# Konfigurationsbeispiel für ACS Version 5.2 und WLC für die WLAN-Authentifizierung

## Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konfigurieren Konfigurieren des WLC Konfigurieren von Cisco Secure ACS Überprüfen Fehlerbehebung

# Einführung

Dieses Dokument enthält ein Konfigurationsbeispiel, um den benutzerbasierten Zugriff auf ein Wireless LAN (WLAN) basierend auf der Service Set Identifier (SSID) zu beschränken.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Konfigurieren von Wireless LAN Controller (WLC) und Lightweight Access Point (LAP) für den Basisbetrieb
- Konfigurieren des Cisco Secure Access Control Server (ACS)
- LWAPP (Lightweight Access Point Protocol) und Wireless-Sicherheitsmethoden

#### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco WLC der Serie 5500 mit Firmware-Version 7.4.110
- Cisco LAP der Serie 1142
- Cisco Secure ACS Server Version 5.2.0.26.11

## Konfigurieren

Um die Geräte für diese Konfiguration zu konfigurieren, müssen Sie:

- 1. Konfigurieren Sie den WLC für die beiden WLANs und den RADIUS-Server.
- 2. Konfigurieren Sie den Cisco Secure ACS.
- 3. Konfigurieren Sie die Wireless-Clients, und überprüfen Sie die Konfiguration.

#### Konfigurieren des WLC

Führen Sie die folgenden Schritte aus, um den WLC für diese Einrichtung zu konfigurieren:

 Konfigurieren Sie den WLC, um die Benutzeranmeldeinformationen an einen externen RADIUS-Server weiterzuleiten. Der externe RADIUS-Server (in diesem Fall Cisco Secure ACS) validiert dann die Benutzeranmeldeinformationen und ermöglicht den Zugriff auf die Wireless-Clients. Gehen Sie wie folgt vor: Wählen Sie Security > RADIUS Authentication (Sicherheit > RADIUS-Authentifizierung) in der Benutzeroberfläche des Controllers aus, um die Seite RADIUS Authentication Servers (RADIUS-Authentifizierungsserver) anzuzeigen.



Klicken Sie auf **Neu**, um die RADIUS-Serverparameter zu definieren. Zu diesen Parametern gehören die IP-Adresse des RADIUS-Servers, der Shared Secret, die Portnummer und der Serverstatus. Die Kontrollkästchen für Netzwerkbenutzer und -verwaltung legen fest, ob die RADIUS-basierte Authentifizierung für Verwaltungs- und Netzwerkbenutzer gilt. In diesem Beispiel wird Cisco Secure ACS als RADIUS-Server mit der IP-Adresse 10.104.208.56 verwendet.

cisco	MONITOR MUANE CONTROLL	ER MIRELESS GEOLRI	TY_ NANAGEMENT	OGNWANDS	HEJE	EBEDBACK	Saus Configuration ( ) ing Lagout (Lefrech
Security	RADIUS Authentication Service	vers > New					< Back Apply
AAA     Generati     FREDIS     Addummonian     Addummonian     Addummonian     Addummonian     Proceeding     Provide Dears     Proceeding     Proceeding     Contribution     Access Control Lists     Winderse Protection     Winderse Stop     Web Auth     TractSec Stop     Advanced	Server Index Sense(s) Server IP Address Shared Sector Format Shared Sector Contron Shared Sector Key Wrap Port Bambur Server Status Support for HHC 3576 Server Torosoft Noteack Over Nanagement IPSec	I II 10 104,005 55 6527 II Categora for F10 are 1212   Packar II Ember II 2 teached 2 teached 2 teached 3 teached 3 teached 4 teached 5 teach		i bay orapand	4*2 R2Dit	i fi en ver	

Klicken Sie auf Übernehmen.

2. Führen Sie diese Schritte aus, um ein WLAN für den Mitarbeiter mit SSID-Mitarbeiter und

das andere WLAN für Auftragnehmer mit SSID-**Auftragnehmer** zu konfigurieren. Klicken Sie in der Controller-GUI auf **WLANs**, um ein WLAN zu erstellen. Das Fenster WLANs wird angezeigt. In diesem Fenster werden die auf dem Controller konfigurierten WLANs aufgeführt.Klicken Sie auf **Neu**, um ein neues WLAN zu konfigurieren.In diesem Beispiel wird ein WLAN mit dem Namen Employee erstellt, und die WLAN-ID ist 1. Klicken Sie auf **Übernehmen**.

