ACS versie 5.2 en WLC voor per WLANverificatievoorbeeld

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Configureren De WLC configureren Cisco beveiligde ACS configureren Verifiëren Problemen oplossen

Inleiding

Dit document biedt een configuratievoorbeeld om de toegang voor elke gebruiker tot een Wireless LAN (WLAN) te beperken op basis van de Service set-identifier (SSID).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Hoe u de draadloze LAN-controller (WLC) en het lichtgewicht access point (LAP) voor basisbediening kunt configureren
- Hoe u de Cisco Secure Access Control Server (ACS) configureren
- Lichtgewicht Access Point Protocol (LWAPP) en draadloze beveiligingsmethoden

Gebruikte componenten

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

- Cisco 5500 Series WLC-software met firmware versie 7.4.10
- Cisco 1142 Series LAP
- Cisco Secure ACS Server versie 5.2.0.2.11

Configureren

Om de apparaten voor deze instelling te configureren hebt u het volgende nodig:

1. Configureer de WLC voor de twee WLAN's en RADIUS-server.

- 2. Configureer de Cisco beveiligde ACS.
- 3. Configureer de draadloze clients en controleer de configuratie.

De WLC configureren

Volg deze stappen om de WLC te configureren voor deze instelling:

 Configureer de WLC om de gebruikersreferenties naar een externe RADIUS-server door te sturen. De externe RADIUS-server (Cisco Secure ACS in dit geval) bevestigt vervolgens de gebruikersreferenties en geeft toegang tot de draadloze clients. Voer de volgende stappen uit: Selecteer Security > RADIUS-verificatie van de controller GUI om de pagina RADIUSverificatieservers weer te geven.



Klik op **New** om de RADIUS-serverparameters te definiëren. Deze parameters omvatten het IP-adres van de RADIUS-server, gedeeld geheim, poortnummer en serverstatus. De selectieteksten Netwerkgebruiker en -beheer bepalen of de op RADIUS gebaseerde verificatie van toepassing is op beheer- en netwerkgebruikers. Dit voorbeeld gebruikt Cisco Secure ACS als de RADIUS-server met IP-adres

ahaha							
CISCO	MOVELOK MEANE CORLECT	TEM MÅMETERE BECTK	T NEVABORE/T	CONFRANCS	H=_F	Feenback	
Security	RADIUS Authentication Se	rvers > New					< 8 ack
General	Server Index (Priority)	1 💌					
* RADIUS	Sarver 37 Address	10104.20555					
Assounting	Shared Secret Format	45C0 📼					
Fallback	Shared Secret	*******					
LDAP	Contino Shared Secret	******			_		
Local Net Dates							
Disabled Clients	KLY WE UP	Catigraphic for E20 are	-mart so red that a	pair yeah comp	Art RODE	IS cerver)	
Hoer Logo Rolinaet	PerCitamber	1:12					
Parenant Palmar	Server Status	Tashari 📼					
Local LAP	Support for RFC 3576	backed in					
Priority Order	Server Timeout	2 example					
Certificate	Notwork User	2 Chatle					
Access Control Lists	Planagement	🖾 Erable					
Wireless Protection	IPSec	Enable					
Policies							
Web Auth							
TrestSec SXP							
Advanced							

Klik op Toepassen.

2. Voltooi deze stappen om één WLAN voor de werknemer met SSID werknemer en de andere WLAN's voor contracteurs met SSID Contractor te configureren. Klik op WLAN's van de controller GUI om een WLAN-functie te maken. Het WLAN-venster verschijnt. Dit venster toont de WLAN's die op de controller zijn geconfigureerd.Klik op **New** om een nieuwe WLAN te configureren.Dit voorbeeld creëert een WLAN met de naam Werknemer en de WLAN-id is 1 Klik op **Toepassen**

1. I XIIIX OP 1	oepassen.								
 cisco	MONITOR MUANE	CONTROLLER ACRELESS	SECURTY	NB/AGENE/T	ODANANOS	HE,F	ESEMACK	Sage Configuration _ ging	Logost Befreit
WLANs	WLANs > New				_			< Back	Apply
 WLANS WLANS ▶ Advanced 	Type Profile Name SSID ID	milAhi ma E-pinyeu F-pinyen 1 m							

Selecteer het WLAN > Bewerken venster en definieer de parameters die specifiek zijn voor WLAN: Selecteer in het tabblad Layer 2 Security **de optie 802.1x**. Layer 2 Security optie is standaard 802.1x. Dit maakt 802.1 x/Extensible Authentication Protocol (EAP) authenticaties mogelijk voor het WLAN.



