Wi-Fi Protected Access (WPA) in een configuratievoorbeeld van Cisco Unified Wireless Network

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Conventies Ondersteuning van WPA en WPA2 Netwerkinstelling De apparaten voor WPA2 Enterprise Mode configureren Configureer de WLC voor RADIUS-verificatie via een externe RADIUS-server Configureer de WLAN voor WPA2 Enterprise Mode De RADIUS-server voor WPA2 Enterprise Mode-verificatie configureren (EAP-FAST) De draadloze client voor WPA2 Enterprise Mode configureren De apparaten configureren voor WPA2 Personal Mode Problemen oplossen Gerelateerde informatie

Inleiding

Dit document beschrijft hoe u Wi-Fi Protected Access (WPA) kunt configureren in een Cisco Unified Wireless Network.

Voorwaarden

Vereisten

Zorg ervoor dat u basiskennis van deze onderwerpen hebt voordat u deze configuratie probeert:

- WPA
- Draadloze LAN (WLAN)-beveiligingsoplossingen**N.B.:** Raadpleeg <u>Cisco Wireless LAN</u> <u>Security - Overzicht</u> voor informatie over Cisco WLAN-beveiligingsoplossingen.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco 1000 Series lichtgewicht access point (LAP)
- Cisco 4404 draadloze LAN-controller (WLC) waarop firmware 4.2.61.0 wordt uitgevoerd
- Cisco 802.11a/b/g-clientadapter waarop firmware 4.1 wordt uitgevoerd
- Aironet Desktop Utility (ADU) werkt met firmware 4.1
- Cisco Secure ACS-server versie 4.1

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg <u>Cisco Technical Tips Conventions</u> (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Ondersteuning van WPA en WPA2

Het Cisco Unified Wireless Network biedt ondersteuning voor de Wi-Fi Alliance-certificeringen WPA en WPA2. WPA is geïntroduceerd door de Wi-Fi Alliance in 2003. WPA2 werd geïntroduceerd door de Wi-Fi Alliance in 2004. Alle producten die Wi-Fi-gecertificeerd zijn voor WPA2 moeten compatibel zijn met producten die Wi-Fi-gecertificeerd zijn voor WPA.

WPA en WPA2 bieden een hoge mate van zekerheid voor eindgebruikers en netwerkbeheerders dat hun gegevens privé zullen blijven en dat de toegang tot hun netwerken wordt beperkt tot geautoriseerde gebruikers. Beide hebben persoonlijke en bedrijfsmodi die voldoen aan de specifieke behoeften van de twee marktsegmenten. In de Enterprise-modus van elk programma worden IEEE 802.1X en EAP gebruikt voor verificatie. De persoonlijke modus van elk gebruik van Pre-Shared Key (PSK) voor verificatie. Cisco raadt geen Personal Mode aan voor bedrijfs- of overheidimplementaties, omdat het een PSK gebruikt voor gebruikersverificatie. PSK is niet veilig voor ondernemingsmilieu's.

Met WPA worden alle bekende WEP-kwetsbaarheden in de oorspronkelijke IEEE 802.11beveiligingsimplementatie aangepakt en wordt een onmiddellijke beveiligingsoplossing voor WLAN's in zowel ondernemingen als in SOHO-omgevingen (Small Office/Home Office) geïntroduceerd. WPA maakt gebruik van TKIP voor de codering.

WPA2 is de volgende generatie van Wi-Fi-beveiliging. Het is de interoperabele implementatie van de Wi-Fi Alliance van de geratificeerde IEEE 802.11i norm. Het implementeert het door het National Institute of Standards and Technology (NIST) aanbevolen AES-encryptie-algoritme met behulp van Counter Mode met Cycle Block Chaining Message Authenticatie Code Protocol (CCMP). WPA2 vergemakkelijkt de naleving van FIPS 140-2 van de overheid.

Vergelijking van WPA- en WPA2-modemtypen

	WPA	WPA2
	Verificatie:	Verificatie:
Entorprise Made	IEEE	IEEE
Bedriif Overbeid	802.1X/EA	802.1X/EA
(Dedriji, Overneid, Onderwijs)	Р	Р
	Encryptie:	 Versleuteli
	TKIP/MIC	ng: AES-

orificatio	 Verificatie[.]
SK ncryptie: KIP/MIC	 PSK Versleuteli ng: AES-
	SK ncryptie: KIP/MIC

In de Enterprise-modus gebruiken zowel WPA als WPA2 802.1X/EAP voor verificatie. 802.1X biedt WLAN's met sterke wederzijdse verificatie tussen een client en een verificatieserver. Daarnaast biedt 802.1X dynamische coderingssleutels per gebruiker, per sessie, waardoor de administratieve belasting en beveiligingsproblemen met betrekking tot statische coderingssleutels worden verwijderd.

Met 802.1X worden de aanmeldingsgegevens die voor de verificatie worden gebruikt, zoals aanmeldingswachtwoorden, nooit op het draadloze medium verzonden, of zonder encryptie. Terwijl 802.1X-verificatietypen zorgen voor sterke verificatie voor draadloze LAN's, zijn TKIP of AES nodig voor codering, naast 802.1X-codering omdat de standaard 802.11 WEP-codering kwetsbaar is voor netwerkaanvallen.

Er bestaan verschillende 802.1X-verificatietypen, die elk een andere benadering van verificatie bieden en tegelijkertijd vertrouwen op hetzelfde framework en EAP voor communicatie tussen een client en een toegangspunt. Cisco Aironet-producten ondersteunen meer 802.1X EAPverificatietypen dan andere WLAN-producten. Ondersteunde typen zijn onder meer:

<u>Cisco LEAP</u>

- EAP-Flexibele verificatie via beveiligde tunneling (EAP-FAST)
- EAP-Transport Layer Security (EAP-TLS)
- Protected Extensible Verification Protocol (PEAP)
- EAP-Tunneling (EAP-TTLS)
- EAP-Subscriber Identity Module (EAP-SIM)

Een ander voordeel van 802.1X-verificatie is gecentraliseerd beheer voor WLANgebruikersgroepen, inclusief op beleid gebaseerde sleutelrotatie, dynamische sleuteltoewijzing, dynamische VLAN-toewijzing en SSID-beperking. Deze functies roteren de coderingstoetsen.

