för anslutningen i en Odyssey-klient-nätverksdefinition. Du måste då även ange den autentiseringsinformation som du tidigare har definierat i en Odyssey-klient-profil (se "Lägga till eller ändra profil – fönstret "Profile Properties"" i avsnittet "Definiera profiler - fönstret "Profiles"").

Med kryssrutan *Connect to network* kan du skapa eller avsluta anslutningen till radionätverket. Se till att denna kryssruta är markerad om du vill ansluta till ett radionätverk.

I urvalsmenyn till höger om *Connect to network* kan du välja ett radionätverk som du vill ansluta till. I den här listan visas alla nätverk som du redan har konfigurerat med hjälp av fönstret *Networks*.

Nätverksnamnet står i raka parenteser efter nätverksbeskrivningen.

Före namnet står följande symbol:



för nätverk

För anslutningen till ett redan konfigurerat nätverk:

- Välj ut det nätverk från urvalsmenyn som du vill ansluta till.
- Markera kryssrutan *Connect to network* om inte detta redan är gjort.

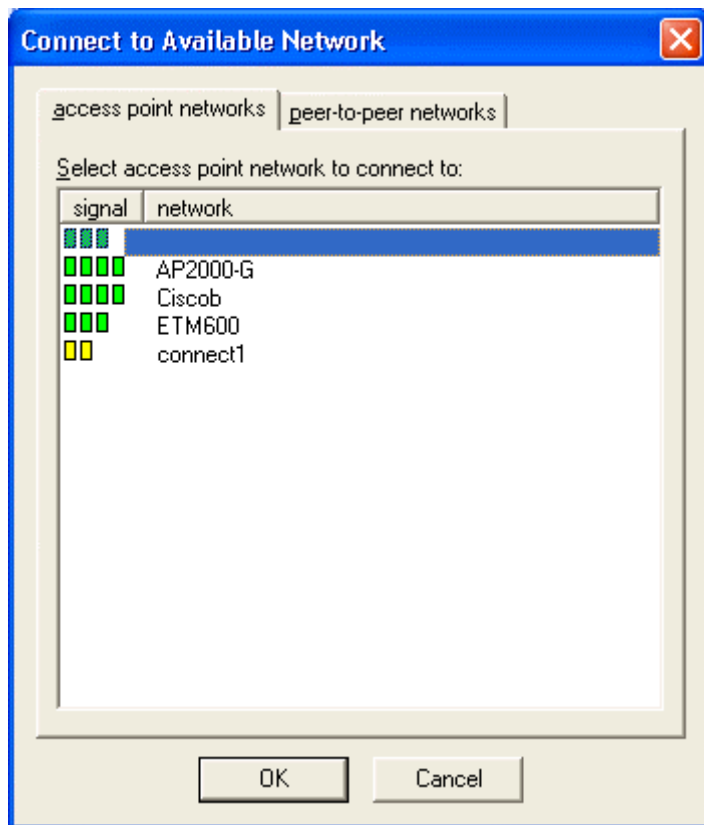
För att avsluta anslutningen till ett nätverk, tar du bort markeringen i kryssrutan *Connect to network*.

Söka efter radionätverk

Om du reser ofta kan du även autentisera dig genom lokalt tillgängliga radionätverk, som du ännu inte har konfigurerat. För att skapa anslutningen till ett ännu inte konfigurerat radionätverk, utför du följande steg:

- Klicka på *Scan* i fönstret *Connection*.

Odyssey-klienten kontrollerar radiovågorna och visar en lista över alla radionätverk som för närvarande kan nås.



- ▶ Välj det nätverk som du vill skapa en anslutning till och klicka på *OK*.
 - Om du redan har konfigurerat inställningarna för det här nätverket, försöker Odyssey-klienten att skapa anslutningen med dessa inställningar.
 - Om du ännu inte konfigurerat inställningarna för det här nätverket, visas först fönstret *Network Properties*. Ange inställningarna och klicka på *OK*.

Odyssey-klienten försöker att skapa anslutningen till nätverket.



Vid sökningen syns endast de radionätverk, för vilka administratören har konfigurerat SSID (nätverksnamnet) synligt ("send beacons"). Om SSID inte är synligt, måste du mata in nätverket i fönstret *Networks*.

Ansluta till ett nätverk igen

Om radioförbindelsen till ett nätverk inte fungerar felfritt kan du koppla från den befintliga anslutningen och skapa en ny anslutning.

- Klicka på *Reconnect* i fönstret *Connection*.

Den befintliga anslutningen kopplas från och en ny anslutning skapas till det valda radionätverket. Den nya anslutningen kan eventuellt skapas med en annan accesspunkt (i samma nätverk) beroende på faktorer såsom signalstyrkan. Om autentisering krävs för detta nätverk, blir du autentiserad en gång till när den nya anslutningen börjar. Om dynamiska kryptonycklar används för krypteringen uppdateras dessa.

Re-autentisera i nätverket

Genom att klicka på *Reauthenticate* i fönstret *Connection* autentiserar Odyssey-klienten dig igen via den befintliga anslutningen, som visas i fönstret, utan att en ny anslutning skapas. Om dynamiska kryptonycklar används för krypteringen uppdateras dessa.

Koppla från nätverksanslutning

För att koppla från en nätverksanslutning tar du bort markeringen i rutan *Connect to network* för radioförbindelser.

Titta på anslutningsdata

Statusfältet i fönstret *Connection* visar den aktuella statusen för din anslutning med nätverket via detta nätverkskort. Ett av följande meddelanden visas:

Statusmeddelande	Definition
open and authenticated	Anslutningen autentiseras, du ansluts.
open / authenticating	Re-autentisering igång, du ansluts.
open / requesting authentication	Du har begärt re-autentisering, du ansluts.
open	Anslutningen autentiseras inte men du ansluts.
peer-to-peer	Nätverkstypen är Peer-to-Peer (ad hoc), du ansluts.
authenticating	Du är ännu inte ansluten men autentiseringen är igång.
requesting authentication	Du är ännu inte ansluten men du har begärt autentisering från accesspunkten.
waiting to authenticate	Du är ännu inte ansluten och den sista autentiseringen misslyckades men du väntar på ett nytt försök.

Statusmeddelande

searching for access point

searching for peer(s)

disconnected

Odyssey is disabled

Adapter not present

Definition

Du är ännu inte ansluten och kommunikationen med en accesspunkt i det begärda nätverket misslyckades. Det kan hända att ditt nätverkskort inte stödjer 802.1X eller att din accesspunkt inte ligger inom radioområdet.

Du är inte ansluten och kommunikationen med andra datorer i Peer-to-Peer-nätverket har inte skapats.

Du är inte ansluten; eventuellt är inte *Connect to network* markerat. Se "Ansluta till ett nätverk".

Du är inte ansluten och Odyssey-klienten är avaktiverad.

Du är inte ansluten och det konfigurerade nätverkskortet är inte tillgängligt just nu. Det kan hända att ditt nätverkskort inte stödjer 802.1X.

Fältet *Elapsed time* i fönstret *Connection* visar den tid som har gått sedan den aktuella anslutningen började.

Fältet *Network (SSID)* visar namnet på det radionätverk som du är ansluten till. Se även "Namn på radionätverk (SSID)".

I fältet *Access point* anges MAC-adressen för Wireless-accesspunkten som du är ansluten till. (En MAC-adress är ett entydigt 48-bit-tal som tillverkaren har skrivit in som kod i en apparat).

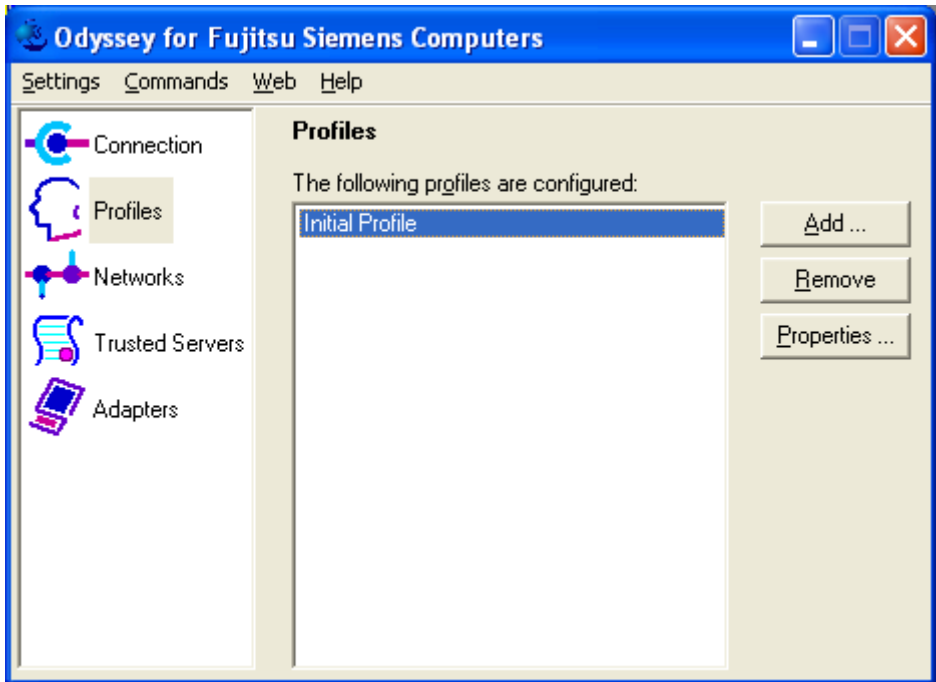
Fältet *Packets in/out* visar det totala antalet nätverkspaket som tagits emot och överförts sedan anslutningen skapades.

Definiera profiler - fönstret "Profiles"

En Odyssey-klientprofil innehåller all information som behövs för att autentisera dig för nätverket. Till detta hör uppgifter såsom inloggningsnamn, ditt lösenord eller certifikat samt protokollen som du kan autentiseras med. Din profil är i grunden den identitet som du visar gentemot nätverket och det medel som du kan bevisa din identitet med.

Du kan använda olika profiler för olika nätverk. På så vis kan du exempelvis använda olika inloggningsnamn eller lösenord för olika nätverk, eller kan du använda ett lösenord i det ena nätverket och ett certifikat i ett annat.

- Klicka på *Profiles* i Odyssey Client Manager för att fönstret ska visas.



I fönstret *Profiles* listas alla profiler som hittills har konfigurerats. Om du använder *Odyssey Client Manager* för första gången, hittar du en profil med beteckningen *Initial Profile*, vilken innehåller de allmänna inställningarna. Som alternativ till detta kan din nätverksadministratör redan ha skapat en eller flera profiler för dig.

- För att lägga till en profil, klickar du på *Add*. Fönstret *Profile Properties* visas. Mata in namnet för den nya profilen, konfigurera inställningarna och klicka på *OK*.
- För att ta bort profilen väljer du profilen och klickar på *Remove*.
- För att ändra en profil väljer du den och klickar på *Properties* respektive dubbelklickar på profilen. Fönstret *Profile Properties* visas. Ändra inställningarna och klicka på *OK*.