Selecteer in het tabblad AAA-servers de juiste RADIUS-server in de vervolgkeuzelijst onder RADIUS-servers. De andere parameters kunnen worden gewijzigd op basis van de vereisten van het WLAN-netwerk. Klik op **Toepassen**.

cisco	MONITOR MITANE CONTROTTER AGAETERS RECTELIA AGARGEMENT COMMANCE METE RECORDOK	Sage Centquisten (Englis Lagest Batresh
WLANs	WLANs > Edit 'Employee'	< Buck Apply
* WLANS WLANS	General Security QaS Advanced	
> Advanced	Layer 2 Layer 3 AAA Servers	
	Select AAA servers below to override use at default servers on this MLXN	Ť.
	Radius Servers LDBP Servers	
	Saler Liber -	-
	Autority beres According beres Strate to a	=
	Server 2 bors a Real	
	Science 2 Barra Tradition	
	the second se	
	Server 5 tone There	
	Server 5 tote a Tex	
	Radius Server Accounting	
	Interim Update	
	Local EAP Authentication	
	x[
	Fost Notes	
	2 West Party memory to use a construction with Party 2 Meet Party in the distribution is not constructed with Party Add META a mention for the state that the state of the state of the state of the state of the state of the INTER a mention for the state of the state of the state of the state of the state of the state of the state of the INTER as mention for the state of the state of the state of the state of the state of the state of the state of the INTER as mention for the state of the stat	

Op dezelfde manier herhaalt u stappen b tot d om een WLAN-oplossing voor contractanten te maken.

Cisco beveiligde ACS configureren

Op de Cisco Secure ACS-server moet u:

- 1. Configureer de WLC als een AAA-client.
- 2. Maak de gebruikersdatabase (Credentials) voor op SSID gebaseerde verificatie.
- 3. MAP-verificatie inschakelen.

Voltooi deze stappen op Cisco Secure ACS:

- Om de controller als een AAA-client op de ACS-server te definiëren, selecteert u Netwerkbronnen > Netwerkapparaten en AAA-clients vanuit de ACS-GUI. Klik onder Netwerkapparaten en AAA-clients op Maken.
- 2. Wanneer de pagina Network Configuration verschijnt, specificeert u de naam van de WLC, IP-adres en gedeelde geheime en verificatiemethode (RADIUS).

States in the latter of the	NAME & ADDRESS OF STREET	the state of the s	· · ·		
🔶 🕞 🥝 Large / 100.00 4.200.56 (scrad)	nn/ D + O Cettle 2 G X 6 Cisco Secure ACS	x and the factor seed			h 🛨 🛙
× Gara Browner WebEc •					
cisco Secure A cisco EVAL(Days left: 5)	CS		acautein	aca licesplaite (Primary)	Log Out About Help
» ∯ MyWorkspace	Network Resources > Network Devices and AAA Clerits > Create				
Notwork Research Notwork Device Groups Location Device Type Notwork Device and AAA Clients Device Type Notwork Device and AAA Clients Device Type Device Type	Name: DOT4 Description: Network Device Groups Location Device Type All Device Types P Address	Serect Serect Authentication Options			
Access Policies Monitoring and Raports Monitoring And Raports Might System Administration	Single IP Address P Range(s) IP: 10.105.98.4	Shared Secret	Nice Single ConnectSupport		
	* Sumi Carce	RADUS RADUS RADUS Shared Secret. 2000 CoAppt: 1780 Enable KeyWrap Nery Encrysten Key.	201		
	Sumic Carca				

3. Selecteer Gebruikers- en identiteitsopslag > Identiteitsgroepen uit de ACS-GUI. Maak de

respectievelijke groepen voor Werknemer en Contractor en klik op **Maken**. In dit voorbeeld wordt de groep gemaakt met de naam Werknemers.

