Exemple de configuration de l'accès WPA (Wi-Fi Protected Access) dans un réseau sans fil unifié Cisco

Table des matières

Introduction Conditions préalables Exigences Composants utilisés Conventions Prise en charge WPA et WPA2 Configuration du réseau Configuration des périphériques en mode WPA2 entreprise Configurer le WLC pour l'authentification RADIUS via un serveur RADIUS externe Configurer le WLAN pour le mode de fonctionnement WPA2 Enterprise Configurer le serveur RADIUS pour l'authentification en mode entreprise WPA2 (EAP-FAST) Configuration du client sans fil pour le mode de fonctionnement WPA2 Enterprise Configuration du client sans fil pour le mode de fonctionnement WPA2 Enterprise Configuration du client sans fil pour le mode de fonctionnement WPA2 Enterprise Configuration des périphériques pour le mode WPA2 Personal Dépannage Informations connexes

Introduction

Ce document décrit comment configurer le Wi-Fi Protected Access (WPA) dans un réseau sans fil unifié Cisco.

Conditions préalables

Exigences

Assurez-vous d'avoir une connaissance de base de ces sujets avant de tenter cette configuration :

- WPA
- Solutions de sécurité LAN sans fil (WLAN)Remarque : reportez-vous à <u>Présentation de la</u> <u>sécurité LAN sans fil Cisco</u> pour obtenir des informations sur les solutions de sécurité WLAN Cisco.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Point d'accès allégé (LAP) Cisco, série 1000
- Contrôleur LAN sans fil (WLC) Cisco 4404 qui exécute le microprogramme 4.2.61.0
- Adaptateur client Cisco 802.11a/b/g qui exécute le microprogramme 4.1
- Aironet Desktop Utility (ADU) qui exécute le microprogramme 4.1
- Serveur Cisco Secure ACS version 4.1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous aux <u>Conventions relatives aux conseils techniques Cisco.</u>

Prise en charge WPA et WPA2

Le réseau sans fil unifié Cisco prend en charge les certifications WPA et WPA2 de la Wi-Fi Alliance. La norme WPA a été introduite par la Wi-Fi Alliance en 2003. WPA2 a été introduit par la Wi-Fi Alliance en 2004. Tous les produits certifiés Wi-Fi pour WPA2 doivent être interopérables avec les produits certifiés Wi-Fi pour WPA.

Les protocoles WPA et WPA2 offrent aux utilisateurs finaux et aux administrateurs réseau un niveau élevé d'assurance que leurs données resteront privées et que l'accès à leurs réseaux sera limité aux utilisateurs autorisés. Les deux modes de fonctionnement, personnel et entreprise, répondent aux besoins distincts des deux segments de marché. Le mode Entreprise de chaque utilise IEEE 802.1X et EAP pour l'authentification. Le mode personnel de chaque utilise la clé prépartagée (PSK) pour l'authentification. Cisco ne recommande pas le mode personnel pour les déploiements professionnels ou gouvernementaux, car il utilise une clé prépartagée pour l'authentification. PSK n'est pas sécurisé pour les environnements d'entreprise.

WPA résout toutes les vulnérabilités WEP connues dans la mise en oeuvre de la sécurité IEEE 802.11 d'origine, apportant ainsi une solution de sécurité immédiate aux WLAN dans les environnements d'entreprise et de petits bureaux/bureaux à domicile (SOHO). WPA utilise TKIP pour le cryptage.

WPA2 est la nouvelle génération de sécurité Wi-Fi. Il s'agit de la mise en oeuvre interopérable de la norme IEEE 802.11i ratifiée par la Wi-Fi Alliance. Il implémente l'algorithme de chiffrement AES recommandé par le National Institute of Standards and Technology (NIST) à l'aide du mode compteur avec le protocole CCMP (Cipher Block Chaining Message Authentication Code Protocol). WPA2 facilite la conformité à la norme FIPS 140-2 du gouvernement.

	WPA	WPA2		
Mode entreprise	Authentific	 Authentific 		
(entreprise,	ation :	ation :		
gouvernement,	IEEE	IEEE		
éducation)	802.1X/EA	802.1X/EA		

Comparaison des types de modes WPA et WPA2

	P • Cryptage : TKIP/MIC	P • Cryptage : AES- CCMP
Mode personnel (SOHO, domicile/personnel)	 Authentific ation : PSK Cryptage : TKIP/MIC 	 Authentific ation : PSK Cryptage : AES- CCMP

En mode Entreprise, WPA et WPA2 utilisent tous deux la norme 802.1X/EAP pour l'authentification. La norme 802.1X fournit aux réseaux locaux sans fil une authentification mutuelle solide entre un client et un serveur d'authentification. En outre, la norme 802.1X fournit des clés de cryptage dynamiques par utilisateur et par session, éliminant ainsi la charge administrative et les problèmes de sécurité liés aux clés de cryptage statiques.

Avec la norme 802.1X, les informations d'identification utilisées pour l'authentification, telles que les mots de passe d'ouverture de session, ne sont jamais transmises en clair, ou sans chiffrement, sur le support sans fil. Alors que les types d'authentification 802.1X fournissent une authentification forte pour les réseaux locaux sans fil, TKIP ou AES sont nécessaires pour le cryptage en plus de la norme 802.1X, car le cryptage WEP 802.11 standard est vulnérable aux attaques réseau.