Lägga till eller ändra profil – fönstret "Profile Properties"

I fönstret *Profile Properties* kan du konfigurera en profil. Fönstret visas om du klickar på *Add* eller *Properties* i fönstret *Profiles*.

När du lägger till en ny profil måste du mata in ett entydigt namn i fältet *Profile Name*. Du kan till exempel använda "Office" för din profil på jobbet respektive "Home" för ditt nätverk hemma.

När du har definierat och sparat en profil, har du inte längre någon möjlighet att ändra profilnamnet när de andra profilegenskaperna redigeras. Du kan dock ta bort profilen eller skapa en ny med ett annat namn.

Förutom profilnamnet kan du konfigurera (och redigera) följande parametrar i en profil:

- Inloggningsnamn i fliken *User Info*
- Lösenord och/eller certifikat i fliken *Authentication*
- En specifikation av autentiseringsprotokollen som kan användas för din autentisering hos nätverket i fliken *TLS Settings* och *PEAP Setting*

Flik "User Info"

I fliken *User Info* kan du ange namnet som du använder för att logga in med, samt ditt lösenord och/eller certifikatsuppgifter.

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

Add Profile

Profile name:

User Info | Authentication | TLS Settings | PEAP Settings

Login name:

Password

☒ Permit login using password

☒ use Windows password

☐ prompt for password

☐ use the following password:

☐ Unmask

Certificate

☐ Permit login using my certificate:

Inloggningsnamn

Mata in ditt användarnamn i fältet *Login name*. Detta namn visas för nätverket när du autentiseras. Om du autentiseras med hjälp av ett Windows Active Directory, använder du syntaxen domän\användarnamn (exempelvis *Acme\george*). I annat fall använder du ett inloggningsnamn enligt den syntax som din administratör har definierat för användarnamn i autentiseringsdatabasen.

Observera följande:

- Om du är inloggad hos din nätverksdomän (i motsats till din lokala inloggning) anger Odyssey-klienten som standard domän-/användarnamnen i detta fält, varvid användarnamnet är ditt användarnamn.
- När du är inloggad lokalt hos din klient (i motsats till en nätverksdomän) matar Odyssey-klienten endast in ditt användarnamn i detta fält.
- Det är möjligt att du måste mata in servernamnet efter ditt inloggningsnamn så att din autentisering förs till rätt server.

Exempel: *acme\george@sales.acme.com*. Din nätverksadministratör kan tala om för dig hur detta fält skall användas korrekt.

Lösenord

Markera *Permit login using password* för att aktivera förfarandet för autentisering med lösenord. Du kan definiera vilket lösenord Odyssey-klienten använder:

- Välj *use Windows password* om du vill använda samma lösenord för att autentisera för nätverket som för Windows-inloggningen.
- Välj *prompt for password* om du vill få en uppmaning av Odyssey-klienten att mata in lösenordet när det är dags för autentisering.
- Välj *use the following password* och mata in ett lösenord i det efterföljande fältet, om Odyssey-klienten ska spara ditt lösenord och använda det varje gång när du autentiseras med den här profilen.

Om du har valt *prompt for password* uppmanas du generellt bara att mata in lösenordet första gången du autentiseras efter starten. Odyssey-klienten kommer ihåg det här lösenordet och använder det under hela din Windows-session. Det lösenord som du har angivit gäller bara för en profil. Om din autentisering gjordes med en annan profil uppmanas du att göra en ny inmatning.

Vid vissa tillfällen kan du också uppmanas att mata in ditt Windows-lösenord när du skapar anslutningen till nätverket:

- Om du av misstag har angivit ett felaktigt lösenord eller något annan autentiseringsfel föreligger. Denna funktion används också för att förhindra utestängning av misstag på grund av upprepad användning av fel lösenord.
- Om du måste ändra ditt Windows-lösenord periodiskt och kommer åt nätverket med hjälp av EAP-TLS eller PEAP-autentisering före Windows-inloggningen.

Certifikat

Markera *Permit login using my certificate* för att aktivera autentiseringsförfarandet där ditt certifikat används för att autentisera.

För att välja ett personligt certifikat för autentiseringen klickar du på *Browse*. En lista med dina personliga certifikat visas. Välj ett certifikat och klicka på *OK*.



Detta är en avancerad funktion. Om nödvändigt, vänd dig till din nätverksadministratör vid valet av det certifikat som du behöver.

Flik "Authentication"

I fliken *Authentication* kan du specificera protokoll som du autentiserar dig med i nätverket.

The screenshot shows a Windows-style dialog box titled "Add Profile" with a red close button in the top right corner. The "Profile name:" text box contains the word "Office". Below this are four tabs: "User Info", "Authentication" (which is selected), "ITLS 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. Below the list box is a checked checkbox labeled "Validate server certificate". At the bottom of the dialog are "OK" and "Cancel" buttons.

Add Profile

Profile name:

User Info | **Authentication** | ITLS Settings | PEAP Settings

Authentication protocols, in order of preference:

EAP / TTLS	↑	↓	Add ...	Remove
------------	---	---	---------	--------

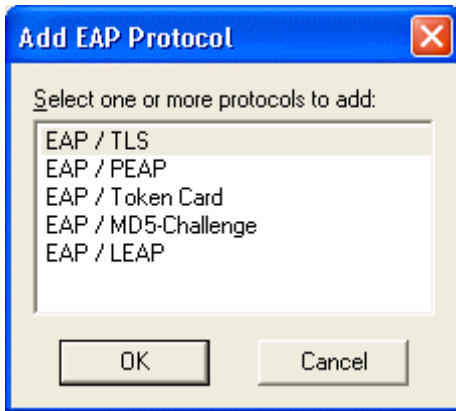
☒ Validate server certificate

OK Cancel

Välja autentiseringsprotokoll

Listan med autentiseringsprotokoll visar de protokoll som är aktiverade för att autentisera. Listan kan innehålla ett eller flera autentiseringsprotokoll. Om du har mer än ett autentiseringsprotokoll kan du ge dem olika prioriteter. Ordningsföljden bestämmer det protokoll som servern använder om det finns mer än ett gemensamt protokoll tillgängligt.

- För att ändra ordningsföljden på protokollen, väljer du ett protokoll och flyttar det med hjälp av pilknapparna.
- För att ta bort ett protokoll väljer du protokollet och klickar på *Remove*.
- För att lägga till ett protokoll klickar du på *Add*. Fönstret *Add EAP Protocol* visas. Välj ett eller flera protokoll som skall läggas till och klicka på *OK*. Du kan välja mer än ett protokoll om du håller knappen **Ctrl** på tangentbordet nedtryckt samtidigt som du väljer med musen. Observera att alla protokoll som du redan har valt ut inte tas med i detta fönster.



Validering av servercertifikatet

Vissa bestämda protokoll såsom exempelvis EAP-TTLS, PEAP och EAP-TLS gör det möjligt för dig att verifiera autentiseringsserverns identitet medan servern kontrollerar din identitet. Detta förfarande betecknas ömsesidig autentisering.

Markera *Validate Server Certificate*, för att kontrollera autentiseringsserverns identitet med certifikatet som grund, när EAP-TTLS, PEAP och EAP-TLS används. (Detta fältet är markerat som standard.) I fönstret *Trusted Servers* kan du se certifikaten till Trusted Authentication Server. Se "Specificera pålitliga servrar – fönstret "Trusted Servers".

I regel bör du markera *Validate server certificate*. Som alternativ kan du stänga av denna viktiga säkerhetsåtgärd, men endast om inget certifikat krävs hos servern. Detta bör du endast göra på inrådan av din nätverksadministratör.

Flik "TTLS Settings"

I fliken *TTLS Settings* kan du ställa in EAP-TTLS som autentiseringsprotokoll. Dessa inställningar är endast relevanta om du använder EAP-TTLS som något av dina autentiseringsprotokoll på fliken *Authentication*.

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

Under the "TTLS Settings" tab, the "Profile name:" field contains the text "Office". Below the tabs, the "Inner authentication protocol:" dropdown menu is set to "MS-CHAP-V2".

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

Further down, there is a text box with the label "Anonymous name" and the following text: "When using EAP-TTLS exclusively, you can keep your login name private and reveal only an anonymous name on the network; for example, 'anonymous' or 'anonymous@myisp.com'". Below this text is another text box with the label "Anonymous name:" and the text "anonymous" entered.

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

EAP-TTLS skapar en säker, krypterad tunnel, med vilken du överlämnar ditt behörighetsbevis till autentiseringsservern. Inom EAP-TTLS existerar också ett annat inre autentiseringsprotokoll (Inner Authentication Protocol), som du måste konfigurera.

Välja inre autentiseringsprotokoll

Välj önskat inre autentiseringsprotokoll i urvalsmenyn *Inner Authentication Protocol*. Följande protokoll står till förfogande:

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

Protokollet som oftast används är MS-CHAP-V2. Protokollet möjliggör autentisering hos en Windows Domain Controller samt hos andra användardatabaser som inte körs under Windows.

CHAP är det protokoll som används mest för autentisering vid användardatabaser som ej körs under Windows.



Du kan inte använda CHAP som förfarande för inre autentisering vid en Windows NT-domän eller Active Directory. Använd därför inte CHAP för autentiseringen vid Odyssey-servern eftersom den endast autentiseras vid en Windows-domän eller ett Active Directory.

PAP/Token är det protokoll som används vid Token-kort. Om du använder PAP/Token sparas aldrig det lösenord som du har matat in i lösenordsdialogen i cacheminnet, eftersom alla Token-baserade lösenord är avsedda att bara användas en gång.

Fråga hos din nätverksadministratör vilket inre autentiseringsprotokoll som används i ditt nätverk.

EAP som inre autentiseringsprotokoll

Om du använder EAP som inre autentiseringsprotokoll, måste du konfigurera listan med inre EAP-protokoll med ett eller flera protokoll.

- För att lägga till ett protokoll klickar du på *Add*. Fönstret *Add EAP Protocol* visas. Välj ett eller flera protokoll som skall läggas till och klicka på *OK*. Du kan välja mer än ett protokoll om du håller knappen **Ctrl** på tangentbordet nedtryckt samtidigt som du väljer med musen. Observera att alla protokoll som du redan har lagt till inte tas med i detta fönster.
- För att ta bort ett protokoll väljer du protokollet och klickar på *Remove*.
- För att ändra ordningsföljden väljer du ett protokoll och flyttar det med hjälp av pilknapparna.

Definiera ett anonymt namn

EAP-TTLS erbjuder en unik funktion jämfört med andra protokoll. Eftersom EAP-TTLS skapar en krypterad tunnel för ditt behörighetsbevis, är det också möjligt att föra över ditt inloggningsnamn genom denna tunnel. Därigenom är inte bara ditt behörighetsbevis säkert för avlyssning utan också din identitet.

Därmed har med EAP-TTLS två identiteter: en inre och en yttre. Den inre identiteten är ditt aktuella inloggningsnamn och tas från inloggningsnamnfältet på fliken *User Info*. Din yttre identitet kan vara fullständigt anonym. Ställ in din yttre identitet i fältet *Anonymous name*.