		Berlings Washing House Bar		
(a) 100,004,200,56/scrat	mm/ D + O Centric. E d X 6 Cisco Secure A	ACS ×		A 🛧 🗉
X Gara Browner WebEc -				
ululu Cisco Secure A	ICS		acastein	acaficmplatic (Primary) Log Out About Help
CISCO EVAL(Days left a)				
» G M/Workspace	Users and Identity Stones > Manify Groups > Create			
 B) Network Resources 	General			
- 🗿 Users and Identity Stores	 Name: Employees 			
Bently Groups	Description:			
Users	Parent Al Groups	Select		
Hosts	D = Required fields			
 External identity stores LDAP 				
Active Directory				
RSA SecuriD Taken Servers				
Certificate Authorities				
Certificate Authentication Profile				
Bersh obre bequences				
· Conception in the second second				
 B Maximum and Reports 				
· · · ·				
· · · · · · · · · · · · · · · · · · ·				
	Frank Frank			
	Suma Carca			

4. Selecteer Gebruikers en identiteitsopslag > Interne identiteitsopslag. Klik op Maken en voer de gebruikersnaam in. Plaats ze in de juiste groep, definieer hun wachtwoord en klik op Inzenden. In dit voorbeeld wordt een gebruiker met de naam worker1 in de groep Werknemer gecreëerd. Creëer ook een gebruiker met de naam contractant1 onder de groepsaannemers.

Constrained Constrained Constrained X X Share Browner WebSt * Interface Constrained X X Share Browner WebSt *	About 1969
x ² There Breaker WebE • scatterer WebE • x Cisco Secture ACS cisco EVAL(Days kett to) scatterer Model x MVAtorispace Log VAL x MVAtorispace Log VAL x MVAtorispace Log VAL x MVAtorispace Log VAL x MVAtorispace Central Mutaris Resources Central Mutaris Resources MVAtorispace	About 1480
Cisco Secure ACS assistant acatemptete (Primary) Leg Od Cisco EVAL(Days kill: 5) Advecting Resources The section of the	About 1980
State of the second secon	
Hently Groups + Internal Kently Stores Oescription:	
Desc Eldentity Group: All Groups Employee Balanct Hosts Password information Enable Password information LDAP Password inst: Password must: Active Directory • Contain 4 - 32 characters • Contain 4 - 32 characters	
RADIUS Identity Senem • Password: ••••• Enable Password: ••••• Ceditate Authorities • Canfirm Password: ••••• Confirm Password: ••••• Kenity Store Sequences • Canfirm Password: ••••• Confirm Password: •••••	
Constraints Constrain	
Buther Carce	

5. Selecteer Beleidselementen > Netwerkomstandigheden > Filters van het eindstation. Klik op Maken.



Voer een betekenisvolle naam in en voer onder het tabblad **IP-adres** het IP-adres van de WLC in. In dit voorbeeld zijn de namen Werknemer en Contractor.



Onder het tabblad CLI/DNIS, laat CLI als ALLE-bestanden en voer DNIS in als *<SSID>. In dit voorbeeld, wordt het DNIS-veld ingevoerd als *Werknemer aangezien dit End-station filter wordt gebruikt om alleen de toegang tot het WLAN-adres van de werknemer te beperken. De DNIS - eigenschap definieert SSID dat de gebruiker toegang mag krijgen. De WLC stuurt de SSID in de DNIS-eigenschap naar de RADIUS-server.Herhaal dezelfde stappen voor het filter van het Eindstation van de Contractor.



6. Selecteer **Beleidselementen > Vergunningen en toegangsrechten > Netwerktoegang > Verificatieprofielen**. Er moet een standaardprofiel zijn voor toegangsrechten.