cisco	MONITOR MLANS	CONTROLLER AGRELES	S SECURTY	Markagement	OBMW4NOS	не,я	ESEDBACK	Sage Configuration ging Lo	gout Befresk
WLANs	WLANs > New							< Back	Apply
<ul> <li>WULANS WULUE</li> <li>▶ Advanced</li> </ul>	Type Profile Name SSID ID	et.At w Employee Employee 1 w							

Wählen Sie das Fenster **WLAN > Bearbeiten** aus, und definieren Sie die für das WLAN spezifischen Parameter: Wählen Sie auf der Registerkarte Layer-2-Sicherheit die Option **802.1x aus**. Standardmäßig ist die Layer-2-Sicherheitsoption 802.1x. Dadurch werden 802.1 x/Extensible Authentication Protocol (EAP)-Authentifizierungen für das WLAN aktiviert.

cisco	MONITOR WEAKS CONTROLLER ATRELESS SECURITY MENAGEMENT CONVANCE HELP ESSCRACK	ada cambaana . Dali rafaa Daana
WLANs	WLANs > Edit 'Employee'	< Back Apply
* WLANS	General Security QaS Advanced	
▶ Advanced	Loyer 2 Loyer 3 AMA Servers	
	Layar 2 Security * What we ap	Î
	Past Transition Past Transition Protocted Pranagement Prane	
	WPA : WPA2 Parameters	-
	WF02 Policy IV WF02 Encryption IVIA55. ETVIP Antifector Serv Panagement	
	UQ2 1.4 M Tunkin CCKM Encloie	
	PSK El feabra	
	Post Notes	

Wählen Sie auf der Registerkarte "AAA-Server" den entsprechenden RADIUS-Server aus der Dropdown-Liste unter "RADIUS-Server" aus. Die anderen Parameter können je nach Anforderung des WLAN-Netzwerks geändert werden. Klicken Sie auf Übernehmen.

cisco	Rovilou Within Coviliante villeter Sectella Mayngement (Chranica Hete Secondok	Saga Cantquration   Eng   Legout Batrach
WLANs	WLANs > Edit 'Employee'	< Back Apply
* WLANS WLANS	General Security QuS Advanced	
F Advanced	Layer 2     Layer 3     AAA Servers       Select AAA servers below to avertide use of default servers as this MLAX.       Refers Servers       Approx Centre operation on an inter       Approx 1       Approx 2       Approx 2       Approx 1       Approx 2       Approx 3       Approx 4       Approx 4       Approx 5       Approx 6       Approx 6       Approx 7       Approx 7 <th></th>	
	Frank Notice 2 Mark Public protect for stand in conductive static Mass 2 Sectionary Investigated a section of a conservation with Notice Add MATE as manufaction. Associate instation when 2 Sectionary Investigated a section of a conservation with Notice Add MATE as manufactive. Associate instation when	

Um ein WLAN für Auftragnehmer zu erstellen, wiederholen Sie die Schritte b bis d.

#### Konfigurieren von Cisco Secure ACS

Auf dem Cisco Secure ACS-Server müssen Sie:

- 1. Konfigurieren Sie den WLC als AAA-Client.
- 2. Erstellen Sie die Benutzerdatenbank (Anmeldeinformationen) für die SSID-basierte Authentifizierung.
- 3. Aktivieren Sie die EAP-Authentifizierung.

Gehen Sie wie folgt vor:

- Um den Controller als AAA-Client auf dem ACS-Server zu definieren, wählen Sie Network Resources > Network Devices and AAA Clients aus der ACS GUI aus. Klicken Sie unter Netzwerkgeräte und AAA-Clients auf Erstellen.
- 2. Wenn die Seite "Network Configuration" (Netzwerkkonfiguration) angezeigt wird, definieren Sie den Namen des WLC, die IP-Adresse sowie die RADIUS-Methode (Shared geheim und Authentication Method).

Clack C	C	nin/ D + 🔾 Catilic	🗄 🖒 🗶 🧭 Circo Secure ACS	× management				
My/Motispace          * W/Motispace       Hervark Resources > Hervar	Cisco Secure A     Cisco Secure A     Cisco Eval(Days eff-b)	cs				scaatnin	acalicmpiais (Primary)	Log Out About Help
Submt Carce	<ul> <li>Al MyNorkapace</li> <li>MyNorkapace</li> <li>Matheoric Device Groups Location Device Type</li> <li>Markot Device Groups Location</li> <li>Device Type</li> <li>Markot Device and AAA Charts</li> <li>Default Network Device External RADAUS Banans</li> <li>Weeks and identity Stores</li> <li>Process Policies</li> <li>Monitoring and Reports</li> <li>System Administration</li> </ul>	Network Resources to Mail Network Device Ge Location Device Type IP Address IP 10 105 98.4 IP 10 105 98.4	Al Device Types Al Device Types Iness O IP Range(s)	Seect. Renet.	Authentication Options • TRCACS+ Shared Secret Single Connect Device © Legacy TRCACS+ Single • RFOLIS • RFOLIS • Shared Secret R0000X CoApot: 1780 Erable ReyWrap Nay Encrysten Rey	Connect Support		