Generellt är *Anonymous name* inställt på *anonymous* som standardvärde. I vissa fall måste du mata in extra text. Därigenom kan exempelvis denna yttre identitet användas för att leda din autentisering till hithörande server och du kan uppmanas att använda *anonymous@acme.com*. Din nätverksadministratör kan tala om för dig hur detta fält konfigureras korrekt.

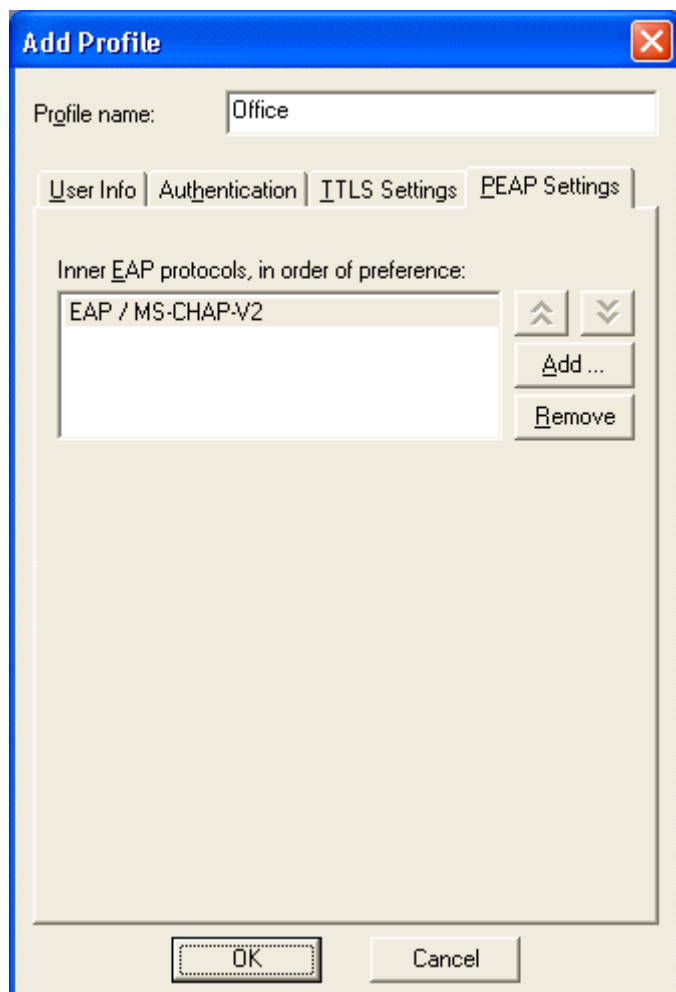


Din yttre identitet kan endast vara anonym om EAP-TTLS är det enda autentiseringsprotokollet som är konfigurerat på fliken *Authentication Protocols*. Om även andra protokoll är aktiverade kan Odyssey-klienten inte hålla din identitet hemlig och fältet *Anonymous name* är avaktiverat. Om du använder anonymiteten som erbjuds av EAP-TTLS, måste du ställa in EAP-TTLS som enda autentiseringsprotokoll.

Flik "PEAP Settings"

Om du definierar EAP/PEAP som autentiseringsförfarande på registerfliken *Authentication*, kan du använda upp till tre inre EAP-autentiseringsförfaranden:

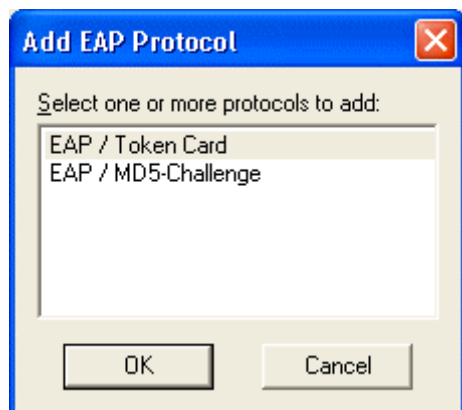
- EAP/MS-CHAP-V2
 - EAP/Token-kort
 - EAP/MD5-Challenge för att lägga till eller ta bort inre autentiseringsförfarande som används vid PEAP:
- Välj fliken *PEAP Settings*.



- Välj de protokoll som du vill ta bort och klicka på *Remove*.
- Klicka på *Add* för att lägga till ett protokoll.

Fönstret *Add EAP Protocol* visas.

- Välj ett eller flera protokoll som skall läggas till och klicka på *OK*.



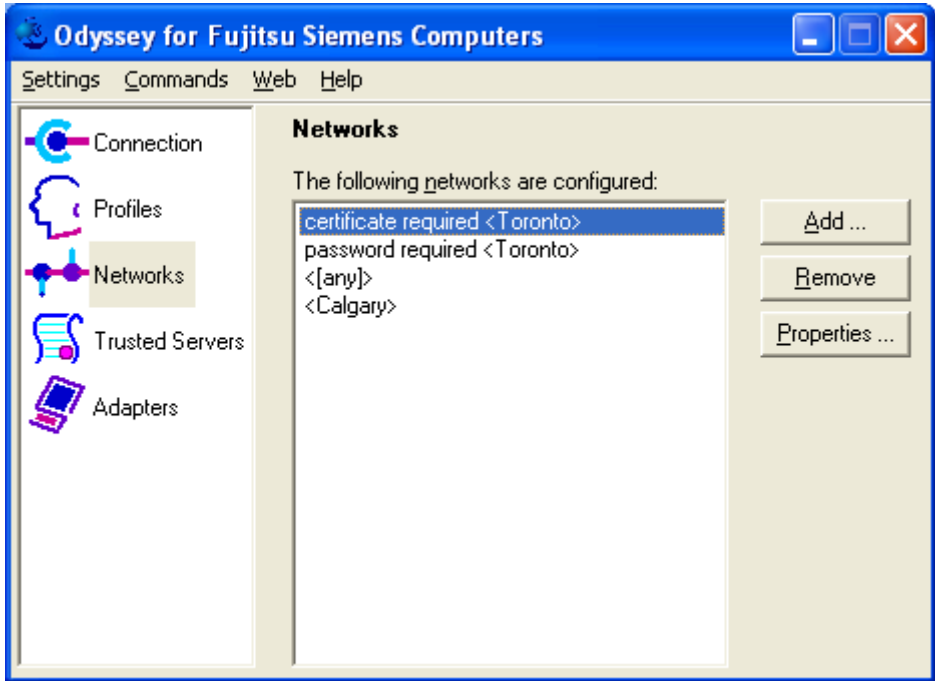
Observera att alla protokoll som du redan har valt ut inte tas med i detta fönster.

- Klicka på *OK* när du helt avslutat ändringen av profilkonfigurationen.

Konfigurera radionätverk – fönstret "Networks"

I fönstret *Networks* kan du göra inställningar för anslutning till ett valfritt antal radionätverk.

- Klicka på *Networks* i Odyssey Client Manager för att fönstret ska visas.



Alla konfigurerade nätverk listas. Du kan genomföra följande uppgifter i fönstret *Networks*:

- För att lägga till ett nätverk, klickar du på *Add*. Fönstret *Network Properties* visas. Konfigurera inställningarna för det nya nätverket och klicka på *OK* (se avsnitt "Lägga till och ändra nätverk – fönstret "Network Properties"").
- För att ta bort ett nätverk väljer du nätverket och klickar på *Remove*.
- För att ändra inställningarna för ett nätverk, väljer du nätverket och klickar på *Properties* eller dubbelklickar på nätverksnamnet. Fönstret *Network Properties* visas. Ändra inställningarna och klicka på *OK* (se avsnitt "Lägga till och ändra nätverk – fönstret "Network Properties"").

Nätverksbeteckningar

Nätverksbeteckningarna i fönstret *Networks* är uppbyggda på följande sätt:

- Nätverkets namn står inom hakparenteser.
- Nätverkets beskrivning står framför namnet. Denna beskrivning tas från fältet *Description* i fönstret *Network Properties*. Du kan lägga till din egen beskrivning till alla konfigurerade nätverk. Det hjälper dig att skilja mellan nätverken.

Fältet för nätverksbeskrivning är användbart i situationer där du vill koppla om mellan olika "personligheter" i ett och samma nätverk. Du kan exempelvis använda olika behörighetsbevis vid olika tidpunkter. Beskrivningsfältet gör också att det går att skilja mellan två olika nätverk med samma nätverksnamn.

Nätverksnamnen är valfri text som väljs av administratören. Därigenom är det möjligt att två nätverk som är oberoende av varandra har samma namn. I bilden av fönstret *Networks* finns det två nätverk "Toronto". De konfigurerade beskrivningarna anger att lösenordsbehörighetsbeviset används vid det ena nätverket och certifikatbeviset vid det andra.

Lägga till och ändra nätverk – fönstret "Network Properties"

I fönstret *Network Properties* kan du konfigurera inställningarna för radionätverket. Klicka på *Add* eller *Properties* i fönstret *Networks* för att visa nätverksegenskaperna. Fönstret *Add Network* resp. *Network Properties* visas.

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

Här kan du konfigurera följande parametrar:

- Nätverksegenskaper i avsnittet *Network*
- Autentiseringsfält i avsnittet *Authentication*
- Förkonfigurerade kryptonycklar (WEP eller WPA) i avsnittet *Pre-configured keys*

Network

I det här avsnittet av fönstret *Network Properties* kan du utföra följande uppgifter:

- Ange nätverksnamn
- Söka efter nätverk
- Konfigurera Odyssey för att ansluta till ett tillgängligt nätverk
- Ange nätverksbeskrivning
- Ange nätverkstyp
- Ange anslutningsläge
- Ange ett lämpat krypteringsförfarande för anslutningsläget

Ange nätverksnamn

Ställ in *Network name (SSID)* på namnet för radionätverket. Nätverksnamnet kan vara upp till 32 tecken långt. Man skiljer mellan versalen och gemener. Detta namn måste matas in rätt så att anslutningen kan skapas korrekt.

Söka efter nätverk

Du kan mata in namnet på nätverket direkt eller klicka på *Scan* för att välja alla nätverk som just finns i en lista.

Om du befinner dig i grannskapet till nätverket som du konfigurerar, är användningen av knappen *Scan* inte bara enklare än att skriva in, utan det garanteras också att nätverksnamnet är korrekt angivet.

Observera att du endast kan se accesspunkter som skickar riktningstrålar när du använder knappen *Scan*.

Konfigurera Odyssey för anslutning till ett valfritt nätverk

Odyssey Client Manager erbjuder ett särskilt nätverk med beteckningen *[any]*. Nätverket *[any]* skapar anslutningen till ett valfritt nätverk, oberoende av namnet. Nätverket *[any]* är användbart för dig på konferenser, hotell eller andra platser där det finns nätverksaccess. Om du väljer nätverket *[any]* i fönstret *Connection* kan du ansluta dig till sådana nätverk utan att konfigurera dem separat.

För att konfigurera ett nätverk *[any]* markerar du *Connect to any available network* och klickar på *OK*.

Fastän du kan använda WEP-kryptonycklar och -profiler med *[any]* är det gängse praxis att använda *[any]* utan 802.11- eller 802.1X-autentisering.