In de persoonlijke werkwijze wordt een vooraf gedeelde sleutel (wachtwoord) gebruikt voor verificatie. Voor de persoonlijke modus zijn alleen een toegangspunt en clientapparaat nodig, terwijl voor de Enterprise-modus doorgaans een RADIUS of andere verificatieserver op het netwerk nodig is.

Dit document bevat voorbeelden voor het configureren van WPA2 (Enterprise-modus) en WPA2-PSK (Persoonlijke modus) in een Cisco Unified Wireless-netwerk.

Netwerkinstelling

In deze installatie worden een Cisco 4404 WLC en een Cisco 1000 Series LAP aangesloten via een Layer 2-Switch. Een externe RADIUS-server (Cisco Secure ACS) is ook verbonden met dezelfde switch. Alle apparaten bevinden zich in hetzelfde subnetje. Het toegangspunt (LAP) is aanvankelijk geregistreerd bij de controller. Er moeten twee draadloze LAN's worden gemaakt, één voor de WPA2 Enterprise-modus en één voor de WPA2 Personal-modus.

WPA2-Enterprise mode WLAN (SSID: WPA2-Enterprise) gebruikt EAP-FAST voor het verifiëren van de draadloze clients en AES voor codering. Cisco Secure ACS-server wordt gebruikt als de externe RADIUS-server voor verificatie van de draadloze clients.

WPA2-Personal mode WLAN (SSID: WPA2-PSK) gebruikt WPA2-PSK voor de verificatie met de vooraf gedeelde sleutel "backdefghijk".

U dient de apparaten voor deze installatie te configureren:



WLC Management IP address: WLC AP Manager IP address: Wireless Client IP address:	10.77.244.204 10.77.244.205 10.77.244.221
Cisco Secure ACS server IP address	10.77.244.196
Subnet Mask used in this example	255.255.255.224

De apparaten voor WPA2 Enterprise Mode configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Voer deze stappen uit om de apparaten te configureren voor de werkmodus WPA2 Enterprise:

- 1. Configureer de WLC voor RADIUS-verificatie via een externe RADIUS-server
- 2. Het WLAN configureren voor WPA2 Enterprise Mode Verification (EAP-FAST)
- 3. <u>De draadloze client voor WPA2 Enterprise Mode configureren</u>

Configureer de WLC voor RADIUS-verificatie via een externe RADIUS-server

De WLC moet worden geconfigureerd om de gebruikersreferenties te kunnen doorsturen naar een externe RADIUS-server. De externe RADIUS-server valideert vervolgens de gebruikersreferenties met EAP-FAST en biedt toegang tot de draadloze clients.

Voltooi deze stappen om WLC voor een externe RADIUS-server te configureren:

- 1. Kies **Beveiliging** en **RADIUS-verificatie** in de GUI van de controller om de pagina RADIUSverificatieservers weer te geven. Klik vervolgens op **Nieuw** om een RADIUS-server te definiëren.
- 2. Definieer de RADIUS-serverparameters op de **RADIUS-verificatieservers > Nieuwe** pagina. Deze parameters omvatten:IP-adres voor RADIUS-serverGedeeld

geheimPoortnummerServerstatusDit document gebruikt de ACS-server met een IP-adres van

10.7.244.196.

ahaha					Sage Co	infiguration Ping	Logout Befresh
CISCO	MONITOR WLANS CONTRO	OLLER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
Security	RADIUS Authentication S	ervers > New				< Back	Apply
AAA General RADIUS Authentication Accounting TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients	Server Index (Priority) Server IPAddress Shared Secret Format Shared Secret	1 • 10.77.244.196 ASCII •				5	
User Login Policies AP Policies	Confirm Shared Secret	****					
Local EAP	Key Wrap	(Designed for F)	IPS customers	and requires a ke	y wrap compliant	t RADIUS server)	
Priority Order	Dort Number	1012					
♦ Access Control Lists	Port Number	1012					
 Wireless Protection Policies 	Server Status	Enabled 💌					
▶ Web Auth	Support for RFC 3576	Enabled 💌					
Advanced	Server Timeout	2 seconds					
	Network User	🗷 Enable					
	Management	Enable Enable					
	IPSec	🗆 Enable					

3. Klik op Apply (Toepassen).

Configureer de WLAN voor WPA2 Enterprise Mode

Configureer vervolgens het WLAN dat de clients zullen gebruiken om verbinding met het draadloze netwerk te maken. De WLAN SSID voor WPA2-Enterprise zal WPA2-Enterprise zijn. Dit voorbeeld wijst dit WLAN toe aan de beheerinterface.

Voltooi deze stappen om WLAN en de bijbehorende parameters te configureren:

- 1. Klik op **WLAN's** vanuit de GUI van de controller om de WLAN-pagina weer te geven.Deze pagina maakt een lijst van de WLAN's die op de controller bestaan.
- 2. Klik op **Nieuw** om een nieuw WLAN te maken.
- Voer de WLAN SSID-naam en de profielnaam in op de WLAN's > Nieuwe pagina. Klik vervolgens op Toepassen.Dit voorbeeld gebruikt WPA2-Enterprise als de SSID.

							Sa <u>v</u> e Co	onfiguration Eing	Logout Befr
CISCO	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
WLANs	WLANs>	New						< Back	Apply
WLANS	Туре		WLAN						
▶ Advanced	Profile Nar	me	WPA2-Ent	erprise					
	WLAN SSI	D	WPA2-Ent	erprise					

- 4. Zodra u een nieuw WLAN maakt, wordt de pagina WLAN > Bewerken voor het nieuwe WLAN weergegeven. Op deze pagina kunt u verschillende parameters definiëren die specifiek zijn voor dit WLAN. Dit omvat Algemeen Beleid, Beveiligingsbeleid, QOS-beleid en Geavanceerde parameters.
- 5. Onder Algemeen beleid schakelt u het selectievakje **Status** in om het WLAN in te schakelen.

alulu			Sage (Configuration Eing Logout Befresh
CISCO	MONITOR WLANS CONTROLLI	R WIRELESS SECURITY	MANAGEMENT COMMANDS	HELP
WLANs	WLANs > Edit			< Back Apply
WI ANS	General Security QoS	Advanced		
WLANS				
Advanced	Profile Name WPA2	-Enterprise		
	Type WLAN			
	SSID WPA2	-Enterprise		
	Status 🗹 En	abled		
	Security Policies [WP/	2][Auth(802.1X)]	will appear after applying the char	land)
	(Hour	cessing done under security ces	will appear arter apprying the cha	1903-7
	Radio Policy All			
	Interface	gement 💌		
	Broadcast SSID	bled		
	Foot Notes			
	1 CKIP is not supported by 10xx m 2 Web Policy cannot be used in col	odel APs nbination with IPsec		
	3 H-REAP Local Switching is not su 4 When client exclusion is enabled	ported with IPsec, CRANITE aut a Timeout Value of zero means	hentication infinity (will require administrativ	e override to reset excluded clients)
	S Client MFP is not active unless W	PA2 is configured		