Il existe plusieurs types d'authentification 802.1X, chacun offrant une approche différente de l'authentification tout en s'appuyant sur le même cadre et le même EAP pour la communication entre un client et un point d'accès. Les produits Cisco Aironet prennent en charge plus de types d'authentification EAP 802.1X que tous les autres produits WLAN. Les types pris en charge sont :

- LEAP Cisco
- EAP-Flexible Authentication via Secure Tunneling (EAP-FAST)
- EAP-TLS (EAP-Transport Layer Security)
- Protocole PEAP (Protected Extensible Authentication Protocol)
- EAP-TTLS (EAP-TTLS)
- Module EAP-SIM (Subscriber Identity Module)

Un autre avantage de l'authentification 802.1X est la gestion centralisée pour les groupes d'utilisateurs WLAN, y compris la rotation des clés basée sur des politiques, l'attribution de clés dynamiques, l'attribution de VLAN dynamiques et la restriction SSID. Ces fonctions font pivoter les clés de cryptage.

En mode de fonctionnement Personnel, une clé pré-partagée (mot de passe) est utilisée pour l'authentification. Le mode Personnel ne nécessite qu'un point d'accès et un périphérique client, tandis que le mode Entreprise requiert généralement un serveur RADIUS ou un autre serveur d'authentification sur le réseau.

Ce document fournit des exemples de configuration de WPA2 (mode Entreprise) et de WPA2-PSK (mode Personnel) dans un réseau sans fil unifié Cisco.

Configuration du réseau

Dans cette configuration, un WLC Cisco 4404 et un LAP Cisco 1000 sont connectés via un

commutateur de couche 2. Un serveur RADIUS externe (Cisco Secure ACS) est également connecté au même commutateur. Tous les périphériques se trouvent dans le même sous-réseau. Le point d'accès (LAP) est initialement enregistré auprès du contrôleur. Deux réseaux locaux sans fil doivent être créés, l'un pour le mode WPA2 entreprise et l'autre pour le mode WPA2 personnel.

WLAN en mode WPA2 entreprise (SSID : WPA2 entreprise) utilise EAP-FAST pour authentifier les clients sans fil et AES pour le cryptage. Le serveur Cisco Secure ACS sera utilisé comme serveur RADIUS externe pour l'authentification des clients sans fil.

WPA2-Personal mode WLAN (SSID : WPA2-PSK) utilise WPA2-PSK pour l'authentification avec la clé prépartagée « abcdefghijk ».

Wireless LAN Controller Lightweight Access Point Layer 2 Switch (WLC) (LAP) 00000 Wireless Client

Vous devez configurer les périphériques pour cette configuration :

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

Configuration des périphériques en mode WPA2 entreprise

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Suivez ces étapes afin de configurer les périphériques pour le mode de fonctionnement WPA2 Entreprise :

- 1. Configurer le WLC pour l'authentification RADIUS via un serveur RADIUS externe
- 2. Configurer le WLAN pour l'authentification WPA2 en mode entreprise (EAP-FAST)
- 3. Configuration du client sans fil pour le mode WPA2 entreprise



Configurer le WLC pour l'authentification RADIUS via un serveur RADIUS externe

WLC doit être configuré afin de transférer les identifiants de l'utilisateur à un serveur RADIUS externe. Le serveur RADIUS externe valide ensuite les informations d'identification de l'utilisateur à l'aide d'EAP-FAST et fournit l'accès aux clients sans fil.

Complétez ces étapes pour configurer le WLC pour un serveur RADIUS externe :

- 1. Sélectionnez Security et RADIUS Authentication depuis la GUI du contrôleur pour afficher la page des serveurs d'authentification RADIUS. Cliquez ensuite sur New afin de définir un serveur RADIUS.
- Définissez les paramètres du serveur RADIUS sur la page RADIUS Authentication Servers > New. Ces paramètres incluent :Adresse IP du serveur RADIUSSecret partagéPort number (numéro de port) État du serveurCe document utilise le serveur ACS avec l'adresse IP 10.77.244.196.

						Sage Co	nfiguration <u>P</u> ing	Logout Befresh
CISCO	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
Security	RADIUS Authentic	cation Server	s > New				< Back	Apply
* AAA	Server Index (Prio	rity) 1						
RADIUS Authentication	Server IPAddress	10.	77.244.196					
Accounting TACACS+ LDAP	Shared Secret For	mat As	ш					
Local Net Users MAC Filtering	Shared Secret	•••	••					
Disabled Clients User Login Policies AP Policies	Confirm Shared Se	cret	••					
Local EAP	Key Wrap		Designed for FI	PS customers	and requires a ke	y wrap complian	t RADIUS server)	
Priority Order	Dout Number	101	9					
Access Control Lists	Port Number	101	2					
 Wireless Protection Policies 	Server Status	End	ibled 💌					
▶ Web Auth	Support for RFC 35	76 En	abled 💌					
► Advanced	Server Timeout	2	seconds					
	Network User	RE	nable					
	Management	R	nable					
	IPSec		nable					

3. Cliquez sur Apply.

Configurer le WLAN pour le mode de fonctionnement WPA2 Enterprise

Configurez ensuite le WLAN que les clients utiliseront pour se connecter au réseau sans fil. Le SSID WLAN pour le mode WPA2 entreprise sera WPA2-Enterprise. Cet exemple attribue ce WLAN à l'interface de gestion.

Complétez ces étapes afin de configurer le WLAN et ses paramètres associés :

- 1. Cliquez sur les WLAN de la GUI du contrôleur afin d'afficher la page des WLAN.Cette page énumère les WLAN qui existent sur le contrôleur.
- 2. Cliquez sur New [nouveau] pour créer un autre WLAN.
- 3. Saisissez le nom SSID du WLAN et le nom du profil sur la page WLANs > New. Cliquez

ensuite sur **Apply**.Cet exemple utilise **WPA2-Enterprise** comme SSID.