Ange nätverksbeskrivning

Nätverksbeskrivningar är användbara för att skilja mellan nätverk med samma eller likartade namn. Du kan ange nätverksbeskrivningen i fältet *Description*.

Ange nätverkstyp

Om du inte har använt knappen *Scan* för att välja ditt nätverk, måste du specificera nätverkstypen genom att välja någon av alternativen i urvalsmenyn.

- Välj *Access point (infrastructure mode)* om detta nätverk använder accesspunkter för att säkra anslutningsmöjligheten för företagsnätverket eller internet. Detta är den vanligaste inställningen.
- Välj *Peer-to-peer (ad-hoc mode)* för att skapa ett privat nätverk med en eller flera datorer.

Ange anslutningsläge

Före autentiseringen måste du ansluta din klient till en accesspunkt. Det anslutningsläge som du begär är beroende av din accesspunkthårdvara och av hur den är konfigurerad. Din nätverksadministratör kan hjälpa dig att konfigurera anslutningsläget som behövs för ditt nätverk.

Mer information om valmöjligheterna för den här krypteringen och anslutningsläget hittar du i "Wired-Equivalent Privacy (WEP) med förkonfigurerade kryptonycklar" och "Wi-Fi Protected Access (WPA) och TKIP-kryptering".

Du kan välja bland tre anslutningslägen:

- *Open* för anslutning till ett nätverk via en accesspunkt eller switch med 802.1X-autentisering. Välj detta läge om du inte måste välja något Shared-läge eller WPA.
- *Shared* för anslutning till ett nätverk via en accesspunkt som kräver WEP-kryptonycklar för autentisering och datakryptering.
- *WPA* för anslutning till ett nätverk via en accesspunkt med WPA (Wi-Fi Protected Access).

Ange ett lämpat krypteringsförfarande för ditt anslutningsläge

Valet av krypteringsförfarandet beror även på accesspunktens krav. Dina valmöjligheter skiljer sig åt beroende på det valda anslutningsläget. Mer information hittar du under "Wired-Equivalent Privacy (WEP) med förkonfigurerade kryptonycklar" och "Wi-Fi Protected Access (WPA) och TKIP-kryptering".

Du har följande alternativ

- *none* för att använda 802.1X-autentiseringen utan WEP-kryptonyckel. Detta alternativ är endast tillgängligt om du har valt anslutningsläget *open*.
- *WEP* för att använda WEP-kryptonyckeln för datakryptering. Detta alternativ står till förfogande i alla anslutningslägen och krävs i Shared-läget. Om du väljer detta alternativ, måste du mata in WEP-kryptonyckeln i delen *Pre-configured keys* i fönstret *Network Properties*. Du måste välja detta alternativ om accesspunkterna i ditt nätverk kräver WEP-kryptonyckel för autentiseringen (Shared-läge).
- *TKIP* för att använda protokollet för temporär kryptonyckelintegritet. Välj detta alternativ om accesspunkterna i ditt nätverk kräver WPA-autentisering och är krypterade för TKIP-datakryptering.
- *AES* när det avancerade standard-krypteringsprotokollet används. Välj detta alternativ om accesspunkterna i ditt nätverk kräver WPS-autentisering och är konfigurerade för AES-datakryptering.

Autentiseringsfält

I delen *Authentication* kan du konfigurera nätverksautentiseringen med följande kännetecken:

- Autentisering med profil
- Automatisk kryptonyckelgenerering

Autentisering med profil

Om det är nödvändigt att du autentiserar dig med ditt personliga behörighetsbevis vid det radionätverk som du har konfigurerat, markerar du *Authenticate using profile*, och väljer motsvarande profil från urvalslistan. **Du måste redan ha konfigurerat en profil som är lämpad att autentisera med för detta nätverk.**

Om du markerar *Authenticate using profile* genomför Odyssey-klienten en 802.1X-autentisering med ditt lösenord, certifikat eller andra medel, på det sätt som det är konfigurerat i den valda profilen.

Automatisk kryptonyckelgenerering

Markera *Keys will be generated automatically for data privacy* om autentiseringsförfarandet som är angivet i profilen för att skapa dynamiska WEP-kryptonycklar, är utformat för användningen mellan din dator och accesspunkten. Vissa bestämda autentiseringsförfaranden såsom EAP-TTLS, PEAP och EAP-TLS genererar kryptonycklar. Andra autentiseringsförfaranden skapar inga kryptonycklar. Om du använder EAP-TTLS, PEAP eller EAP-TLS för att autentisera, markerar du detta fält. Du kan använda vart och ett av dessa autentiseringsförfaranden för accesspunkter med 802.1x-autentisering. Detta alternativ är säkrare än att använda statiska (förkonfigurerade) kryptonycklar. Markera inte detta alternativ om du uppmanas att använda förkonfigurerade WEP-kryptonycklar, eller när det rör sig om WPA-autentisering; en pre-shared-kryptonyckel.

Förkonfigurerade kryptonycklar (WEP eller WPA)

Radionätverket kan begära att du förkonfigurerar WEP-kryptonycklar eller att du vid WPA-autentisering använder en lösenfras gemensamt dessförinnan (pre-share). Kryptonycklar kan du mata in i nedre delen av *Network Properties*.

Pre-shared-kryptonycklar (WPA)

Om du har valt WPA-läget och inte genererar kryptonyckeln automatiskt när du ansluter en autentiseringsprofil till nätverksanslutningen, måste du mata in en pre-shared-ASCII-lösenfras i fältet *Password*. Denna lösenfras används som bas vid genereringen av den kryptonyckel som behövs.

Förkonfigurerade kryptonycklar (WEP)

Om du har valt Shared-läget måste du konfigurera minst en WEP-kryptonyckel. Du måste även konfigurera minst en WEP-kryptonyckel om du väljer WEP-kryptering för det öppna läget, och kryptonycklar inte genereras automatiskt när du ansluter en autentiseringsprofil till nätverksanslutningen. WEP-kryptonycklar är till för följande saker:

- Anslutning till en accesspunkt innan en anslutning kan skapas (Shared-läge).
- Kryptering av data mellan din dator och accesspunkten (eller andra datorer i ett Peer-to-Peer-nätverk) (se "Wired-Equivalent Privacy (WEP) med förkonfigurerade kryptonycklar").

Om du använder radionätverket 802.1X-autentisering och dynamiska WEP-kryptonycklar genereras, (dvs. du har markerat *Authenticate using profile* und *Keys will be generated automatically for data privacy*) behöver du inte mata in några förkonfigurerade WEP-kryptonycklar som dataskydd. Det är dock nödvändigt, även om det inte är typiskt, att använda förkonfigurerade WEP-kryptonycklar för att autentisera förutom 802.1X. EAP-MD5 skapar exempelvis inga WEP-kryptonycklar för datakryptering, så att du måste ställa en kryptonyckel till förfogande om din profil är inställd på denna metod för att autentisera.

Om du implementerar någon av dessa tillämpningar av förkonfigurerade WEP-nycklar, måste du markera motsvarande fält och ställa in en eller flera WEP-kryptonycklar på motsvarande sätt:

- Markera *authenticate to access points (shared mode)* om förkonfigurerade WEP-kryptonycklar krävs för autentisering hos en accesspunkt före anslutningen till radionätverket.
- Markera *Keys will be generated automatically for data privacy* för att använda förkonfigurerade WEP-kryptonycklar för kryptering av data via radionätverket. Mata in WEP-kryptonyckeln i fälten *Key 0* till *Key 3*. Värdena som matats in här måste motsvara värdena för accesspunktern eller Peer-datom som du vill ansluta till. Allmänt används *Key 0* även om ditt nätverk också kan kräva andra kryptonycklar. Du kan mata in kryptonycklar antingen som vanliga texttecken (ASCII) eller hexadecimala tecken.

WEP-kryptonycklar är 40 eller 104 bit långa. Detta motsvarar antingen 5 eller 13 tecken, om du matar in dem som ASCII-tecken resp. 10 eller 26 tecken, om du matar in dem som hexadecimala tecken.

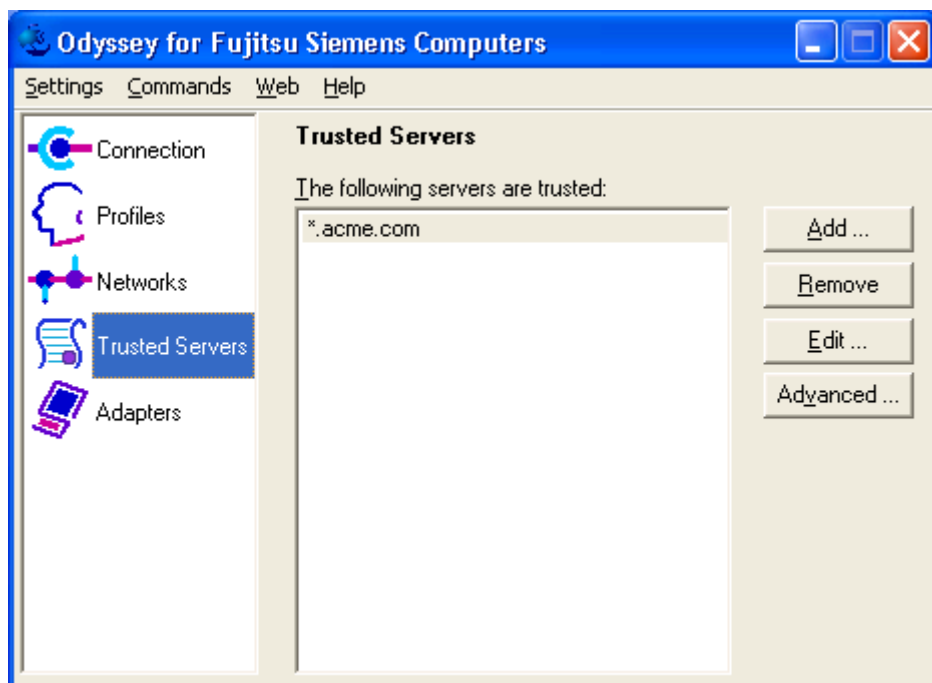
Inmatning av en förkonfigurerad WEP-kryptonyckel:

- I listan *Format for entering keys* väljer du antingen ASCII-tecken eller hexadecimala tecken, beroende på hur du vill mata in kryptonycklarna.
- Mata in varje kryptonyckel i textfälten *Key 0* till *Key 3* som du vill förkonfigurera.

Specificera pålitliga servrar – fönstret "Trusted Servers"

I fönstret *Trusted Servers* kan du konfigurera vilka autentiseringsserverar du litar på för din nätverksinslogging som Trusted Server (pålitlig server).

- Klicka på *Trusted Servers* i Odyssey Client Manager för att fönstret ska visas.



När du konfigurerar en Trusted Server, måste du inte bara ange serverns namn utan också certifikatkedjan som den tillhör. Odyssey-klienten är mycket flexibel och erbjuder ett enkelt och högutvecklat förfarande för att konfigurera Trusted-serverar.

Mer information hittar du under "Extensible Authentication Protocol (EAP)".