3. Wählen Sie **Benutzer und Identitätsdaten > Identitätsgruppen** in der ACS-GUI aus. Erstellen Sie die entsprechenden Gruppen für Mitarbeiter und AN, und klicken Sie auf **Erstellen**. In diesem Beispiel trägt die erstellte Gruppe den Namen Employees.

		BUILDE BALLE BALLER		
(-) (-) (-) (-) (-) (-) (-) (-) (-) (-)	nn/ D + O Cettric. E d X 6 Cisco Securi Ad	cs ×		A 🛨 🗉
X G Share Browner WebEc -				
cisco Eval(Days left: 5)	CS		anadeir	acatumptele (Primary) Log Out. About. Help
» G MyWorkspace	Users and Identity Stones > Hantly Groups > Grade			
Software Resources     Software Resources     Software Resources     Software Resources     Software Resources     Software Resources     Robust Resour	General Nami: Employees Description: Parent Al Groups D = Required Telds	(Serect)		
PolicyElements				
S Notitering and Reports				
+ 🥷 System Administration				
	Submit Cance			

4. Wählen Sie Benutzer und Identitätsdaten > Interne Identitätsdatenbanken aus. Klicken Sie auf Erstellen, und geben Sie den Benutzernamen ein. Platzieren Sie sie in der richtigen Gruppe, definieren Sie ihr Kennwort, und klicken Sie auf Senden. In diesem Beispiel wird ein Benutzer mit dem Namen employee1 in der Gruppe Employee erstellt. Erstellen Sie unter den Auftragnehmern der Gruppe einen Benutzer mit dem Namen Auftragnehmer1.

C S http:// 20.28 4.208 58/scratteres	17 P + O Cerebicu, E d X			6 🕁 🖯
🗶 🍚 Shara Browser - WebEc 🔹				
cisco Secure AC		-	aadmin acationybelo (Primary) i	Log Chat Albert Help
» ∰ MyWorkspace	Jears and kiertity Stoves > Internal Bentity Stoves > Users > Create			
Network Resources      Henry and Meetry Stores      Henry Croups      Henry Croups      Henry Croups      Hons      Loor      Hons      Hons	General         Name:       employee1       Bithus: Enabled • •         Description:         • Identity Group: All Groups Employee       Balact         Password Information         Password Information         Password Information         • Conten 4 - 32 characters         • Confirm Password:         • Confirm Password:         • Confirm Password:         • Charge password on ned login         User Information         There are no additional identity attributes defined for user records         • • Required feetos	Enable Password Information Password must. • Contain 4 - 32 characters Enable Password Confirm Password		
	e   Submit   Cance			

5. Wählen Sie **Richtlinienelemente > Netzwerkbedingungen > Filter für Endstationen aus**. Klicken Sie auf **Erstellen**.



Geben Sie einen aussagekräftigen Namen ein, und geben Sie unter der Registerkarte **IP** address (**IP-Adresse**) die IP-Adresse des WLC ein. In diesem Beispiel sind die Namen Mitarbeiter und Auftragnehmer.



Belassen Sie auf der Registerkarte CLI/DNIS die CLI als -ANY-, und geben Sie DNIS als \*<SSID> ein. In diesem Beispiel wird das DNIS-Feld als \*Employee eingegeben, da dieser Endstation-Filter verwendet wird, um den Zugriff auf das Employee WLAN zu beschränken. Das DNIS-Attribut definiert die SSID, auf die der Benutzer zugreifen darf. Der WLC sendet die SSID im DNIS-Attribut an den RADIUS-Server.Wiederholen Sie die gleichen Schritte für den Auftragnehmer-Endstationsfilter.



6. Wählen Sie **Richtlinienelemente > Autorisierung und Berechtigungen > Netzwerkzugriff > Autorisierungsprofile aus**. Es sollte ein Standardprofil für "Zugriff zulassen" vorhanden sein.