						Saye Co	infiguration Bing	Logout Befr
NITOR ;	<u>w</u> lans	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
LANs > N	New						< Back	Apply
pe		WLAN						
ofile Nam	10	WPA2-Ent	erprise					
LAN SSID		WPA2-Ent	erprise					
	NITOR "ANS > I pe ofile Nam AN SSID	NITOR WLANS ANS > New pe file Name AN SSID	NITOR WLANS CONTROLLER ANS > New pe WLAN ofile Name WPA2-Entr AN SSID WPA2-Entr	ANS SID	NITOR WLANS CONTROLLER WIRELESS SECURITY ANS > New pe WLAN ofile Name WPA2-Enterprise AN SSID WPA2-Enterprise	NITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT ANS > New or WLAN offile Name WPA2-Enterprise AN SSID WPA2-Enterprise	NITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS ANS > New pe WLAN file Name WPA2-Enterprise AN SSID WPA2-Enterprise	NITOR WLANS CONTROLLER WIPELESS SECURITY MANAGEMENT COMMANDS HELP ANS > New

- 4. Une fois que vous avez créé un nouveau WLAN, la page WLAN > Edit du nouveau WLAN apparaît. Sur cette page, vous pouvez définir divers paramètres spécifiques à ce WLAN. Cela inclut les stratégies générales, les stratégies de sécurité, les stratégies QOS et les paramètres avancés.
- 5. Sous General Policies, cochez la case Status afin d'activer le



- 6. Si vous voulez que le point d'accès diffuse le SSID dans ses trames de balise, cochez la case **Broadcast SSID**.
- Cliquez sur l'onglet Security. Sous Layer 2 Security, sélectionnez WPA+WPA2.Cela active l'authentification WPA pour le WLAN.

aludu	Sa <u>v</u> e Configuration Bing (Logout <u>R</u> efresh
CISCO	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP	
WLANS WLANS WLANS MLANS Advanced	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP WLANS > Edit <td>Apply</td>	Apply
	802.11 Data Encryption Current Key: 0 bits CKIP Key (Key Index= 0) Key Size Key Index Encryption Key Not set 1 ASCII Image: Second Secon	eded clients)

8. Faites défiler la page vers le bas pour modifier les paramètres **WPA+WPA2**.Dans cet exemple, la stratégie WPA2 et le cryptage AES sont sélectionnés.

- alialia -		Sage Configuration Eing Logout Befresh
cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT	COMMANDS HELP
WLANS WLANS WLANS Advanced	WLANs > Edit General Security QoS Advanced Layer 2 Layer 3 AAA Servers	< Back Apply
	802.11 Data Encryption Current Key: 0 bits CKIP Key (Key Index= 0) Key Size Key Index Encryption Key Image:	Key Format ASCII
	WPA2 Policy Image: Constraint of the second secon	e administrative override to reset excluded clients)

- 9. Sous Auth Key Mgmt, sélectionnez **802.1x**.Cela active le WPA2 à l'aide de l'authentification 802.1x/EAP et du cryptage AES pour le WLAN.
- 10. Cliquez sur l'onglet **AAA Servers**. Sous Authentication Servers, sélectionnez l'adresse IP du serveur approprié.Dans cet exemple, 10.77.244.196 est utilisé comme serveur

				Sa <u>v</u> e C	onfiguration Ping	Logout Befree
cisco	MONITOR WLANS CONTROL	LER WIRELESS SECURI	TY MANAGEMENT	COMMANDS	нецр	
CISCO WLANS WLANS WLANS Advanced	MONITOR WLANS CONTROL WLANS > Edit General Security Qat Layer 2 Layer 3 AA Select AAA servers below to Radius Servers Authentication Set Authentication Server None Server Server None Server Local EAP Authentication Local EAP Authentication Foot Notes I CKIP is not supported by I0xx 2 Web Policy cannot be used in c	ER WIRELESS SECURI	TY MANAGEMENT rvers on this WLAN rvers Server 1 Server 2 Server 3	COMMANDS	KELP < Back	Apply

11. Cliquez sur Apply.Remarque : il s'agit du seul paramètre EAP qui doit être configuré sur le contrôleur pour l'authentification EAP. Toutes les autres configurations spécifiques à EAP-FAST doivent être effectuées sur le serveur RADIUS et les clients qui doivent être authentifiés.

<u>Configurer le serveur RADIUS pour l'authentification en mode entreprise WPA2</u> (EAP-FAST)

Dans cet exemple, Cisco Secure ACS est utilisé comme serveur RADIUS externe. Procédez comme suit afin de configurer le serveur RADIUS pour l'authentification EAP-FAST :

- 1. <u>Créer une base de données utilisateur pour authentifier les clients</u>
- 2. Ajouter le WLC en tant que client AAA au serveur RADIUS

3. <u>Configurer l'authentification EAP-FAST sur le serveur RADIUS avec le provisionnement PAC intrabande anonyme</u> Remarque : EAP-FAST peut être configuré avec l'approvisionnement PAC intrabande anonyme ou l'approvisionnement PAC intrabande authentifié. Cet exemple utilise le provisionnement PAC intrabande anonyme. Pour obtenir des informations détaillées et des exemples sur la configuration d'EAP FAST avec la mise en service PAC intrabande anonyme et la mise en service intrabande authentifiée, référez-vous à <u>Exemple de configuration d'authentification EAP-FAST avec des contrôleurs LAN sans fil et un serveur RADIUS externe</u>.