- 6. Als u wilt dat het toegangspunt de SSID uitzendt in de beacon-frames, vinkt u het aanvinkvakje **Broadcast SSID aan**.
- 7. Klik op het tabblad **Beveiliging**. Kies onder Layer 2 Security de optie **WPA+WPA2**.Dit schakelt WPA-verificatie in voor het WLAN.

cisco	Sage Configuration Bing Logout Befresh MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANS	WLANs > Edit < Back Apply General Security QoS Advanced
WLANs Advanced	Layer 2 Layer 3 AAA Servers Layer 2 Security WPA+WPA2 MAC Filtering Static WEP Parameters
	802.11 Data Encryption Current Key: 104 bits WEP Static Key (Key Index = 0) Type Key Size Key Index Encryption Key WEP not set 1 ASCII
	CKIP Parameters & 802.11 Data Encryption Current Key: 0 bits CKIP Key (Key Index= 0) Key Size Key Index Encryption Key Key Format
	Foot Notes
	1 CKIP is not supported by 10xx model APs 2 Web Policy cannot be used in combination with IPsec 3 H-REAP Local Switching is not supported with IPsec, CRANITE authentication 4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients) 5 Client MIP is not active unless WPA2 is configured

8. Blader naar beneden om de WPA+WPA2-parameters aan te passen. In dit voorbeeld zijn WPA2 Policy en AES encryptie

geselecteerd.				
ակսիս			Save Configuration + Eing	Logout <u>R</u> efresh
CISCO 🔤	ONITOR WLANS CONTR	COLLER WIRELESS SECURITY MANAGEMENT	COMMANDS HELP	
WLANs W	/LANs > Edit		< Back	Apply
WLANS W WLANS WLANS Advanced	ALANS > Edit General Security Layer 2 Layer 3 002.11 Data Encryption MMH Mode Key Permutation 802.11 Data Encryption 802.11 Data Encryption 802.11 Data Encryption 802.11 Data Encryption WPA+WPA2 Parameters WPA2 Policy WPA2 Policy WPA2 Encryption Auth Key Mgmt 4 Foot Notes 1 CKIP is not supported by IN 2 Web Policy coanot be used by IN 3 W-BEAP Local Switching is in 4 When cleat exclusion is en	QoS Advanced AAA Servers	E edministrative override to reset exclu	Apply

- 9. Kies onder Auth Key Management **802.1x**.Dit schakelt WPA2 in met 802.1x/EAP-verificatie en AES-encryptie voor het WLAN.
- 10. Klik op het tabblad **AAA-servers**. Kies onder Verificatieservers het juiste IP-adres van de server. In dit voorbeeld wordt 10.77.24.196 gebruikt als de RADIUS-

cisco	MONITOR V	VLANS CO	NTROLLER	WIRELESS	SECURITY	MANAGEMENT		HELP	Eng I	.ogout <u>B</u> efre
UANS WLANS WLANS Advanced	WLANS > E General Layer 2 Select AA Radius Se Server 1 Server 3 Local EAP Local EAP Local EAP	dit Security Layer 3 A servers be rvers Authentica [IP:10.77.2] None None None Authentica AP Authentica	QoS AAA Se clow to ove tion Server 44.196, Port tion tion tion p 10xx mode red in combin is not support	Advanced rvers rride use of rs Acc is Acc is No is No is No is Acc is A	default serve ounting Serve inabled ne • ne •	rs on this WLAN LDAP Server ers Server 1 Server 2 Server 3	None x None x	HELP < Ba	ack	Apply

11. Klik op Apply (Toepassen).Opmerking: dit is de enige EAP-instelling die op de controller moet worden geconfigureerd voor EAP-verificatie. Alle andere configuraties die specifiek zijn voor EAP-FAST, moeten worden uitgevoerd op de RADIUS-server en de clients die moeten worden geverifieerd.

De RADIUS-server voor WPA2 Enterprise Mode-verificatie configureren (EAP-FAST)

In dit voorbeeld wordt Cisco Secure ACS gebruikt als de externe RADIUS-server. Voer de volgende stappen uit om de RADIUS-server te configureren voor EAP-FAST-verificatie:

- 1. Een gebruikersdatabase maken om clients te verifiëren
- 2. Voeg de WLC als AAA-client toe aan de RADIUS-server
- 3. <u>EAP-FAST-verificatie op de RADIUS-server configureren met anonieme in-band PAC-provisioning</u>Opmerking: EAP-FAST kan worden geconfigureerd met Anonymous In-band PAC Provisioning of Authenticated In-band PAC Provisioning. In dit voorbeeld wordt anonieme in-band PAC Provisioning gebruikt. Zie <u>EAP-FAST-verificatie met draadloze LAN-controllers</u> en <u>externe RADIUS-serverconfiguratievoorbeeld voor</u> gedetailleerde informatie en voorbeelden voor het configureren van EAP FAST met anonieme in-band PAC-provisioning <u>en geverifieerde in-band provisioning</u>.

Een gebruikersdatabase maken voor verificatie van EAP-FAST-clients

Voltooi deze stappen om een gebruikersdatabase te maken voor EAP-FAST-clients op de ACS. In dit voorbeeld worden de gebruikersnaam en het wachtwoord van de EAP-FAST-client respectievelijk ingesteld als Gebruiker1 en Gebruiker1.

