Configuratie-voorbeeld van splitste pagina voor draadloze LAN-controllers

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Conventies Achtergrondinformatie Netwerkinstelling Configureren Stap 1. Configureer de WLC voor RADIUS-verificatie via de Cisco Secure ACS-server. Stap 2. Configureer de WLAN's voor de afdeling Beheer en bewerkingen. Stap 3. Configureer de Cisco Secure ACS om de functie voor omleiding van spatpagina's te ondersteunen. Verifiëren Problemen oplossen Gerelateerde informatie

Inleiding

Dit document beschrijft hoe u de spatpagina kunt configureren en de functie voor omleiding naar de draadloze LAN-controllers kunt omleiden.

Voorwaarden

Vereisten

Voordat u deze configuratie uitvoert, moet aan de volgende vereisten worden voldaan:

- Kennis van LWAP-beveiligingsoplossingen
- Kennis van de configuratie van Cisco Secure ACS

Gebruikte componenten

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

 Cisco 4400 Series draadloze LAN-controller (WLC) waarop firmware versie 5.0 wordt uitgevoerd

- Cisco 1232 Series lichtgewicht access point (LAP)
- Cisco Aironet 802.a/b/g draadloze clientadapter waarop firmware versie 4.1 wordt uitgevoerd
- Cisco Secure ACS-server waarop versie 4.1 wordt uitgevoerd
- Alle externe webservers van derden

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

Achtergrondinformatie

Splash Page Web redirect is een functie die is geïntroduceerd met Wireless LAN Controller versie 5.0. Met deze functie wordt de gebruiker omgeleid naar een bepaalde webpagina nadat de 802.1x-verificatie is voltooid. De omleiding gebeurt wanneer de gebruiker een browser opent (geconfigureerd met een standaard startpagina) of probeert om toegang te krijgen tot een URL. Nadat de omleiding naar de webpagina is voltooid, heeft de gebruiker volledige toegang tot het netwerk.

U kunt de omleidingspagina opgeven op de RADIUS-server (Remote Authentication Dial-In User Service). De RADIUS-server moet worden geconfigureerd om het Cisco av-paar url-redirect RADIUS-kenmerk naar de draadloze LAN-controller terug te sturen bij succesvolle 802.1x-verificatie.

De functie Splash page web redirect is alleen beschikbaar voor WLAN's die geconfigureerd zijn voor 802.1x of WPA/WPA2 Layer 2-beveiliging.

Netwerkinstelling

In dit voorbeeld worden een Cisco 4404 WLC en een Cisco 1232 Series LAMP aangesloten via een Layer 2 switch. De Cisco Secure ACS-server (die als een externe RADIUS-server fungeert) is ook verbonden met dezelfde switch. Alle apparaten bevinden zich in hetzelfde subnetje.

De LAP is oorspronkelijk geregistreerd bij de controller. U moet twee WLAN's maken: een voor de **Admin Department**-gebruikers en een voor de gebruikers van de **Operations Department**. Beide draadloze LAN's gebruiken WPA2/AES (EAP-FAST wordt gebruikt voor verificatie). Beide WLAN's gebruiken de functie Splash Page Redirect om gebruikers te doorsturen naar de juiste URL's van de startpagina (op externe webservers).

Het netwerk in dit document is als volgt opgebouwd:



Cisco Secure ACS server

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

In het volgende gedeelte wordt uitgelegd hoe u de apparaten voor deze installatie kunt configureren.

Configureren

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

Opmerking: Gebruik de <u>Command Lookup Tool (alleen voor geregistreerde klanten) voor meer</u> informatie over de opdrachten die in deze sectie worden gebruikt.

Voltooi deze stappen om de apparaten te configureren voor het gebruik van de splash pagina omleiden functie:

- 1. <u>Configureer de WLC voor RADIUS-verificatie via de Cisco Secure ACS-server.</u>
- 2. Configureer de WLAN's voor de Admin- en Operations-afdelingen.
- 3. <u>Configureer de Cisco Secure ACS-software om de functie voor omleiding van spatpagina's te ondersteunen.</u>

Stap 1. Configureer de WLC voor RADIUS-verificatie via de Cisco Secure ACSserver.