X Shes Brown Webs -	n/ D + O Cwetter B C X		A 116
cisco Secure Al cisco EVAL(Days left: 5)	CS esaleir	aca licenplaite (Primary)	Log Out About 1989
» 分 MyWorkspace	Policy Berneris > Autorization and Permissions > Network Access > Autorization Police		
» (§2 Network Resources	Authorization Profiles	Shawing 1-1 of 1	0 • perpage 00
B Users and Identity Stores	File: Webh # Kebh # Cib *		
Policy Elements     Ecology Constitutes	Rame - Description		
Date and Time	Parmit Access		_
Custom * Nation: Condition End Station Filters Device Filters * Autorization and Permissions * Nation: Access Subort Access Subort Access Device Administration * Named Permission Objects * Co. Access Palcies * Co. Access Palcies * Co. Monitoring and Reports * Signten Administration			
	Create Dupleate Edit Delate	H K Page	1 of 1 10 H

7. Wählen Sie Zugriffsrichtlinien > Zugriffsdienste > Serviceauswahlregeln aus. Klicken Sie auf Anpassen. Fügen Sie eine geeignete Bedingung hinzu. In diesem Beispiel wird Protocol als Radius als übereinstimmende Bedingung verwendet.Klicken Sie auf Erstellen. Nennen Sie die Regel. Wählen Sie Protokoll und dann Radius aus.Wählen Sie unter Ergebnisse den entsprechenden Zugriffsdienst aus. In diesem Beispiel wird es als Standard-Netzwerkzugriff beibehalten.

🔁 Webpage Dialog		×
😂 https://10.104.208.56/acsadmin/	PolicyInputAction.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: Protocol	
OK Cancel		

Cisco Secure ACS webpage Dialog	
Attps://10.104.208.56/acsadmin/PolicyInputAction.do	ificate error
General	
Name: Rule-4 Status: Enabled - O	
The Customize button in the lower right area of the policy rules screen controls which policy of conditions and results are available here for use in policy rules.	icy
Conditions	
Protocol: match - Radius Select	
Results	
Service: Default Network Access 👻	
OK Cancel	Help

8. Wählen Sie **Zugriffsrichtlinien > Zugriffsdienste > Standardnetzwerkzugriff > Identität aus**. Wählen Sie Single Result Selection und **Identity Source** als Internal Users aus.

a second a second second		BUILDING WAS AND DOLLAR WAS	the second se		
(-) (-) (-) (-) (-) (-) (-) (-) (-) (-)	min/ D + O Centric. E d X Cisco Secure A	NCS ×			6 🕁 🕮
X Gara Browser WebEc -					
cisco Eval(Days left 5)	CS		scadnin	acaliemplaie (Primary)	Log Cut About Help
» ∰ MyWorkspace	Access Policies > Access Services > Default Network Acc	cess > Marthy			
+ (52 Nelwork Resources	· Single result selection · Rule based result s	election			
B Users and Identity Stores	Identity Source: Internal Upers	figurest.			
» Qv PolicyElements	Advanced Orders				
- 🕵 Access Policies					
Access Services     Service Talenting Bulan					
* O Default.Device Admin					
idently a thornton					
* O Debuit Network Access					
a dentry					
<ul> <li>Monitoring and Reports</li> </ul>	1				
System Administration	1				
	1				
	Save Changes Discard Changes				

Wählen Sie **Zugriffsrichtlinien > Zugriffsdienste > Standardnetzwerkzugriff > Autorisierung aus.** Klicken Sie auf **Anpassen** und fügen Sie die angepassten Bedingungen hinzu. In diesem Beispiel werden in dieser Reihenfolge Identity Group, NDG:Device Type (Gerätetyp) und End Station Filter (Endgeräte-Filter) verwendet.



Klicken Sie auf **Erstellen**. Nennen Sie die Regel, und wählen Sie unter Alle Gruppen die entsprechende Identitätsgruppe aus. In diesem Beispiel ist dies Employee.

🕘 Closo Secure ACS Weltpage Dialog 🦰 🔤	Cisco Secure ACS Wetpage Dialog
🖉 https://10.194200.19/www.drvin:PalayleputAction.do 📀 Carificute area	🍘 https://10.114200. 🖬 has a drein Platwork Invice Groups RegutAction de Prostact Data, a tare a Fritar-Idantity Group -Manthylin 💡 0
Coop Secure ACS Wetgage Dialog Coop Secure ACS Wetgage Coop Secure ACS Wetgage Dialog Coop Secure ACS Wetgage Dialog Coop Secure ACS Wetgage Dialog Coop Secure ACS Wetgage Coop Secure ACS	Coso Secure ACS Wethouse Datage Coso Secure ACS Wethouse Datage Datage Filter:  Filter
Select Descrict	TIMARE   TEDOCRE   Full   TERRIN   _ FOR INTERNAL   FORM

Klicken Sie auf das Optionsfeld **Employee End Stn Filter**, oder geben Sie den Namen ein, den Sie in Schritt 1b im Abschnitt "Konfigurieren des WLC" eingeben.