1. Selecteer vanuit de ACS GUI in de navigatiebalk de optie Gebruikersinstelling. Maak een nieuwe draadloze gebruiker en klik vervolgens op Toevoegen/Bewerken om naar de pagina Bewerken van deze gebruiker te

File Edit View Fa	worites Tools Help	Links ** Oos
Address http://127.	0.0.1:1065/	• D 00
Cisco Svorems	User Setup	×.
Cisco System User Setup Configuration	Sebect Sebect User: User1 Find Add/Edit List users beginning with letter/number: ABCDKFCHISKLM NOPOBSITYYTYT OlddfSCT List all users Remove Dynamic Users Back to Help	 Help Stars Sature and External User Databases Stars Sature and External User Databases Configure 10 Stars 10 Stars 10 Starbases Addres a User to the ACS Internal Databases Listing Usernames that Deain with a Particular Cheracter Listing Usernames that Deain with a Particular Cheracter Listing Usernames in the ACS Internal Outabase Listing Usernames in the ACS Internal Outabase Listing a December of the ACS Internal Outabase Listing a User to the ACS Internal Outabase Listing a User setue in the ACS Internal Outabase Remove Opeand: User User Setue enables you to configure individual user information, add users, and delete users in the ACS Internal User Database Refere ACS can authenticate users with an external user database Star Setue enables you to configure individual user information, add users, and delete users in the ACS internal on the Database Star Setue enables you to configure individual user information, add users, and delete users in the ACS internal on the Database You must have the database users and running on the external user for a starter of the applicable parameters in the External User Databases You must have configuration overrides Group Setue configuration. If you rely on the Unknown User Policy in the External User Databases sections to create entries in the ACS internal database for users defined in an external user database, usernames cannot be located or listed here until the user database. Itself, Fer added security, authorization, and accessing out the database. User Setue bases to exis of users to a streterization, and accessing user database. User Starp here to access in the ACS internal database. Note: User Setue bases to exis of users to the authorization, and accessing user database. User Starp here
		To find a user already in the ACS internal database, type the first few latters of the usersame in the User field, add an asterisk (*) as a widdard, and click Field. From the list of usersames displayed, click the usersame whose information you want to view or change.

2. Van de Instelling van de Gebruiker Bewerk pagina, vorm Echte Naam en Beschrijving evenals de Wachtwoordinstellingen zoals in dit voorbeeld.Dit document maakt gebruik van ACS Interne Database voor

wachtwoordverificatie.

ess [@] http://127.0.	0.1:1065/	
isco Svorems	User Setup	
adhaadha.	Edit	Help
User Setup	User: User1 (New User)	Account Disabled Deleting a Username
Setup SharedProfile Components	Account Disabled	Supplementary User Infe Password Authentikation Group to which the user is assigned
Network Configuration	Supplementary User Info 💡	Callback Client 3P. Address Assignment Advanced Settlings
System Configuration	Real Name Description	Network Access Restrictions Has Session Usage Destas Access Network
Interface Configuration		Account Unsets Devening adable AfLs Advanced TACACS+ Sections TACACS+ Control
Control External User Databases	User Setup	TACACS - Control Control TACACS - Control Parament TACACS - Outboard Parament TACACS - Outboard Parament TACACS - Solid Commund Authorization
Posture Validation	Password Authentication:	Command Authorization for Network Device Hanagement Applications TACACS + Unknown Services TIT RADIUS Attributes
Network Access Profiles	CiscoSecure PAP (Also used for CHAP/MS- CHAP/ARAP, if the Separate field is not	RADIUS Yeadar-Specific Attributes
Reports and Activity	Password •••••	Account Disabled Status
Documentation	Password	Safect the Account Disabled check bow to disable this account: clear the check box to enable the account.
	Separate (CHAP/MS-CHAP/ARAP) Dassword	[Back to Tep]
	Confirm	Deleting a Username The Delete botton area are solv when you are edition to existing over
	Submit Cancel	account not before appears and ding a new year account. To delete the current user account from the database, click Delete . When asked to

- 3. Kies ACS Interne Database uit de vervolgkeuzelijst Wachtwoordverificatie.
- 4. Configureer alle andere vereiste parameters en klik op Indienen.

Voeg de WLC als AAA-client toe aan de RADIUS-server

Voltooi deze stappen om de controller te definiëren als een AAA-client op de ACS-server:

- 1. Klik op **Netwerkconfiguratie** vanuit de ACS GUI. Klik onder de sectie AAA-client toevoegen op de pagina Netwerkconfiguratie op **Add Entry** om WLC als AAA-client aan de RADIUSserver toe te voegen.
- Definieer op de AAA-clientpagina de naam van de WLC, het IP-adres, de gedeelde geheimen verificatiemethode (RADIUS/Cisco Aironet). Raadpleeg de documentatie van de fabrikant voor andere niet-ACSverificatieservers.

Cisco Systems	Network Configuration	2
addissaddiss.	-dit	🗅 Help
Group Setup	Add AAA Client	Add Cleant Heatmann Add Cleant Heatman Shared Secont Shared Secont Network Revice Group Ref(0): Key Wran
V Components Net work Configuration	AAA Client Hostname WLC AAA Client IP Address 10.77.244.204	AnthenState Using AnthenState Using Single Connect TACACS- AAA Client Leg Update./Watchdog Packets from this AAA Client Leg RADIUS Tunneling Packets from this
Configuration	Shared Secret Cisco	Add. Cleast • Replace RADIUS Part info with Username from this Add. Cleast • Match Framed IP-Address with user IP address for accounting packets from this Add. Cleast
Doternal User Databases Posture Validation	Key Encryption Key Message Authenticator Code Key	AAA Client Hostname
Network Access Profiles	Key Input Format CASCII @ Hexadecimal	The AAA Client Hostname is the name assigned to the AAA client.
Reports and Activity	Authenticate Using RADIUS (Cisco Airespace)	(Back to Tep)
0nline Documentation	Single Connect TACACS+ AAA Client (Record stop in accounting on failure)	AAA Client IP Address
	Log Update/Watchdog Packets from this AAA Client Log RADIUS Tunneling Packets from this AAA Client	The AAA Client IP Address is the IP address assigned to the AAA client.
	Replace RADIUS Port info with Username from this AAA Client	If you want to designate more than one AAA client with a single AAA client entry in ACS, you can
	Match Framed-IP-Address with user IP address for accounting packets from this AAA Client	specify the IP address for each AAA client to be represented by this A&A client antro To

Opmerking: De gedeelde geheime sleutel die u op de WLC en de ACS-server configureren moet overeenkomen. Het gedeelde geheim is hoofdlettergevoelig.

3. Klik op Indienen+Toepassen.

EAP-FAST-verificatie op de RADIUS-server configureren met anonieme in-band PAC-provisioning

Anonieme in-band provisioning

Dit is een van de twee in-band provisioningmethoden waarin de ACS een beveiligde verbinding met de eindgebruiker-client tot stand brengt met als doel de klant een nieuwe PAC te geven. Deze optie maakt een anonieme TLS-handdruk mogelijk tussen de eindgebruiker client en ACS.