X Shere Browner WebEr •	m/ D + Q Centricu ≅ d X Scice Securi ACS ×		
CISCO CISCO Secure Al CISCO EVAL(Days left b)	CS et al.	nim acalomptate (Primary)	Log Out About Help
» G MyWorkspace	Policy Bernetix > Authorization and Permissions > Network Access > Authorization Profiles		
» (5) Network Resources	Authorization Profiles	Stawing 1-1 of 1	0 • perpage 00
B Users and Identity Stores	Filer. Volsh # Nolsh #		
Policy Elements Ecology Conditions	Name + Description		
Date and Time	Fermit Access		
Data and Time Casism • Nation Conditions End States Piters Dates Piters Dates Piters • Automation and Parmissions • Nation Access <u>Cincern Conditions</u> • Dates Administration • Samed Permission Objects • Condens Patiens • Condens P			
	Create Dupicate Edt Delate	H 4 Page	1 of 1 10 10

7. Selecteer Toegangsbeleid > Toegangsservices > Service- en serviceselectieregels. Klik op Aanpassen. Voeg een geschikte toestand toe. Dit voorbeeld gebruikt Protocol als Straal als de matchingsvoorwaarde.Klik op Maken. Naam de regel. Selecteer Protocol en selecteer Straal.Kies onder Resultaten de juiste toegangsservice. In dit voorbeeld blijft het standaard toegang tot een netwerk.

Webpage Dialog		x
Https://10.104.208.56/acsadmin/Policyl	InputAction.do 😣	Certificate error
Customize Conditions Available: ACS Host Name Compound Condition Device Filter Device IP Address Device Port Filter End Station Filter NDG:Device Type NDG:Location Time And Date UseCase	Selected:	× ×
OK Cancel		

Cisco Secure ACS Webpage Dia	alog	
https://10.104.208.56/acsadmin/F	PolicyInputAction.do	😮 Certificate error
General		
Name: Rule-4	Status: Enabled 💌 \Theta	
The Customize butt conditions and resu	on in the lower right area of the p Its are available here for use in p	olicy rules screen controls which policy olicy rules.
Conditions		
Protocol: match	 Radius 	Select
Results		
Service: Default Network Acces	15 🔻	
OK Cancel		Help

8. Selecteer **Toegangsbeleid > Toegangsservices > Standaardnetwerktoegang > Identity**. Kies als interne gebruikers één resultaat-selectie en **identiteitsbron**.

Composition and Reports System Administration System Administration System Administration		and the second se			in the second se
Access Proteins A	🗲 🛞 🧭 https://20.384.200.56/scrade	nin/ P + O Centric E C X Craco Secure ACS ×			6 🕁 🕮
Cisco Secure ACS Example (Pinney) Lig 04 And Particle (Cisco Secure ACS) ************************************	🗶 🍚 Shara Browser WebEc 💌				
Image:	cisco Secure A	CS	esatnia	aca templake (Primary)	Log Out About 1940
Songle result selection Rules Songle result selection Rule based result selection Montaining Access Access Access	» 🛃 MyWorkspace	Access Policies > Access Services > Default Network Access > Berlity			
Ident and Identity States Identity Source Image: Clamanits Image: Clamanits	 (5) Nelwork Resources 	· Single result selection · Rule based result selection			
Que Pauxy Charmants Access Frances Access	B Users and Identity Stores	Identity Source: Internal Upers Balact			
Rear Channel Distant Channel	Poic Elements Poic Elements Poic elements Access Dentes Sector Rates O Detaut Device Annin Renty Autorization O Detaut Network Access Intern Autorization Monising and Reports Secten Administration	 Advanced Options 			
saw president in portical film		Save Changes Discard Changes			

Selecteer **Toegangsbeleid > Toegangsservices > Standaardnetwerktoegang > autorisatie.** Klik op **Aanpassen** en voeg de aangepaste voorwaarden toe. Dit voorbeeld gebruikt Identity Group, NDG:Apparaattype en End Station Filter in deze volgorde.



Klik op **Maken**. Geef de regel een naam en kies de juiste identiteitsgroep onder Alle groepen. In dit voorbeeld is het de werknemer.