Créer une base de données utilisateur pour authentifier les clients EAP-FAST

Complétez ces étapes afin de créer une base de données utilisateur pour les clients EAP-FAST sur l'ACS. Cet exemple configure le nom d'utilisateur et le mot de passe du client EAP-FAST comme User1 et User1, respectivement.

 Dans la barre de navigation de l'interface graphique utilisateur ACS, sélectionnez User Setup. Créez un nouvel utilisateur sans fil, puis cliquez sur Add/Edit afin d'accéder à la page Edit de cet

F/P Very Envertes Tools Help	2 (1912) Marine (1912) Marine (1912)
es al ben //122.0.0.1-1065/	v 🖬 🖓
and an other stands	
User Setup	
select	Help
User Servep Servep Servep Servep Serven Component Component Component Component Component Serven Serven Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuratio Configuratio Configuration Configuratio Configuratio Configurati	 Versisting and External User Databases Finding a Specific User in the ACS Internal Databases Adding a User to the ACS Internal Outabase Adding a User to the ACS Internal Outabase Listing Usernames in the ACS Internal Outabase Listing AII Usernames in the ACS Internal Outabase Remove Deparate Users User Setup anables you to configure individual user information, add users, and delete users in the database. User Setup and External User Database Pour mut have the database up and running on the external server. For example, if you are using token card authentication, your token server must be running and properly configured. You mut have configured the applicable parameters in the External User Databases section. Note: User Setup configuration overrides Group Setup configuration. If you rely on the Unknown User Policy in the External User Databases are section 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 has successfully euthenticated ence. External user database, modification must be done from within the enternal user database. User Setup Leapt toxic of Group view outbornation, add users, and delete users in the ACS internal database. Meter User Setup heapt toxic of outborn two authenticates with an enternal user database. User Setup heapt toxic of outborn two authonics we without a user factobase. User Setup heapt toxic of outboard we authenticate with an enternal user database. User Setup heapt toxic of outboard we authonic the view maternal user database. User Setup heapt toxic of outboard we authonic toxic with an enternal user database.

 Dans la page User Setup Edit, configurez Real Name et Description, ainsi que les paramètres Password, comme indiqué dans cet exemple.Ce document utilise la base de données interne ACS pour l'authentification de mot de passe.

kess http://127.0	.0.1:1065/	- 61
Cisco Svorems	User Setup	
alb alb	Edit	Help
User Setup Setup Setup	User: User1 (New User)	Account Disabled Oxisting & Oremann Supplementary User Info Password Avdientication Group to which the user is assigned
Network Configuration System Configuration	Supplementary User Info Real Name Description	Callback Client 3D Advanced SetSings Advanced SetSings Network Access Restrictions Nan Seasions Usage Operan Access to hable Overvised able Covervised able
Administration Centrol Control Control Posture Posture Validation Network Access Profiles	User Setup ? Password Authentication: ACS Internal Database CiscoSecure PAP (Also used for CHAP/MS- CHAP/ARAP, if the Separate field is not	Advanced TACACS+ Settings TACACS+ Enable Parsword TACACS+ Enable Parsword TACACS+ Dutheand Parsword TACACS+ Shell Command Authorization Command Authorization for Network Device Nanagement Applications TACACS+ Unknown Services TACACS+ Unknown Services RADIUS Attributes RADIUS Yeador-Specific Attributes
Reports and Activity	Checked.) Password Confirm Password Separate (CHAP/MS-CHAP/ARAP) Password	Account Disabled Status Select the Account Disabled check box to disable this account: clear the check box to enable the account. [Back to Top]
	Confirm Password Submit Cancel	Deleting a Username The Delete button appears only when you are editing an existing user account, not when you are adding a new user account. To delete the connect user account from the database, click Delete . When asked to confirm your action, click OK .

- 3. Choisissez ACS Internal Database dans la liste déroulante Password Authentication.
- 4. Configurez tous les autres paramètres requis et cliquez sur Submit.

Ajouter le WLC en tant que client AAA au serveur RADIUS

Complétez ces étapes afin de définir le contrôleur en tant que client AAA sur le serveur ACS :

- 1. Cliquez sur **Network Configuration depuis l'interface graphique ACS.** Dans la section Add AAA client de la page Network Configuration, cliquez sur **Add Entry** afin d'ajouter le WLC comme client AAA au serveur RADIUS.
- Sur la page AAA Client, définissez le nom du WLC, l'adresse IP, le secret partagé et la méthode d'authentification (RADIUS/Cisco Airespace). Référez-vous à la documentation du constructeur pour d'autres serveurs d'authentification non-ACS.

Care Systems	Notwork Configuration	X
als als	Network Conliguration	
User Setup Setup Setup Setup Setup Setup Setup Seture Components Setures Configuration Suffer Suffer Configuration Suffer Configuration Suffer Configuration	AAA Client Hostname WLC AAA Client IP Address Shared Secret cisco RADIUS Key Wrap Key Encryption Key	Help AAA Cleant Hostname AAA Cleant IP Address Shared Secont Network Device Group BADIVS Key Wrag Arthenticute Uring Single Connect TACAS* AAA Cleant Lea Undata:/Watchdee Packets from this AAA Cleant Lea RADIUS Transeling Packets from this AAA Cleant Badiace RADIUS Part info with Username from this AAA Cleant Match Framed IP-Address with user IP address for accounting packets from this AAA Cleant
Posture Validation	Message Authenticator Code Key Key Input Format C ASCII @ Hexadecimal	AAA Client Hostname The AAA Client Hostname is the name assigned to the AAA client.
Reports and Activity	Authenticate Using RADIUS (Cisco Airespace)	(Back to Tep) AAA (Sent IP Address
Documentation	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 Match Framed-IP-Address with user IP address for accounting packets from this AAA Client	If you want to designate more than one AAA client with a single AAA client entry in ACS, you can specify the IP address for acts AAA client to be represented by this AAA client to be represented by

Remarque : la clé secrète partagée que vous configurez sur le WLC et le serveur ACS doit correspondre. Le secret partagé distingue les majuscules et minuscules.