Deze methode werkt in een geverifieerde Diffie-Hellman-Key Overeenkomst Protocol (ADHP)tunnel voordat de peer de ACS-server authenticeert.

Voor de ACS is EAP-MS-CHAPv2-verificatie van de gebruiker vereist. Bij een succesvolle gebruikersverificatie creëert de ACS een Diffie-Hellman-tunnel met de eindgebruiker-client. De ACS genereert een PAC voor de gebruiker en verstuurt deze naar de eindgebruiker client in deze tunnel, samen met informatie over deze ACS. Bij deze provisioningmethode wordt EAP-MSCHAPv2 gebruikt als de verificatiemethode in fase nul en EAP-GTC in fase twee.

Omdat een niet-geverifieerde server is voorzien, is het niet mogelijk om een wachtwoord in onbewerkte tekst te gebruiken. Daarom kunnen alleen MS-CHAP referenties worden gebruikt binnen de tunnel. MS-CHAPv2 wordt gebruikt om de identiteit van de peer aan te tonen en om een PAC te ontvangen voor verdere verificatiesessies (EAP-MS-CHAP wordt alleen als interne methode gebruikt).

Voltooi deze stappen om EAP-FAST-verificatie in de RADIUS-server te configureren voor anonieme in-band provisioning:

1. Klik op **Systeemconfiguratie** vanuit de RADIUS-server GUI. Kies op de pagina Systeemconfiguratie de optie **Globale verificatie**



 Klik op de pagina Globale verificatie-instellingen op EAP-FAST-configuratie om naar de EAP-FAST-instellingenpagina te gaan.

ress [] http://127.	0.0.1:1065/	
Cisco Systems	System Configuration	2
à Lillear	EAP Configuration	A Help
Setup Setup Shared/hoffs Configuration Surterizer Surterizer Surterizer Configuration Surterizer Configuration Configuration Administration Control External User	PEAP Allow EAP-MSCHAPv2 Allow EAP-GTC Allow Posture Validation Allow EAP-TLS Select one or more of the following options: Certificate SAN comparison Certificate CN comparison Certificate Binary comparison EAP-TLS session timeout (minutes): 120	Use this page to specify settings for various authentication protocols. • EAP Configuration • PTAP • EAP-RAST • EAP-RS • EAP-RS • EAP-RS • EAP-RSS • EAP-RSS • EAP-RSS • EAP-RSS • EAP-Request Timesout • VS-CHAP Configuration EAP Configuration
Posture Validation	Cisco client initial message: PEAP session timeout (minutes): Enable Fast Reconnect: EAP-FAST	authentication information (RFC 2284), EAP is layered on tap of another protocol such as UDP, 802.3x or RADIUS and supports multiple "authentication" types. [Back to Top] PEAP PEAP is the outer layer protocol for the secure tunnel.
	EAP-FAST Configuration EAP-TLS Callow EAP-TLS Select one or more of the following options: Certificate SAN comparison Submit Submit + Restart Cancel	Aleber AEAP is a certificate-based authentication proton. AEAP authentication can occur only after you have completed the required stops as the ACS Certificate Setup page. • Allow EAP-MSCHAPv2 – Use to enable EAP-MSCHAPv2 within MS PEAP authentic ation. Enable this protocol for any repository that supports MS- CHAPv2, such as Microsoft AD, and the ACS Internal Database.

 Selecteer op de pagina EAP-FAST-instellingen het aanvinkvakje Allow EAP-FAST om EAP-FAST in te schakelen op de RADIUSserver.

GscoSecure ACS - M	Skrosoft Internet Explorer	LIDIX
Ele Edt Yew Fav	onites Iools Help	Lirks 🍟 🤱
Address http://127.0	.0.1:1065/	💌 🛃 Go
CISCO STOTEMS	Sustan Configuration	×
بابر بابر	System Configuration	
ad the address	EAP-FAST Configuration	A Help
User.		
C Decib	EAD-EART Politicar	EAP-FAST Configuration Page
Setup	EAP-FAST settings	Use this page to configure EAP-FAST authentication settings.
(b. SharedProfile	EAP-FAST	EAD-EAST Sutting
10 Components	M Allow EAP-FAST	Client initial message
Network Configuration	Active master key TTL 1 months	Authority ID Infe
and the consideration	Retired master key TTL 3 months 🕱	Allow astrophess in band PAC previousing Allow authenticated in-band PAC previousing
Sustem Configuration		Allow machine authentication
	Tunnel PAC TTL 1 Weeks	Allow stateless session resume
Configuration	Client initial message: tacwebacs	Certificate Comparison
-90 LAdministration	Authority ID Info: tacwebacs	EAP-TLS session timeout (minutes)
Centrel	Allow approximate in-band DAC provisioning	EAP-FAST mester server Actual EAP-FAST server status
Doternal User	E show anonymous in-band PAC provisioning	
D C T Databases	C Allow authenticated in-band PAC provisioning	EAP-FAST Settings
Posture Validation	Accept client on authenticated provisioning	Allow EAD-EAST-To anable EAD-EAST authentication, select this check
	Require client certificate for provisioning	box.
Profiles	C Allow Machine Authentication	a define the fact for Weight and the factor of the second of the second s
Reports and	Machine PAC TTL 1 weeks	 Active Marter Key TiL –Enter a value for the amount of time that a master key is used to generate new Protected Access Credentials (PACs). When the
Activity	E Allow Stateless session resume	time to live (TTL) defined for the Master Key expires, the master key is considered retired and a new master key is generated.
Online Descentation	tuthorization 010 TTI	
Caller conversion	Authonization PAC TTL 1 nours	 Retired master key TREnter a value for the amount of time that PACs dependented using a setting master key are acceptable for EAD-EAST
	Allowed inner methods	authentication. When an end-user client gains network access using a PAC
	R EAP-GTC	based on a retired master key, ACS sends a new PAC to the end-user client.
	EAP-MSCHAPv2	 Tunnel PAC TEL - Enter a value for the amount of time that a PAC is used
	EAP-TLS	before it expires and must be replaced. If the master key used to generate the Tunnel PAC has not expired, new PAC creation and assignment is
	Submit Submit + Restart Cancel	automatic. If the master key used to generate the Tunnel PAC expired, automatic or manual provinging must be used to provide the endruger
		client with a new PAC.
2		Internet
💐 Start 🕞 🥭	CiscoSecure ACS - Mic	👮 7:58 PM