De WLC moet worden geconfigureerd om de gebruikersreferenties te kunnen doorsturen naar een externe RADIUS-server.

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.
- 2. Klik op Nieuw om een RADIUS-server te definiëren.
- 3. Definieer de RADIUS-serverparameters op de RADIUS-verificatieservers > Nieuwe pagina.Deze parameters omvatten:IP-adres voor RADIUS-serverGedeeld geheimPoortnummerServerstatus

- ahaha				Sage Co	nfiguration Eing	Logout Befresh
CISCO	MONITOR WLANS CONTRO	OLLER WIRELESS SECURITY	MANAGEMENT	COMMANDS	нецр	_
Security	RADIUS Authentication S	ervers > New			< 8ack	Apply
Security AAA General RADIUS Authentication Accounting TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Local EAP Priority Order Access Control Lists Wireless Protection Policies Web Auth Advanced	RADIUS Authentication S Server Index (Priority) Server IPAddress Shared Secret Format Shared Secret Confirm Shared Secret Key Wrap Port Number Server Status Support for RFC 3576 Server Timeout Network User Management IPSec	I I I IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	s and requires a key	y wrap compliant	< Back	Apply

Dit document gebruikt de ACS-server met een IP-adres van 10.7.244.196.

4. Klik op Apply (Toepassen).

Stap 2. Configureer de WLAN's voor de afdeling Beheer en bewerkingen.

In deze stap configureert u de twee WLAN's (een voor de Admin-afdeling en een voor de Operations-afdeling) die de clients zullen gebruiken om verbinding te maken met het draadloze netwerk.

De WLAN-SSID voor de Admin-afdeling is *Admin*. WLAN SSID voor de afdeling Verrichtingen zal Verrichtingen zijn.

Gebruik EAP-FAST-verificatie om WPA2 als Layer 2-beveiligingsmechanisme in te schakelen op zowel WLAN's als het webbeleid - Splitpagina Web Redirect-functie als Layer 3-

beveiligingsmethode.

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.			_			Sage Co	nfiguration Bing	Logout Refresh
cisco	MONITOR WLANS		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
WLANs	WLANs > New						< Back	Apply
WLANS	Туре	WLAN	×					
▶ Advanced	Profile Name	Admin						
	WLAN SSID	Admin						

- 3. Voer op de WLAN's > Nieuwe pagina de WLAN-SSID-naam en de profielnaam in.
- 4. Klik op Apply (Toepassen).
- 5. Laat ons eerst het WLAN voor de Admin-afdeling maken.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, Veiligheidsbeleid, beleid QOS, en Geavanceerde parameters.
- 6. Onder Algemeen beleid schakelt u het selectievakje **Status** in om het WLAN in te schakelen.

CISCO MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP WLANS WLANS > Edit Apply WLANS WLANS General Security QoS Advanced Profile Name Admin YULANS Profile Name Admin						Sa <u>v</u> e Co	onfiguration Ei	ng Logout <u>R</u> efre
WLANs WLANs > Edit < Back	CISCO	MONITOR WLANS	CONTROLLER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
	CISCO WLANS WLANS WLANS Advanced	WLANS > Edit General Secur Profile Name Type SSID Status Security Policies Radio Policy Interface Broadcast SSID	CONTROLLER WIRELESS ity QoS Advanced Admin WLAN Admin I Enabled Splash-Page-Web-R (Modifications done under All ■ admin ■ Enabled	SECURITY edirect[WPA2 tr security tab	MANAGEMENT 2][Auth(802.1X)] will appear after aj	COMMANDS	HELP C Back	Apply

- 7. Klik op het tabblad Beveiliging en klik vervolgens op het tabblad Layer 2.
- Kies WPA+WPA2 in de vervolgkeuzelijst Layer 2 Security.Deze stap schakelt WPAverificatie in voor het WLAN.
- 9. Selecteer onder WPA+WPA2-parameters de selectievakjes **WPA2-beleid** en **AES**encryptie.