3. Cliquez sur Envoyer+Appliquer.

<u>Configurer l'authentification EAP-FAST sur le serveur RADIUS avec le provisionnement PAC intrabande anonyme</u>

Approvisionnement en bande anonyme

Il s'agit de l'une des deux méthodes de mise en service intrabande selon lesquelles l'ACS établit une connexion sécurisée avec le client de l'utilisateur final dans le but de fournir au client un nouveau PAC. Cette option permet une connexion TLS anonyme entre le client de l'utilisateur final et ACS.

Cette méthode fonctionne à l'intérieur d'un tunnel ADHP (Authenticated Diffie-HellmanKey Agreement Protocol) avant que l'homologue authentifie le serveur ACS.

Ensuite, l'ACS requiert l'authentification EAP-MS-CHAPv2 de l'utilisateur. Une fois l'authentification utilisateur réussie, l'ACS établit un tunnel Diffie-Hellman avec le client utilisateur final. L'ACS génère un PAC pour l'utilisateur et l'envoie au client de l'utilisateur final dans ce tunnel, avec des informations sur cet ACS. Cette méthode d'approvisionnement utilise EAP-MSCHAPv2 comme méthode d'authentification dans la phase zéro et EAP-GTC dans la phase deux.

Étant donné qu'un serveur non authentifié est configuré, il n'est pas possible d'utiliser un mot de passe en texte clair. Par conséquent, seules les informations d'identification MS-CHAP peuvent

être utilisées à l'intérieur du tunnel. MS-CHAPv2 est utilisé pour prouver l'identité de l'homologue et recevoir un PAC pour d'autres sessions d'authentification (EAP-MS-CHAP sera utilisé comme méthode interne uniquement).

Complétez ces étapes afin de configurer l'authentification EAP-FAST dans le serveur RADIUS pour l'approvisionnement en bande anonyme :

1. Cliquez sur **System Configuration** dans l'interface utilisateur graphique du serveur RADIUS. Dans la page System Configuration, sélectionnez **Global Authentication**

Setup.	
CiscoSecure ACS - Microsoft Internet Explorer	× (b)
Ele Edt Yew Fgvorkes Iools Help	Links " Loose
Address an http://127.0.0.1:1065/	S 🔁 🖄
Lot yow Pycotes Los yop Address A http://L27.0.0.1:1005/ Chee Stricts System Configuration Strict Image: Stricts Bard Profile Bard Profile Bard Profile Bard Profile Date Format Control Date Format Control Date Format Control Date Format Control Date Score ACS Internal Database Replication ACS Internal Database Replication ACS Service Management ACS Service Management ACS Service Management ACS Certificate Setup Administrion Administrion Administrion Date Format Control Action Database Bate Total Database Bate Total Database Bate Total Database <th>Brand Research Confront Configuration Service Control Service Control Service Control Control Service Control</th>	Brand Research Confront Configuration Service Control Service Control Service Control Control Service Control
Reports and Activity Online Documentation	Legging Select to configure various Cisco Secure ACS reports and customize the type of information that is logged. [Reck to Tep] Date Format Control Select to configure the date format, either month/day/year or day/month/year, for CSV files and Service Logs and in the GUI.
	[Back to Tep]
	g Internet
🐮 Start 🛛 🕝 🍏 CiscoSecure ACS - Mic	📑 7:57 PM

 Dans la page de configuration de l'authentification globale, cliquez sur EAP-FAST Configuration afin d'accéder à la page des paramètres EAP-FAST.

Address a http://127.0	0.1-1065/	
Citco Svorems	System Configuration	
Trà Ulter	EAP Configuration	
Group Setup Group Setup Group Shared/hudia Components Configuration Configuration	PEAP Allow EAP-MSCHAPv2 Allow EAP-GTC Allow Posture Validation Allow EAP-TLS Select one or more of the following options: If Certificate SAN comparison If Certificate Binary comparison EAP-TLS session timeout (minutes): 120 Cisco client initial message:	Use this page to specify settings for various authentication protocols. • LAP Configuration • PEAP • LAP-INS • LAP IS • LAP IS • LAP IS • LAP IS • LAP Is a flexible request response protocol for arbitrary sothertication information (IPFC 2284). EAP is largered on tap of another protocol such as UDP, 802.1x or RAD DUS and supports multiple "authentication" types.
Reports and Activity	Enable Fast Reconnect:	PEAP PEAP Is the exter layer protocol for the secure tunnel.
Online Documentation	EAP-FAST Configuration EAP-TLS C Allow EAP-TLS Select one or more of the following options: C Certificate SAN comparison	Notes AEAP is a cartificate-based authentication protocol. AEAP authentication can occur only after you have completed the required steps so the ACS Centificate Setup page. Allow EAP-MSCHAPv2 — Use to enable EAP-MSCHAPv2 within MS PEAP authentication. Enable this protocol for any repository that supports MS- CHAPv2, such as Microsoft AD, and the ACS Internal Database.
	Submit Submit + Restart Cancel	