- 4. Configureer de TTL-waarden (Time-to-Live) van de actieve/uitgestelde hoofdsleutel zoals gewenst of stel deze in op de standaardwaarde zoals in dit voorbeeld.Raadpleeg Master Keys voor meer informatie over actieve en uitgestelde master keys. Raadpleeg ook Master Keys en PAC TTL's voor meer informatie.Het veld Autoriteit ID Info geeft de tekstidentiteit van deze ACS-server weer, die een eindgebruiker kan gebruiken om te bepalen welke ACS-server moet worden geverifieerd. Dit veld invullen is verplicht.In het veld Bericht voor eerste weergave van client wordt een bericht ingesteld dat moet worden verzonden naar gebruikers die verificatie uitvoeren met een EAP-FAST-client. De maximale lengte is 40 tekens. Een gebruiker ziet het eerste bericht alleen als de eindgebruikerclient de weergave ondersteunt.
- 5. Als u wilt dat de ACS anonieme in-band PAC-levering uitvoert, controleer dan het vakje **Anonieme in-band PAC-levering toestaan**.
- 6. Toegestane interne methoden—Deze optie bepaalt welke interne EAP-methoden kunnen worden uitgevoerd binnen de EAP-FAST TLS-tunnel. Voor anonieme in-band provisioning moet u EAP-GTC en EAP-MS-CHAP inschakelen voor compatibiliteit met de achterwaartse modus. Als u Anonieme in-band PAC-levering toestaan selecteert, moet u EAP-MS-CHAP (fase nul) en EAP-GTC (fase twee) selecteren.

De draadloze client voor WPA2 Enterprise Mode configureren

De volgende stap is het configureren van de draadloze client voor de modus WPA2 Enterprise.

Voltooi deze stappen om de draadloze client te configureren voor de WPA2 Enterprise-modus.

1. Klik vanuit het venster van het Aironet Desktop Utility op **Profielbeheer > Nieuw** om een profiel te maken voor de WPA2-Enterprise WLAN-gebruiker.Zoals eerder vermeld, gebruikt dit document de WLAN/SSID-naam als WPA2-Enterprise voor de draadloze client.

2. Klik vanuit het venster Profielbeheer op het tabblad **Algemeen** en configureer de profielnaam, de clientnaam en de SSID-naam zoals in dit voorbeeld. Klik vervolgens op **OK**

Profile M	anagement		? 🗙
General	Security Advanc	ed	
Profile	e Settings Profile Name:	WPA2-Enterprise	
	Client Name:	Wireless-Client1	
Netw	ork Names		
	SSID1:	WPA2-Enterprise	
	SSID2:		
	SSID3:		
		ΟΚ	Cancel

 Klik op het tabblad Beveiliging en kies WPA/WPA2/CCKM om de WPA2-bedrijfsmodus in te schakelen. Kies onder WPA/WPA2/CCKM EAP-Type EAP-FAST. Klik op Configureren om de EAP-FAST-instelling te configureren.

Profile Management		? 🗙
General Security Advanced		
- Set Security Options		
⊙ WPA/WPA2/CCKM	WPA/WPA2/CCKM EAP Type: EAP-FAST	
WPA/WPA2 Passphrase		
○ 802.1x	802.1x EAP Type: LEAP	
O Pre-Shared Key (Static WEP)		
○ None		
Configure	Allow Association to Mixed Cells	
	Limit Time for Finding Domain Controller To: 0 0 sec	
Group Policy Delay:	60 🗘 sec	
	OK C	ancel

4. Schakel in het venster EAP-FAST configureren het aanvinkvakje Automatisch PACprovisioning toestaan in. Als u anonieme PAC-levering wilt configureren, wordt EAP-MS-CHAP gebruikt als de enige interne methode in fase nul.

onfigure EAP-FAST	2 💈
EAP-FAST Authentication Method	
MSCHAPv2 User Name and Password	Configure
Protected Access Credentials (PAC)	
Select One or More PAC Authorities	
 Use Any PAC Belonging to the Same Group Allow Automatic PAC Provisioning 	Manage
Use Machine Information for Domain Logon	
	OK Cancel

- 5. Kies MSCHAPv2 Gebruikersnaam en wachtwoord als verificatiemethode in het vervolgkeuzevenster EAP-FAST-verificatiemethode. Klik op **Configureren**.
- Kies in het venster Gebruikersnaam en wachtwoord instellen voor MSCHAPv2 de juiste gebruikersnaam en wachtwoord. In dit voorbeeld wordt automatisch om gebruikersnaam en wachtwoord gevraagd.

Always Resume the Secu	re Session	
Validate Server Identity		
isted Root Certification Au	thorities	
\ny>		~
er Name and Password S	ettings	
💿 Use Temporary User	Name and Password	
🔘 Use Windows I	Jser Name and Password	
 Automatically P 	rompt for User Name and Password	l.
Manually Promp	ot for User Name and Password	
O Use Saved User Nar	ne and Password	
User Name:	Administrator	
Password:		
Confirm Password:		
Domain		
And the second se	L	
—		

ezelfde gebruikersnaam en wachtwoord dienen te worden geregistreerd bij de ACS. Zoals eerder vermeld, gebruikt dit voorbeeld respectievelijk Gebruiker1 en Gebruiker1 als gebruikersnaam en wachtwoord. Merk ook op dat dit een anonieme in-band levering is. Daarom kan de client het servercertificaat niet valideren. U dient ervoor te zorgen dat het aanvinkvakje Server Identity valideren niet is ingeschakeld.

7. Klik op **OK**.

Controleer de activiteitsmodus van WPA2 Enterprise.

Voltooi deze stappen om te verifiëren of uw configuratie van de WPA2 Enterprise-modus correct werkt:

- 1. Selecteer in het venster van het Aironet Desktop Utility het profiel **WPA2-Enterprise** en klik op **Activeren** om het profiel van de draadloze client te activeren.
- 2. Als u MS-CHAP ver2 hebt ingeschakeld als uw verificatie, zal de client u om de

Enter Wireless N	etwork Password 🗙
Please enter your E/ network	AP-FAST username and password to log on to the wireless
User Name :	User1
Password :	•••••
Log on to :	
Card Name :	Cisco Aironet 802.11 a/b/g Wireless Adapter
Profile Name :	WPA-Enterprise
	OK Cancel

vragen.