- ahaha					Saye Co	infiguration Ping	Logout Befre
CISCO	MONITOR WLANS	CONTROLLER WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	
WLANS WLANS WLANS WLANS Advanced	MONITOR WLAWS WLANS > Edit General Secur Layer 2 Layer Layer 2 Security WPA+WPA2 Paraton WPA Policy WPA2 Policy WPA2 Encryptio Auth Key Mgmt	CONTROLLER WIRELESS	SECURITY	MANAGEMENT		HELP < Back	Apply

- 10. Kies **802.1x** in de vervolgkeuzelijst Beheer autosleutel. Met deze optie wordt WPA2 met 802.1x/EAP-verificatie en AES-encryptie voor het WLAN ingeschakeld.
- 11. Klik op Layer 3 Security tabblad.
- 12. Controleer het vakje **Web Policy** en klik vervolgens op het keuzerondje **Splash Page Web Redirect**.Deze optie maakt de splash pagina web Redirect functie mogelijk

CISCO MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP WLANS WLANS > Edit < Back Apply WLANS WLANS General Security QoS Advanced WLANS WLANS Layer 3 AAA Servers Itayer 3 Security None Itayer 3 Security None Itayer 3 Security None Itayer 3 Security Itayer 3 Security None Itayer 3 Security Itayer 3 Security						Sa <u>v</u> e Co	nfiguration + Ping	Logout <u>R</u> efre
WLANS WLANS > Edit < Back Apply WLANS WLANS General Security QoS Advanced I Layer 2 Layer 3 AAA Servers I Layer 3 Security None Web Policy 4 Authentication Passthrough Conditional Web Redirect Splash Page Web Redirect Preauthentication None Preauthentication None None	CISCO	MONITOR WLANS	ONTROLLER WIRELES	SECURITY	MANAGEMENT	COMMANDS	HELP	_
	WLANS WLANS WLANS Advanced	WLANS > Edit General Security Layer 2 Layer Layer 3 Security Web Policy 2 Authentication Passthrough Conditional Wel Splash Page We Preauthentication ACL	QoS Advanced 3 AAA Servers None b Redirect eb Redirect None				< Back	Apply

- 13. Klik op het tabblad **AAA-servers**.
- 14. Kies onder Verificatieservers het juiste IP-adres van de server in de vervolgkeuzelijst Server

	Sa <u>v</u> e Configuration <u>P</u> ing Logo	ut i <u>8</u> e
CISCO	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP	
WLANs	WLANs > Edit < Back A General Security QoS Advanced	ipply
WLANS WLANS Advanced	Layer 2 Layer 3 AAA Servers	4
	Select AAA servers below to override use of default servers on this WLAN Radius Servers Authentication Servers Accounting Servers Server 1 None • Server IP:10.77.244.196, Port:1812 • None • Server 3 None • Server None • None • Server 3 None • Server None • None • Server 3 None • Local EAP Authentication Enabled Enabled Server 3 None •	
	web-auth user	ł

In dit voorbeeld wordt 10.77.24.196 gebruikt als de RADIUS-server.

- 15. Klik op **Apply** (Toepassen).
- 16. Herhaal stap 2 tot en met 15 om het WLAN voor de Operations-afdeling te maken.De WLAN-pagina maakt een lijst van de twee WLAN's die u hebt gemaakt

gemaakt.									
ahaha								onfiguration	<u> Ping Logout R</u> efresh
CISCO	MONITOR	<u>W</u> LANs		WIRELESS	S SECURITY	MANAGEMENT	COMMANDS	HELP	
WLANs	WLANs								New
WLANS WLANS	Profile Na	me	Ту	pe w	LAN SSID		Admin Status	Security Poli	icies
Advanced	Admin		WI	AN A	dmin		Enabled	[WPA2][Auth(802.1X)], Splash-Page
	Operations		WI	AN O	perations		Enabled	[WPA2][Auth(802.1X)], Splash-Page

Bericht dat het veiligheidsbeleid de spatpagina omvat richt opnieuw.