3. Sur la page EAP-FAST Settings, cochez la case **Allow EAP-FAST** pour activer EAP-FAST dans le serveur RADIUS.

EiscoSecure AES - M	Skrosoft Internet Explorer	<u>-101 ×</u>
Ele Edt Yew Fav	ronites Iools Help	Lirks 🤲 🦓
Address http://127.0	0.0.1:1065/	💌 🛃 Go
Cinco Syntems	System Configuration	×
and to have been by	EAP-FAST Configuration	- Help
User Setup		EAP-FAST Configuration Page
Group	EAP-FAST Settings	?
R Setup	EAP-FAST	Use this page to configure EAP-FAST authentication settings.
SharedProfile Components	R Allow EAP-FAST	EAP-EAST Settings
Markey I Markawark	Active master key TTI	Client initial message Authority ID Infe
Configuration	Pathod seater hay TT	 Allow anonymous in-band PAC previsioning
Sustem	Retired master key TTL 3 months	Allow as then ticated in-band PAC previsioning Allow machine as then tication
Con Consideration	Tunnel PAC TTL 1 weeks	Allow stateless session resume.
Configuration	Client initial message: tacwebacs	Allowed inser methods Certificate Comparison
	Authority ID Info: tacwebacs	 EAP-TLS session timeout (minutes)
Centrel	Allow approximates in-band BAC provisioning	CAPTAST master server Actual EAP-FAST server status
Deternal User	Allow authenticated in-band PAC provisioning	
	Accept cleat on withoutinated provisioning	EAP-FAST Settings
Validation	Descript client on addienticated provisioning	Allow EAP-FAST-To enable EAP-FAST authentication, select this check
Network Access	C cleve Machine Authentication	bes.
S Promet	La allow machine Authentication	Active Master Key TTL-Enter a value for the amount of time that a master
Activity	Machine PAC TTL 1 Weeks	time to live (TTL) defined for the Master Key expires, the master key is
and 1 Online	C Allow Stateless session resume	considered retired and a new master key is generated.
Documentation	Authorization PAC TTL 1 hours	 Retired master key TIL – Enter a value for the amount of time that PACs
	Allowed inner methods	generated using a retired master key are acceptable for EAP-PAST authentication. When an end-user client gains network access using a PAC
	EAP-GTC	based on a retired master key, ACS sends a new PAC to the end-user client.
	EAP-MSCHAPv2	Tunnel PAC TR - 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 provisioning must be used to provide the end-user clinest with a new DAC.
2)		internet
🍠 Start 🛛 🔂 🥭	CiscoSecure ACS - Mic	👮 7:58 PM

- 4. Configurez les valeurs TTL (Time-to-Live) de la clé principale active/retirée comme vous le souhaitez, ou définissez-la sur la valeur par défaut, comme indiqué dans cet exemple.Référez-vous à Clés maîtres pour des informations sur les clés maîtres actives et retirées. Consultez également Clés principales et TTL PAC pour plus d'informations.Le champ ID d'autorité Info représente l'identité textuelle de ce serveur ACS, qu'un utilisateur final peut utiliser pour déterminer le serveur ACS à authentifier. Il est obligatoire de renseigner ce champ.Le champ Client initial display message spécifie un message à envoyer aux utilisateurs qui s'authentifient auprès d'un client EAP-FAST. La longueur maximale est de 40 caractères. Un utilisateur ne verra le message initial que si le client de l'utilisateur final prend en charge l'affichage.
- 5. Si vous voulez que l'ACS effectue le provisionnement PAC dans la bande anonyme, cochez la case **Autoriser le provisionnement PAC dans la bande anonyme**.
- 6. Allowed inner methods : cette option détermine quelles méthodes EAP internes peuvent être exécutées dans le tunnel EAP-FAST TLS. Pour l'approvisionnement en bande anonyme, vous devez activer EAP-GTC et EAP-MS-CHAP pour la rétrocompatibilité. Si vous sélectionnez Allow anonymous in-band PAC provisioning, vous devez sélectionner EAP-MS-CHAP (phase zéro) et EAP-GTC (phase deux).

Configuration du client sans fil pour le mode de fonctionnement WPA2 Enterprise

L'étape suivante consiste à configurer le client sans fil pour le mode de fonctionnement WPA2 Entreprise.

Complétez ces étapes afin de configurer le client sans fil pour le mode WPA2 Entreprise.

- Dans la fenêtre Aironet Desktop Utility, cliquez sur Profile Management > New afin de créer un profil pour l'utilisateur WLAN WPA2-Enterprise.Comme mentionné précédemment, ce document utilise le nom WLAN/SSID comme WPA2-Enterprise pour le client sans fil.
- 2. Dans la fenêtre Profile Management, cliquez sur l'onglet **General** et configurez le nom du profil, le nom du client et le nom du SSID comme indiqué dans cet exemple. Cliquez ensuite sur

י <i>ת</i>	
Profile Management	
General Security Adva	anced
Profile Settings	
Profile Nam	ne: WPA2-Enterprise
Client Nam	ne: Wireless-Client1
Network Names	
SSID	1: WPA2-Enterprise
SSID	2
SSID	3
	OK Cancel

 Cliquez sur l'onglet Security et choisissez WPA/WPA2/CCKM pour activer le mode de fonctionnement WPA2. Sous WPA/WPA2/CCKM EAP Type, sélectionnez EAP-FAST. Cliquez sur Configure afin de configurer le paramètre EAP-FAST.