3. Tijdens EAP-FAST-verwerking van de gebruiker wordt u door de client gevraagd om PAC aan te vragen bij de RADIUS-server. Wanneer u op **Ja** klikt, wordt de PAC-provisioning gestart.

EAP-FAST Authentication	×
You do not have a valid PAC from the authentication server. Do you want to proceed and request automatic provisioning?	
Yes No	

4. Na succesvolle PAC-levering in fase nul volgen fase één en twee en vindt een succesvolle verificatieprocedure plaats.Na succesvolle verificatie wordt de draadloze client gekoppeld aan WLAN WPA2-Enterprise. Dit is de screenshot:

😤 Cisco Aironet Desktop Utility	y - Current Profile: WPA2-E	nterprise (? 🗙
<u>A</u> ction <u>O</u> ptions <u>H</u> elp			
Current Status Profile Management	Diagnostics		
CISCO SYSTEMS			
Profile Name:	WPA2-Enterprise		
Link Status:	Authenticated	Network Type: Infrastructure	
Wireless Mode:	5 GHz 54 Mbps	Current Channel: 149	
Server Based Authentication:	EAP-FAST	Data Encryption: AES	
IP Address:	10.77.244.221		
Signal Strength:		Good	
		Advanced	

U kunt ook controleren of de RADIUS-server het verificatieverzoek van de draadloze client ontvangt en valideert. Controleer de Overgegaan Verificaties en de Ontbroken rapporten van Pogingen over de server ACS om dit te verwezenlijken. Deze rapporten zijn beschikbaar onder Rapporten en Activiteiten op de ACS-server.

De apparaten configureren voor WPA2 Personal Mode

Voer deze stappen uit om de apparaten te configureren voor de WPA2-Personal-werkmodus:

- 1. Het WLAN configureren voor WPA2 Personal Mode-verificatie
- 2. De draadloze client configureren voor WPA2 Personal Mode

Configureer de WLAN voor WPA2 Personal Mode

U moet het WLAN configureren dat de clients zullen gebruiken om verbinding te maken met het draadloze netwerk. De WLAN SSID voor WPA2 Personal-modus is WPA2-Personal. Dit voorbeeld wijst dit WLAN toe aan de beheerinterface.

Voltooi deze stappen om WLAN en de bijbehorende parameters te configureren:

- 1. Klik op **WLAN's** vanuit de GUI van de controller om de WLAN-pagina weer te geven.Deze pagina maakt een lijst van de WLAN's die op de controller bestaan.
- 2. Klik op Nieuw om een nieuw WLAN te maken.
- Voer op de WLAN's > Nieuwe pagina de WLAN-SSID-naam, de profielnaam en de WLAN-id in. Klik vervolgens op Toepassen.Dit voorbeeld gebruikt WPA2-Personal als de SSID.

		-					Sa <u>r</u> e Co	infiguration <u>P</u> ing 1	Logout Befresh
CISCO	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECORITY	MANAGEMENT	COMMANDS	нецр	
WLANs	WLANs > N	New						< Back	Apply
WLANS WLANS	туре		WLAN						
▶ Advanced	Profile Nam	ne	WPA2-Per	sonal					
	WLAN SSID	,	WPA2-Per	sonal					

- 4. Zodra u een nieuw WLAN maakt, wordt de pagina WLAN > Bewerken voor het nieuwe WLAN weergegeven. Op deze pagina kunt u verschillende parameters definiëren die specifiek zijn voor dit WLAN. Dit omvat Algemeen Beleid, Beveiligingsbeleid, QOS-beleid en Geavanceerde parameters.
- 5. Onder Algemeen beleid schakelt u het selectievakje Status in om het WLAN in te schakelen.
- 6. Als u wilt dat het toegangspunt de SSID uitzendt in de beacon-frames, vinkt u het aanvinkvakje **Broadcast SSID aan**.
- 7. Klik op het tabblad **Beveiliging**. Kies onder Layer Security de optie **WPA+WPA2**.Dit schakelt WPA-verificatie in voor het

NLAN.	Sage Configuration : Bing Logout Befre
cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
WLANS	WLANs > Edit CBack Apply General Security QoS Advanced
Advanced	Layer 2 Layer 3 AAA Servers Layer 2 Security WPA+WPA2 MAC Filtering Static WEP Parameters
	802.11 Data Encryption Current Key: 104 bits WEP Static Key (Key Index = 0) Type Key Size Key Index Encryption Key WEP not set Image: Contract Contrel Contract Contract Contract Contract Contract Contract Contract
	B02.11 Data Encryption Current Key: 0 bits CKIP Key (Key Index= 0) Key Size Key Index Encryption Key Key Size I ASCII

- 8. Blader naar beneden om de **WPA+WPA2-parameters** aan te passen. In dit voorbeeld zijn WPA2 Policy en AES encryptie geselecteerd.
- 9. Kies onder Auth Key Management **PSK** om WPA2-PSK in te schakelen.
- 10. Voer de vooraf gedeelde sleutel in het juiste veld in zoals aangegeven in de afbeelding.

	Saye Configuration > <u>Ping</u> Logou MONITOR (1914) - CONTROLLER (1915) - SECURITY MANAGEMENT, COMMANING (1915)	t i <u>R</u> efresh
WLANS WLANS WLANS Advanced	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP WLANS > Edit Image: Security QOS Advanced Image: Security CommanDS HELP WLANS > Edit Image: Security QOS Advanced Image: Security Command Image: Security Command Image: Security Image: Security Command Image: Security Image: Securit	Apply
	x >	-
	Foot Notes I CKIP is not supported by 10xx model APs 2 Web Policy cannot be used in combination with IPsec 3 IN-REAP Local Switching is not supported with IPsec, CRANITE authentication 3 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded of 5 Client MPP is not active unless WINA2 is configured	lients)

Opmerking: Vooraf gedeelde sleutel die gebruikt wordt op de WLC moet overeenkomen met de sleutel die geconfigureerd is op de draadloze clients.

11. Klik op Apply (Toepassen).

De draadloze client configureren voor WPA2 Personal Mode

De volgende stap is het configureren van de draadloze client voor de WPA2-Personal-modus.