Stap 3. Configureer de Cisco Secure ACS om de functie voor omleiding van spatpagina's te ondersteunen.

De volgende stap is de RADIUS-server voor deze functie te configureren. De RADIUS-server moet EAP-FAST-verificatie uitvoeren om de clientreferenties te valideren en de gebruiker, na succesvolle verificatie, door te sturen naar de URL (op de externe webserver) die in het Cisco avpair *url-redirect* RADIUS-kenmerk is gespecificeerd.

De Cisco Secure ACS-software voor EAP-FAST-verificatie configureren

N.B.: In dit document wordt ervan uitgegaan dat de draadloze LAN-controller aan Cisco Secure ACS wordt toegevoegd als een AAA-client.

Voltooi de volgende stappen om EAP-FAST-verificatie in de RADIUS-server te configureren:

1. Klik op **Systeemconfiguratie** vanuit de RADIUS-server GUI en kies vervolgens **Globale verificatie-instellingen** op de pagina



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

🙆 hetp://127.0	.0.1:1065/	• 🖸 🛛
STATEMA	System Configuration	[
in and in the second	EAP Configuration	P Help
roup etup	PEAP	Use this pape to specify settings for various authentication protocols. • CAP Conferentiate
nd Profile onenAs	Allow Posture Validation	• <u>PEAP</u> • <u>EAP-FASX</u> • <u>EAP-FASX</u>
ation.	Allow EAP-TLS Select one or more of the following options: E Certificate SAN comparison	LAP_SED AP_EAP_Report Dimensit Statistic Configuration
	EAP-TLS session timeout (minutes): 120	EAP Configuration EAP is a flavible request-response protocol for arbitrary
1	Cisco client initial message:	authentication information (RPC 2284). EAP is layered on top of another protocol such as UOP, 802.1× or RADIUS and supports multiple "authentication" types.
1	Enable Fast Reconnect:	(Back to Tip) PEAP
	EAP-FAST EAP-FAST Configuration	PEAP is the outer layer protocol for the secure tunnel.
1	EAP-TLS	— Notes HAP is a contribute-based authentication protocol. HAP authentication can occur only after you have completed the required steps on the ACS Certificate Setup page .
	Select one or more of the following options: Certificate SAN comparison	Allow EAP-MSCHAPv2 - Use to enable EAP-MSCHAPv2 within MS PEAP authentication. Enable this protacol for any repository that supports MS- CHAPv2, such as Microsoft AD, and the ACS Internal Database.
	Submit Submit + Restart Cancel	s()

3. Selecteer op de pagina EAP-FAST-instellingen het aanvinkvakje **Allow EAP-FAST** om EAP-FAST in de RADIUS-server in te schakelen.