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	
	ОК	Cancel

 Dans la fenêtre Configure EAP-FAST, cochez la case Allow Automatic PAC Provisioning. Si vous souhaitez configurer le provisionnement PAC anonyme, EAP-MS-CHAP sera utilisé comme seule méthode interne de la phase zéro.

Configure EAP-FAST	? 🔀
EAP-FAST Authentication Method	
MSCHAPv2 User Name and Password	Configure
Protected Access Credentials (PAC)	
Select One or More PAC Authorities	
	Manage
	>
Use Any PAC Belonging to the Same Group	
Allow Automatic PAC Provisioning	
Use Machine Information for Domain Logon	
No Network Connection Unless User Is Logged In	
	OK Cancel

- 5. Sélectionnez Nom d'utilisateur et mot de passe MSCHAPv2 comme méthode d'authentification dans la liste déroulante Méthode d'authentification EAP-FAST. Cliquez sur **Configure**.
- Dans la fenêtre Configurer le nom d'utilisateur et le mot de passe MSCHAPv2, sélectionnez les paramètres de nom d'utilisateur et de mot de passe appropriés.Cet exemple choisit Automatically Prompt for User Name and Password.

1

même nom d'utilisateur et le même mot de passe doivent être enregistrés auprès de l'ACS. Comme mentionné précédemment, cet exemple utilise respectivement User1 et User1 comme nom d'utilisateur et mot de passe. Notez également qu'il s'agit d'une mise en service intrabande anonyme. Par conséquent, le client ne peut pas valider le certificat du serveur. Vous devez vous assurer que la case Valider l'identité du serveur est décochée.

7. Click OK.

Vérification du mode de fonctionnement WPA2 Enterprise

Complétez ces étapes afin de vérifier si votre configuration du mode WPA2 Entreprise fonctionne correctement :

- 1. Dans la fenêtre Aironet Desktop Utility, sélectionnez le profil **WPA2-Enterprise** et cliquez sur **Activate** afin d'activer le profil client sans fil.
- 2. Si vous avez activé l'authentification MS-CHAP ver2, le client vous demandera le nom

d'utilisateur et le mot de

Please enter your E. network	AP-FAST username and password to log on to the wireles
User Name :	User1
Password :	[•••••
Log on to :	
Card Name :	Cisco Aironet 802.11a/b/g Wireless Adapter
Profile Name :	WPA-Enterprise

3. Pendant le traitement EAP-FAST de l'utilisateur, le client vous demandera de demander PAC au serveur RADIUS. Lorsque vous cliquez sur **Yes**, l'approvisionnement PAC démarre.

EAP-FAST Authenticat	on	×
You do not have a valid P/ automatic provisioning?	C from the authentication server. Do you want to proceed and request	
	Yes No	

4. Une fois le provisionnement PAC réussi dans la phase zéro, les phases un et deux suivent et une procédure d'authentification réussie a lieu.Une fois l'authentification réussie, le client sans fil est associé au WLAN WPA2-Enterprise. Voici la capture d'écran

😨 Cisco Aironet Desktop Utility	y - Current Profile: WPA	2-Enterprise 🛛 🛛 🛛 🔀
Action Options Help		
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

Vous pouvez également vérifier si le serveur RADIUS reçoit et valide la demande d'authentification du client sans fil. Pour ce faire, vérifiez les rapports Passed Authentications et Failed Attempts sur le serveur ACS pour savoir si l'authentification a réussi ou échoué. Ces rapports sont disponibles sous l'option Reports and Activities sur le serveur ACS.

Configuration des périphériques pour le mode WPA2 Personal

Procédez comme suit afin de configurer les périphériques pour le mode de fonctionnement WPA2-Personal :

- 1. Configuration du WLAN pour l'authentification en mode personnel WPA2
- 2. <u>Configuration du client sans fil pour le mode WPA2 personnel</u>

Configuration du WLAN pour le mode de fonctionnement personnel WPA2

Vous devez configurer le WLAN que les clients utiliseront pour se connecter au réseau sans fil. Le SSID WLAN du mode WPA2 personnel est WPA2 personnel. Cet exemple attribue ce WLAN à l'interface de gestion.

Complétez ces étapes afin de configurer le WLAN et ses paramètres associés :

- 1. Cliquez sur les WLAN de la GUI du contrôleur afin d'afficher la page des WLAN.Cette page énumère les WLAN qui existent sur le contrôleur.
- 2. Cliquez sur New [nouveau] pour créer un autre WLAN.
- Saisissez le nom SSID WLAN, le nom du profil et l'ID WLAN dans la page WLANs > New. Cliquez ensuite sur Apply.Cet exemple utilise WPA2-Personal comme SSID.