Voltooi deze stappen om de draadloze client te configureren voor de WPA2-Personal-modus:

- 1. Klik vanuit het venster van het Aironet Desktop Utility op **Profile Management > New** om een profiel te maken voor WPA2-PSK WLAN-gebruiker.
- Klik vanuit het venster Profielbeheer op het tabblad Algemeen en configureer de profielnaam, de clientnaam en de SSID-naam zoals in dit voorbeeld. Klik vervolgens op OK.

Profile Management		? 🗙
General Security Advanc	ed	
Profile Settings Profile Name:	WPA2-Personal	
Client Name:	Wireless-Client2	
Network Names		
SSID1:	WPA2-Personal	
SSID2:		
SSID3:		
	OK C	Cancel

3. Klik op het tabblad **Beveiliging** en kies **WPA/WPA2-wachtwoordgroep** om de werkwijze van WPA2-PSK in te schakelen. Klik op **Configureren** om de voorgedeelde sleutel met WPA-PSK te

configureren.

Profile Management			?	×
General Security Advanced				
Set Security Options				
○ WPA/WPA2/CCKM	WPA/WPA2/CCKM EAP Type:	LEAP	×	
WPA/WPA2 Passphrase				
○ 802.1x	802.1x EAP Type:	LEAP		
O Pre-Shared Key (Static WEP)				
◯ None				
Configure	Allow Association to Mixed Co Profile Locked	ells		
	Limit Time for Finding Domain	Controller To: 0	tec sec	
Group Policy Delay:	60 😂 sec			
			OK Cancel	

4. Voer de vooraf gedeelde toets in en klik op

Configure WPA/WPA2 Passphrase	? 🔀
Enter a WPA/WPA2 passphrase (8 to 63 ASC	II or 64 hexadecimal characters)
abcdefghijkl]
	OK Cancel

Verifieer de WPA2-Personal-modus van de handeling

Voltooi deze stappen om te verifiëren of uw WPA2-Enterprise-modemconfiguratie correct werkt:

- 1. Selecteer in het venster van het Aironet Desktop Utility het profiel **WPA2-Personal** en klik op **Activeren** om het profiel van de draadloze client te activeren.
- Nadat het profiel is geactiveerd, wordt de draadloze client bij de WLAN aangesloten op een succesvolle verificatie.Dit is de screenshot:

🛜 Cisco Aironet Desktop Utility - Current Profile: WPA2-Personal 🛛 🔗 🔀					
Action Options Help					
Current Status Profile Management	Diagnostics				
CISCO SYSTEMS					
Profile Name:	WPA2-Personal				
Link Status:	Authenticated	Network Type: Infrastructure			
Wireless Mode:	5 GHz 54 Mbps	Current Channel: 149			
Server Based Authentication:	None	Data Encryption: AES			
IP Address:	10.77.244.221				
Signal Strength:		Good			
		Advanced			

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Deze debug opdrachten zijn handig voor het oplossen van problemen in de configuratie:

N.B.: Raadpleeg <u>Belangrijke informatie over debug-opdrachten</u> voordat u **debug-**opdrachten gebruikt.

• debug dot1x gebeurtenissen inschakelen-Schakelt de debug van alle dot1x gebeurtenissen in. Hier is een voorbeeld debug uitvoer op basis van succesvolle verificatie: Opmerking: sommige regels van deze output zijn verplaatst naar tweede regels vanwege ruimtebeperkingen. (Cisco Controller)>debug dot1x events enable Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Sending EAP -Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 1) Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Received EAPOL START from mobile 00:40:96:af:3e:93 Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 2) Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Received EAP Response packet with mismatching id (currentid=2, eapid=1) from mobile 00:40:96:af:3e:93 Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Received Identity Response (count=2) from mobile 00:40:96:af:3e:93 Wed Feb 20 14:19:57 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93

Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 19, EAP Type 43)

Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 20) Wed Feb 20 14:20:01 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 43) Wed Feb 20 14:20:29 2007: Creating dot1x interface with key 00:0b:85:91:c3:c0 -0 Wed Feb 20 14:20:29 2007: Resetting the group key timer for 3689 seconds on AP 00:0b:85:91:c3:c0 Wed Feb 20 14:20:29 2007: Creating dot1x interface with key 00:0b:85:91:c3:c0 -1 Wed Feb 20 14:20:29 2007: Resetting the group key timer for 3696 seconds on AP 00:0b:85:91:c3:c0 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAPOL START from mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 22) Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received Identity Response (count=3) from mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 WARNING: updated EAP-Identifer 22 ===> 19 for STA 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 19) Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 19, EAP Type 3) Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 20) Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 43) Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 21) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 21, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 22) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 22, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 23) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 23, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 24) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 24, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 25) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 25, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93

Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 26) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 26, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 27) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 27, EAP Type 43) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Reject for mobile00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Failure to mobile 00:4096:af:3e:93 (EAP Id 27) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Setting quiet timer for 5 seconds for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 1) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 1) Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAPOL START from mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 2) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received Identity Response (count=2) from mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 WARNING: updated EAP-Identifer 2 ===> 20 for STA 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 20) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 3) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 21) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 21, EAP Type 43) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 22) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 22, EAP Type 43) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 WARNING: updated EAP-Identifer 22 ===> 24 for STA 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 24) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 24, EAP Type 43) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 25) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 25, EAP Type 43) Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Accept for mobile 00:40:96:af:3e:93 Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Creating a new PMK Cache Entry for tation 00:40:96:af:3e:93 (RSN 0)

```
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP-Success to
mobile 00:40:96:af:3e:93 (EAP Id 25)
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending default RC4 key to
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending Key-Mapping RC4 key to
mobile 00:40:96:af:3e:93
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received Auth Success while in
Authenticating state for mobile 00:40:96:af:3e:93
```

- **debug dot1x-pakket-inschakelen**-Hiermee kunt u debug van 802.1x-pakketberichten inschakelen.
- debug aaa gebeurtenissen enable-Enabled de debug output van alle aaa gebeurtenissen.

Gerelateerde informatie

- WPA2 Wi-Fi Protected Access 2
- EAP-FAST-verificatie met draadloze LAN-controllers en externe RADIUSserverconfiguratievoorbeeld
- Configuratie-voorbeeld van EAP-verificatie met WLAN-controllers (WLC)
- Overzicht van WPA-configuratie
- Ondersteuning voor wireless producten
- <u>Technische ondersteuning en documentatie Cisco Systems</u>

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.