Enkelt förfarande för Trusted Server-konfiguration

I det flesta fall kan du använda det enkla förfarandet för att konfigurera Trusted Server. Vid detta förfarande måste du bestämma två element:

- Namn på serverdomänen eller slutet på domännamnet (exempelvis *acme.com*)
- Certifikatet för en Certificate Authority i kedjan. Det kan vara certifikatet för en Root- eller Intermediate Certificate Authority.

Domännamn

Varje server har ett domännamn som identifierar den entydigt, och detta domännamn finns normalt sett i fältet "Subject CN" på servercertifikatet.

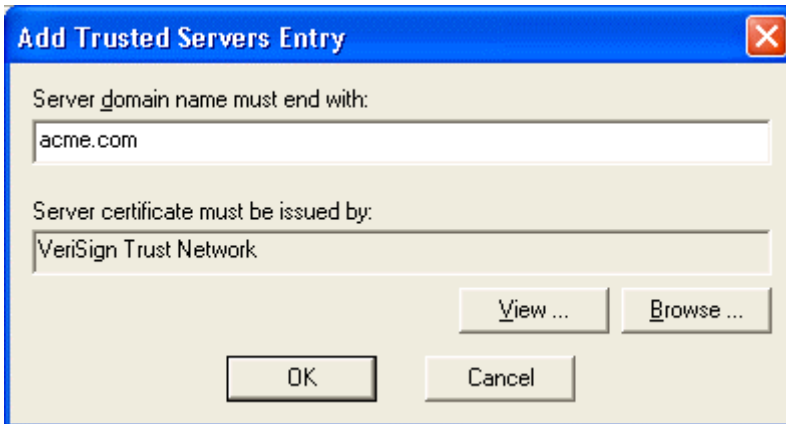
En servers domännamn slutar med namnet på en större administrativ domän som servern tillhör. Acme-företaget kan då exempelvis ha ett domännamn som *acme.com*. Bolaget skulle också kunna ha olika autentiseringsservrar med namnen *auth1.acme.com*, *auth2.acme.com* och *auth3.acme.com*.

Såsom framgår i exemplet, kan du definiera förtroendet för alla servrar i ett företag med en enda post genom att ange den bindande ändelsen för servers domännamn.

Lägga till en Trusted Server-post

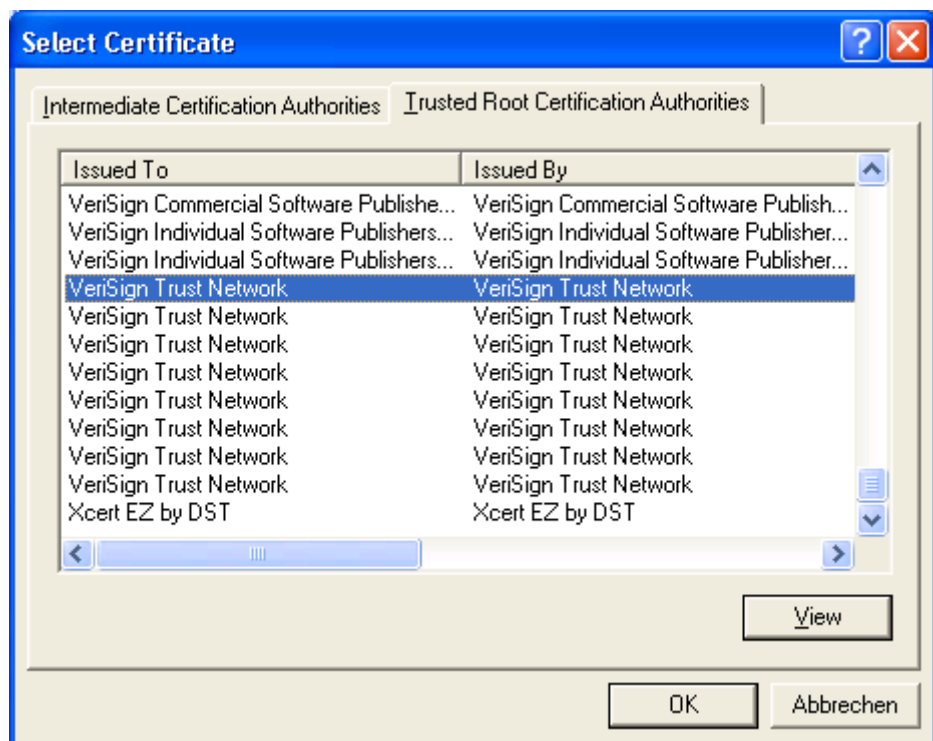
För att lägga till en post i listan med Trusted Server genomför du följande steg:

- Klicka på *Add*. Fönstret *Add Trusted Servers Entry* visas.



- I fältet *Server domain name must end with* matar du in namnet (eller namnets ändelse) på domänen som Trusted Server skall tillhöra. Detta fält får inte förbli tomt.

- Ställ in fältet *Server certificate must be issued by* på certifikatet för Certificate Authority, som har tilldelat servercertifikatet direkt eller indirekt. För att tilldela ett certifikat genomför du följande steg:
 - Klicka på *Browse* för att få fram en lista över certifikaten.
 - Välj ett certifikat från listan och klicka på *OK*.



Du kan välja en Root- eller Intermediate Certificate Authority som certifikat. Det behöver inte vara det certifikat som tilldelats direkt som servercertifikat. Det kan vara vilket certifikat som helst i listan.

Radera en Trusted Server-post

För att radera en post i listan Trusted Server väljer du posten och klickar på *Remove*.

Redigera en Trusted Server-post

För att bearbeta en post i listan med Trusted Server, väljer du posten och klickar på *Edit*. Fönstret *Edit Trusted Servers Entry* visas och gör att du kan redigera serverdomänen och certifikatet för det tilldelande stället.

Avancerat förfarande för Trusted Server-konfiguration

Om du behöver ytterligare förtroendekontroll kan du använda det avancerade förfarandet.



Om du inte har någon praktisk erfarenhet av certifikat och certifikatkedjor, bör du inte försöka göra konfigurationen med det avancerade förfarandet. Informera dig hos din nätverksadministratör om hur Trusted-serverar konfigureras.

Vid detta förfarande visas hela Trust-trädet. Trust-trädet visar alla konfigurerade Trusted-serverar.

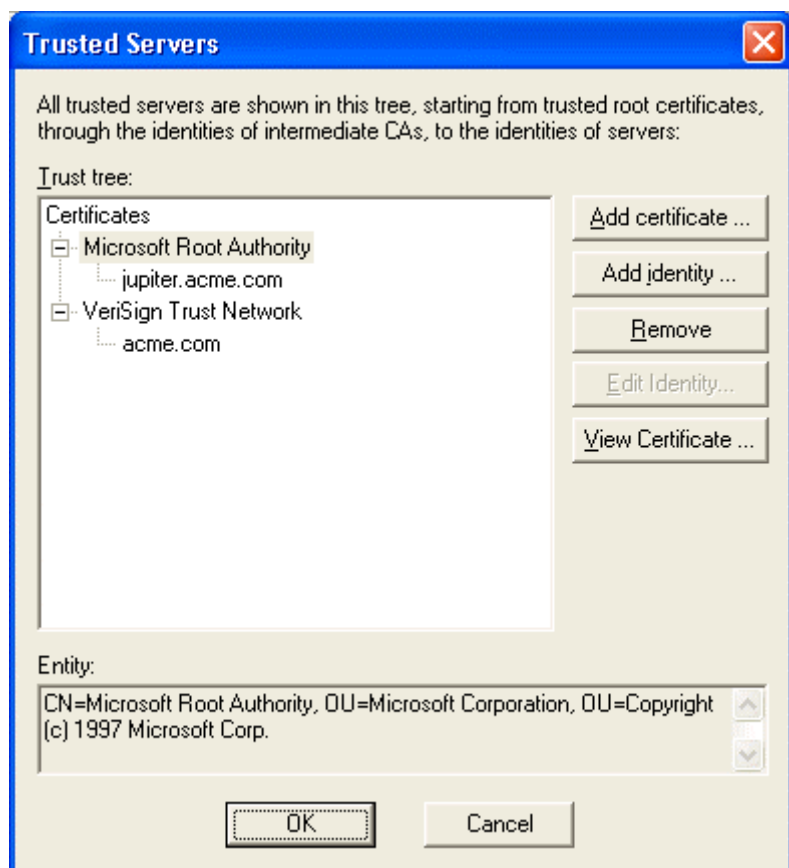
Varje väg genom Trust-trädet bestämmer en regleringsmängd för avstämningen av en certifikatkedja. Odyssey-klienten litar endast på en autentiseringsserver om dess certifikatkedja minst överensstämmer med en sökväg i Trust-trädet.

En väg genom Trust-trädet består av en eller flera noder:

- Varje nod på den översta nivån är certifikatet för en Root eller Intermediate Certificate Authority.
- Varje mellannod (om det finns) är namnet på en Intermediate Certificate Authority i kedjan.
- Varje slutnod är namnet på en server som du litar på för autentiseringen. Namnen för Certificate Authorities och server kan anges som subjektnamn eller domännamn. Dessutom kan du definiera att namnet i ett certifikat exakt måste motsvara det konfigurerade namnet eller att det måste sluta med det konfigurerade namnet.

Visa Trust-trädet

För att visa Trust-trädet, klickar du på *Advanced*. Fönstret *Trusted Servers* visas där du kan se och ändra Trust-reglerna.

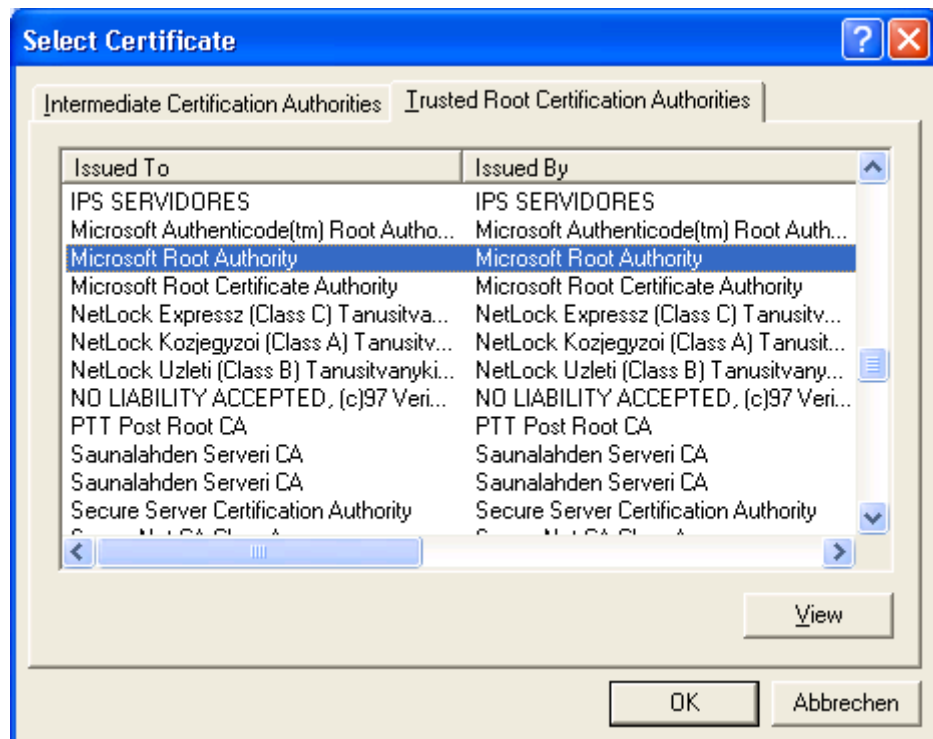


Lägga till certifikatnoder

För att lägga till ett nytt certifikat vid början av Trust-trädet:

- ▶ Klicka på *Add certificate*. Fönstret *Select Certificate* visas.
- ▶ Välj ett certifikat och klicka på *OK*. Du kan antingen välja i listan för Intermediate eller Trusted Root-certifikat.