CiscoSecure ACS - N	Scrosoft Internet Explorer	<u>= 10 ×</u>
Ele Edt Yew Fg	vonkes Iools Help	Links 🍄 🤷
Address http://127./	0.0.1:1065/	💌 🛃 60
Cisco Storens	System Configuration	
Uger Setup Uger Setup Daved Profile Composents Network Composents Setup Network Configuration Config	EAP-FAST Configuration EAP-FAST Settings EAP-FAST Active master key TTL Active master key TTL Retired master key TTL Tunnel PAC TTL Client initial message: Authority ID Info: Allow anonymous in-band PAC provisioning Allow authenticated in-band PAC provisioning Allow authenticated in-band PAC provisioning Require client certificate for provisioning Allow Machine Authentication Machine PAC TTL Weeks	 Help EAP-FAST Configuration Page Use this page to configure EAP-FAST authentication settings. CAP-FAST Settings Client initial measures Authority ID Jafe Authority ID Jafe Allers assigness in Sand PAC provisioning Allers machine systematication Allers tatafasts session thread CAP-TAST Sectings Allers EAP-FAST Settings Allers EAP-FAST To enable EAP-FAST authentication, select this check base. Active Master Key TR – Enter a value for the amount of time that a master key is used to generate new Pertected Access Credentials (PACe), bithes the the term of the set CTM bits after the set of the set
Online Documentation	Allow Stateless session resume Authorization PAC TTL 1 hours Allowed inner methods REAP-GTC REAP-MSCHAPV2 EAP-TLS Submit Submit + Restart Cancel	 Under the lowe (TTL) defined have the Master Key is generated. Retered master key TIL -Enter a value for the amount of time that PACs generated using a retired master key is capability for EAD-FAST authentication. When an end-user client gains network access using a PAC based on a retired master key. ACS sends a new PAC to the end-user client. Tennel PAC TIL - Enter a value for the amount of time that a PAC is used on a retired master key. ACS sends a new PAC to the end-user client. Tennel PAC TIL - Enter a value for the amount of time that a PAC is used baffore it explores and must be repliced. If the master key used to generate the Tunnel PAC expired, automatic, if the master key used to generate the Tunnel PAC expired, automatic, or amound provisioning must be used to provide the end-user client with a new PAC.
		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.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. De optie *Toegestane innerlijke methoden* bepaalt welke innerlijke EAP-methoden binnen de EAP-FAST TLS-tunnel kunnen worden uitgevoerd. 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.
- Klik op Verzenden.N.B.: Raadpleeg <u>EAP-FAST-verificatie met draadloze LAN-controllers</u> en <u>externe RADIUS-serverconfiguratievoorbeeld voor</u> gedetailleerde informatie <u>en</u> voorbeelden voor het configureren van EAP FAST met anonieme in-band PAC_provisioning <u>en</u> geverifieerde in-band <u>provisioning</u>.

De gebruikersdatabase configureren en het kenmerk url-redirect RADIUS definiëren

In dit voorbeeld worden de gebruikersnaam en het wachtwoord van de draadloze client geconfigureerd als respectievelijk Gebruiker1 en Gebruiker1.

Voltooi de volgende stappen om een gebruikersdatabase te maken:

- 1. Kies Gebruiker instellen in de ACS GUI op de navigatiebalk.
- 2. Maak een nieuwe draadloze gebruiker en klik vervolgens op **Toevoegen/Bewerken** om naar de pagina Bewerken van deze gebruiker te

Bit dat yow Fyrontes look help Last Address Provides Percental Control	CiscoSecure ACS - Mi	icrosoft Internet Explorer	
Agentes Agentes Petrop Pe	Ele Edit Yew Favo	anites Isols Help	Links 🏁 📿
Cittee Strives User Setup Store Store Image: Strives Store <tr< th=""><th>lgdress 😸 http://127.0.</th><th>.0.1:1065/</th><th>• 🔁 😡</th></tr<>	lgdress 😸 http://127.0.	.0.1:1065/	• 🔁 😡
 Stort Stort	Cinco Syntems	User Setup	Σ
Were Bere Were Steps Were Steps Bere Steps	alberalber	Select	Help
Finding a Specific User in the ACS Internal Gatabase To find a user already in the ACS Internal Gatabase To find a user already in the ACS internal database, type the first fe of the username in the Buer field, add an articrist (*) as a wildcard, Find. From the bits of usernames dispert. Set the username when information you want to view or change.	Viser Setup Setup Setup Setup Seturation Se	User: User1 Find Add/Edit List users beginning with letter/number: ARSPOPBSISYYXX DDPOPBSISYYXX List all users Remove Dynamic Users Reat to help	 Shee Satup and External Over Databases Gudina a Specific Uver in the ASS Internal Database Addina a Uver in the ASS Internal Database Uring Uvernames that Devin with a Particular Cheracter Uring Uvernames in the ASS Internal Outboard Chanding a Uvernames in the ASS Internal Database Uring Uvernames in the ASS Internal Outboard Chanding a Uvernames in the ASS Internal Outboard Chanding a Uvernames in the ASS Internal Uver Database Emmers Database in the ASS Internal Uver Database Benness Database uses in the database. Uver Satup and External Uver Databases Before ASS can authenticate upper with an external user databases You must have the database user Satup and External Uver Databases You must have the database user of authentication, your taken server must be running and pengerly configuration overrides Group Satup configuration. You must have configuration overrides Group Satup configuration. Mess Uver Satup configuration overrides Group Satup configuration in an external user database, user has successfully authenticate occ. Database section. Deter Satup Canfiguration overrides Group Satup configuration in an external user database, usernames cannot be located or listed here ustil the user has successfully authenticated once. Datamal user database modification must be done from within the external user database. User Satup configure individual outer information, add users, and delete users in the ACS internal Database. Neter User Satup keeps track of users who authenticate with an external user database. User Satup keeps track of users who authenticate with an external user database. User Satup keeps track of users and authenticates information, add users, and delete users in the ACS internal database. Database Individual outer field, add an asternal dutabase. Database subser fissel for a fastemes displayed. Cick