Cisco Secure ACS Weltpage Dialog	Cisco Secure ACS Webpage Dialog
🍘 https://10.104200.56/www.dwine/Policy/opertubrities.dw 💿 Carrifords.arm	🍘 https://10.114.200, 96 / secondreim National Device Groups, NeputAction, do Prosetor Outs, externa Fritzers Educativy Groups, Marstey Group
General Name: Rule 2 Blafue: Enabled + 0	Petwork Davids Groups Filler F
The Custernize butten in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.	Name Description All Document All Document Contractor Contractor
Conditions	Instance
IZ Identity Group: In	MLC DAY
R NDOLDevice Type: In	
End Station Filter, match *	23 Chine Service 4/5 Wettenage Onderg
Fasults	🖉 https://ILTILLILLW/secularie/literation/attenti
You may select multiple authorization profiles. Attitudes calined in marging profiles will use the value from the first profile defined.	Prope: • Landon 2 • ID *

Klik op de radioknop **End-of-**support van **Werknemers** of voer de naam in die u in Stap1b hebt ingevoerd in de sectie "Configure the WLC".

🦲 Ciso	o Secure ACS Webpage Dia	log		X
🥭 http	ps://10.104.208.56/acsadmin/N	IARsLPInputAction.do?listType=EndStatio	n	😵 Certificate error
End	Station Filters		Showing 1-2 of 2 50	🕶 per page 😡
Filte	er: 🗾 Match if:	🗕 🐨 🗢		
	Name 🔺	Description		
0	Contractor End Stn Filter			
۲	Employee End Stn Filter			_
Cre	eate Duplicate Edit	Delete	🖂 🚽 Page	1 of 1 🕨 🕨
OK	Cancel			Help

Controleer het vakje Toegang toestaan.

Ę	Cisco Secure ACS Webpage Dialog		X
	Https://10.104.208.56/acsadmin/NetworkAccessLPEnputAction.do		🙁 Certificate error
	Authorization Profiles	Showing 1-2 of 2 50	▼ per page G0
	Filter: 🔹 Match if: 🔹 Go 💌		
	Name Description		
	DehyAccess		
	Permit Access		
	Create Duplicate Edit Delete	🔳 🖣 Page	1 of 1 🕨 Ы
	OK Cancel		Help

Herhaal de bovenstaande stappen voor Contractorregels. Zorg ervoor dat de

standaardinstelling is om **toegang** te **weigeren**. Zodra u stap e hebt voltooid, zouden uw regels er als dit voorbeeld uit moeten zien:

C Terpe //20.28 4.200.56/sciele X Shew Browser WebEr -	n/ P · O Centric E C X			L I I I I I I I I I I I I I I I I I I I
cisco EvaL(Days MIL 5)		stadmin	aca bemplate (Primary)	Log Out About Help
* 🚱 My/Workspace	Access Policies > Access Services > Default Network Access > Authorization			
* (57 Nelwork Resources	Standard Policy Enception Policy			
 Jusers and identity Stores 	Network Access Authorization Policy			
* Q/ PolicyElements	Fiter Status + Match it Equals + + Clear Filter De +			
Access Folices Access Services Service Selection Rules	Status Name Mently Group NDD Device Type End Station Filter	Results Authorization Profiles	HEGOVE	
 O Default/Device Admin 	1 🔲 0 Contractor in Al Groups:Contractor in Al Device Types:WLC match Contractor End Stri Pitter	Permit Access	7	
identity Autorization • O Debut Network Access	2 🖸 🛛 Engloyee in Al Groups Employee in Al Device Types WLC match Employee End Sth Filter	Pernit Access	5	
Autorization				
 Identifying and Reports 				
System Administration				
	En Default If no rules defined or no enabled rule matches.	DenyAccess	9	
	GreateI Dupicate • Edt Delete 🔨 More to Y			nize Hit Count
	Save Changes Discard Changes			

Dit sluit de configuratie af. Na deze sectie moet de client dienovereenkomstig met de SSID en de veiligheidsparameters worden geconfigureerd om verbinding te maken.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.