				-		Sa <u>v</u> e Co	onfiguration <u>P</u> ing 1	Logout Refresh
cisco	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
WLANs	WLANs > New						< Back	Apply
WLANS	Туре	WLAN						
▶ Advanced	Profile Name	WPA2-Per	sonal					
	WLAN SSID	WPA2-Per	sonal					

- 4. Une fois que vous avez créé un nouveau WLAN, la page WLAN > Edit du nouveau WLAN apparaît. Sur cette page, vous pouvez définir divers paramètres spécifiques à ce WLAN. Cela inclut les stratégies générales, les stratégies de sécurité, les stratégies QOS et les paramètres avancés.
- 5. Sous General Policies, cochez la case Status afin d'activer le WLAN.
- 6. Si vous voulez que le point d'accès diffuse le SSID dans ses trames de balise, cochez la case **Broadcast SSID**.
- 7. Cliquez sur l'onglet **Security.** Sous Layer Security, sélectionnez **WPA+WPA2**.Cela active l'authentification WPA pour le

cisco	Sage Configuration (Bing Logout MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
LANs	WLANs > Edit < Back A
WLANS WLANS	General Security QoS Advanced Layer 2 Layer 3 AAA Servers
Advanced	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 Key Format WEP not set 1 ASCII
	Allow Shared Key Enabled Enabled
	802.11 Data Encryption Current Key: 0 bits CKIP Key (Key Index= 0)
	Key Size Key Index Encryption Key Key Format
	not set \star 1 \star ASCII \star
	Foot Notes I CKIP is not supported by 10xx model APs 2 Web Policy cannot be used in combination with IPsec 3 M-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 client 5 Client MFP is not active unless WPA2 is configured

- 8. Faites défiler la page vers le bas pour modifier les paramètres **WPA+WPA2**.Dans cet exemple, la stratégie WPA2 et le cryptage AES sont sélectionnés.
- 9. Sous Auth Key Mgmt, choisissez **PSK** afin d'activer WPA2-PSK.
- Saisissez la clé pré-partagée dans le champ approprié, comme indiqué.

/LANs	WLANs > Edit General Security QoS	Advanced		< Back	Apply
♥ WLANS WLANS ▶ Advanced	Layer 2 Layer 3 AAA 5 Key no MMH Mode E Key Permutation E B02.11 Data Encryption C WPA+WPA2 Parameters	Size Key Index Enco set I I I abled abled ype Key Size VEP 104 bits I	ryption Key	Key Format ASCII	
	WPA Policy WPA2 Policy WPA2 Policy WPA2 Encryption Authors Authors Mant PS3 PSK Format Associated as a second seco	s Пткір т			
	Foot Notes 1 CKIP is not supported by 10xx mo 2 Web Policy cannot be used in com 3 H-REAP Local Switching is not supp 4 When client exclusion is enabled, a 5 Client MPP is not active unless WPP	el APs nation with IPsec rted with IPsec, CRANITE au Timeout Value of zero mean ? is configured	uthentication is infinity (will require	administrative override to reset ex	cluded clients

Remarque : la clé pré-partagée utilisée sur le WLC doit correspondre à celle configurée sur les clients sans fil.

11. Cliquez sur Apply.

Configuration du client sans fil pour le mode WPA2 personnel

L'étape suivante consiste à configurer le client sans fil pour le mode de fonctionnement WPA2-Personal.

Complétez ces étapes afin de configurer le client sans fil pour le mode WPA2-Personal :

- 1. Dans la fenêtre Aironet Desktop Utility, cliquez sur **Profile Management > New** afin de créer un profil pour l'utilisateur WLAN WPA2-PSK.
- 2. Dans la fenêtre Profile Management, cliquez sur l'onglet **General** et configurez le nom du profil, le nom du client et le nom du SSID comme indiqué dans cet exemple. Cliquez ensuite sur

OK.

Profile Management	2 🔀
General Security Advanc	ed
Profile Settings	
Profile Name:	WPA2-Personal
Client Name:	Wireless-Client2
Network Names	
SSID1:	WPA2-Personal
SSID2:	
SSID3:	
	OK Cancel

 Cliquez sur l'onglet Security et choisissez WPA/WPA2 Passphrase pour activer le mode de fonctionnement WPA2-PSK. Cliquez sur Configure afin de configurer la clé pré-partagée WPA-

PSK.

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 Cells	
	Limit Time for Finding Domain Controller To: 0 0 sec	
Group Policy Delay:	60 😂 sec	
	ОК СА	ancel

4. Entrez la clé pré-partagée et cliquez sur

Configure WPA/WPA2 Passphrase	20
Enter a WPA/WPA2 passphrase (8 to 63 ASCI	II or 64 hexadecimal characters)
abcdefghijkl	
	OK Cancel

Vérification du mode de fonctionnement WPA2-Personal

:

Complétez ces étapes afin de vérifier si votre configuration du mode WPA2-Enterprise fonctionne correctement :

- 1. Dans la fenêtre Aironet Desktop Utility, sélectionnez le profil **WPA2-Personal** et cliquez sur **Activate** afin d'activer le profil client sans fil.
- 2. Une fois le profil activé, le client sans fil s'associe au WLAN après une authentification réussie.Voici la capture d'écran

🖻 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		

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Ces commandes debug seront utiles pour dépanner la configuration :

Remarque : Consulter les <u>renseignements importants sur les commandes de débogage</u> avant d'utiliser les commandes de **débogage**.

 debug dot1x events enable : active le débogage de tous les événements dot1x. Voici un exemple de résultat de débogage basé sur une authentification réussie :Remarque : certaines des lignes de cette sortie ont été déplacées vers des secondes lignes en raison de limitations d'espace.

```
(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
```

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 packet enable : active le débogage des messages de paquets 802.1x.
- debug aaa events enable : active la sortie de débogage de tous les événements aaa.

Informations connexes

- WPA2 Wi-Fi Protected Access 2
- Exemple de configuration d'authentification EAP-FAST avec des contrôleurs de réseau local sans fil et un serveur RADIUS externe
- Exemple de configuration de l'authentification EAP avec des contrôleurs de réseau local sans fil (WLC)
- Présentation de la configuration WPA
- <u>Assistance produit sans fil</u>
- Assistance et documentation techniques Cisco Systems

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.