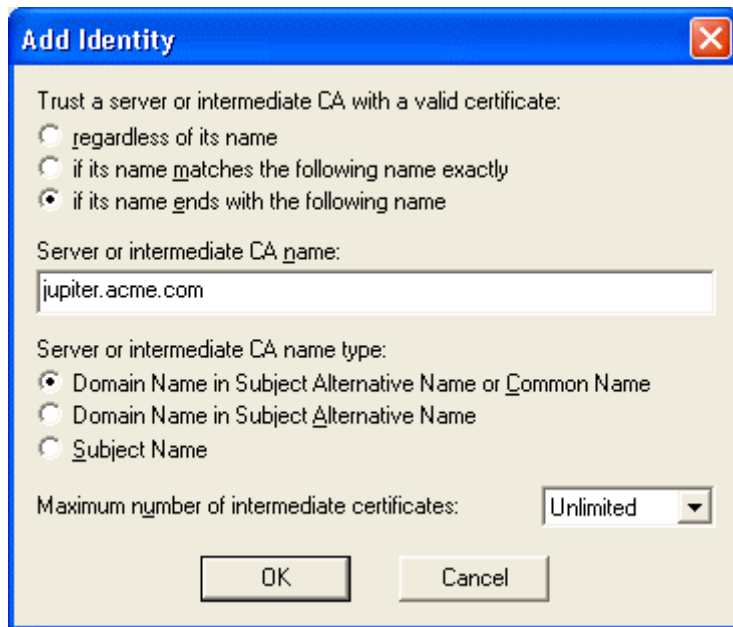
För att få utförliga uppgifter om ett certifikat innan det läggs till, väljer du certifikatet och klickar på *View*.



Lägga till autentiseringsservrar eller Intermediate CA-noder

Alla noder under den övre nivån betecknar antingen autentiseringsservrar eller Intermediate Certificate Authorities. Vid en slutnod utgår man från att den betecknar en autentiseringsserver. I annat fall utgår man från att den betecknar en Intermediate Certificate Authority. För att lägga till en autentiseringsserver eller en Intermediate Certificate Authority till trädet:

- Välj noden vid det träd, under vilket du vill lägga till det nya elementet.
- Klicka på *Add Identity*. Fönstret *Add Identity* visas.
- Mata in information som bestämmer de regler som Odyssey-klienten använder för att anpassa ett certifikat till servercertifikatkedjan vid den här noden.
- Klicka på *OK*.



Med hjälp av fönstret *Add Identity* kan du ställa in anpassningsreglerna för en enskild nod i Trust-trädet.

För att bestämma en Trusted Server eller Intermediate CA med giltigt certifikat väljer du:

- *regardless of its name* för att anpassa ett certifikat oberoende av dess namn, förutsatt att det har signumet för Certificate Authority i noden ovanför.
- *if its name matches the following name exactly* för att definiera att namnet i certifikatet exakt motsvarar det namn som du har angivit.
- *if its name ends with the following name* för att definiera att namnet i certifikatet är underordnat det namn som du har angivit. Ett certifikat med exempelvis namnet *sales.acme.com* skulle motsvara en inmatning *acme.com*.

För *Name of Server or intermediate CA* matar du in det namn (eller ändelser för ett namn) som du vill att det skall överensstämma med. (Detta fält behövs inte om du väljer oberoende av namn). Namnets form beror på ditt val av namntyp.

För *Name type* måste du ange hur namnet tolkas och var namnet hittas i certifikatet. Välj ett av följande alternativ:

- *Domain name in Subject Alternative Name or Common Name*, om domännamnet (t.ex. *acme.com*) finns i fältet *Subject Alternative Name* i certifikatet, eller om det inte finns, *Common Name* i fältet *Subject* på certifikatet (det är det vanligaste valet).
- *Domain name in Subject Alternative Name*, om domännamnet finns i fältet *Subject Alternative Name* i certifikatet. Det liknar med vissa begränsningar det tidigare urvalet.

- *Subject Name* om namnet är ett X.500-namn och finns i fältet *Subject* på certifikatet. Om du matar in ett Subject-namn fullständigt eller delvis måste du göra det i X.500-form. Det motsvarar varje jämställt eller underordnat Certificate Subject-namn.

- Om du till exempel matar in följande:

`OU=acme.com, C=US`

motsvarar namnet ett av följande Subject-namn:

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



Om du matar in text som innehåller kommatecken, måste varje kommatecken omges av enkla citationstecken.

Som maximalt antal för Intermediate Certificates definierar du det maximala antal certifikat, som kan finnas i kedjan mellan denna nod eller noden direkt över denna nod. Du kan välja en siffra mellan 0 och 5 respektive *unlimited* (obegränsat):

- Om du väljer 0 måste det certifikat som motsvarar denna nod vara signerad, varvid det certifikat används, som motsvarar noden över denna nod.
- Om du väljer 1 kan det certifikat som motsvarar denna nod, vara signerad av det certifikat som motsvarar noden över, eller av ett certifikat som i sin tur är signerat av det certifikat som motsvarar noden över.
- Om du väljer *unlimited* kan vilket antal certifikat som helst komma upp i kedjan mellan certifikatet, som motsvarar den här noden och en, som motsvarar noden över.

Ta bort noder

För att ta bort en nod, väljer du den nod i trädet som du vill ta bort och klickar på *Remove*. Den valda noden och alla noder under tas bort från trädet.

Följande noder kan tas bort:

- Top-Level Certificate-nod
- Intermediate CA-nod
- Server-nod

Visa certifikatinformation

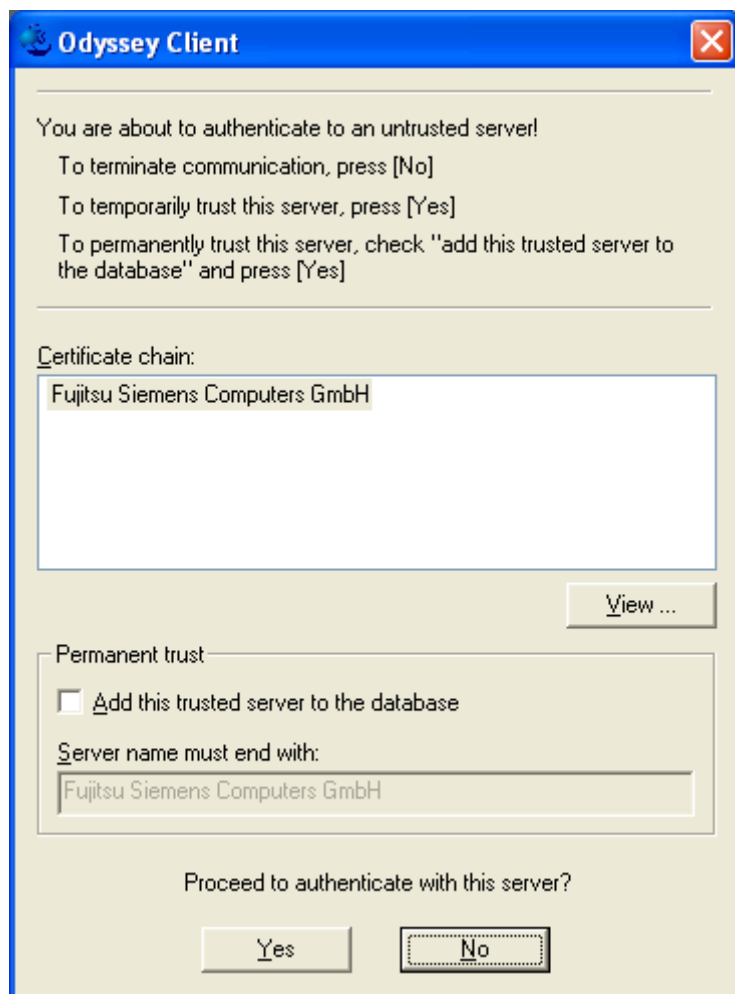
För att få utförlig information om ett certifikat på den övre nivån av Trust-trädet, väljer du certifikatet och klickar på *View Certificate*.

Untrusted server

Under följande villkor får du alternativet att välja en server som tidigare var "Untrusted Server" som Trusted Server under nätverksautentiseringen:

- Du har ställt in temporär Trust (*Enable Server temporary trust*) i menyn *Security Settings*.
- Autentiseringsprofilen kräver servervalidering.
- Trusted Root Certificate Authority för servercertifikatet (i exemplet nedan certifikatet "ACMERootCA") installeras i din klient.

Följande fönster kommer upp när du autentiserar nätverket.



Fönstret visar hela certifikatkedjan mellan autentiseringsservern och en Trusted Root Certificate Authority. Mer information om ett certifikat i kedjan får du genom att välja certifikatet och klicka på *View*.

Om denna server delvis skall användas som Trusted Server (dvs. tills Odyssey startas om) för att autentisera och skapa anslutningen till nätverket, klickar du på *Yes*. I annat fall klickar du på *No*. Du kan bli uppmanad att mata in ditt lösenord, beroende på den profil, som du ställer in för anslutningen.

Om du vill ha den här servern permanent som Trusted Server och vill lägga till den i listan över Trusted Servers, markerar du *Add this trusted Server to the database* och klickar på *Yes*. Servern läggs till i listan med Trusted Server, varvid servernamnet och det namn som används i fältet *Server name must end with* måste vara desamma. Du kan redigera servernamnet. Till exempel kan du, om servernamnet är *auth2.acme.com* ändra det till *acme.com*, om du vill använda alla autentiseringsservrar som tillhör domänen *acme.com* som Trusted Server.

Konfigurera nätverkskort – fönstret "Adapters"

I fönstret *Adapters* kan du välja ett eller flera nätverkskort för trådlös nätverksdrift. Du kan bestämma mer än ett nätverkskort, om du håller knappen **Ctrl** på tangentbordet nedtryckt samtidigt som du väljer med musen.