3. Van de Opstelling van de Gebruiker Bewerk pagina, vorm Echte Naam en Beschrijving, evenals de Instellingen van het Wachtwoord, zoals in dit voorbeeld wordt getoond.Dit document maakt gebruik van de ACS Interne Database voor wachtwoordverificatie.

Edit Yew Fa	workes Tools Help	Links *
8 (a) http://127.	0.0.1:1065/	-
tes Statema	User Setup	
h. d.	Edit	Help
User Setup Setup	User: User1 (New User)	Account Disabled Defeting a Username Septementary User Info
Shared Profile Components	Account Disabled	Password Anthentication Group to which the user is assigned Callback
Network Configuration	Supplementary User Info	Client UP Address Assignment Advanced Sattlens Natured: Access Restrictions
System Configuration Interface Configuration	Description	Han Searcon Units Overlag Occount.Disable Occount.Seable
Administration Control	User Setup 9	Advanced IACACS - Settings IACACS - Coulds Control IACACS - Coulds Control IACACS - Coulds Parament IACACS - Defining Parament
Databases Porture Validation	Password Authentication: ACS Internal Database	IACACS - Shell Command Authorization Command Authorization IACACS - Unknown Service Network Device Nanasement Auditations IACACS - Unknown IET RADIUS Attributes
Network Access Profiles Reports and	CiscoSecure PAP (Also used for CHAP/MS- CHAP/ARAP, if the Separate field is not checked.)	BADUDS Yeadar Sanoth: Attributes
Activity Online Documentation	Password	Account Disabled Status Select the Account Disabled check box to disable this account: clear
	Separate (CHAP/MS-CHAP/ARAP)	[Rack to Trp]
	Password	Deleting a Username
	Password Submit Cancel	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 current user account from the database, click Delete . When asked to confirm your action, click OK .

- 4. Blader naar beneden om de RADIUS-kenmerken aan te passen.
- 5. Controleer het aanvinkvakje [009\001] Cisco-av-paar.
- 6. Voer dit Cisco v-paar in het bewerkingsvak [009\001] cisco-av-paar in om de URL te specificeren waarnaar de gebruiker wordt doorgestuurd:urlredirect=http://10.77.244.196/Admin-Login.html



Dit is de startpagina van de Admin afdeling gebruikers.

- 7. Klik op Verzenden.
- 8. Herhaal deze procedure om Gebruiker2 (Operations Department user) toe te voegen.
- Herhaal stap 1 tot en met 6 om meer gebruikers van de Admin-afdeling en gebruikers van de Operations-afdeling aan de database toe te voegen. Opmerking: de RADIUS-kenmerken kunnen op gebruikersniveau of groepsniveau worden geconfigureerd op Cisco Secure ACS.

Verifiëren

Om de configuratie te verifiëren, koppelt u een WLAN-client van de Admin-afdeling en de Operations-afdeling aan hun juiste WLAN's.