Cisco Secure ACS Webpage Dialog										
	https://10.104.208.56/acsadmin/NARsLPInputAction.do?listType=EndStation									
	End St	ation Filters		Showing 1-2 of 2 50	🕶 per page 😡					
	Filter:	<ul> <li>Match if:</li> </ul>	🗕 🐨							
		Name 🔺	Description							
	0	Contractor End Stn Filter								
	۲	Employee End Stn Filter								
	Crea	te Duplicate Edit	Delete	🖂 🖪 Page	1 of 1 🕨 📄					
	OK C	ancel			Help					

#### Aktivieren Sie das Kontrollkästchen Zugriff zulassen.

Cisco Secure ACS Webpage Dialog					
G https://10.104.208.56/acsadmin/NetworkAccessLPInputAction.do					
Authorization Profiles	Showing 1-2 of 2 50 🔹 per page 😡				
Filter: Thatch if: Go 🔻					
Name  Description					
DehyAccess					
Permit Access					
Create Dunlicate Edit Delete					
	Help				

Wiederholen Sie die oben genannten Schritte auch für die Regeln des AN. Stellen Sie sicher,

dass die Standardaktion "**Zugriff verweigern**" lautet. Wenn Sie Schritt e abgeschlossen haben, sollten Ihre Regeln wie folgt aussehen:

Clisco Secure ACC      Control      Clisco Secure ACC      Control      Clisco Secure ACC      Clisco Secure	and the	and the second second								
x	10.134208.54/scratemin/ D = O Cettro 2 d X 55 c	Cisco Secure AC5 ×		_		A 🕆 8				
Cisco Socure ACS     Evaluation Resources     Access Policies	WebE: •									
CISCO EVAL(Days HIL 5)	o Secure ACS			acastein as	ntemplate (Primary)	lag Out About Help				
	Nagis lie R. 5)									
Standard Policy Exception Policy      Note and Policy Exception Policy      Note and Policy Exception Policy      Standard Policy Exception Policy      Note and Policy Exception P	Access Policies > Access Services > Defect	Il Network Access > Authorization								
Bernard Menthy Stores     Operand Menthy     Operand     Operand Menthy     Operand	standard Policy Enception Policy	Standard Policy Enception Policy								
	ers and identity States Vetwark Access Authorization Policy									
Access Enders     Access Enders     Access Dentice     Status Name     St	B Filter Status + Mate	Filter States • Match if Gauge • • Clear Filter De -								
I Service Selection Rules     O Debut Device Admin     1      O Contactor in All Groups Contractor in All Device Types MLC match Contractor End Shi Filter Permit Access     7	and and a state of the state of	Conditions		Results	Carl					
O Debut Device Admin     1      O Contractor in All Groups.Contractor in All Device Types.VLC match Contractor End Stin Filter Fermit Access     7	tion Rules lands rearries lands	tently Group NDG Device Type	End Station Filter A	uthorization Profiles						
iterti	te Admin 1 🖸 O <u>Contractor</u> in	All Groups:Contractor in All Device Types:WLC	match Contractor End Stn Filter Pr	emitAccess 7						
Authorization 2 C 4 Engloyee in Al Oroups Employee in Al Device Tiges VLC match Employee End Sh Fifter Permit Access 5	2 🖸 🔍 Employee in	All Groups Employee in All Device Types WLC	match Employee End Sth Filter Pr	emit Access 5						
C Debut Network Acces	ark Access									
New York Control of Co										
* 💭 Monitoring and Reports	d Reports									
* 👯 System Administration	istration									
Central Fino tales defined on to enabled rule matchine.     Denylocess 8	T E Default P	Detault I no rules defined or no enabled rule matches. Denykcess 8								
Create + Duplicate + Edd Dates A Marets V Customer Hed	CreateL. DuplicateI Ex	CreateI DuplicateI • Edt Delete A More to V				HitCount				
Bave Changes Discard Changes	Save Changes Discard Cha	anges								

Damit ist die Konfiguration abgeschlossen. Nach diesem Abschnitt muss der Client für die Verbindung entsprechend mit der SSID und den Sicherheitsparametern konfiguriert werden.

## Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

## Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.