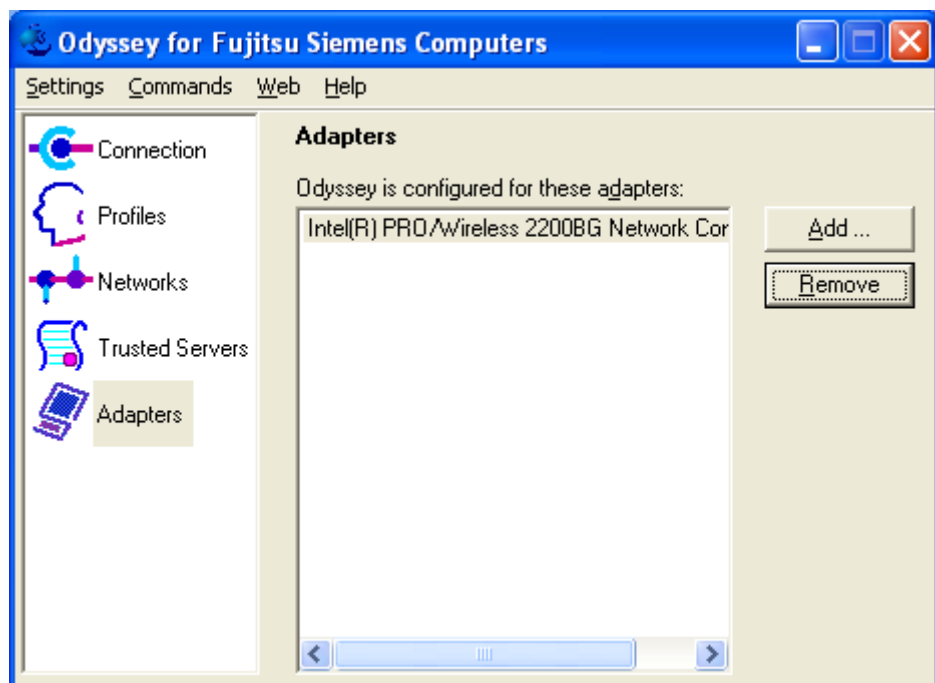
I fönstret *Adapters* listas alla trådlösa nätverkskort som är konfigurerade för Odyssey-klienten. Förmodligen har du bara konfigurerat ett nätverkskort. Du kan dock konfigurera mer än ett nätverkskort. Du kan använda fönstret *Adapters* för följande uppgifter:

- Lägga till radionätverkskort
- Ta bort nätverkskort från listan



Ditt nätverkskort måste redan vara installerat i systemet innan du kan konfigurera det i Odyssey-klienten.

- Klicka på *Adapters* i Odyssey Client Manager för att fönstret ska visas.



Lägga till radionätverkskort

För att lägga till ett trådlöst nätverkskort som Odyssey-klienten inte har identifierat, genomför du följande steg i fönstret *Adapters* i Odyssey Client Manager:

- Klicka på *Add*. Fönstret *Add Adapter* visas och visar alla nätverkskort som finns installerade i dator (förutom dem som Odyssey-klienten redan har konfigurerats för).



- Välj fliken *Wireless*.
- Välj önskat nätverkskort från listan och klicka på *OK*.

Observera att endast nätverkskort som du ännu inte har lagt till visas. Om du inte ser ditt radionätverkskort i listan, väljer du *All Adapters*.



Se till att alla de nätverkskort som du valt på fliken *Wireless* också verkligen är trådlösa.

Ta bort nätverkskort från listan

För att ta bort ett nätverkskort från listan med nätverkskort i fönstret *Adapters*, väljer du det nätverkskort som du vill ta bort och klickar på *Remove*.

Odyssey-klienten använder inte detta nätverkskort längre. Nätverkskortet är fortfarande installerat i ditt system, det uppför sig dock så som om Odyssey-klienten inte finns.

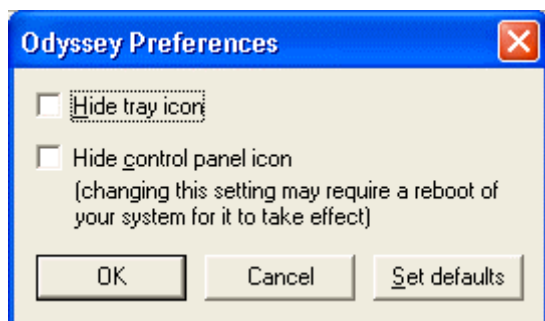
Odyssey Client Manager - menyn "Settings"

I menyn *Settings* i fönstret *Odyssey Client Manager* finns följande menypunkter:

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

Menypunkt "Preferences"

Du kan ändra Odyssey-klientens arbetssätt med hjälp av menypunkten *Preferences*. Fönstret *Odyssey Preferences* visas.



Definiera dina preferenser och *OK* så definitionen blir verksam:

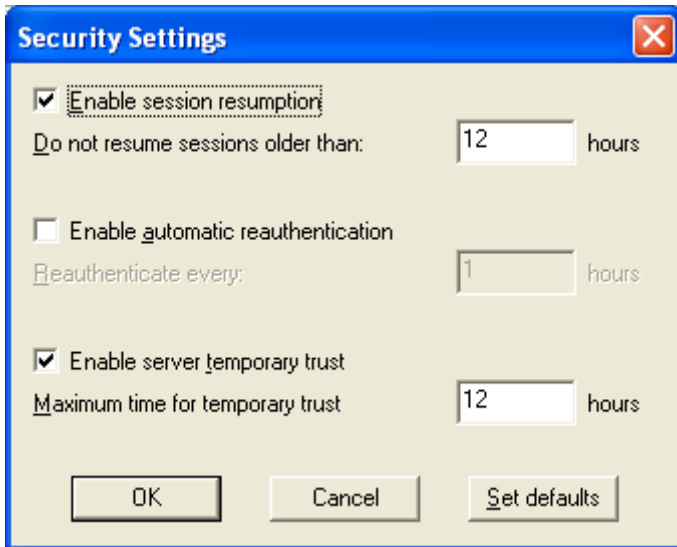
- Om du väljer *Hide tray icon* visas inte Odyssey-symbolen i aktivitetsfältet (nere till höger på bildskärmen).
- Om du väljer *Hide control panel icon* visas inte Odyssey-symbolen i Windows kontrollpanel.



Om du har öppnat Windows kontrollpanel när du väljer *Hide control panel icon* och därefter klickar på *OK*, uppdateras kontrollpanelen. (Tryck på knappen **F5** för att se uppdateringen). I vissa fall syns uppdateringen först efter att datorn startats om.

Menypunkt "Security settings"

För att konfigurera avancerade säkerhetsalternativ för autentiseringen, väljer du *Security Settings*. Fönstret *Security Settings* visas.



Säkerhetsalternativen är ursprungligen standardvärden som skall lämpa sig för de flesta syften. Du kan alltid återställa dessa standardvärden igen genom att välja *Set defaults*.

Tidsfälten anger timvärden med upp till två decimaler. Om du exempelvis vill ange en timme och femton minuter, matar du in *1.25*.

Återuppta en session

Med fönstret *Security Settings* kan du aktivera att sessionen återupptas.

För att aktivera att sessionen återupptas:

- Markera *Enable session resumption*.
- Ställ in *Do not resume sessions older than* på det maximala antal timmar som en autentisering kan användas för att påskynda den nya autentiseringen. När tidsfristen har passerat, görs en fullständig uppdaterad autentisering vid din nästa re-autentisering. Antalet timmar kan ha upp till två decimaler. Om du exempelvis vill ange en timme och femton minuter, matar du in *1.25*.

Som standardinställning är *Session resumption* aktiverad, och autentiseringen görs för upp till 12 timmar.

För att avaktivera denna funktion tar du bort markeringen för *Enable session resumption*.

Automatisk re-autentisering

Du kan även aktivera resp. avaktivera funktionen *Automatic reauthentication* för Odyssey-klienten.

Markera *Enable automatic reauthentication* i fönstret *Security Settings* så att Odyssey-klienten inleder re-autentiseringen periodiskt för servern.

Ställ in tiden i timmar i fältet *Reauthenticate every* så att re-autentiseringen sker automatiskt.

Ta bort markeringen för *Enable automatic reauthentication* i fönstret *Security Settings* för att avaktivera denna funktion.

Som standardinställning är inte *Automatic reauthentication* aktiverat. Anledningen är att din nätverksadministratör eventuellt kan ha konfigurerat dina accesspunkter eller autentiseringsservern så att autentiseringen periodvis måste uppdateras. Fråga din nätverksadministratör om rätt inställning för det här alternativet.

Server temporary trust

Normalt sett konfigurerar du din autentiseringsserver i fönstret *Trusted Servers*. Det kan dock hända att du letar upp ett nätverk, vars autentiseringsserver ännu inte är konfigurerad som Trusted Server i fönstret *Trusted Servers*. I det här fallet kan du aktivera alternativet *Temporary Trust* (temporär pålitlighet) för den här Untrusted-servern (ej pålitlig server).

Markera *Enable Server temporary trust* i fönstret *Security Settings* för att aktivera *Temporary Trust*. Om du tar bort denna markering avaktiveras funktionen igen. Observera följande vid denna funktion:

- Om *Temporary Trust* är aktiverad har du alternativet att temporärt lita på en *Untrusted Server* vid försöket att autentisera en Untrusted Server. Se även "Untrusted server".
- I fönstret *Untrusted Server*, som öppnas vid försöket att autentisera en server utan den konfigurerade Trust-egenskapen, kan du lägga till servern permanent till ditt Trust-träd. Därför kan du använda *Temporary trust* som alternativ till fönstret *Trusted Servers* för att konfigurera pålitliga servrar vid behov.
- Om *Temporary trust* inte är aktiverad, misslyckas alla autentiseringsförsök som kräver validering av ett servercertifikat om inte servern explicit är en Trusted Server.

Ställ in *Maximum time for temporary trust* på maxantalet timmar när Odyssey-klienten även i fortsättningen skall använda en server som Trusted Server efter att den har accepterats.

Som standardinställning är *Temporary trust* aktiverad och 12 timmar är den maximala tiden för en särskild temporär Trusted Server, efter att den har accepterats.



Dessa inställningar är inte relevanta om du bestämmer dig för att behandla servern permanent som Trusted Server, genom att markera fältet *Add this trusted Server to the database* i fönstret *Untrusted Server*.

Menypunkt "Enable/Disable Odyssey"

Välj *Enable Odyssey* eller *Disable Odyssey* för att aktivera eller avaktivera Odyssey-klienten. Till att börja med är Odyssey-klienten aktiverad och normalt sett behöver den inte avaktiveras. Om du väljer *Disable Odyssey Client* kopplas alla nätverkskort från utan att inställningarna i fönstret *Connection* förändras. Odyssey-klientprogrammet är fortfarande igång men det är helt fränkopplat från radionätverksanslutningarna.

Du bör endast avaktivera Odyssey-klienten om du har problem med din aktuella Odyssey-konfiguration. Du kan exempelvis avaktivera Odyssey-klienten, om du befärar att den har en osäker status och du vill säkerställa att du är fränkopplad från nätverket, fram till att du får möjlighet att kontrollera dina inställningar.

Odyssey-klienten kan även aktiveras och avaktiveras via kontextmenyn, vilken visas om du klickar med höger musknapp på Odyssey-symbolen i aktivitetsfältet.