Wanneer een gebruiker van de beheerafdeling verbinding maakt met de draadloze LANbeheerder, wordt de gebruiker gevraagd om 802.1x-referenties (EAP-FAST-referenties in ons geval). Zodra de gebruiker de referenties verstrekt, gaat de WLC die referenties over naar de Cisco Secure ACS-server. De Cisco Secure ACS-server valideert de referenties van de gebruiker aan de hand van de database en retourneert, na succesvolle verificatie, het kenmerk url-redirect naar de draadloze LAN-controller. De authenticatie is in dit stadium voltooid.

🛜 Cisco Aironet Desktop Utility	y - Current Profile: Admin		? 🗙
Action Options Help			
Current Status Profile Management	Diagnostics		
CISCO SYSTEMS			
utilituu Profile Name:	Admin		
Link Status:	Not Associated	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	

Wanneer de gebruiker een webbrowser opent, wordt de gebruiker omgeleid naar de startpagina URL van de Admin afdeling. (Deze URL wordt door het Cisco-av-paar attribuut teruggegeven aan de WLC.) Nadat de omleiding is uitgevoerd, heeft de gebruiker volledige toegang tot het netwerk. Hier zijn de screenshots:



De zelfde opeenvolgingen van gebeurtenissen komen voor wanneer een gebruiker van de

afdeling van Verrichtingen met de Verrichtingen van WLAN verbindt.

cisco Anoner	and the second		· · · · · · · · · · · · · · · · · · ·
ion <u>O</u> ptions <u>H</u> e	elp		
urrent Status Pro	ofile Management	Diagnostics	
CISCO SYSTEMS			
ահուսդիր	Profile Name:	Operations	
	Link Status:	Authenticated	Network Type: Infrastructure
	Wireless Mode:	5 GHz 54 Mbps	Current Channel: 149
Server Based	ed Authentication:	EAP-FAST	Data Encryption: AES
	IP Address:	10.77.244.221	
	Signal Strength:		Good
			Advanced
			Advanced
			Advanced
ome to the Operations Departm	ent - Nicrosoft Internet Explor	¢f	Advanced
me to the Operations Departm	ert - Microsoft Internet Laplar	" A 2 -	Advanced
ome to the Operations Departm	ent - Microsoft leternet Explor	er 🏂 چ 🖼 🎕	Advanced
one to the Operations Repartm	ent - Nicrosoft leternet Explor	er 🏂 📚 🕞 🎕	Advanced
ome to the Operations Departm	ert Microsoft leternet Lupler	e to the Operation	Advanced
ome to the Operations Departm	eet Microsoft Internet Laplar	e to the Operation	Advanced Image: Second secon
orne to the Dyenations Departm Control Control Contro	ert - Microsoft Internet Lapler	to the Operation	Advanced Image: Second state Image: Second state <t< td=""></t<>
ome to the Operations Departm	welcome	to the Operation	Advanced
erre to the Operations Department () () () () () () () () () () () () () (ert Microsoft leternet Lupler	to the Operatio	Advanced Image: Second state Image: Second state <t< td=""></t<>
erree to the Operations Department Control Control Con	ert Microsoft Internet Laplar	to the Operation	Advanced Image: Second state Image: Second state Image: Second state
erre fo the Operations Departm Constructions (Constructions) Constructions (Constructions)	welcome	to the Operation	Advanced
orne to the Operations Department () () () () () () () () () () () () () (eet Microsoft leternet Lupler	e to the Operatio	Advanced The second se
orne to the Operations Department Control of the Operations Departmen	ert - Microsoft Internet Laplar	to the Operation	Advanced Image: State of the st

🛃 start 👔 😨 Gees Associ Deskte...... 🗿 Welcone to the Oper...

Problemen oplossen

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

.

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

U kunt de volgende opdrachten gebruiken om problemen met uw configuratie op te lossen.

 show wlan_id-Toont de status van het web omleiden functies voor een bepaalde WLAN.Hierna volgt een voorbeeld:

WLAN Identifier	1	
Profile Name	Admin	
Network Name (SSID)	Admin	
Web Based Authentication		
Web-Passthrough	Disabled	
Conditional Web Redirect	Disabled	
Splash-Page Web Redirect	Enabled	

- debug dot1x gebeurtenissen enabled-laat het debug van 802.1x pakketberichten toe.Hierna volgt een voorbeeld:
 - Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Sending EAP Request from AAA to
 mobile 00:40:96:ac:dd:05 (EAP Id 16)
 - Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Received EAPOL EAPPKT from
 mobile 00:40:96:ac:dd:05
 - Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Received EAP Response from
 mobile 00:40:96:ac:dd:05 (EAP Id 16, EAP Type 43)
 - Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Processing Access-Challenge for mobile 00:40:96:ac:dd:05
 - Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Setting re-auth timeout to 1800
 seconds, got from WLAN config.
 - Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Station 00:40:96:ac:dd:05
 setting dot1x reauth timeout = 1800
 - Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Creating a new PMK Cache Entry
 for station 00:40:96:ac:dd:05 (RSN 2)
 - Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Adding BSSID 00:1c:58:05:e9:cf
 to PMKID cache for station 00:40:96:ac:dd:05
 - Fri Feb 29 10:27:16 2008: New PMKID: (16)
 - Fri Feb 29 10:27:16 2008: [0000] 79 ee 88 78 9c 71 41 f0 10 7d 31 ca fb fa 8e 3c
 - Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Disabling re-auth since PMK
 lifetime can take care of same.
 - Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Sending EAP-Success to mobile 00:40:96:ac:dd:05 (EAP Id 17)
 - Fri Feb 29 10:27:16 2008: Including PMKID in M1 (16)
 - Fri Feb 29 10:27:16 2008: [0000] 79 ee 88 78 9c 71 41 f0 10 7d 31 ca fb fa 8e 3c
 - Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Sending EAPOL-Key Message to mobile 00:40:96:ac:dd:05
 - state INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00
 Fri Feb 29 10:27:16 2008: 00:40:96:ac:dd:05 Received Auth Success while
 in Authenticating state for mobile 00:40:96:ac:dd:05
- debug aaa gebeurtenissen enable-Enabled de debug output van alle aaa gebeurtenissen.Hierna volgt een voorbeeld:
 - Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Successful transmission of Authentication Packet (id 103) to 10.77.244.196:1812, proxy state 00:40:96:ac:dd:05-00:00

Thu Feb 28 07:55:18 2008: ****Enter processIncomingMessages: response code=11 Thu Feb 28 07:55:18 2008: ****Enter processRadiusResponse: response code=11 Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Access-Challenge received from RADIUS server 10.77.244.196 for mobile 00:40:96:ac:dd:05 receiveId = 3

```
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Successful transmission of
```

```
Authentication Packet (id 104) to 10.77.244.196:1812, proxy state
    00:40:96:ac:dd:05-00:00
Thu Feb 28 07:55:18 2008: ****Enter processIncomingMessages: response code=2
Thu Feb 28 07:55:18 2008: ****Enter processRadiusResponse: response code=2
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Access-Accept received from
   RADIUS server 10.77.244.196 for mobile 00:40:96:ac:dd:05 receiveId = 3
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 AAA Override Url-Redirect
    'http://10.77.244.196/Admin-login.html' set
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Applying new AAA override for
   station 00:40:96:ac:dd:05
Thu Feb 28 07:55:18 2008: 00:40:96:ac:dd:05 Override values for station
   00:40:96:ac:dd:05
      source: 4, valid bits: 0x0
      qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1
      dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
      vlanIfName: '', aclName: '
```

Gerelateerde informatie

- Configuratiehandleiding voor Cisco draadloze LAN-controllers, release 5.0
- Configuratie van draadloze LAN-controller en webverificatie voorbeeld
- <u>Configuratie-voorbeeld van externe webverificatie met draadloze LAN-controllers</u>
- Pagina voor draadloze ondersteuning
- <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.