För att avsluta Odyssey-klienten helt, väljer du menypunkten *Exit*, när du klickar med höger musknapp på Odyssey-symbolen i aktivitetsfältet.

Menypunkt "Close"

Välj *Close* för att stänga Odyssey Client Manager-fönstret. Även om användargränssnittet inte syns längre fortsätter Odyssey-klienten nätverksdriften normalt.

Du kan när som helst starta om Odyssey Client Manager på följande sätt:

- utifrån aktivitetsfältet: dubbelklicka på Odyssey-symbolen resp. klicka med höger musknapp på den och välj *Odyssey for Fujitsu Siemens Computers*.
- utifrån kontrollpanelen: dubbelklicka på symbolen *Odyssey for Fujitsu Siemens Computers*.
- utifrån Windows-startmenyn: Välj *Start – Program – Fujitsu Siemens Computers – Odyssey Client for Fujitsu Siemens Computers – Odyssey Client Manager for Fujitsu Siemens Computers*.



För att avsluta Odyssey-klienten helt, väljer du menypunkten *Exit*, när du klickar med höger musknapp på Odyssey-symbolen i aktivitetsfältet.

Odyssey Client Manager - menyn "Commands"

Följande menypunkter finns tillgängliga i menyn *Commands*:

- *Forget Password*
- *Forget Temporary Trust*

Menypunkt "Forget Password"

När du autentiseras första gången med en profil som är inställd på *prompt for password* blir du uppmanad att mata in ditt lösenord. Odyssey Client lagrar detta lösenord och använder det för varje efterföljande autentisering med hjälp av den här profilen utan att du blir uppmanad att mata in det igen. Detta lösenord sparas normalt sett tills du startar om din dator eller Odyssey-klient.

Om Odyssey-klienten inte skall spara det inmatade lösenordet, väljer du *Forget Password*. När ditt lösenord behövs igen blir du uppmanad att mata in det igen.

Du kan behöva den här menypunkten igen om du skriver in ditt lösenord felaktigt eller om ditt lösenord ändrades på autentiseringsservern.

Menypunkt "Forget Temporary Trust"

Om du aktiverar *Temporary trust* via inställningarna *Settings - Security Settings* öppnas ett fönster varje gång du träffar på en icke pålitlig autentiseringsserver. I detta fönster kan du använda respektive server som temporär Trusted Server. Odyssey-klienten kommer ihåg denna Trusted Server så länge som den är konfigurerad i *Security Settings*.

Om listan med temporära Trusted-servrar skall raderas direkt, väljer du *Forget Temporary Trust*.

Du kan behöva den här menypunkten om du accepterar en server som temporär Trusted Server och därefter bestämmer dig för att avsluta anslutningen till den. Om du vill säkerställa att anslutningen bryts omedelbart, avaktiverar du *Session resumption* och klickar på *Reconnect* i fönstret *Connection*.

Odyssey Client Manager - menyn "Help"

Menyn *Help* omfattar följande menypunkter:

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

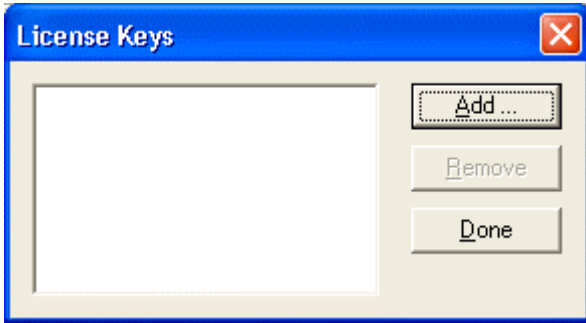
Menypunkt "Help topics"

Välj *Help Topics* för att komma till Odyssey-klientens hjälpsystem.

Du kan alltid få kontextrelaterad hjälp genom att trycka på knappen **F1**. Hjälpsystemet öppnas vid det kapitel där din momentana situation tas upp bäst.

Menypunkt "License keys"

Välj *License Keys* i hjälpmenyn för att förvalta dina Odyssey-klient-licensnycklar.



En licensnyckel är en text som visar licensen för användningen av Odyssey-klienten.

Kontextmeny "Odyssey"

Om du klickar med höger musknapp på Odyssey-symbolen i aktivitetsfältet, visas följande menypunkter:

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

Menypunkt "Odyssey for Fujitsu Siemens Computers"

Om du väljer menypunkten *Odyssey for Fujitsu Siemens Computers* visas Odyssey Client Manager (användargränssnittet för Odyssey-klienten).

Menypunkt "Enable Odyssey/Disable Odyssey"

Välj *Enable Odyssey* eller *Disable Odyssey* för att aktivera eller avaktivera Odyssey-klienten.

Till att börja med är Odyssey-klienten aktiverad och normalt sett behöver den inte avaktiveras. Om du väljer *Disable Odyssey Client* kopplas alla nätverkskort från utan att inställningarna i fönstret *Connection* förändras. Odyssey-klientprogrammet är fortfarande igång men det är helt fränkopplat från radionätverksanslutningarna.

Du bör endast avaktivera Odyssey-klienten om du har problem med din aktuella Odyssey-konfiguration. Du kan exempelvis avaktivera Odyssey-klienten, om du befarar att den har en osäker status och du vill säkerställa att du är fränkopplad från nätverket, fram till att du får möjlighet att kontrollera dina inställningar.

Det går även att aktivera och avaktivera Odyssey-klienten via Odyssey Client Manager.

Menypunkt "Help"

En av menypunkterna som visas när du klickar med höger musknapp på Odyssey-symbolen i aktivitetsfältet är *Help*. Två alternativ finns att välja mellan: *Help Topics* och *About*.

Om du väljer *Help Topics* visas hjälpsystemet i ett fönster med den öppnade innehållsförteckningen.

Om du väljer *About* visas produktversionen och copyrightinformation.

Menypunkt "Exit"

Om du väljer *Exit* stoppar Odyssey-klienten direkt användningen i bakgrunden. Det här alternativet vill du kanske ha när du inte skall använda radionätverket under en längre tid.

Du kan starta om Odyssey-klienten med hjälp av *Odyssey Client Manager* under *Start – Program – 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)...

Sökregister

802.11-nätverkssäkerhet 3
802.1X-autentisering 33
 beskrivning 4
 läge Open 31
 utan WEP-kryptonyckel 31
802.1X-standard 5

A

Access point (infrastructure mode) 31
AccessPoint 2
Adapters 12
Adhoc-läge 2
AES-datakryptering 31
Anonymous name 24
Anonymt namn, definiera 24
Användarnamn 19
Autentisering 4
 ange anslutningsläge 31
 automatisk kryptonyckelgenerering 32
 automatisk re-autentisering 48
 avancerade säkerhetsalternativ 46
 läge Open 31
 läge Shared 31
 läge WPA 31
 med profil 32
 WEP-kryptonyckel 4, 31
Autentiseringsprotokoll 21
 EAP 5
 EAP-TLS 21
 EAP-TTLS 22
 inre 23
 PEAP 21
Autentiseringsserver 21
 Enable Server temporary trust 42
 lägga till till Trust-trädet 39
 Server temporary trust 48
 Trusted Server 34
 verifiera identitet 21
Automatisk re-autentisering 48

B

Behörighetsbevis 5

C

CE-märkning 6
Certificate Authority 35
Certifikat 19, 35
Certifikatinformation, visa 41
Certifikatkedja 37
Certifikatnod, lägga till 38
CHAP 23

Close 49
Configure and Enable Wizard 9
Connect to any available network 30
Connection 12
 visa anslutningsstatus 15

D

Direktiv 1999/5/EG 6

E

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

F

Forget Password 50
Forget Temporary Trust 50
Fönster
 Adapters 12, 43
 Connection 12, 15
 Networks 12, 27
 Profiles 12, 16
 Trusted Servers 12, 34

I

IEEE-standard
 802.11a, frekvenser 7
 802.11b, frekvenser 8
Infrastruktur-läge 2
Inloggningsnamn 19
Inner Authentication Protocol 23
Installation, Odyssey-klient 9
Intermediate Certificates
 lägga till till Trust-trädet 39
 maximalt antal 41

K

Konfiguration, Odyssey-klient 11
Kontextmeny Odyssey 51

- L**
 - License keys 51
 - Lösenord
 - inmatning 19
 - inte spara 50
- M**
 - Meny
 - Commands 49
 - Help 50
 - Settings 46
 - MS-CHAP-V2. 23
- N**
 - Network name (SSID) 30
 - Networks 12, 27
 - Nätverk, söka 30
 - Nätverksanslutning
 - koppla från 15
 - re-autentisera 15
 - skapa 13
 - skapa (till valfritt nätverk) 30
 - styra 12
 - visa status 15
 - Nätverksbeskrivning 30
 - Nätverksbeteckning 28
 - Nätverkskort
 - aktivera 44
 - avaktivera 45
 - konfigurera 43
 - Nätverksnamn 28
 - Nätverkssäkerhet
 - autentisering 3
 - WEP-kryptonyckel 3
 - Nätverkstyp
 - adhoc 2
 - ange 31
 - infrastruktur 2
- O**
 - Odyssey Client Manager 11
 - visa 51
 - Odyssey-klient
 - avsluta 49, 52
 - installera 9
 - konfigurera 11
 - Odyssey-klient-licensnycklar 51
 - Odyssey-session, återuppta 47
 - Odyssey-symbol
 - inte visa i aktivitetsfältet 46
 - visa i aktivitetsfältet 46
 - Open, läge 31
- P**
 - PAP/Token 23
 - PEAP 32
 - PEAP Settings 25
 - Peer-to-peer (ad-hoc mode) 31
 - Peer-to-peer-läge 2
 - Pre-shared-kryptonyckel
 - beskrivning 4
 - mata in 33
 - Profiler, definiera 16
 - Profiles 12, 16
 - Pålitliga servrar, se Trusted Servers 34
- R**
 - Radiofrekvenser 7
 - Radioförbindelse, dålig 15
 - Radionätverk
 - IEEE 802.11-standard 1
 - konfigurera 27, 28
 - namn 3
 - Reconnect 15
 - Service Set Identifier (SSID) 3
 - skapa nätverksanslutning 13
 - söka 13
 - Radionätverkskort, konfigurera 44
- S**
 - Server temporary trust 48
 - Serverdomän 35
 - Shared, läge 31
 - Symboler och grafiska attribut 1
 - Säkerhetsföreskrifter 6
- T**
 - TKIP-kryptering 4, 31
 - Trusted Root Certificate Authority 43
 - Trusted Servers 12, 34
 - avancerad förtroendekontroll 37
 - enkel förtroendekontroll 35
 - lägga till 35
 - radera 36
 - redigera 36
 - Trust-träd 37
 - Trust-träd 37
 - lägga till certifikatnoder 38
 - ta bort certifikatnoder 41
 - visa 38
- U**
 - Untrusted Server 42

V,W

WEP-kryptonyckel 4

mata in 33

Wi-Fi Protected Access (WPA) 4

Wired-Equivalent Privacy (WEP) 4

WPA, beskrivning 4

WPA-autentisering 31

AES 31

lösenfras 32

pre-shared-kryptonyckel 32